



AX3500 XGSPON OLT Device Operation

QRG

Revision B

ACT AX3500 XGSPON OLT Device Operation QRG

ACT Document Number: ACT AX3500 XGSPON OLT Device Operation QRG

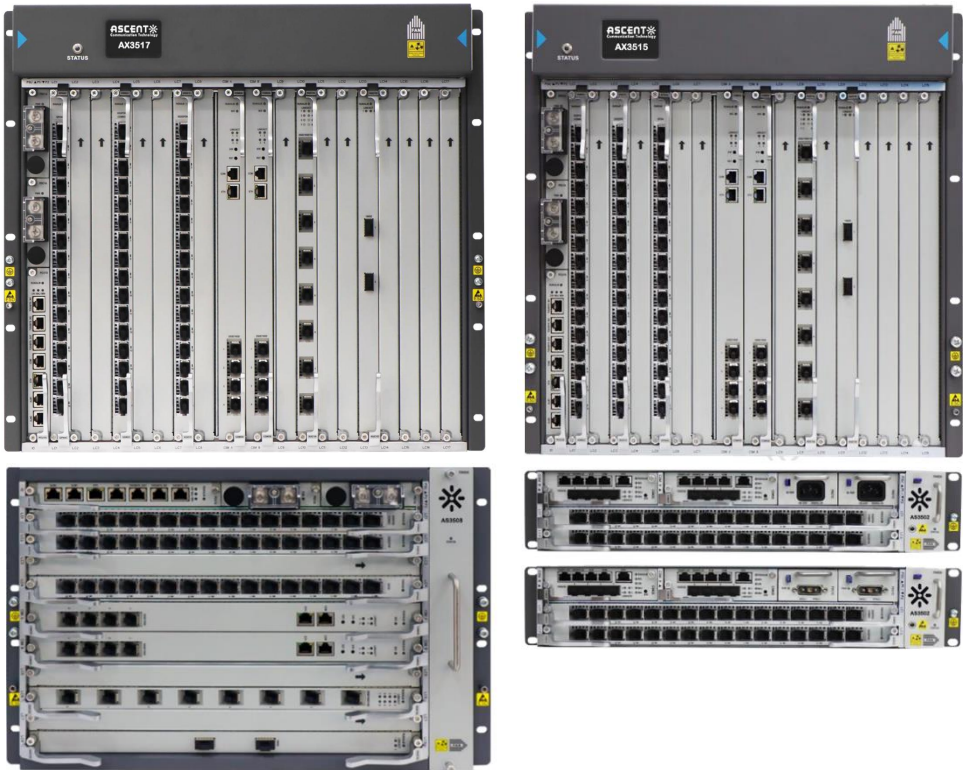
Quick Reference Guide Revision B

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	02/20/2025	Initial release
B	07/04/2025	Update format

Table of Contents

1 Device Manager.....	8
1.1 Login Device Manager.....	8
1.2 Configure Device Manager.....	9
1.3 Exit Device Manager	9
2 View Hardware	10
2.1 View System Shelf	10
2.2 View Board Information.....	11
2.3 View ONU Status	12
3 Startup OLT Product	14
3.1 System Interfaces Introduction.....	14
3.2 Configure Base Data Services.....	15
4 System Configuration	24
4.1 SNMP.....	24
4.2 SNMP.....	25
4.3 Sntp	28
4.4 NE Access Control	31
5 Layer 2 Configuration	32
5.1 Port Attribute	32
5.2 Link Aggregation.....	35
5.3 VLAN	37
5.4 MAC Address Table	39
5.5 Mirror Port.....	40
5.6 Spanning tree	43
6 Layer 3 Configuration	46

6.1 SVI Concept	46
6.2 Application Description	47
6.3 Add SVI	47
6.4 Configure ARP	48
6.5 Relay Option	50
7 GPON Configuration	52
7.1 ONU Authentication	52
7.2 ONU Register	53
7.3 ONU Traffic	56
7.4 OLT Management	72
7.5 ONU Management	73
7.6 PON Energy Saving	81
7.7 Based on Flow Speed Limit	81
7.8 FEC	82
7.9 Downstream Encryption	83
7.10 PON Protection	84
7.11 PON Optical Power Detection	86
7.12 Rogue ONU Detection	89
8 Multicast Configuration	89
8.1 IP Multicast Introduction	89
8.2 IGMP Snooping Introduction	90
8.3 Standard IGMP Snooping Configuration Instance	90
8.4 Standard MLD proxy Configuration Instance	96
9 Multicast Configuration	100
9.1 ACL Instance	100
10 QoS Configuration	105
10.1 QoS Introduction	105
10.2 Rate Limit	105
10.3 Queue Mapping	106

10.4 DSCP Mapping Table	107
10.5 Schedule Mode	108
10.6 Weight Configuration.....	108
10.7 Egress Queue Metering	109
10.8 Flow-Based QoS	109
11 SyncE.....	112
11.1 Introduction	112
11.2 SyncE Configuration Instance	112
12 PTP	114
12.1 Introduction	114
12.2 Principles of GPON Transmission Time.....	118
12.3 PTP Configuration Instance.....	120
13 Security Management	130
13.1 Anti-MAC Spoofing.....	130
13.2 ARP Snooping Scalars	130
13.3 MACFF (MAC-Forced Forwarding)	131
13.4 DHCP Snooping	132
14 System Management	133
14.1 Save System Configuration	133
14.2 Reset System	134
14.3 Reset Line Card	134
14.4 Upgrade System	135
14.5 Active/Standby Switchover	136
15 Alarm Management	137
15.1 Configure TCA	137
15.2 View Alarms and Events.....	140
16 External Alarm Input/Output	142
16.1 Introduction	142

16.2 Product Specifications 142

16.3 Operating Steps..... 142

17 Performance Statistics 145

17.1 Ethernet Port Performance Statistics 145

17.2 OLT Port Performance Statistics 146

About This Guide

Introduction

This document describes the configuration procedures of AX3500 series XGSPON series OLTs.

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 Device Manager

AX3500 series OLT is a frame telecom level access device, that provides photoelectric interface directly to the core Ethernet / IP network. Working with optical Network units (ONU), OLT combines GPON with embedded 2 / 3 layer exchange and routing, making it the best last mile access and delivery platform for bandwidth- intensive applications.

The NuMax Cloud 4000 Device Management System (Device Manager, DVM) provides the configuration, system performance, and alarm management capabilities for the OLT systems. This manual introduces the network management configuration management of AX3500 system. Use cases and illustrations take AX3517 as an example.

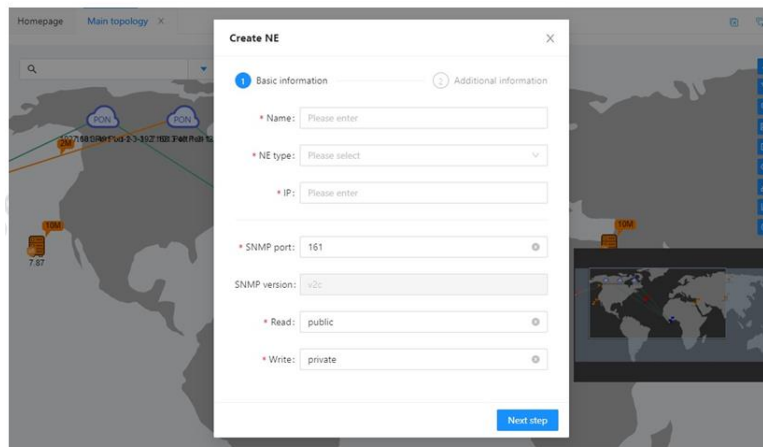
This chapter mainly describes the following contents:

- Log in to the Device Manager
- Configuration management of the Device Manager
- Exit the Device Manager

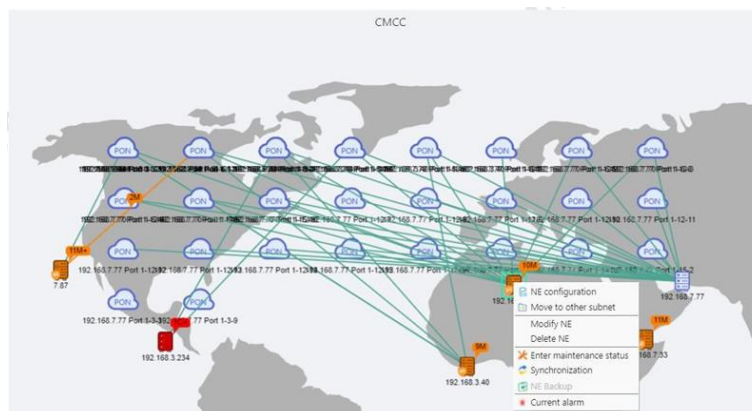
1.1 Login Device Manager

Suppose that the NuMax Cloud 4000 system starts normally. Log in to the Device Manager as per these steps:

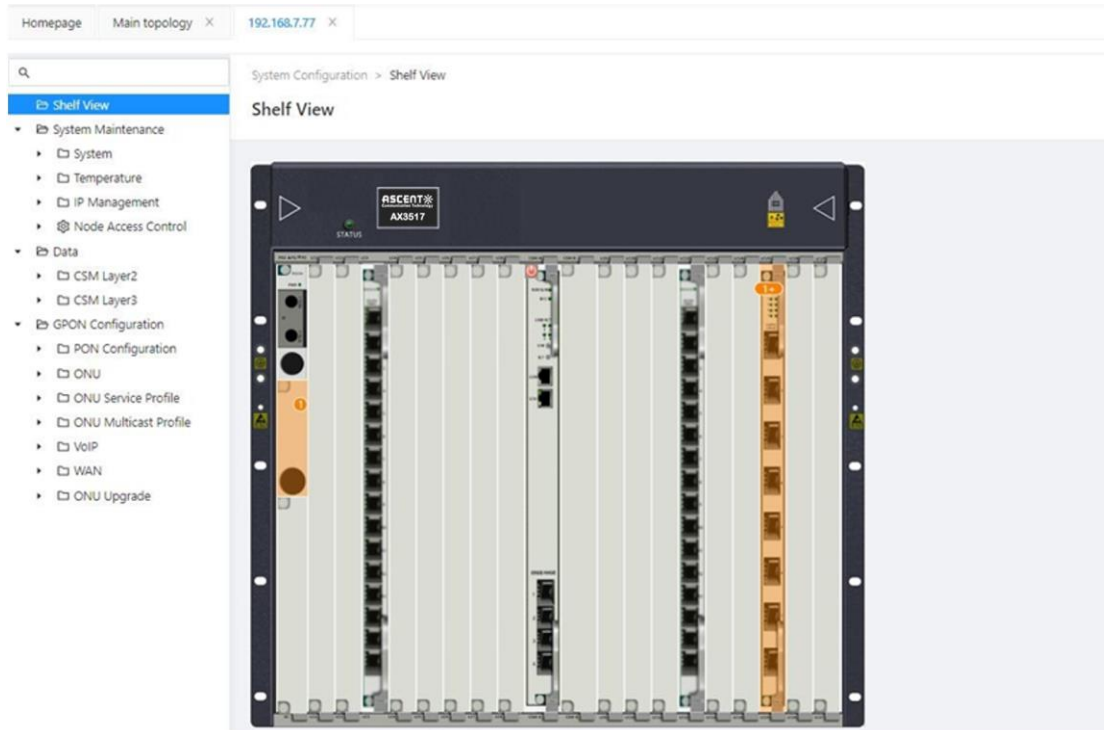
- In the topology map interface, select Main Topology, double-click MainView, right-select New NE blank, and enter NE information to create a new NE.



- In the topology interface, double-click the OLT NE that you need to configure, or right-click it, and then select NE Configuration.



- The device manager interface for OLT will appear, with the Function View navigation tree on the left and the corresponding function visualization interface on the right.



1.2 Configure Device Manager

The Device Manager Function View provides the following configuration management features for each NE:

Configuration Level	Function Abstract
Configuration Management	System-level configuration. Includes system information configuration, data service configuration, multicast service configuration, and GPON service configuration.
Alarm	View and manage the alarm.
Performance	View and monitor the performance data.
Optical Layer Measurement	Optical power monitoring for ports and ONU.
Batch Configuration	Provide bulk configuration data table items.

1.3 Exit Device Manager

Exit the Device Manager by either of these methods: Click on [x] to exit.

2 View Hardware

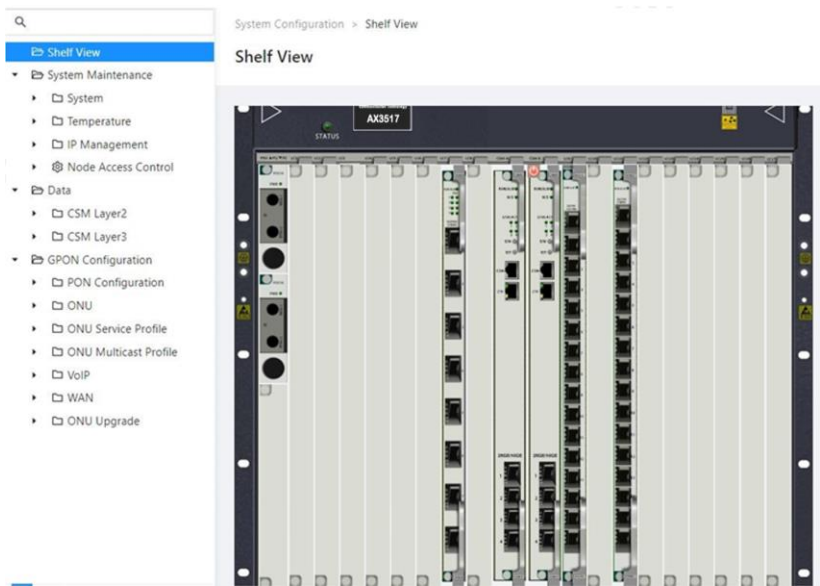
This chapter includes the following contents:

- View the system shelf
- View the board information
- View the ONU status

2.1 View System Shelf

【Operating Steps】

In the [Function View] navigation tree, click [Shelf View].



【Parameter Declaration】

Machine Hardware Configuration

Description

Control System Module (CSM)	Slot A, B are CSM, providing MGNT, CONSOLE, respectively configured with 4 XGE ports. The master board card supports redundant backups.
Upper Card	XUC1A is an upper card, and 4 XGE ports can be configured at slot 1-2 and 16-17, 8 XGE ports at the other slots.
Service Module	Slot 1-17 provides the PON service module, GPN4C, XSM2C, XGS1C.
Power Module	Slots P1, P2 are power modules, and provide redundant backup.
Fan Module	The FAN slot provides the fan module.
DC Power Module	DC power-supply module. Redundant configuration.

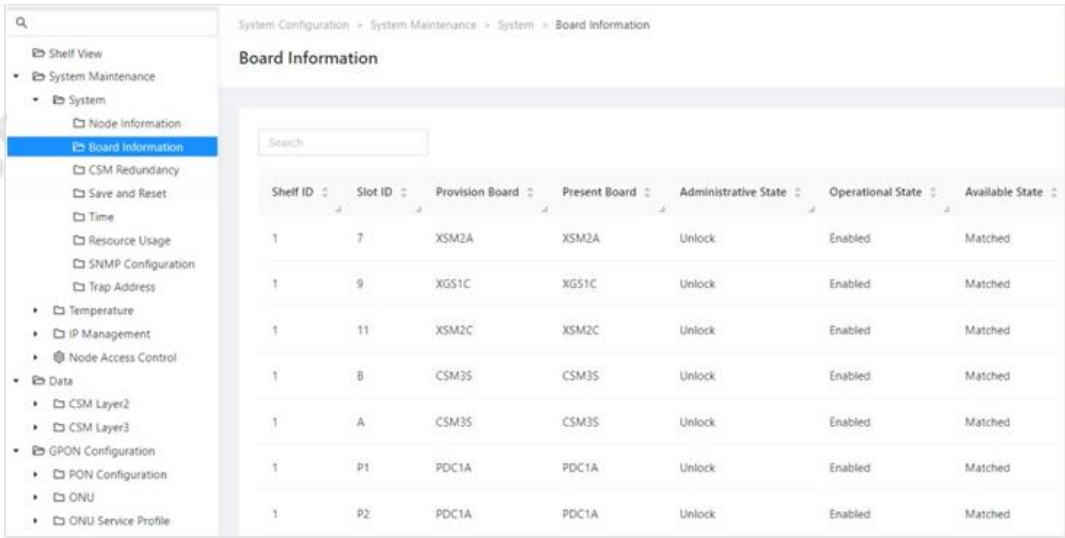


Note: This manual is based on GPON business description, for GPN, XGN, XGS, XSM, using GPON card / GPON port.

2.2 View Board Information

【Operating Steps】

In the [Function View] navigation tree, click [Shelf View].



【Parameter Declaration】

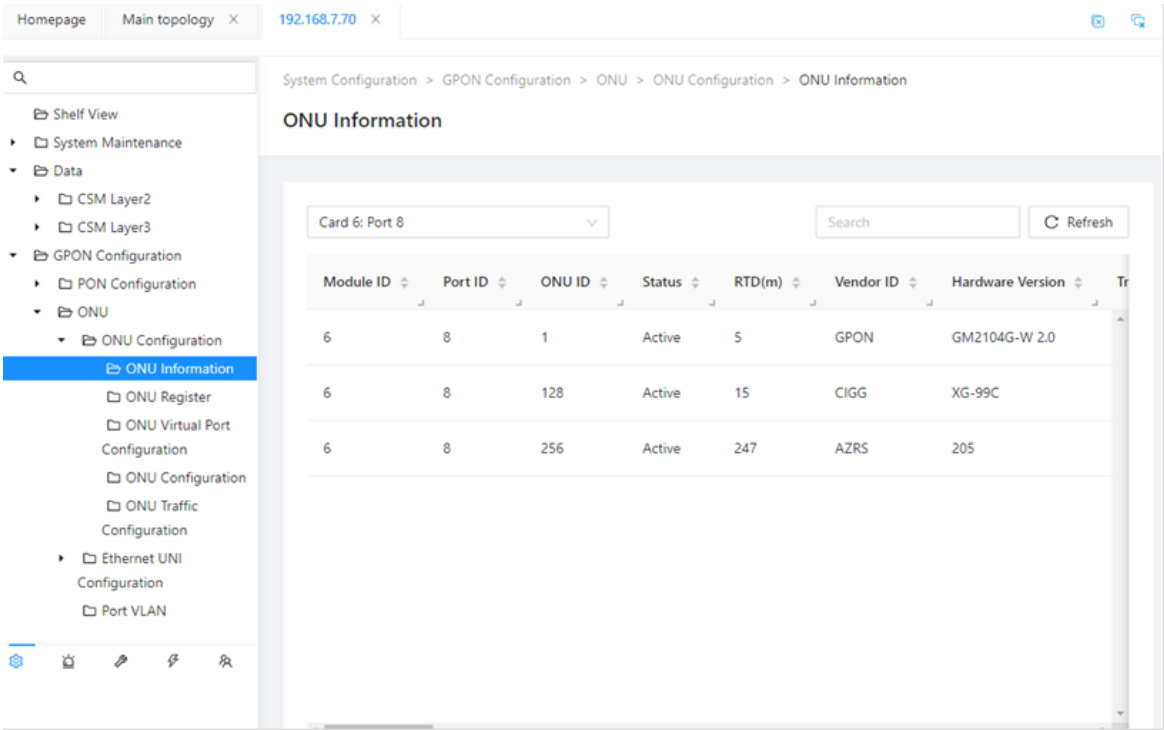
Machine Hardware Configuration	Description
Shelf ID	Machine frame identification.
Slot ID	Slot identification.
Provision Board	Card type pre-set.
Present Board	The type of the slot is currently running.
Administrative State	Management status of the board card.
Operational State	Operation status of the board card.
Available State	Is the board card available.
Serial Number	Card serial number.
Part Number	Board card part number.
Hardware Revision	Board card hardware version.
Software Revision	Card software version.
UP Time	Start time of the card.
Failure Reason	Card failed reason.

2.3 View ONU Status

【Operating Steps】

In the [Function View] navigation tree, select [GPON Configuration > ONU> ONU Configuration> ONU Basic Information].

In the upper left port navigation tree of the Device Manager, select the GPON card and port to view the ONU status under a single PON port.



Machine Hardware Configuration

Description

Module ID

Line card slot number

Port ID

port number.

ONU ID

ONU ID

Status

ONU activated / inactive state.

RTD(m)

Range measurement value, measured in "meter".

Vendor ID

The Vendor ID.

Hardware Version

ONU hardware version.

Traffic Management Option

The ONU traffic management type.

Equipment ID

ONU equipment identification.

OMCC Version

The OMCC version that is supported by the ONU.

Hardware type

The ONU hardware type.

Hardware Revision

ONU hardware version number.

Machine Hardware Configuration	Description
Priority Queue Number	Number of Priority Queue's supported by the ONU.
Traffic Scheduler Number	Number of Traffic Scheduler's supported by the ONU.
GEM Port Number	Number of GEM Port's supported by the ONU.
T-CONT Number	Number of T-CONT's supported by the ONU.
UNI Port Number	Number of ONU user ports.
System Uptime	Start-up time of the ONU.
Image Instance 0 Version	ONU firmware 0 version number.
Image Instance 0 Valid	Is the ONU firmware 0 valid.
Image Instance 0 Activate	Is the ONU firmware 0 currently active and running.
Image Instance 0 Commit	Whether ONU firmware 0 runs next time.
Image Instance 1 Version	ONU firmware 1 version No.
Image Instance 1 Valid	Is the ONU firmware 1 valid.
Image Instance 1 Activate	Is the ONU firmware 11 currently active operation.
Image Instance 1 Commit	Whether the ONU firmware 1 starts or not the next time.
Piggyback DBA Report	Does the ONU support the Piggyback DBA Report.
Whole ONU DBA Report	Does the ONU support the Whole ONU DBA Report.
Working Voltage(V)	The ONU optical module power supply voltage, in unit V.
Rx Optical Power(dBm)	The optical module receives the light power in dBm.
Tx Optical Power(dBm)	The light module sends the light power in dBm.
Bias Current(mA)	Optical module bias current in mA.
Temperature(°C)	Optical module operating temperature, per unit of degrees Celsius.

3 Startup OLT Product

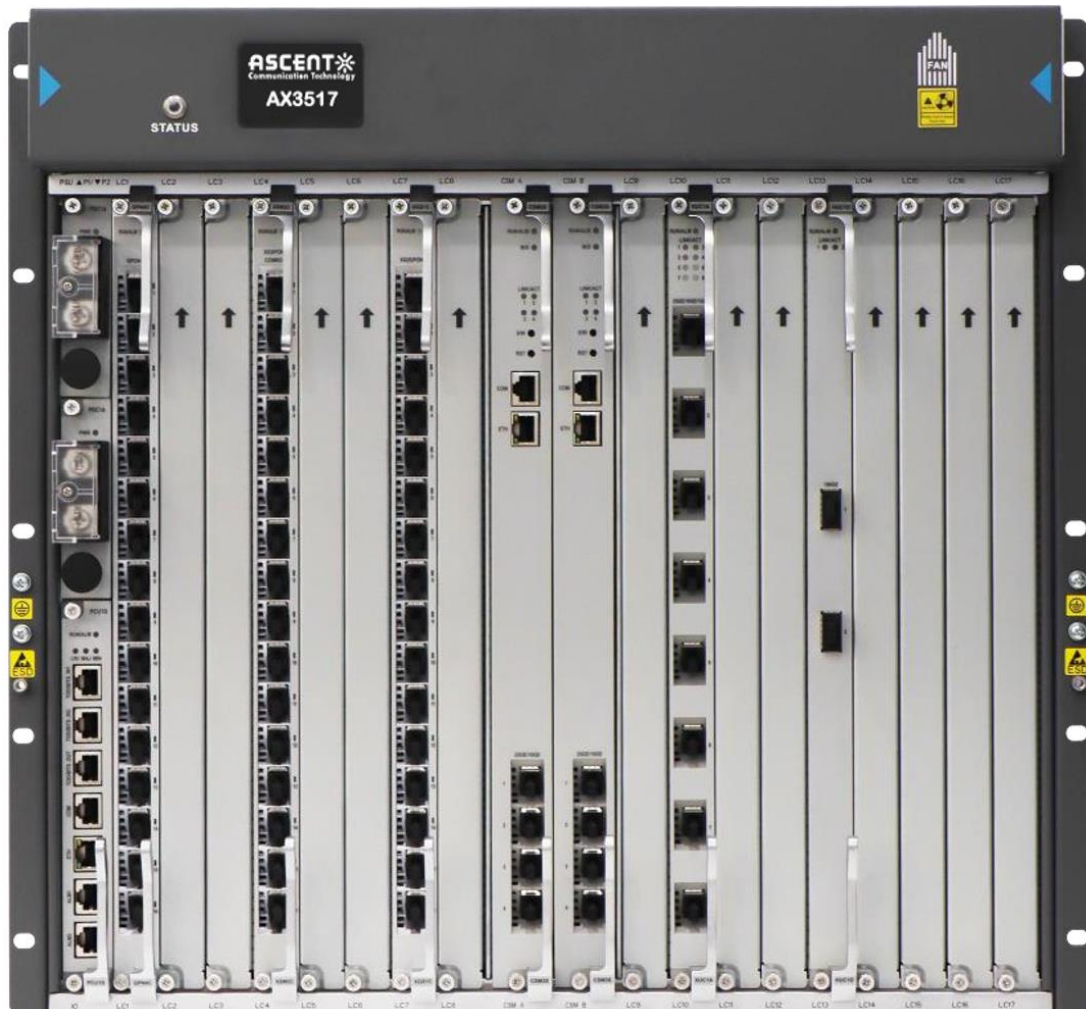
This chapter describes the startup steps for OLT, including the basic data service preconfiguration tasks.

The tasks required to start the OLT system include:

- System Interfaces Introduction
- Configure Base Data Services

3.1 System Interfaces Introduction

Chassis OLTs adopt the frame design. The user side supports 17 slots, 15 slots, 10 slots, 8 slots, 5 slots and 2 slots separately. You can configure with GPON, XGPON, XGSPON service card flexibly. The network side provides different 10GE interfaces to ensure non-blocking transmission of services. The specific deployment diagram is shown in below figure:



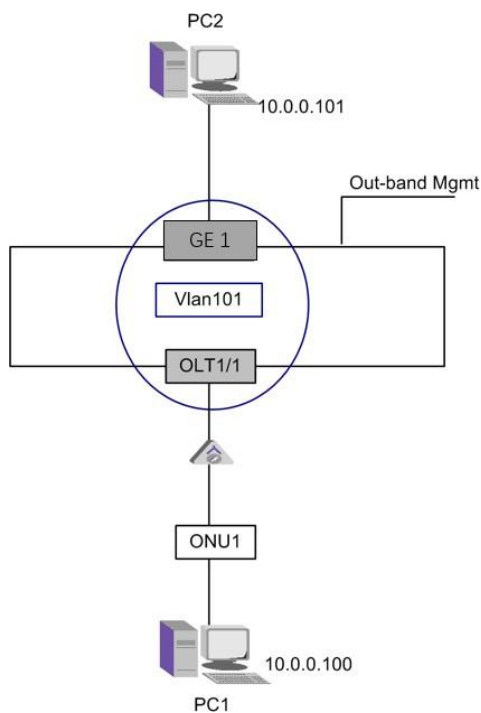
3.2 Configure Base Data Services

3.2.1 Application Description

VLAN planning is required before configuring the basic data business. In the following topology instance, the system VLAN ID is 101. The uplink OLT XGE port and the downlink OLT OLT port are both members of the VLAN 101s of the system.

In the following example, the PC connected to the ONU and the OLT statically receives its IP address. In a typical network configuration, the PC can also dynamically obtain the IP addresses via either the DHCP or the PPPoE.

3.2.2 Instance Topology



The topology shown in the figure above describes the basic data business configuration. ONU connects to OLT 1 / 1 port (slot 1 port 1) to PC 1 and the network side connects PC 2 using XGE 1 to PC 2.

In this example, ONU VLAN mode is "Tag mode", ONU is upward Untag stream plus VLAN label 101, and downward stripping VLAN label 101 (ONU configuration is not within the scope of this document, refer to ONU related manual for details).

To ensure that the layer 2 operation of OLT works properly, the connection between the two PC can be checked from PC1 ping PC2 (or PC2 ping PC1).

3.2.3 Configuration Tasks

The OLT configuration is as follows:

- Configure the upper connection port and the VLAN
- Configure the ONU registration
- Configure the ONU data stream services
- Configure the VLAN translate
- Connection test

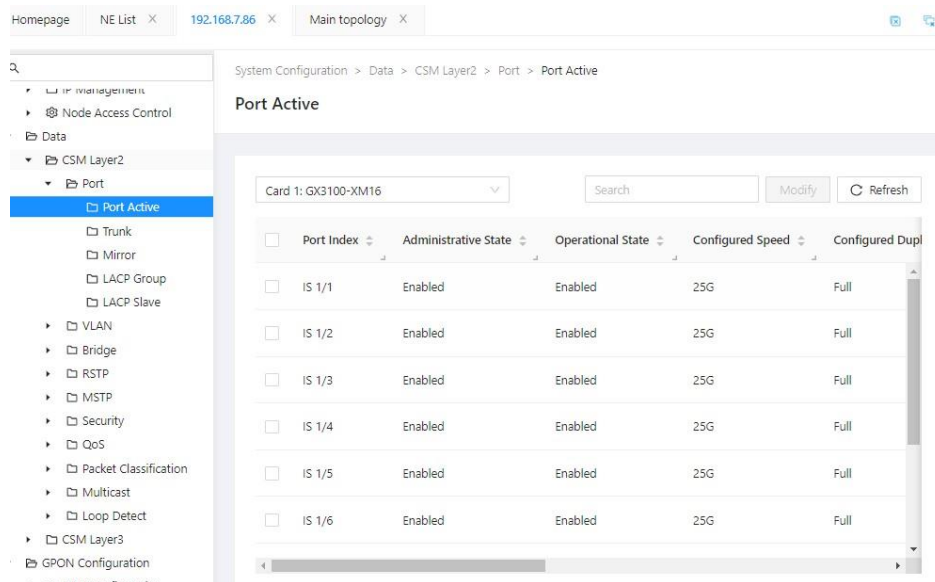
The detailed steps of each task are illustrated with the topology in below figure.

3.2.4 Configure Port and VLAN

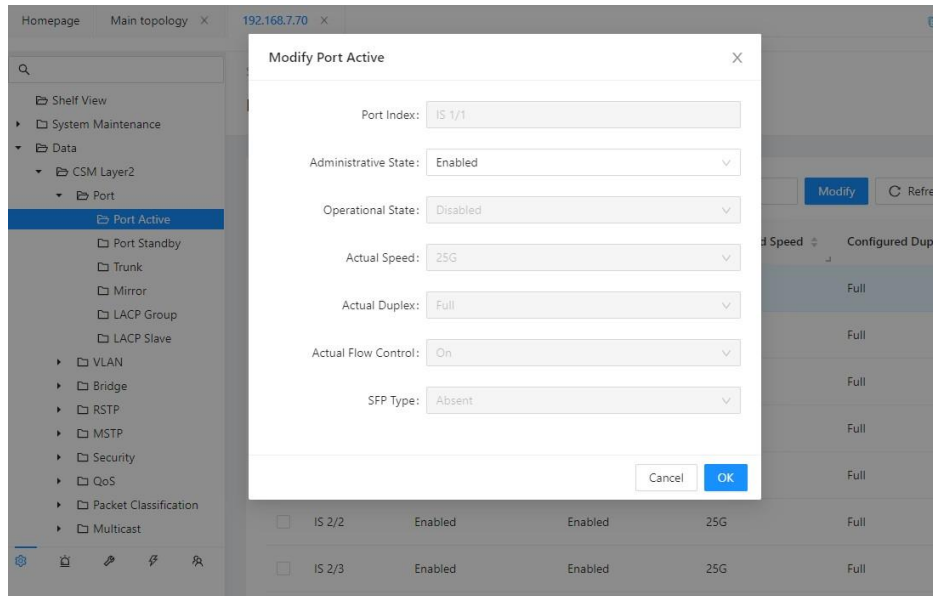
【Operating Steps】

Enable port.

In the “Function View” navigation tree, select “Data > CSM Layer 2 > Ports > Port Active”.



Check the XGE1 interface, and click “Modify”.



Set the corresponding interface management status to “Enabled”, click <OK>.

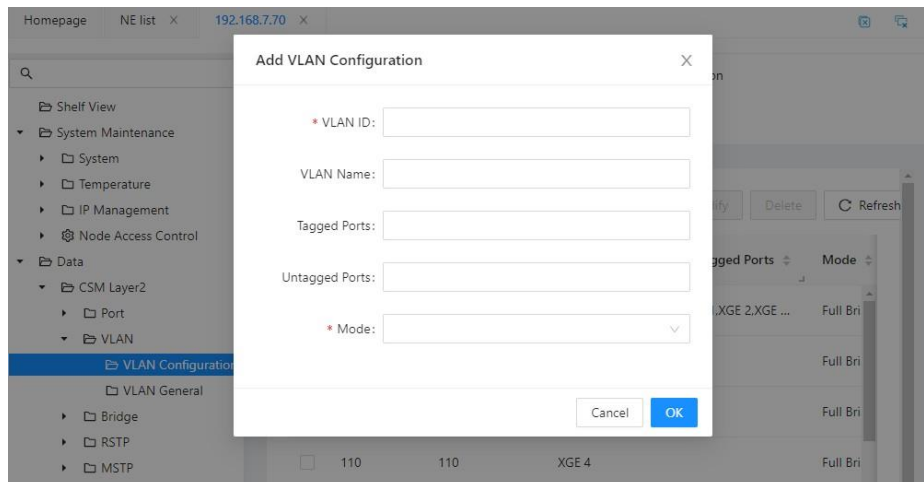


Note: Operation status "Enabled" indicates that the port link communication is established.

Create a VLAN 101.

In the Function View navigation tree, select “Data> CSM Layer 2> VLAN> VLAN Configuration”.

Click Add, enter the VLAN ID 101, and select the Tagged port: XGE1. Click <OK> Save the configuration.



3.2.5 Configure the ONU Registration

The GPON system supports 5 authentication modes (serial-number authentication, serial-number and password authentication, password authentication, logical identification authentication, logical identification and password authentication) or closed authentication. OLT assigns the corresponding ONU ID to the certified ONU.

Note: To facilitate ONU maintenance related to the VLAN assignment, serial number authentication is recommended.

OLT enables serial-number authentication mode by default.

With 64 ONU ID s per GPON port and 256 per XGPON / XGSPON, the ONU connected to the same PON port can be bound to either ONU ID.

In the Function View navigation tree, select the “GPON Configuration> ONU> ONU Configuration> ONU Register”.

Select the GPON port in the upper left port navigation tree.

Click Add, enter the slot number, then port number, then ONU ID, and serial number, and click <OK> Save Configuration.

The screenshot displays the 'Add ONU Register' dialog box in the AX3500 OLT web interface. The dialog box has a title bar with a close button (X). It contains the following fields:

- * Module ID:
- * Port ID:
- * ONU ID:
- Password:
- Serial Number:
- * Onu Type:
- LOID:
- LOID CheckCode:

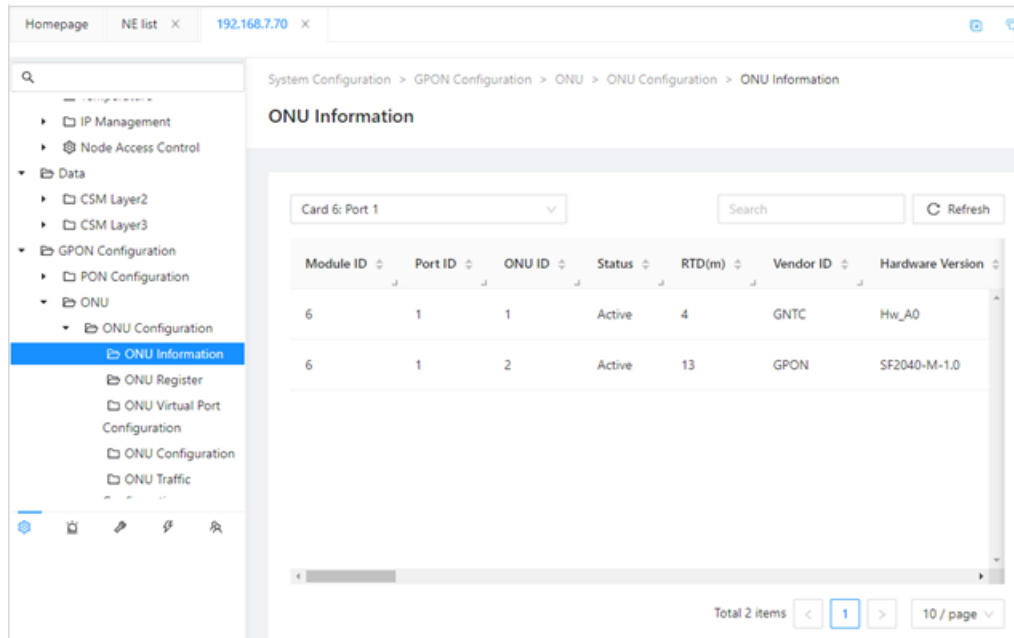
At the bottom of the dialog box are 'Cancel' and 'OK' buttons. The background shows the web interface with the navigation tree on the left, where 'ONU Register' is selected under 'GPON Configuration > ONU > ONU Configuration'. The main area shows a table of registered ONUs with columns for Number, Onu Type, and LOID.

Number	Onu Type	LOID
1820C1FA1	XGPON	
1000B5339	GPON	

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

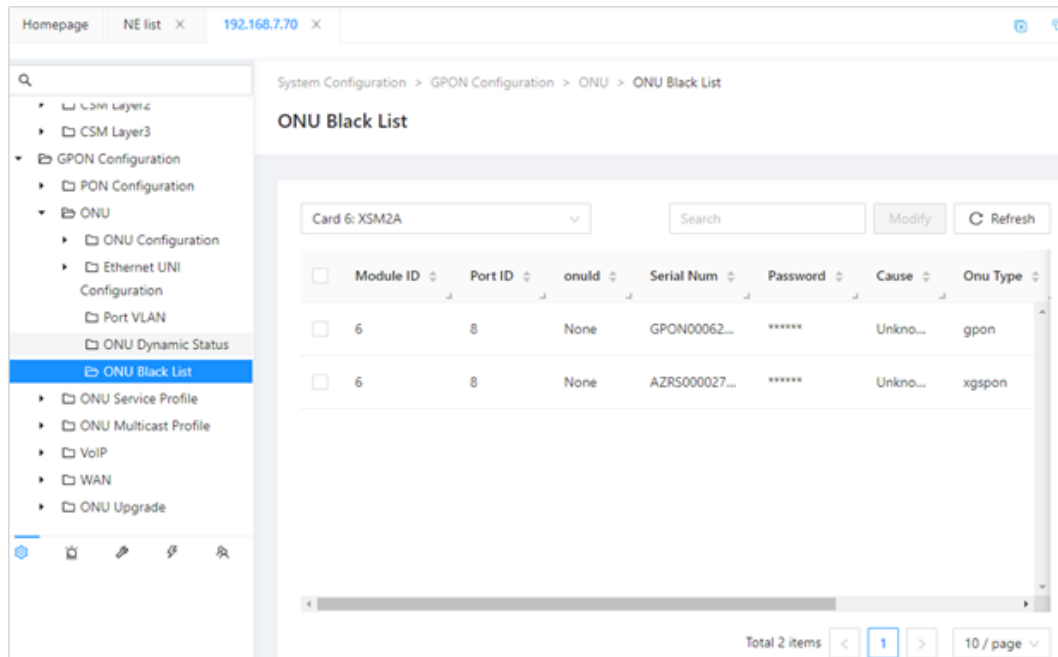
Note: When the communication link between ONU and OLT is normal, the ONU Blacklist can be used to obtain the serial number information of authentication ONU.

In the Function View navigation tree, select GPON Configuration> ONU> ONU Configuration> ONU Basic Information to view the ONU status.



Note: The Status Active indicates that the ONU has successfully completed the registration and authentication.

If the ONU does not register successfully, in the Function View navigation tree, select GPON Configuration> ONU> ONU Blacklist to see why the ONU is not registered.

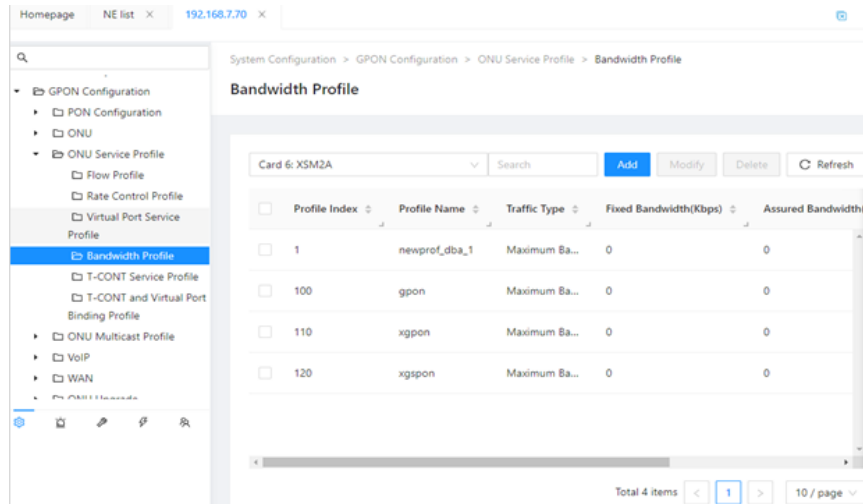


3.2.6 Configure the ONU Data Stream Services

In the Function View navigation tree, select GPON Configuration> ONU Service Profile. OLT created profile 1 by default, and to more clearly describe the configuration process, this instance takes the new profile 2 as an example, you can read the GPON Configuration section for the details of the parameters involved.

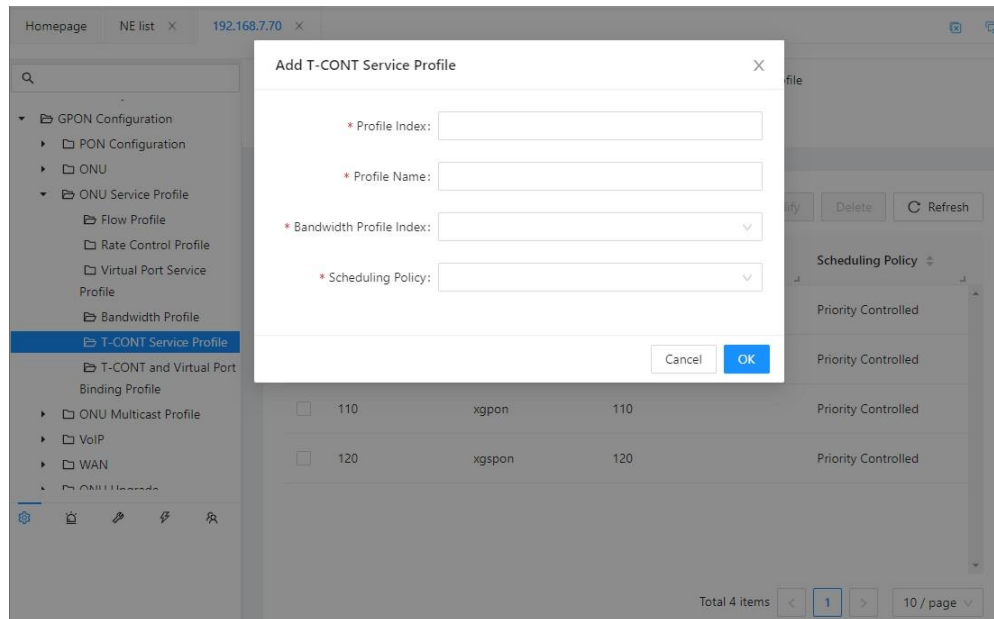
Note: The following pages configure a bandwidth profile to describe the uplink DBA bandwidth patterns and parameters.

Select the Bandwidth profile, and click Add to add the bandwidth profile” 2”.



Note: The following page configuration is T-CONT service profile, which will reference the bandwidth profile.

Select “T-CONT Service Profile”, and click “Add” to add the T-CONT service profile 2.



Note: The following pages configure a flow profile describing ONU uplink parameters including

connection mode, VLAN ID, virtual ports, etc.

Select “Flow Profile”, and click “Add” to add the flow profile 2.



Note: The following page is used to bind the virtual port to the T-CONT service profile.

Select “T-CONT and Virtual Port Binding Profile”, and click “Add” to add the binding profile 2.



Note: The following page configures the ONU virtual port.

Select the PON port in the upper left port navigation bar.

In the Function View navigation tree, select “GPON Configuration> ONU> ONU Configuration> ONU Virtual Port Configuration”.

Click “Add” to add the virtual port number 1.

Homepage NE list 192.168.7.70

System Configuration

ONU Virtual Port Configuration

Card 6: Port 1

Module ID

Port ID

ONU ID

Virtual Port ID

Admin State: Unlock

T-CONT Index

OLT VLAN Translate Profile

GEM Port

Alloc ID

Cancel OK

Note: The following configuration applies the service profile to the ONU.

In the Function View navigation tree, select “GPON Configuration> ONU> ONU Configuration> ONU Traffic Configuration”. Check the ONU, and click “Modify” to apply the profile to the ONU.

Homepage NE list 192.168.7.70

System Configuration

ONU Traffic Configuration

Card 6: Port 1

Module ID

Port ID

ONU ID

Upstream Traffic Mapping Type: map-filtering

Flow Profile: 70

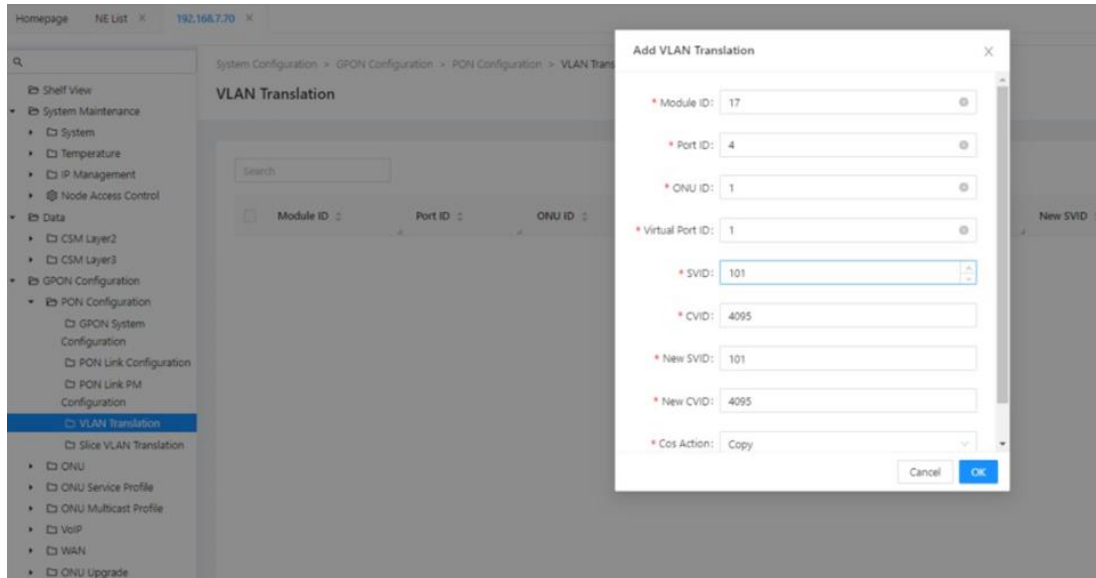
T-CONT and Virtual Port Binding Profile Index: 70

VoIP Profile: 0

Cancel OK

3.2.7 Configure VLAN Translation

In the navigation tree to the left of Device Manager, select “GPON Configuration> PON Configuration> VLAN Translation”. Read the “GPON Configuration” section for specific parameter descriptions.



3.2.8 Perform Connection Test

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

4 System Configuration

- System information
- SNMP
- SNTP

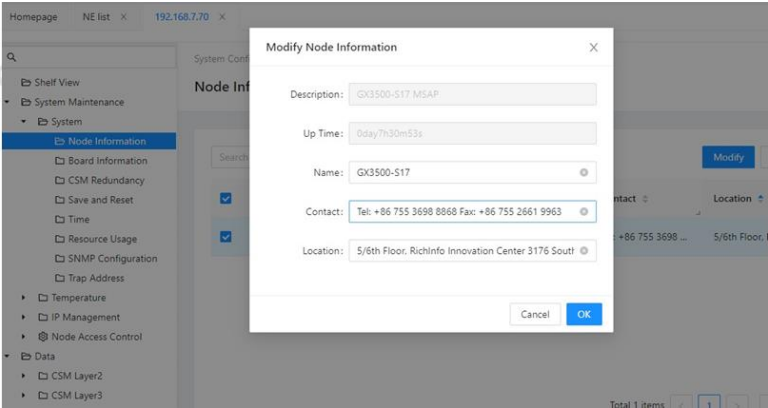
4.1 SNMP

Configuring the SNMP includes the SNMP community table items and a Trap server.

【Operating Steps】

In the Function View navigation tree, select [System Maintenance> System> Node Information].

Check the node, and click “Modify” to modify the node information.



【Parameter Declaration】

Field	Description
Description	System description. Fixed to the AX3517 MSAP.
Up Time	Total time elapsed after the last initialization of the network pipe portion of the system. The NuMax Cloud 4000 system generation user needs to click <Refresh> to reflect the most recent system startup time.
Name	The name of the system. Configurable fields.
Contact	Contact information of the product service provider
Location	Address of the system. Configurable fields.

4.2 SNMP

Configuring the SNMP includes the SNMP community table items and a Trap server.

4.2.1 Configure the SNMP Community Table Item

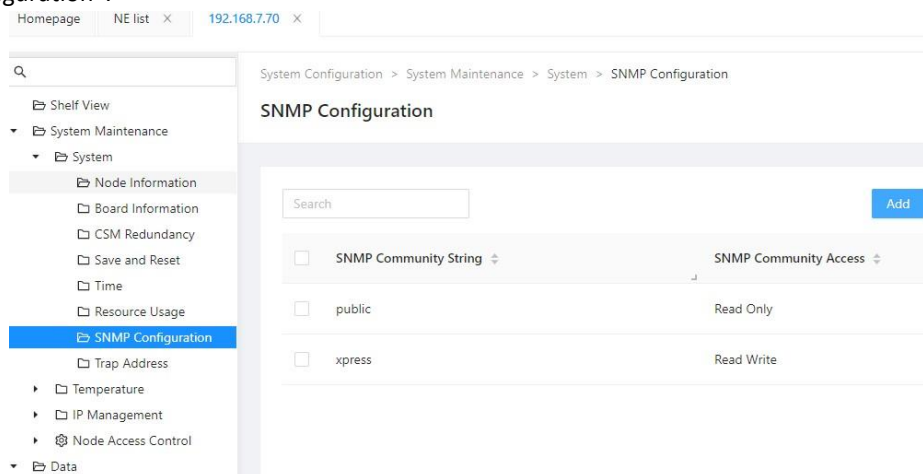
The SNMP community table item contains the access rights and a group name string. There are two permissions, read-only and read-write. Read-only allows only GET for SNMP, and read-write allows GET and SET for SNMP.

The SNMP community table item is added and at least one table item should have “Read-Write” permission.

By default, the value of the community string is “xpress” for read-write and “public” for read-only. If the permission or community string is changed, the NE properties must also be changed.

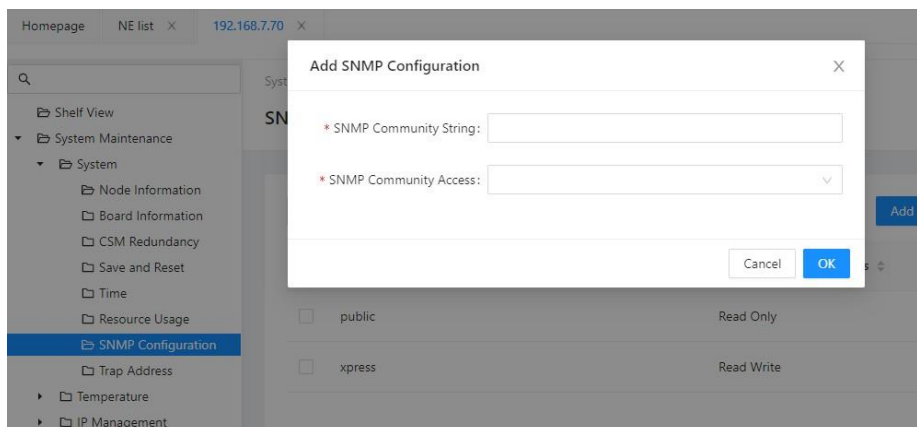
For system security, users are advised to change the default configuration for SNMP.

In the Function View navigation tree, click “System Maintenance> System> SNMP Configuration”.

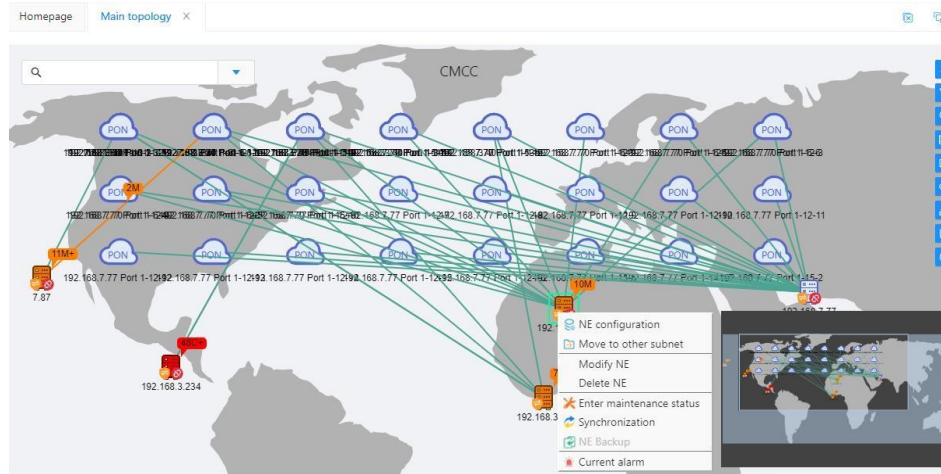


【Operating Steps】

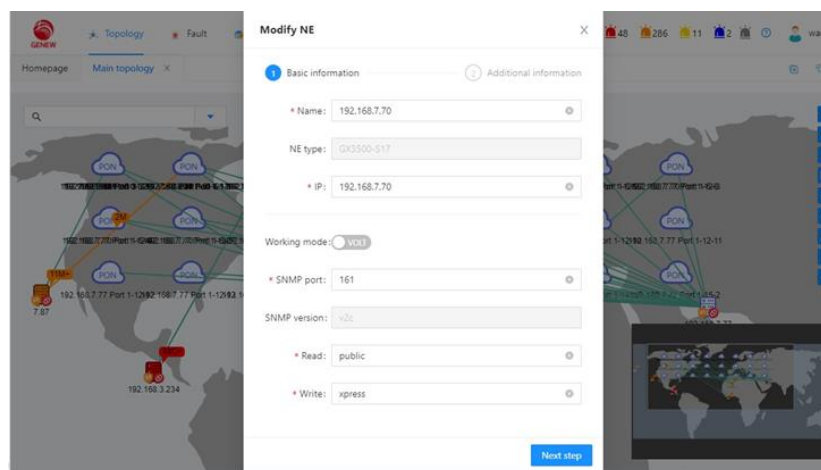
On the “SNMP Configuration” page, click “Add”.



- Enter a community string and select the group permission to be “Read-only”.
- Click <OK> to add the table item in the SNMP community table.
- According to steps 1-3, add a “Read-Write” group string.
- Open the “NuMax Cloud 4000” window (also called a topology map window).
- Right-click the NE in the topology map window, and pop up the shortcut menu.



Click “Modify NE” on the shortcut menu to open the “Modify NE” window



Verify that the “Read” and “Write” fields are the same as set above. If not, change to the same settings in the “SNMP Configuration” window, and then click <OK>.



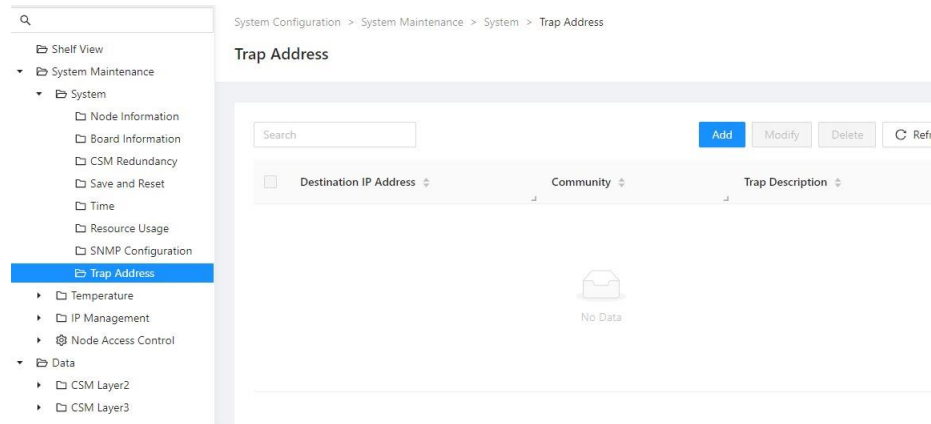
Note: You can delete the default community string.

4.2.2 Configure the Trap server

The user can specify the alarm save server generated by the OLT system, namely the Trap server. Generally, the Trap server is set as the network management server of AX3517/AX3508/AX3502 OLT. Of course, you can also set up the Trap server separately. The OLT system supports up to 4 trap servers.

4.2.2.1 View the Trap server

In the Function View navigation tree, click “System Maintenance > System> Trap Addresses”.



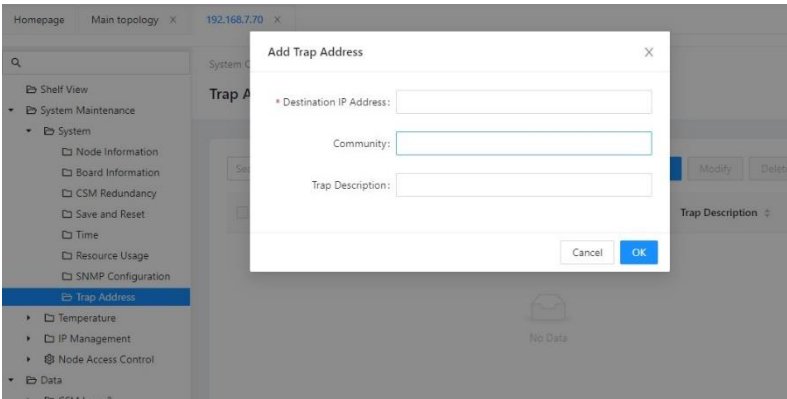
【Parameter Declaration】

Field	Description
Destination IP address	The IP address of the Trap server.
Community	The Group string is the basic password.The Trap community string allows the user to receive a trap from the SNMP agent.The default value is public.The string length is between 0-32.
Trap Description	Descriptor

4.2.2.2 Add Trap server

【Operating Steps】

- In the Function View navigation tree, click “System Maintenance> System> Trap Addresses”.
- In the “Trap Addresses” configuration page, click “Add”.



- Set up the IP address of the Trap server, Community.
- Set up the Trap Community. You can enter a string which length of between 0-32.

Click <OK> to Add the Trap server.

4.3 SNTP

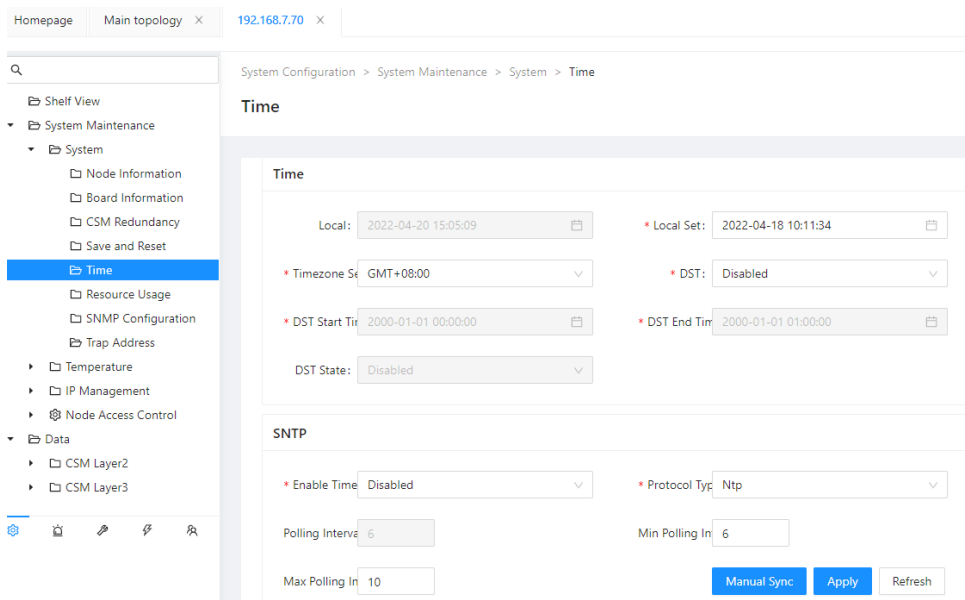
SNTP enables the OLT system to set its internal clock based on regular updates from the NTP server. With the internal clock and NTP, the OLT system enables the system log to record events with a precise system time.

If you want to configure the NTP server, the user needs to open the NTP client and set the time zone for the NTP information. Users can configure up to 3 NTP servers from which the OLT system can get time.

4.3.1 Time

【Operating Steps】

In the Function View navigation tree, click “System Maintenance> System> Time”.



【Parameter Declaration】

Field	Description
Local	Displays the current year, date, and time settings, coming from the OLT system itself.
Local Set	Local-set time.
Timezone Set	Assign time zone names to the internal clock of the client. The time zone was selected according to the country where the OLT is located.
DST	Open daylight saving time or not.
DST Start Time	The start time of daylight saving time.
DST End Time	The end time of daylight saving time.
DST State	Whether daylight saving time is enabled.
Enable Time Syncing	Is the time synchronization function turned on.
Protocol Type	Time synchronization protocol used: NTP or SNTP.

Polling Interval(s)	The interval between the client polling the time messages from the SNTP server. Configurable fields.
Min Polling Interval(s)	Minimum synchronization interval.
Max Polling Interval(s)	Maximum synchronization interval.
Manual Sync	Manually enforce synchronization.

4.3.2 Configure NTP Parameter

If you want to configure the SNTP synchronization time, you need to open the SNTP server and set the time zone.

【Operating Steps】

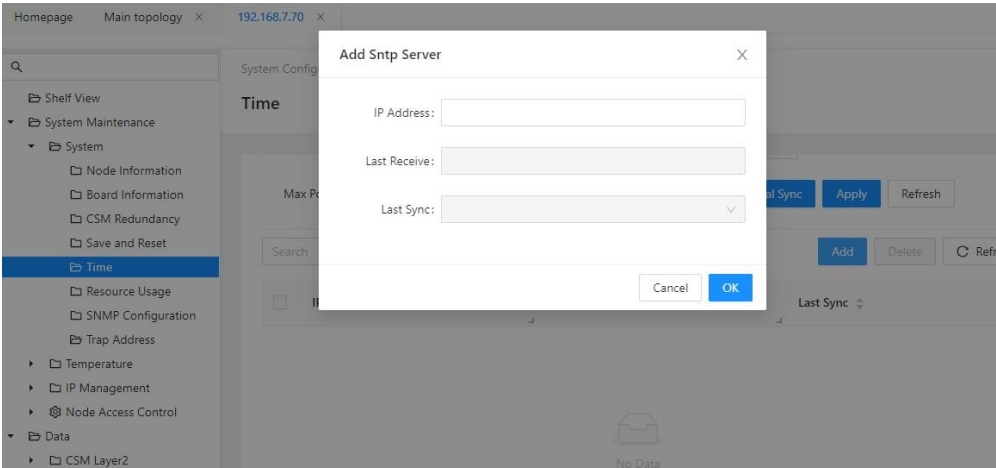
- In the “Time” page, convert the “Time Synchronization” to “Enable” to open the NTP service.
- Select “SNTP” in the “Protocol Type” column.
- Set the Time Zone to (GMT + 08:00).Other default values.See the detailed description in the Time window.
- Click <Apply>.

4.3.3 Add SNTP Server

Users can configure up to 3 SNTP servers. The exchange opportunity attempts to poll the time message for each server in the configured order.

【Operating Steps】

- On the “Time” page, click “Add”.



- Enter the IP address of the SNTP server.
- Click <OK>.

【Result Note】

When the SNTP server is Up, the “Device Time” on the “Time” page appears as the time synchronized from the SNTP server.

【Parameter Declaration】

Field	Description
IP address	The IP address of the NTP server.
Last Receive	Last synchronization time.
Last Sync	Whether the time is synchronized.

4.4 NE Access Control

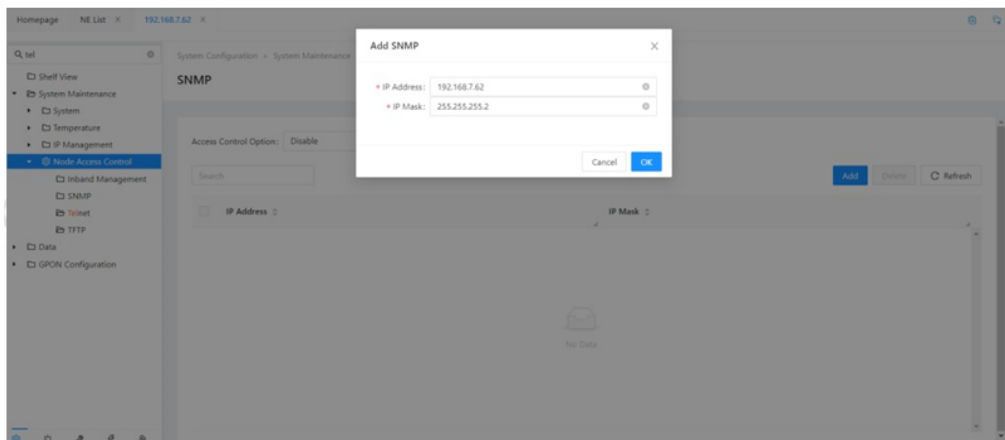
This function controls Telnet, SNMP, tftp, SSH, and FTP access permissions based on IP. When enabled, only the configured IP range is accessible.

4.4.1 Configure SNMP Access Control

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

【Operating Steps】

1. In the Function View navigation tree, click [System Maintenance> Node Access Control> SNMP].
2. Click <add>.

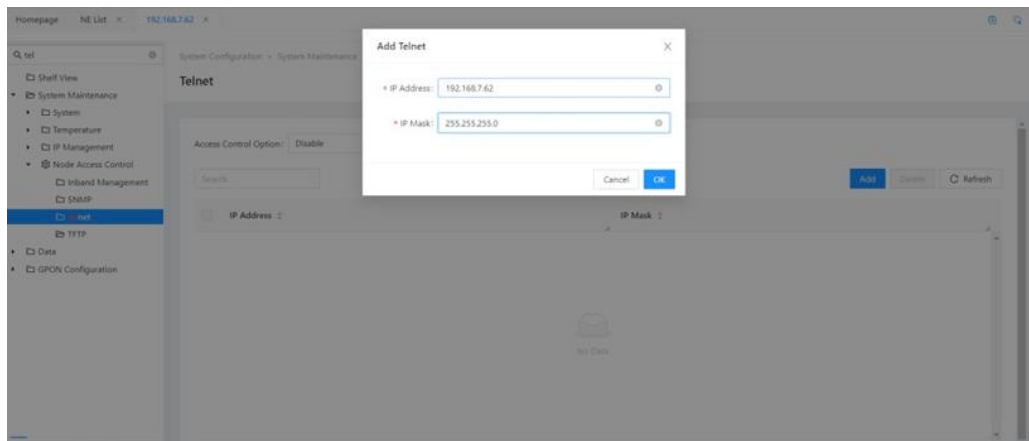


4.4.2 Telnet Access Control

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

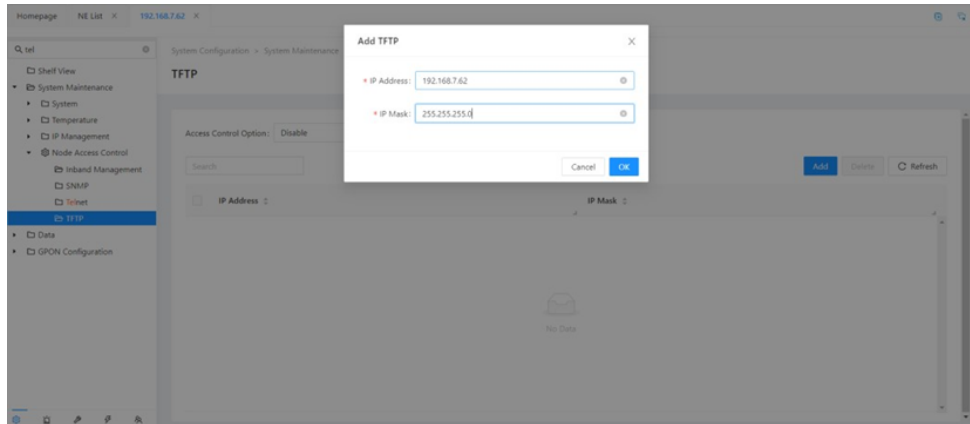
【Operating Steps】

1. In the Function View navigation tree, click [System Maintenance> Node Access Control> Telnet].
2. Click <add>.



4.4.3 TFTP Access control

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



5 Layer 2 Configuration

An OLT is suitable for various network applications. This chapter describes the steps to configure this equipment system for specific network requirements and the following basic configuration:

- Port attribute
- Link aggregation
- VLAN
- MAC Address Table
- Mirror Port
- Spanning tree

5.1 Port Attribute

Gigabit Ethernet (XGE) ports, link aggregation ports, IS ports, or a range of interfaces can be configured as layer-2 ports.

- The XGE port is uplink physical port for AX3517, AX3508, AX3502.
- The link aggregation port consists of one or more converged XGE ports.
- The IS port is the XGE port inside the OLT downlink connected to the OLT port, fixed to “On”.



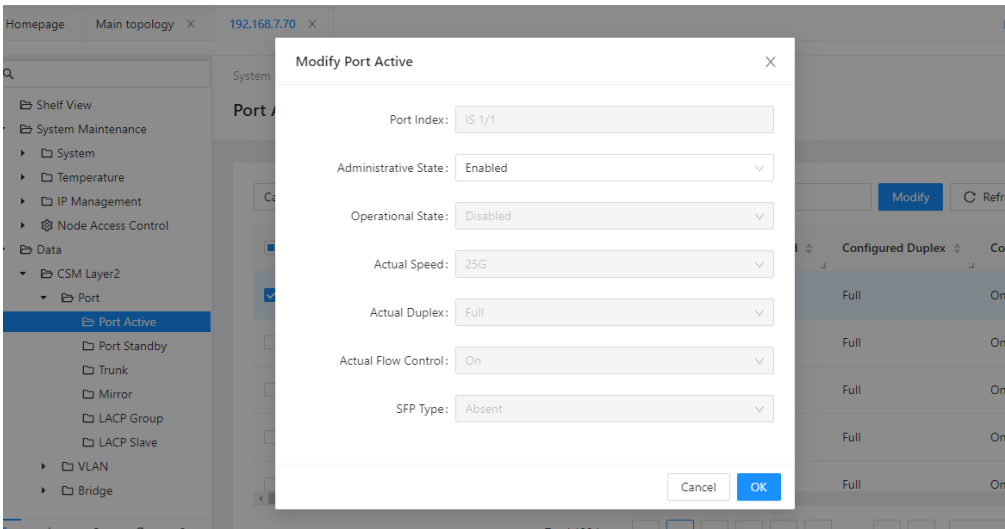
Note: For the OLT PON port configuration, please read OLT.

5.1.1 Administrative Status

XGE ports can be turned on or off by setting the administrative status of the port. The XGE port administrative status is closed by default.

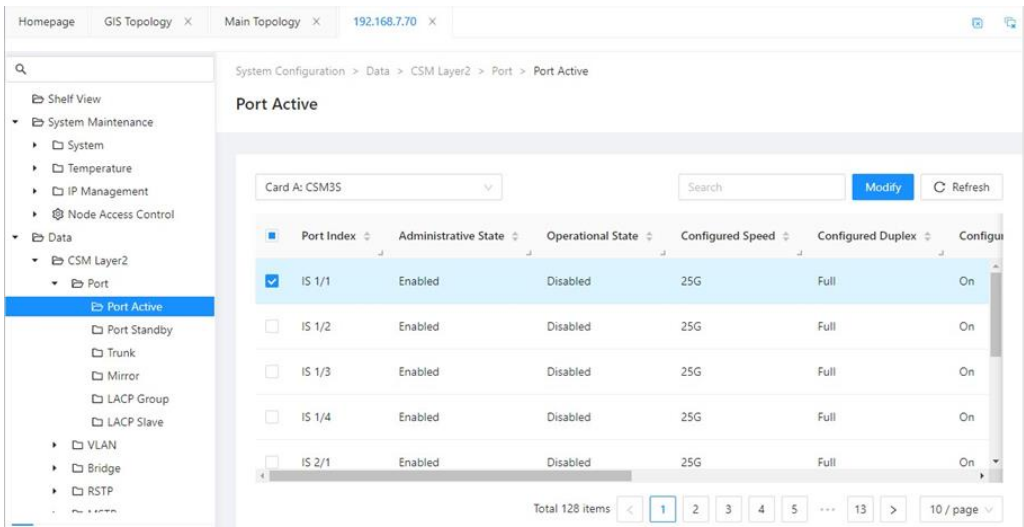
【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> Port> Port Active”.
- Check the port and click "Modify", and set "Administrative Status" to open.



Click <OK> to Save configuration.

Click “Refresh”, and the administrative status appears as “Enabled” in the port list.



【Parameter Declaration】

Field

Description

Port Index

Port number, read-only

Port Administrative State

Port administrative status: on / off.

Operational state

Port running status: on / off.

Actual Speed

The rate of the actual negotiation.

Actual Duplex

Duplex mode of actual negotiation.

Actual Flow Control

Actual negotiated flow control.

SFP Type

Module type.

5.1.2 Running State

The XGE port operation status indicates whether the link is active, and the default running status is "Closed".

Depending on the ports, the link status changes based on the following rules:

- OLT uplink XGE port: If a physical connection is established to the active node and the management status is on, the link status is "On".
- OLT downlink IS (Internal Slot) port connected to PON, management status remains "On", not allowed closed.

5.1.3 Self-Negotiation and Rate Duplex

The OLT supports the automatic negotiation function of the uplink XGE port. When the ports on both ends are on for self-negotiation, duplex mode and rate are automatically set to the highest level both ports can provide.

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

5.1.4 Flow Control

OLT, while providing traffic flow control in the receiving and transmission directions. Provide this function to the remote device for a proper flow control function. Flow control is turned on by default.

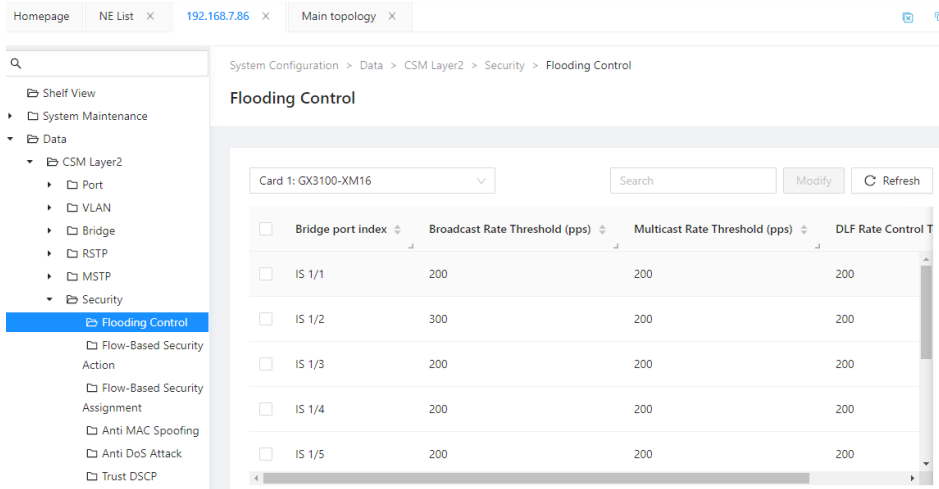
5.1.5 Storm Control

OLT provides three types of operational storm control: broadcast, unknown multicast, and unknown unicast. Data storms are prevented by setting the threshold for each packet type. The threshold represents the number of packets passing through the port per second and is part of the total available bandwidth. Packets were discarded when the threshold was exceeded.

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

【Operating Steps】

In the Function View navigation tree, click “Data> CSM Layer 2> Security> Flooding Control”.



【Operating Steps】

Field

Description

Bridge Port Index

Port number identification

Broadcast Rate Threshold (pps)

Broadcast rate limit threshold. In package / second (PPS). Range of values: 0-1488100.

Multicast Rate Threshold (pps)

Multicast rate limit threshold. In package / second (PPS). Range of values: 0-1488100.

DLF Rate Control Threshold (pps)

Unknown unicast rate limit threshold, measured in packet/second (PPS). Range of values: 0-1488100.

Note: On AX3517/AX3508/AX3502, the Generation Tree Protocol (STP) packets are treated as multicast packets, and all STP packets are discarded when the multicast storm control threshold is 0.

Warning: Discard some type of broadcast frame at will causes network instability, sometimes disrupting network operations.

5.2 Link Aggregation

The XGE port operates as a layer-2 interface. Ports can be managed separately or uniformly managed as LAG (Link Aggregation Group). A LAG is a collection of multiple physical ports, just as a single port runs.

5.2.1 LAG Interface Limits

Note when using the port LAG:

- Ports on both ends must be configured as LAG ports.
- Port can belong to one LAG. If the network administrator tries to assign an XGE port that is already a LAG B member to the LAG A, the action fails.

- All LAG member ports of the same LAG must be configured in the same configuration, including bandwidth (1 Gbps), duplex mode, and VLAN allocation.
- All of the ports in the LAG must be in the same spanning tree state.
- When a port belongs to a LAG, its attributes (such as bandwidth, VLAN attributes, administrative status, and duplex mode) cannot be configured separately.
- Before activating the cable, activate the LAG to avoid forming the loop.
- Before removing the LAG, disconnect all LAG port cables or close the LAG ports to avoid loop formation

5.2.2 LAG Load Balancing Rules

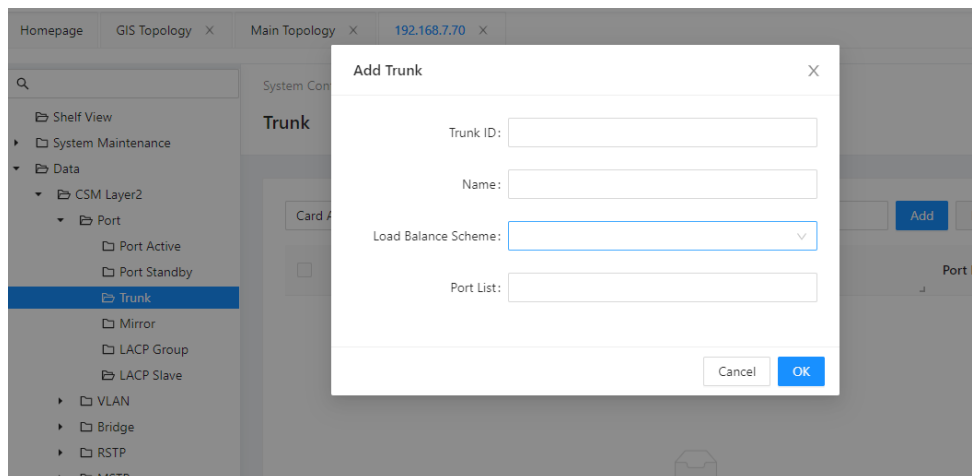
OLT provides the following methods:

- Source MAC address
- Destination MAC address
- Source and destination MAC address
- Source IP address
- Destination IP address
- Source and destination IP address

5.2.3 Create a LAG

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> Ports> Trunk”.
- Click Add to configure the parameters with reference to below table.



- Click <OK> to save configuration.

【Parameter Declaration】

Field	Description
Trunk ID	The number of the link aggregation group that you created.
Name	Specifies the name of the aggregate port. The system supports 6 load balancing methods:
Load Balancing Scheme	Source MAC; destination MAC; source and destination MAC; source IP address; destination IP address; source and destination IP address.
Port List	Link aggregate member ports. The member must be an uplink XGE port.

5.3 VLAN

OLT supports up to 4094 VLAN IDs (1-4094), VID 1 and 4094 are retained by the system for internal functions and are not configurable.

By default, All OLT ports are assigned to the VID 1 and are the untagged.

5.3.1 VLAN Management

When adding ports to a VLAN, the port can be configured as a tagged or untagged port. This VLAN ID is set to port PVID when configured as Untagged.

Layer-2 ports can belong to multiple VLAN Tagged ports, but can only be an Untagged port of one VLAN.

VLAN 1 is the default VLAN for each layer-2 port and can't be deleted or modified.

5.3.2 Ingress Filter

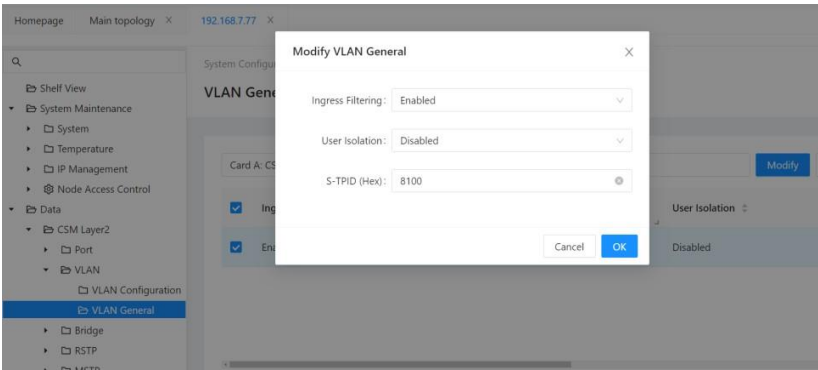
If the XGE port receives the downlink tagged packet, it will forward it according to the port configuration, as follows:

- If XGE port entry filtering is enabled, only packets belonging to the VLAN of this port will be forwarded. Other packets are discarded.
- If XGE port entry filtering is turned off, all packets with VLAN IDs listed in OLT VLAN table will be forwarded, regardless of whether the port is a member of VLAN or not. Other packets are discarded.

By default, entry filtering is off.

【Operating Steps】

In the Functional View navigation tree, click "Data> CSM Layer 2> VLAN> VLAN General".



【Parameter Declaration】

Field	Description
Ingress Filtering	Whether the ingress filter is turned on.
User Isolation	Whether the user isolation is on. the default is enabled.
S-TPID (Hex)	S-TPID values, expressed in hexadecimal.

5.3.3 VLAN configuration

5.3.3.1 Application Description

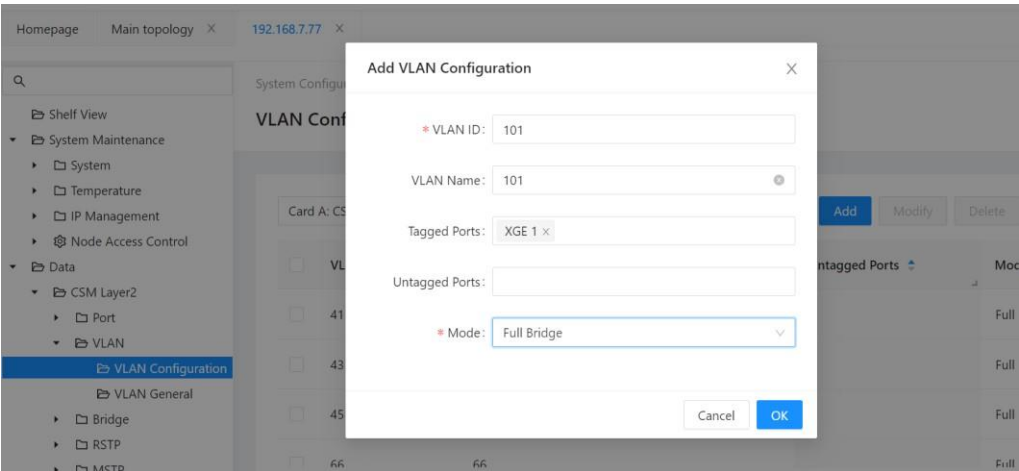
Business VLAN 101. The uplink OLT XGE port is a member of the VLAN 101 of this system.

5.3.3.2 Instance Topology

This instance takes OLT basic data business configuration topology figure as an example.

5.3.3.3 Add a VLAN

- In the Function View navigation tree, select “Data> CSM Layer 2> VLAN> VLAN Configuration”.
- Click “Add”, enter the VLAN ID 101, and select the Tagged port: XGE1.



- Click <OK>, save the configuration.

5.3.3.4 Delete VLAN

Can be deleted even if the VLAN is not empty.

Check the VLAN to be deleted and click "Delete".

【Parameter Declaration】

Field	Description
VLAN ID	VLAN ID, the value range is from 2 to 4093. VLAN1 is retained as the system default VLAN.
VLAN Name	User-defined VLAN name
Tagged Ports	Tagged port list of all label ports listed.The value range is a list of members: link aggregate port identification, interface identification, or interface scope.
Untagged Ports	Untagged ports list of all de-label ports listed.The value range is a list of members: link aggregate port identification, interface identification, or interface scope.
Mode	VLAN, working mode: Full-bridge mode, Limit bridge mode, Routing mode

5.4 MAC Address Table

OLT maintains a MAC address table for packet forwarding. Each table item includes a MAC address, a VLAN ID, and a port number. Layer-2 table items can learn from OLT switching chip hardware or can be created manually.

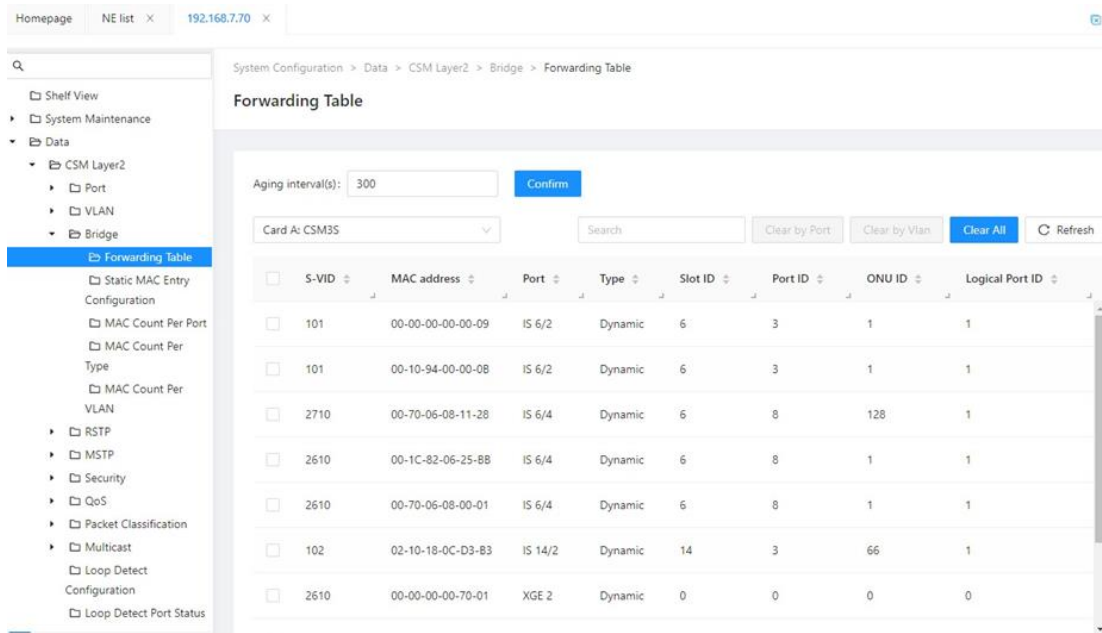
Layer-2 table items transfers can also be removed by hardware-based or software- based aging.

Dynamic table items created by the system are aged after a configurable MAC aging time with a default of 300 seconds.Manual created items remain in the table until manually deleted.

MAC table items shall be specified manually in the following cases.A specified user device with a specific MAC address will only allow access to the specific ports in the VLAN.

【Operating Steps】

In the Function View navigation tree, click “Data> CSM Layer 2> Bridges> Forwarding Table”.



【Parameter Declaration】

Field	Description
S-VID	The VLAN ID range is from 1 to 4,094.
MAC Address	The Physical MAC address.A 48-bit 16 hexadecimal.
Port	Forwarding port number.
Type	Represents whether the MAC address is dynamic or static.
Slot ID	Slot ID
Port ID	Port ID
ONU ID	ONU ID
Logical Port ID	Logical Port ID

5.5 Mirror Port

By configuring another port to "mirror" the service on the port that needs to be monitored, you can connect the protocol analyzer to the mirror port to observe the service on the monitored port.

- The destination interface must be a single upper interface rather than a set of interfaces. The destination interface cannot be a source interface either.
- The system only supports the 1 mirror port.

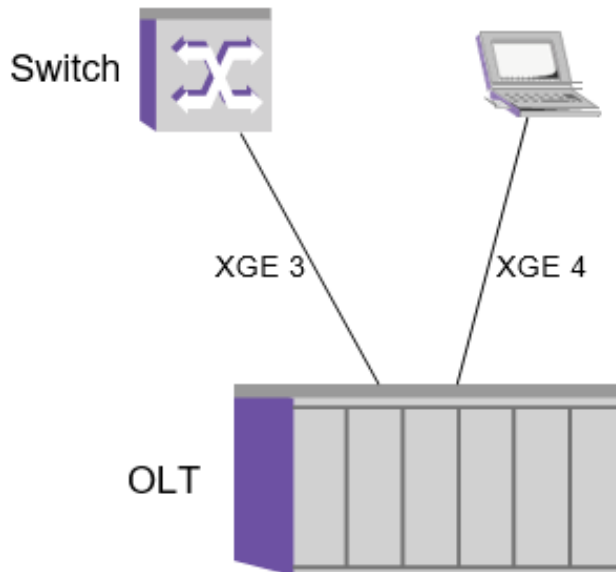
Close the current mirror port when it is no longer needed.

5.5.1 Mirror Port Configuration Instance

5.5.1.1 Application Description

The OLT operates as a layer-2 switcher with an abnormal uplink port, XGE3. The XGE4 will be configured to mirror port that monitor bidirectional data of XGE3 port.

5.5.1.2 Instance Topology



5.5.1.3 Configuration Requirements

The Port physical link is normal.

5.5.1.4 The Tasks of Configuration

The list of tasks for the mirror port configuration is listed below:

- Configure mirror port
- Delete Mirror Port

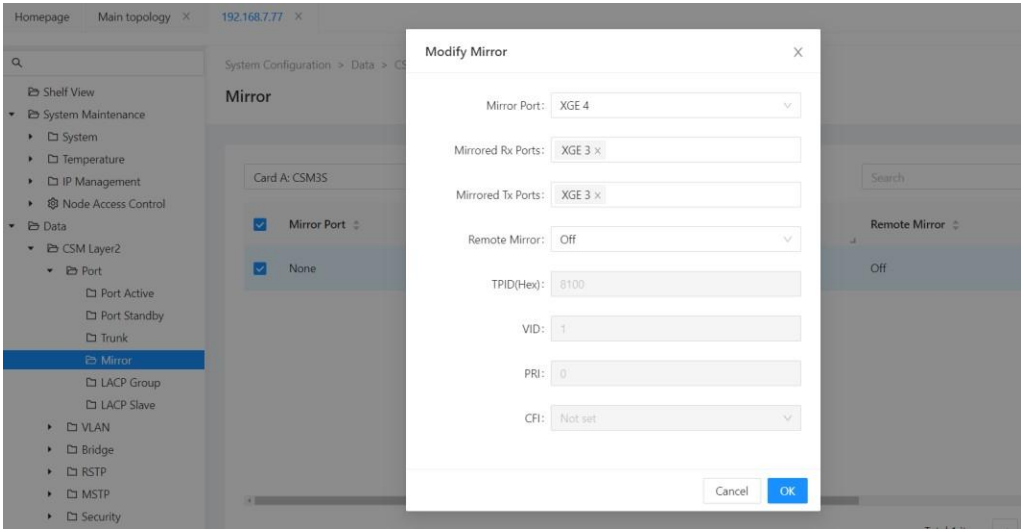
The detailed steps for each task are described below with Figure5-8 topology as an example.

5.5.1.5 Configure Mirror Port

【Operating Steps】

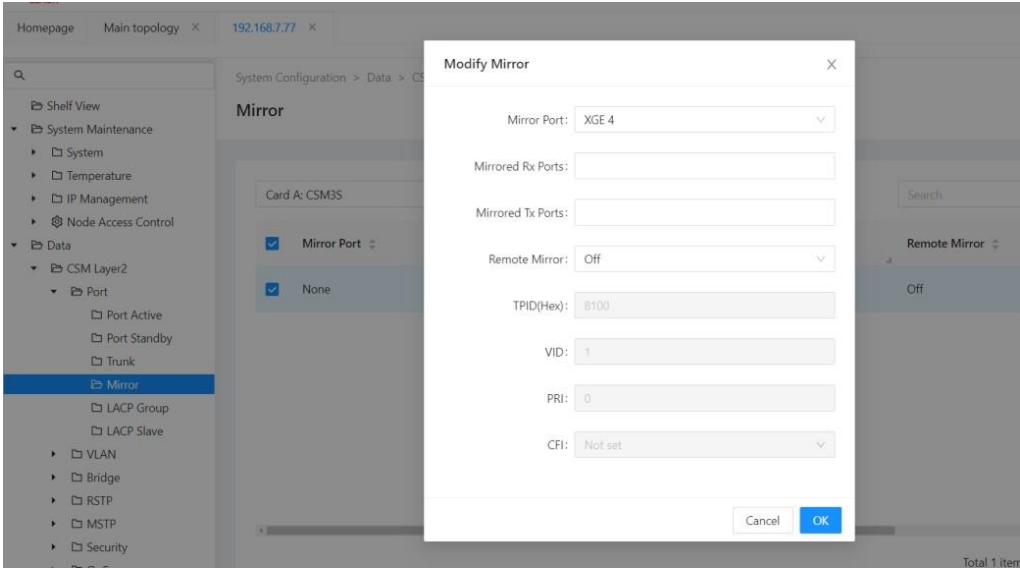
- In the function view navigation tree, click Data > CSM tier 2 > port > mirror.

- Check the ports required to be configured.



5.5.1.6 Delete Mirror Port Configuration

Mirror port select None, click <OK> to remove mirror port configuration.



【Parameter Declaration】

Field	Description
Mirror Port	Single source interface, such as: XGE 4. Can not be a set of interfaces. And the destination interface cannot be one of the source interfaces.
Mirroedr RX Port	Port-based source receiving interface.Can be a set of interfaces or a single interface. Determines that the source entry port list and the destination interface do not duplicate.If only this attribute is configured and

Field	Description
	the exit port lists remain blank, meaning that only received services are monitored.
Mirrored TX	Port-based source send interface.Can be a set of interfaces or a single interface. Determines that the source entry port list and the destination interface do not duplicate. If only this attribute is configured and the list of exit ports remains blank, meaning that only the sent service is monitored.
Remote Mirror	Turn on the remote mirror image

5.6 Spanning tree

5.6.1 RSTP Introduction

The OLT system supports both the RSTP protocol and the MSTP protocol.

5.6.2 RSTP Configuration

5.6.2.1 Enable RSTP

【Operating Steps】

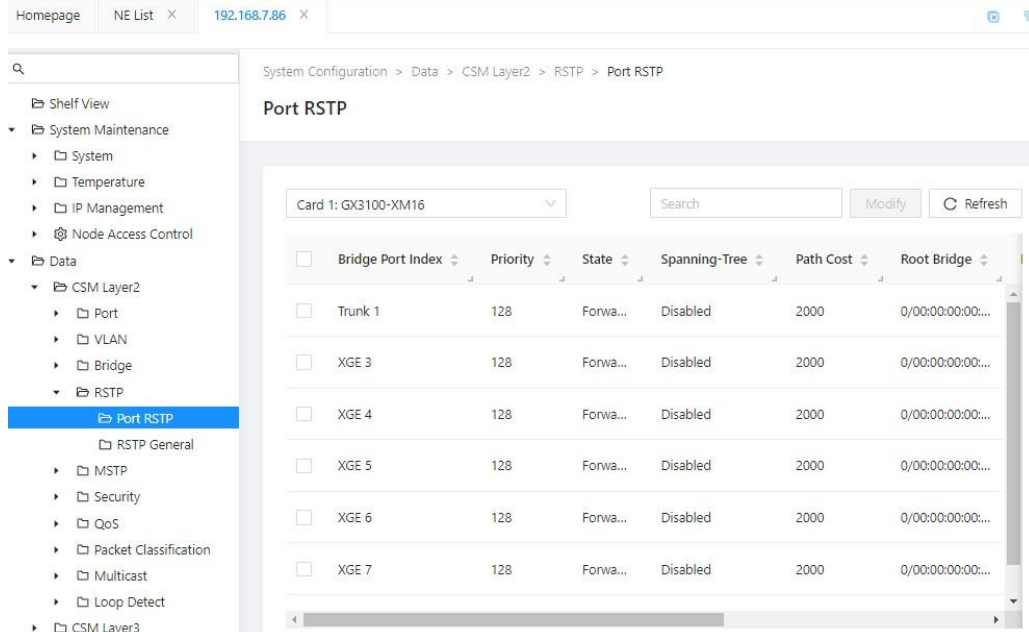
- In the Function View navigation tree, click “Data> CSM Layer 2> RSTP> RSTP General”.

- Set the RSTP port status to Enable.
- Set the RSTP protocol parameters.
- Click <OK> to save the configuration.

5.6.2.2 Configure the RSTP Port

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> RSTP> Port RSTP”.

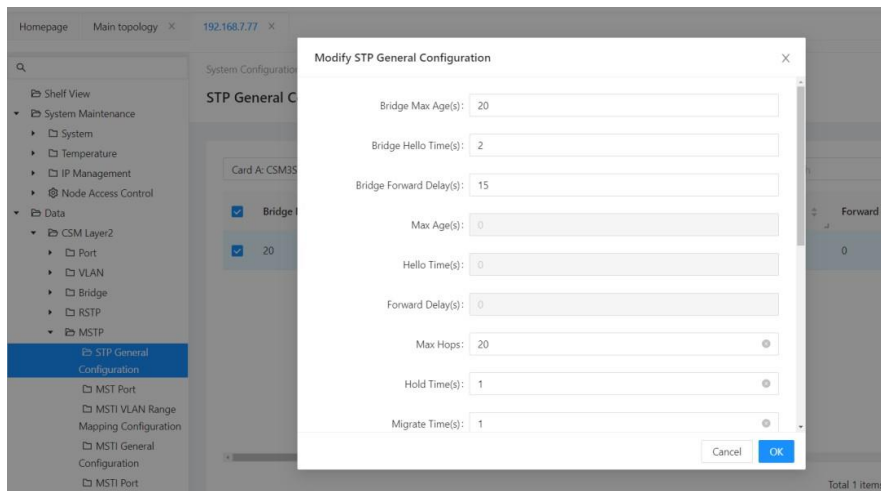


- Select the RSTP bridge that you want to configure;
- Set the RSTP protocol parameters;
- Click <OK> to save the configuration.

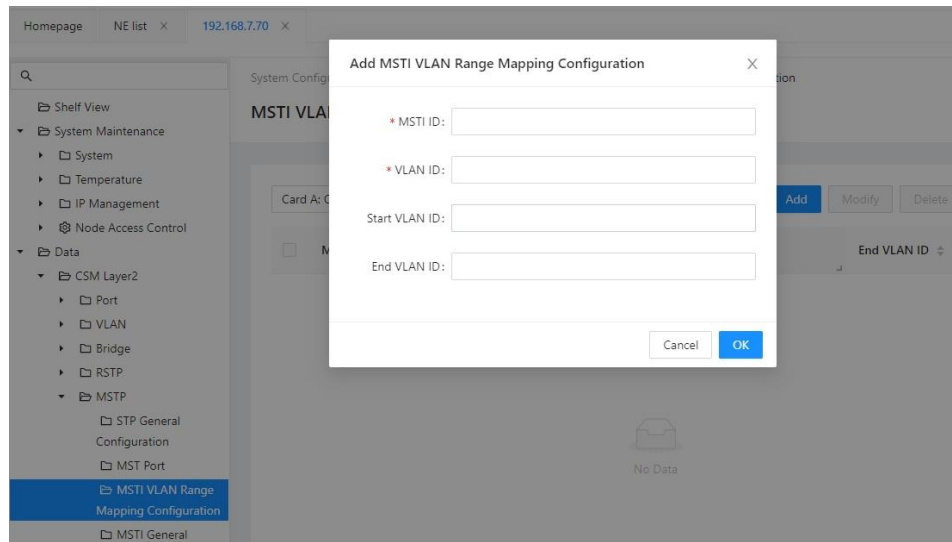
5.6.3 MSTP Configuration

【Operating Steps】

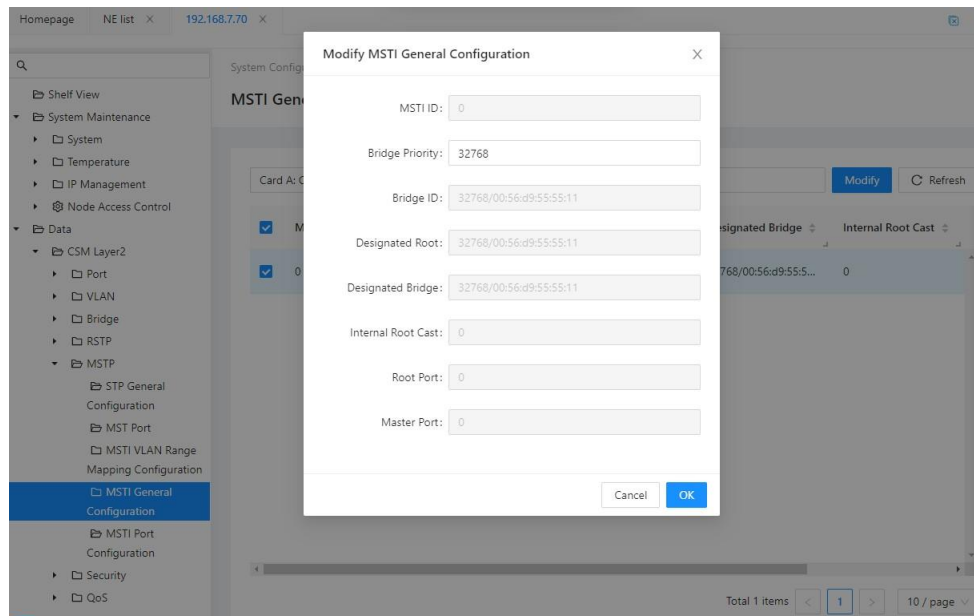
- Configure STP general information, in the Function View navigation tree, click “Data> CSM Layer 2> MSTP> STP General Information”.



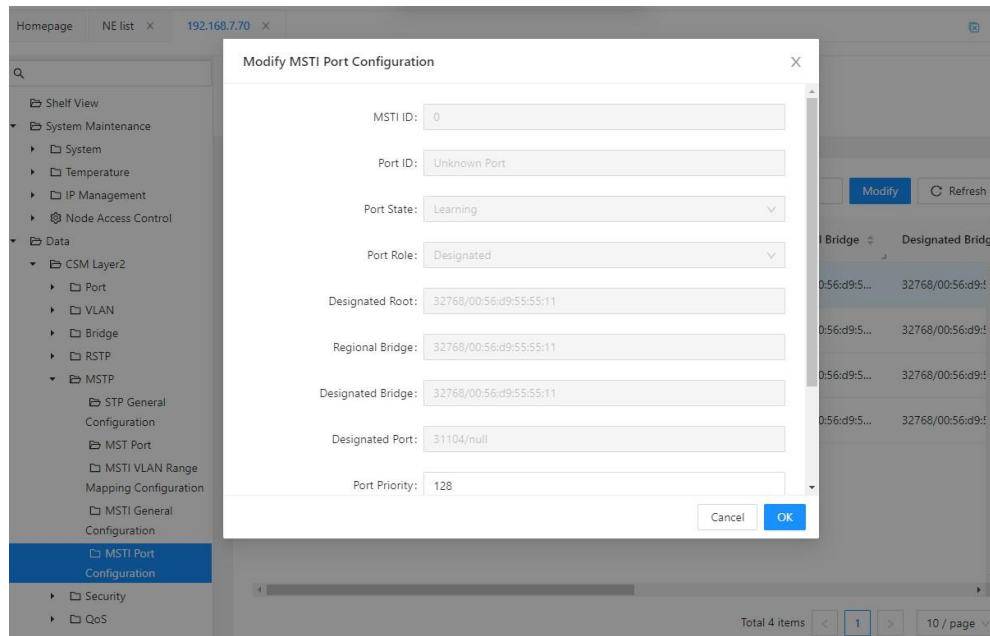
- Configure Instance, in the Function View navigation tree, click “Data> CSM Layer 2> MSTP> MSTI Range Mapping Configuration”.



- Set up MSTI general Information, and click “Data> CSM Second Floor> MSTP> MSTI General Information”.



- MSTI port configuration, click “Data> CSM Layer 2> MSTP> MSTI Port Configuration”.



6 Layer 3 Configuration

This section describes the configuration of the layer-3 SVI on OLT.

6.1 SVI Concept

When packets communicate on the layer-2, they can only be forwarded within the same VLAN. For packets to be transmitted between different VLAN, layers-3 of communication are required. OLT uses the SVI (Switch Virtual Interface) to enable OLT to route packets between the VLAN.

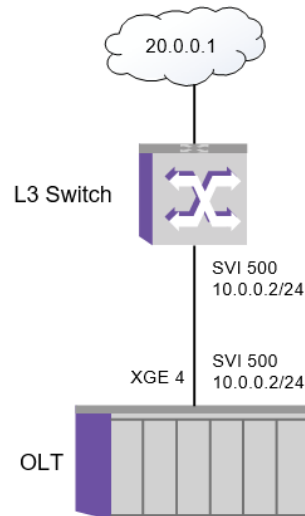
By configuring SVI, one or more OLT XGE ports can be configured as a virtual single interface and assigned an IP address to activate routing.

Only one SVI can be configured per VLAN.

The SVI is a layer-3 interface, and the packet processing on the layer-3 interface includes layer-2 switching and layer-3 routing. Layer-3 routing forward packets according to the routing table.

6.2 Application Description

In the topology of below figure, OLT is connected to the network via a layer-3 switch. Upper layer-3 switch works in layer-3 mode, SVI 500(10.0.0.2/24 already configured), OLT configured SVI 500(10.0.0.1/24).



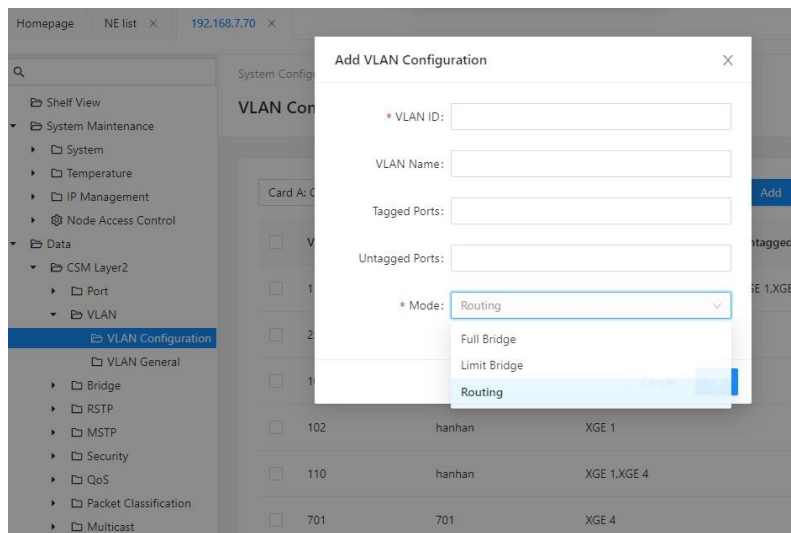
The next section describes the configuration steps for the SVI.

This configuration instance uses the network topology of below figure. Configure the SVI for the XGE4 port of the OLT to establish layer-3 of communication between the OLT and the switch.

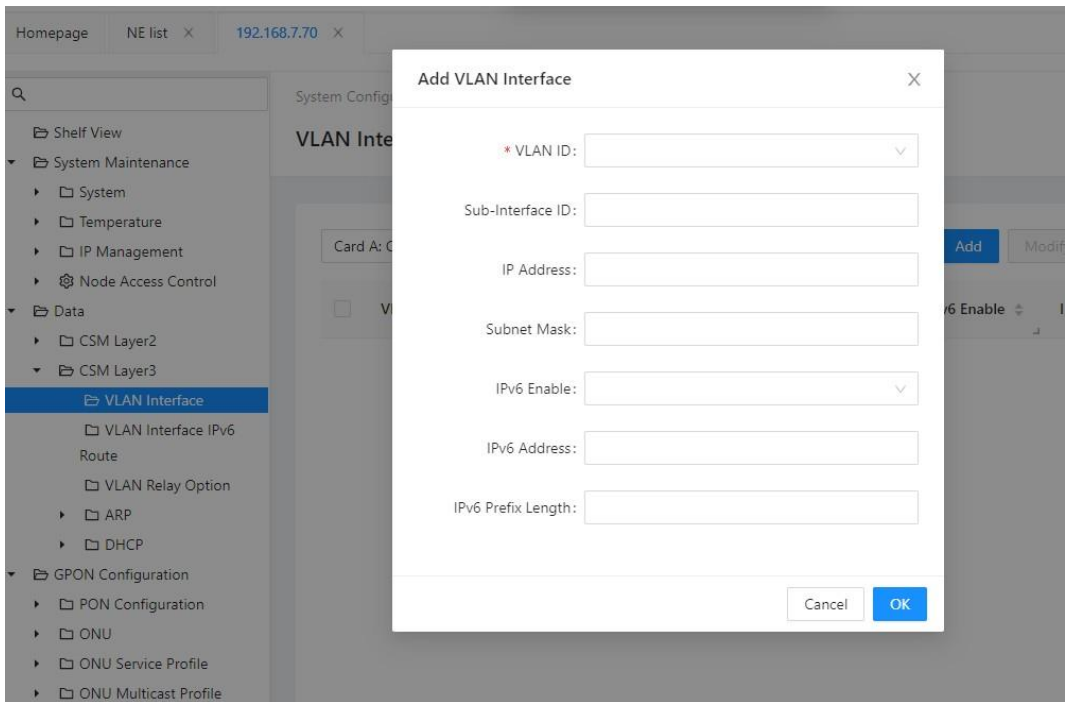
6.3 Add SVI

【Operating Steps】

- Create a VLAN 500 and assign an XGE4 to it, and set it to routing mode.



- In the Function View navigation tree, click “Data> CSM Layer 3> VLAN Interface”.
- Click “Add” to set the IP address, 10.0.0.10/24.



- Click <OK> to save the configuration.

Field	Description
VLAN ID	VLAN ID.
Sub-Interface ID	Sub-Interface ID
IP Address	IP address
Subnet Mask	Subnet mask
IPv6 Enable	Whether enable IPv6 or not.
IPv6 Address	Configure IPv6 address, valid when IPv6 is enabled.
IPv6 Prefix Length	Configure IPv6 address prefix length, valid when IPv6 is enabled.

6.4 Configure ARP

The Address Resolution Protocol (ARP) is used to map IP address to MAC address, as defined by RFC 826.

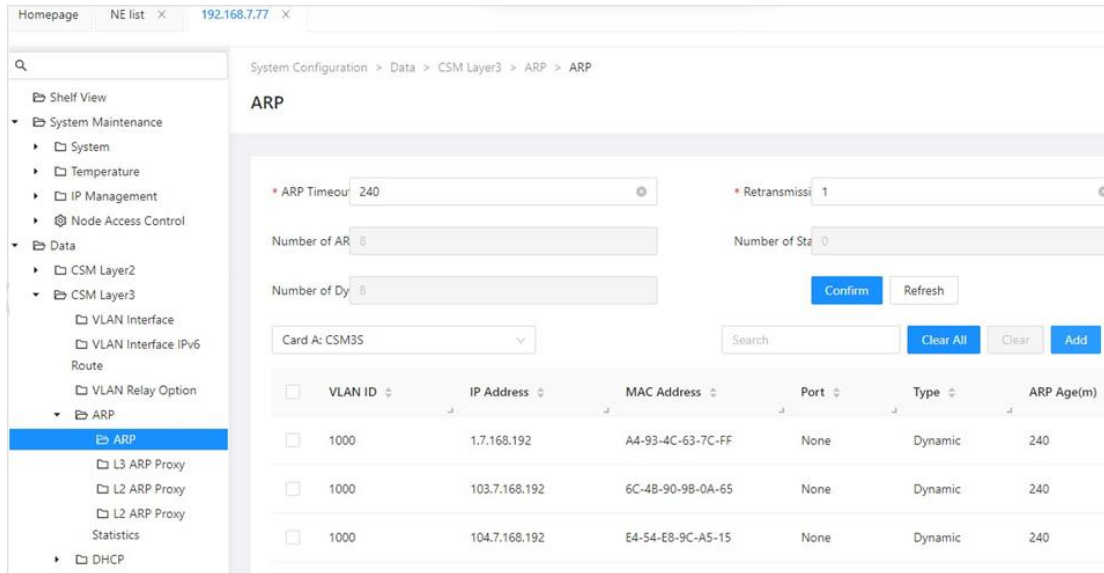
The fields of the ARP table are IP address, MAC address and Interface ID, etc. The ARP table items can be either dynamic or static. Dynamic items are automatically learned by the system, and static items are specified manually.

Create a dynamic ARP table item when:

OLT communicates with upstream and downstream network devices above layer 3.

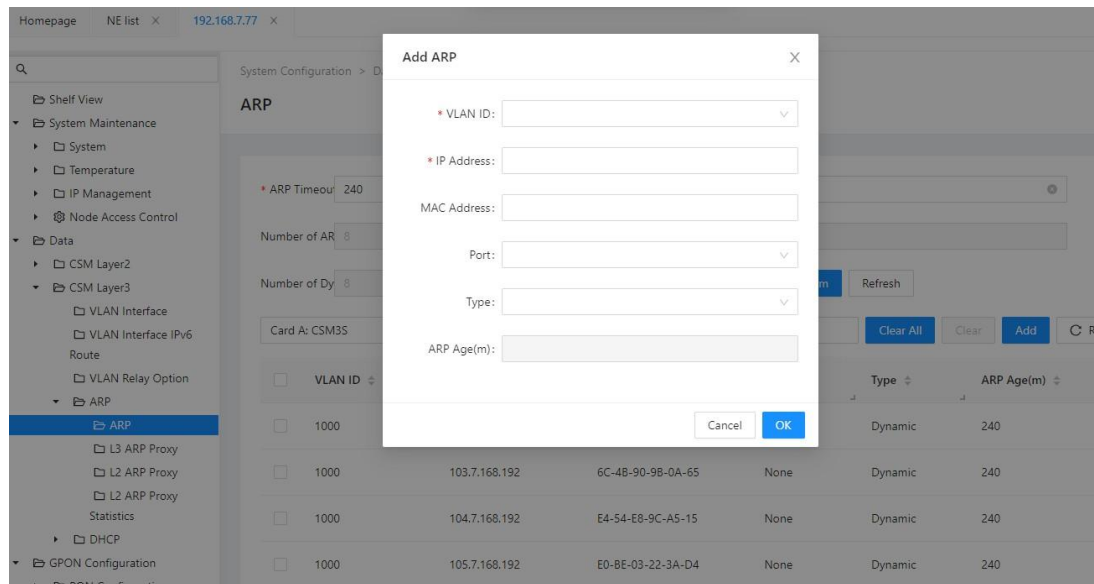
【Operating Steps】

- In the Functional View navigation tree, click “Data> CSM Layer 3> ARP> ARP”.



VLAN ID	IP Address	MAC Address	Port	Type	ARP Age(m)
1000	1.7.168.192	A4-93-4C-63-7C-FF	None	Dynamic	240
1000	103.7.168.192	6C-48-90-98-0A-65	None	Dynamic	240
1000	104.7.168.192	E4-54-E8-9C-A5-15	None	Dynamic	240

- Click “Add” to enter the IP address, layer 3 interface, and MAC address.



- Click <OK> to save the configuration.

【Parameter Declaration】

Field

ARPTIMEOUT(m)

Retransmission(s)

Number of ARP

Number of Static ARP

Number of Dynamic ARP

VLAN ID

Description

ARP table item aging time.

Send time again after the timeout.

Statistical number of ARP.

Statistical number of static ARP.

Statistical number of dynamic ARP.

VLAN ID

Field	Description
IP Address	The IP address of the ARP table item.
MAC Address	The MAC address of the IP address mapped to the ARP table item.
VLAN ID	VLAN ID of ARP table item.
Type	The ARP learning type that identifies the ARP table item: Static: It is created by the system operator. The ARP type of the static ARP table item in the Host Routing window appears as an inherited ARP. Dynamic: learned from the ARP protocol. Invalid: incomplete
ARP Age(m)	Aging time

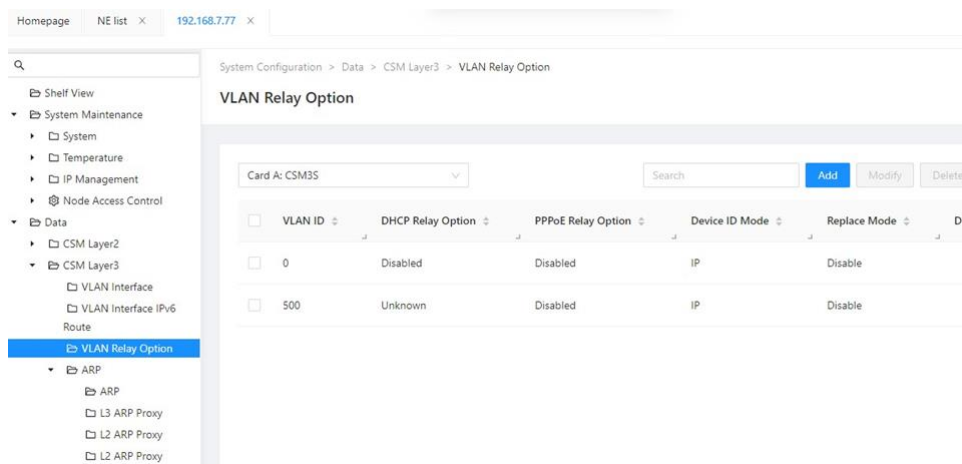
6.5 Relay Option

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

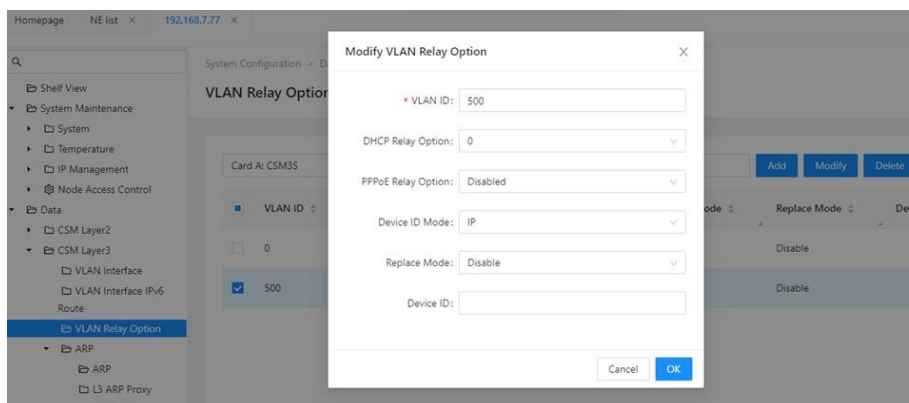
【Operating Steps】

To Create a VLAN, please refer to the VLAN Configuration.

In the Functional View navigation tree, click “Data> CSM Layer 3> Relay Option”.



Select VLAN.



Field	Description
VLAN ID	VLAN ID.
DHCP Relay Option	Whether turn on DHCP relay option function or not.
PPPoE Relay Option	Whether turn on PPPoE relay option function or not.
Device ID Mode	Device ID mode
Replace Mode	Open the replace mode or not
Device ID	Device ID

7 GPON Configuration

OLT follows the ITU-T G.984 / G.988 series standards.

This chapter describes the configuration steps for all passive optical networks (GPON):

- ONU authentication
- ONU register
- ONU traffic
- OLT Management
- ONU Management
- Based on Flow Speed Limit
- FEC
- Downstream Encryption
- PON Protection
- PON Optical Power Detection
- Rogue ONU Detection

7.1 ONU Authentication

The ONU needs to access to the OLT. The ONU without authentication cannot produce normal data links. The OLT supports five authentication modes:

- Serial number authentication
- Serial number and password authentication
- Password authentication
- Logic identification authentication
- Logical identification and password authentication
- Close certification

The system default is serial number (SN) authentication, and the serial number of the ONU can be viewed at the bottom of the ONU.

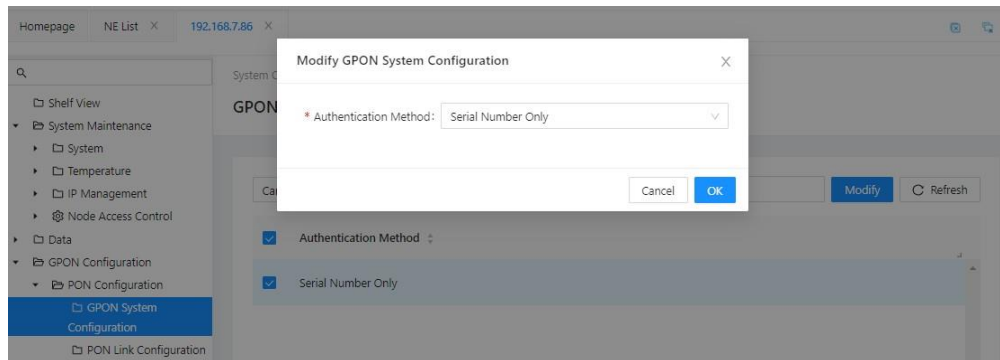
Each OLT GPON downlink port (PON port) can connect to a certain number of ONU (determined by port mode, such as Combo card GPON up to 256). Since these ONU are all connected to the same physical PON port, it is recommended to bind different ONU ID for ONU.



Note: Modify the authentication mode, the system will automatically clear the original ONU related configuration.

【Operating Steps】

In the Function View navigation tree, click “GPON Configuration> PON Configuration> GPON System Configuration”.



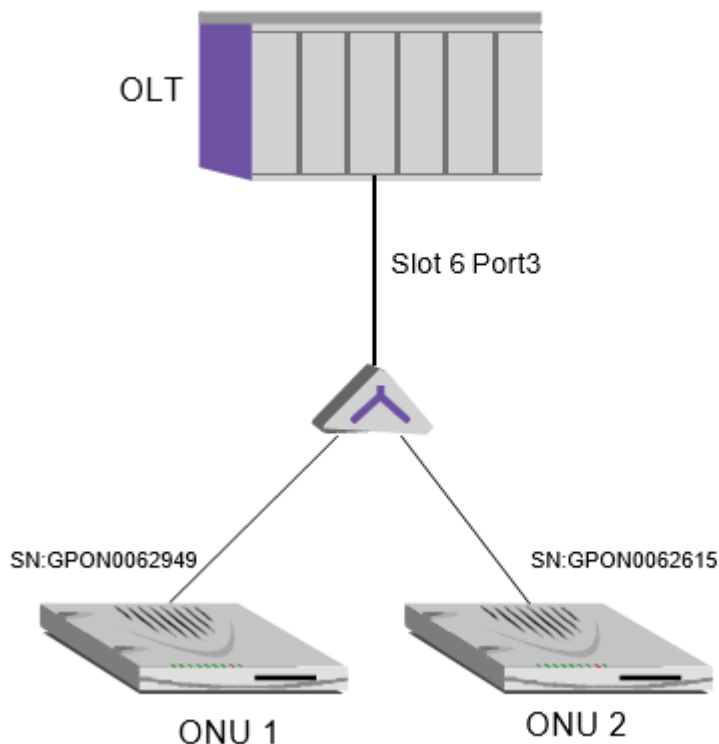
7.2 ONU Register

When OLT turns on SN authentication, you need to configure the binding ONU SN and ONU ID.

7.2.1 Application Description

In this case, ONU1 and ONU2 must be successfully registered successfully on the AX3517/AX3508/AX3502system.

7.2.2 Instance Topology



As shown in the above figure, the slot 6 port 3 port of the OLT is connected to both ONU1 and ONU2 via an optical separator.

7.2.3 The Task List of Configuration

The tasks to configure the ONU registration are listed below:

- Configure the ONU SN and ONU ID bindings
- View the ONU registration status.

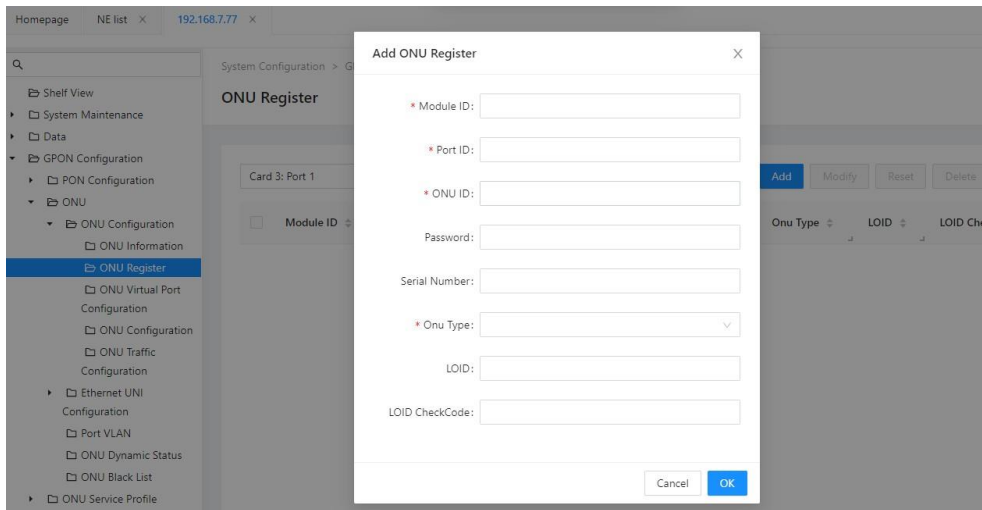
7.2.4 Configure the ONU SN and ONU ID Bindings

The ONU connected to the same OLT downlink port can be bound to either ONU ID.

In this case, ONU ID of ONU1 is 1 and ONU ID of ONU2 is 2.

【Operating Steps】

- In the Function View navigation tree, click “GPON Configuration> ONU> ONU Configuration> ONU Register”.
- Click on Add.



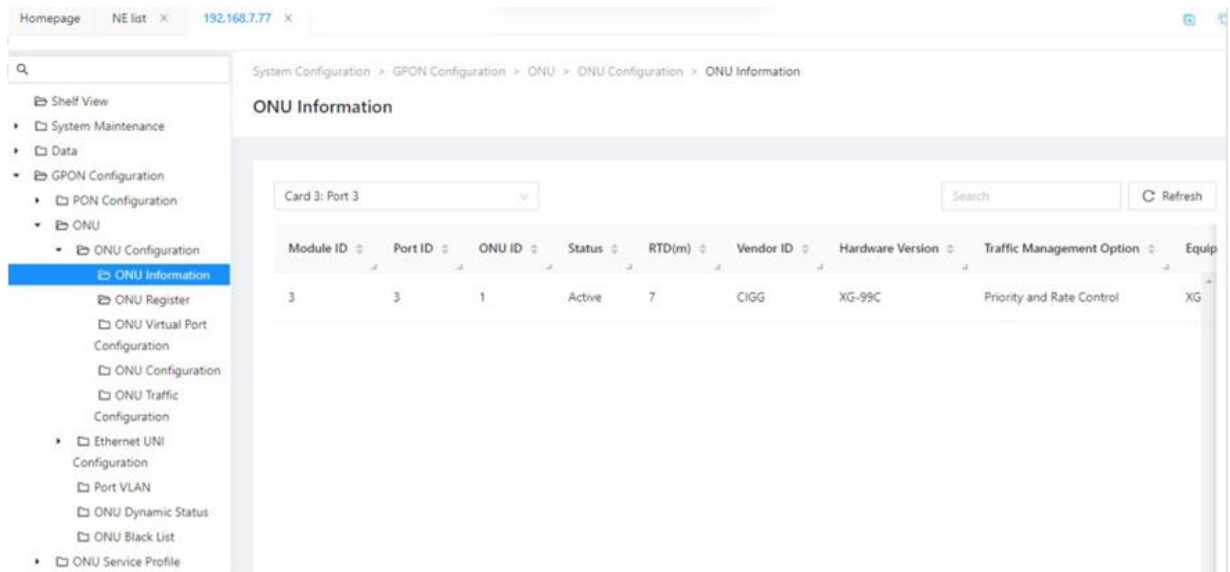
- Enter the ONU ID and serial number, and click <OK>.
- Add a second ONU in the same step.



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

7.2.5 View the ONU Registration Status

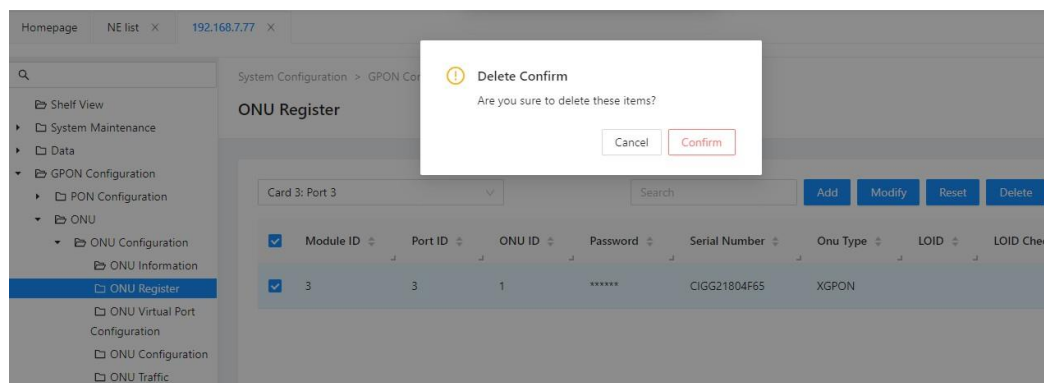
In the Function View navigation tree, click “GPON Configuration> ONU> ONU Configuration> ONU Information”.



When the status is Active, the ONU completed registration.

7.2.6 Delete Instance Configuration

- In the Function View navigation tree, click “GPON Configuration>ONU> ONU Configuration>ONU Register” to check the ONU, select the “Confirm”.



- Click on “Submit”.

7.3 ONU Traffic

The GPON data is based on flow management and forwarding.

7.3.1 Concept Introduction

- **Virtual Port**

OLT defines specific streams using a virtual port Virtual Port, with flow profile describing the properties of each stream mapped to a virtual port, depending on the application model, one or more virtual ports can be bound to the same T-CONT.

- **T-CONT**

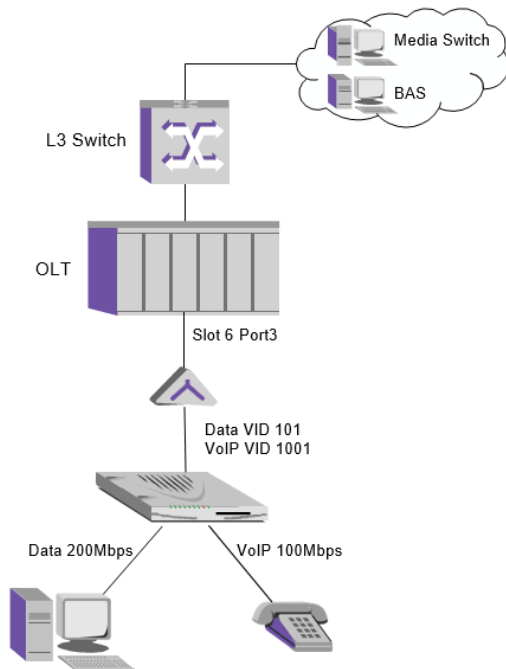
G.984.3 Use T-CONT to describe the uplink bandwidth and define three bandwidth parameters: fixed bandwidth, assured bandwidth, and maximum bandwidth. According to the different needs of users, five T-CONT types are established: TYPE1-TYPE5.

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

7.3.2 Application Description

In this example, data and voice services are configured for users. The uplink bandwidth of data services is fixed at 200Mbps, and the maximum uplink bandwidth of voice services is 100Mbps.

7.3.3 Topology Instance



The OLT connects to the network via uplink port XGE1, PC and phone connects to ONU 6/3/1.

Configuration requirements:

- The ONU has completed the registration. About registration process, please refer to ONU register.
- The ONU WAN configuration is completed, About data traffic of VLAN ID 101 and voip traffic of VLAN ID 1001 configuration, please refer to ONU Configuration manual.
- The upper online switch has been configured according to the network plan.

7.3.4 The Task List of Configuration

Configuring the ONU business tasks are listed as follows:

- Configure the uplink port and the VLAN
- Configure flow profile
- Configure the rate control profile
- Configure the virtual port business profile
- Configure the bandwidth profile
- Configure the T-CONT service profile
- Configure the T-CONT with the virtual port binding profile
- Configure the ONU virtual port
- Configure the VLAN translation

7.3.5 Configure the Uplink Port and the VLAN

【Operating Steps】

- 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.

7.3.6 Configure Flow Profile

【Operating Steps】

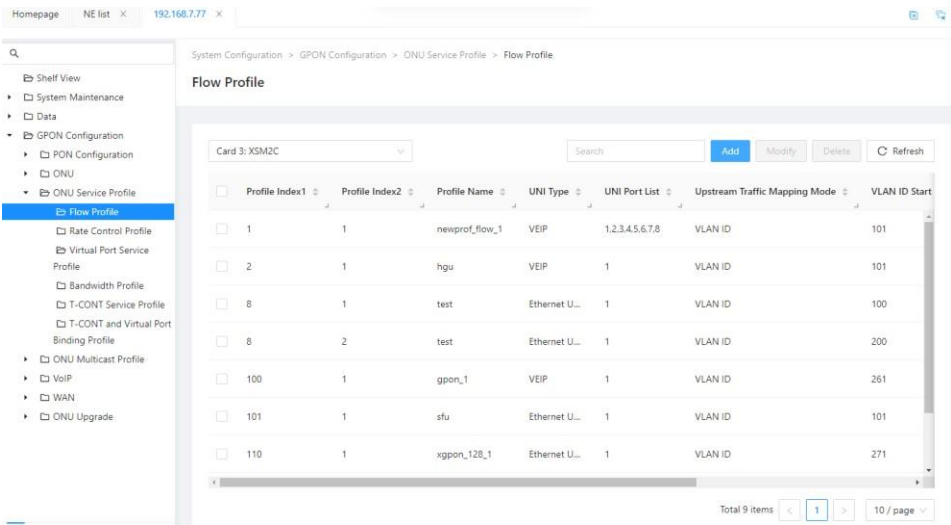
- In the Function View navigation tree, click GPON Configuration> ONU Service Profile> Flow Profile”.

In this case, ONU has data streams and voice streams, VLAN ID is 101,1001.

- Click “Add” to configure the Data flow profile, and enter the following parameters, click <OK> to save the configuration.

- Click “Add” to configure the VoIP flow profile, and enter the following parameters, click <OK> to save the configuration.

- View Flow profile.



【Parameter Declaration】

Field

Description

Profile Index 1	Required, first index, main index, When multiple virtual ports need to be bound to the same TCONT, selecting the main index means that a series of virtual ports with the same main index are selected.
Profile Index 2	Required, the second index.
Profile Name	Pprofile name
Uni Type	Required, user port mode, determined by ONU work, select the appropriate type according to different types of ONU.
Uni Port List	Required, user port mask, specify the selected port ID, say 0x01 for port 1,0x03 for ports 1 to 2.
Upstream Traffic Mapping Mode	Required, uplink mapping type.
VLAN ID	Required, uplink VLAN-filtered VLAN ID range, with up to 12 VLAN support.
802.1p Bit	Required, priority mask, specify the selected priority, like 0x01 for 0,0x03 for priority 0,1.
Virtual Port ID	Required to specify the defined virtual port ID.

7.3.7 Configure the Rate Control Profile

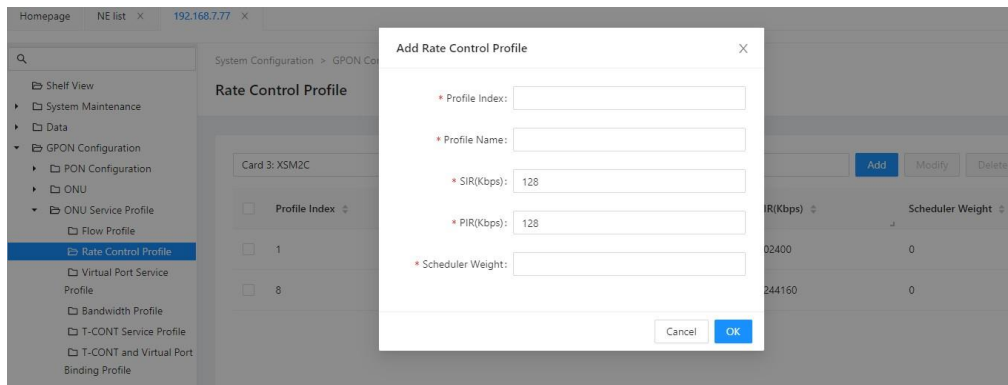
The Rate Control profile is used to describe the rate control of the flow.

【Operating Steps】

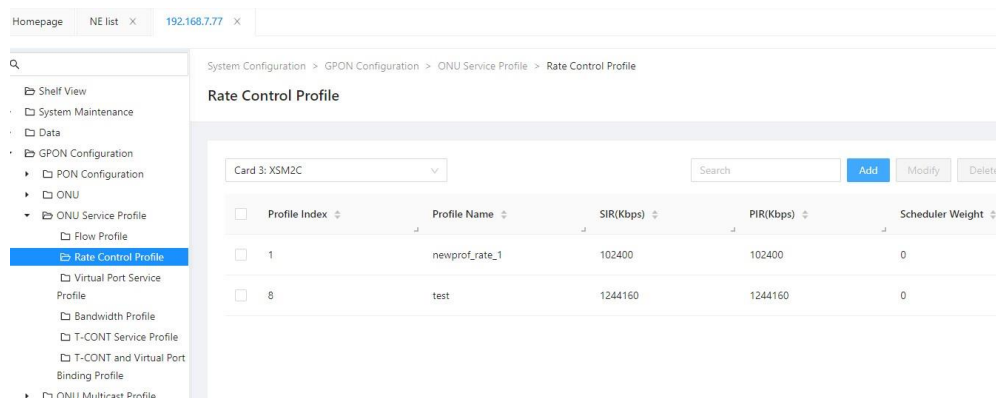
- In the Function View navigation tree, click GPON Configuration> Business profiles> Rate Control profile.

In this case, there is no rate limiting requirement, both streams set a bidirectional rate of 1000Mbps and can share the same profile.

- Click Add to configure the rate control profile, and input the following parameters.
- Click <OK> to save the configuration.



- View Rate Control profile.



【Parameter Declaration】

Field	Description
Profile Index	Required, the profile index
Profile Name	Profile name
SIR (Kbps)	Required, guaranteed bandwidth, unit Kbps, configuration particle size 64Kbps.Range of values: 128- 1244160
PIR (Kbps)	Required, peak bandwidth, and is in unit of Kbps , Configure a particle size of 64Kbps.Range of values: 128-1244160
Scheduler Weight	0-255

7.3.8 Configure the Virtual Port Business Profile

The virtual port business profile is used to define the queue properties and rates of the stream, with the rate parameters described by the Rate Control profile, to which you need to be bound to the Rate Control profile.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration> ONU service profile > Virtual Port Service Profile”.

In this case, there is no rate-limiting requirement, and the corresponding rate-control profile is bound.

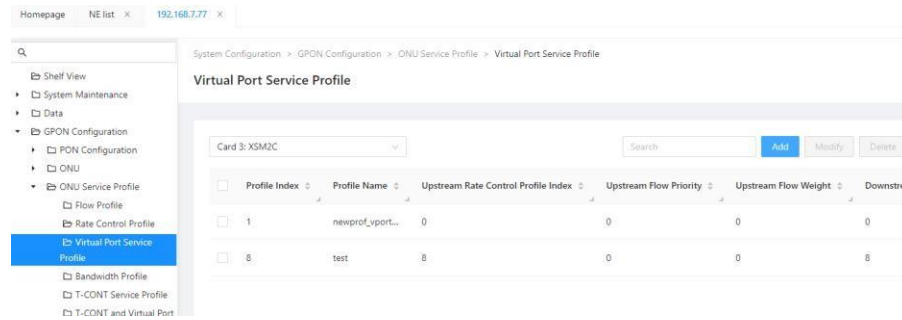
- Click “Add” to configure the Virtual Port Business profile and enter the following paramete

The screenshot shows the 'Add Virtual Port Service Profile' dialog box. The background shows the configuration tree with 'Virtual Port Service Profile' selected. The dialog box has the following fields:

- Profile Index:
- Profile Name:
- Upstream Rate Control Profile Index:
- Upstream Flow Priority:
- Upstream Flow Weight:
- Downstream Rate Control Profile Index:

At the bottom right of the dialog box are 'Cancel' and 'OK' buttons.

- Click <OK> to save the configuration.



【Parameter Declaration】

Field	Description
Profile index	Required, the profile index
Profile name	Profile name
Upstream Rate Control Profile Index	Required, pointing to the Rate Control profile index, and 0 indicates no speed limit
Upstream Flow Priority	Required, the priority of the uplink queue
Upstream Flow Weight	0-255
Downstream Rate Control Profile Index	Required, pointing to the Rate Control profile index, and 0 indicates no speed limit

7.3.9 Configure the Bandwidth Profile

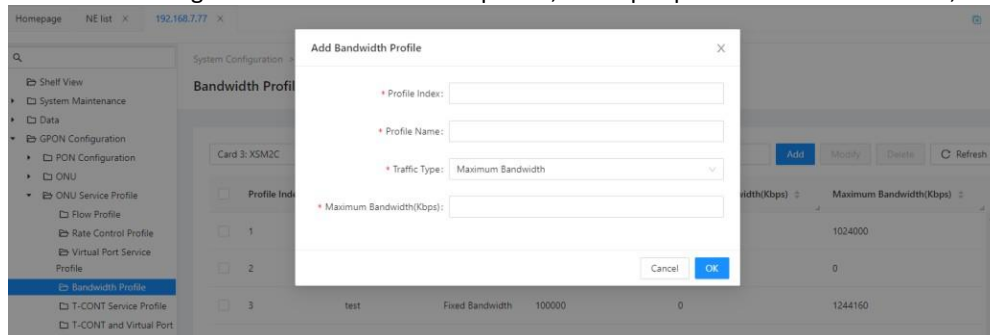
The Bandwidth Profile describes the DBA (uplink dynamic bandwidth allocation) attributes, including T-CONT types, and bandwidth parameter values.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration> ONU service profile > Bandwidth Profile”.

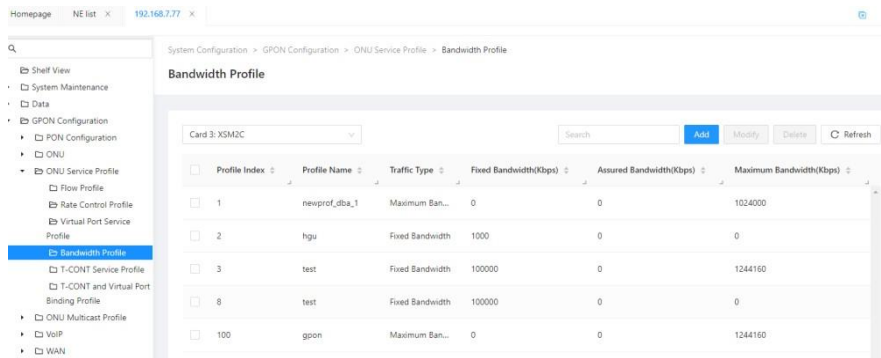
In this example, 200Mbps fixed bandwidth is configured for data services and 100M maximum bandwidth is configured for voice service.

- Click Add to configure the 200M Bandwidth profile, The input parameters are as follows,click <OK>.



- Configure a 100M Bandwidth profile again as described with step 2.

- View the Bandwidth profile



【Parameter Declaration】

Field	Description
Profile Index	Required, Profile Index
Profile Name	Profile Name
T-CONT type	Required, T-CONT type. Values: Type1, Type2, Type3, Type4, Type5
Fixed Bandwidth(Kbps)	Optional, fixed bandwidth, per unit of Kbps, with a configured particle size of 64Kbps. Range of values: 256- 6242304
	Optional, guaranteed bandwidth, unit Kbps, configuration particle size 64Kbps. Range of values: 256-9512064
Maximum Bandwidth(Kbps)	Optional, maximum bandwidth in Kbps, configuration size of 64Kbps. Range of values: 256-9953280

7.3.10 Configure the T-CONT Service Profile

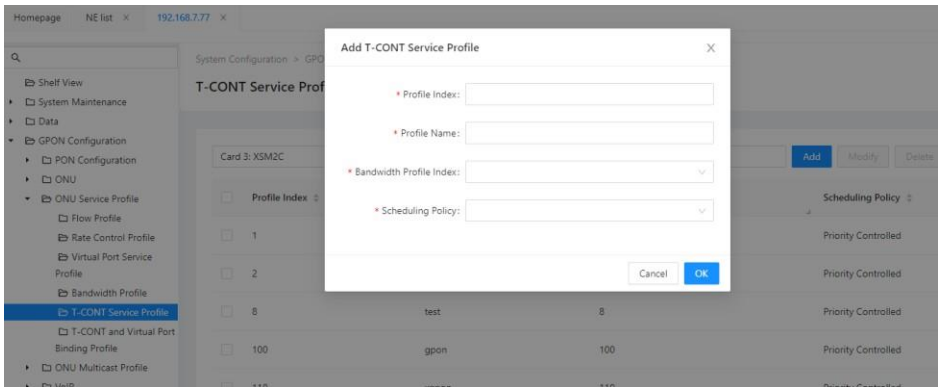
T-CONT service profile is used to describe the T-CONT attribute, binding to the Bandwidth profile.

【Operating Steps】

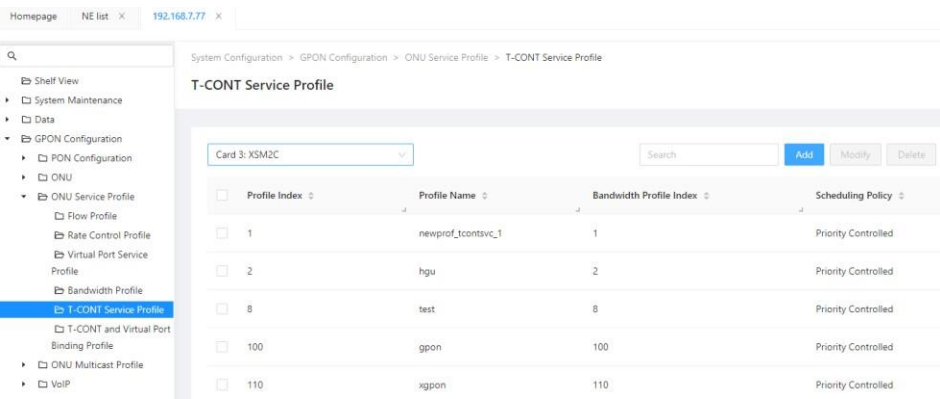
- In the Function View navigation tree, click “GPON configuration > ONU service profile > T-CONT Service Profile”.

In this example, 200Mbps fixed bandwidth is configured for data services and 100M maximum bandwidth is configured for voice service. Bind the corresponding Bandwidth profile separately.

- Click Add to configure the “200M T-CONT service profile”, Bind the 200M bandwidth profile, Click <OK> to save the configuration.



- Configuring the 100M T-CONT service profile as above.
- View the T-CONT service profile.



【Parameter Declaration】

Field

Description

Profile Index

Required, Profile Index

Profile Name

Profile name

Bandwidth Profile Index

Required, pointing to the bandwidth profile index.

Scheduling Policy

Priority Controlled/Rate Controlled/Priority and Rate Controlled

7.3.11 Configure the T-CONT with the Virtual Port Binding Profile

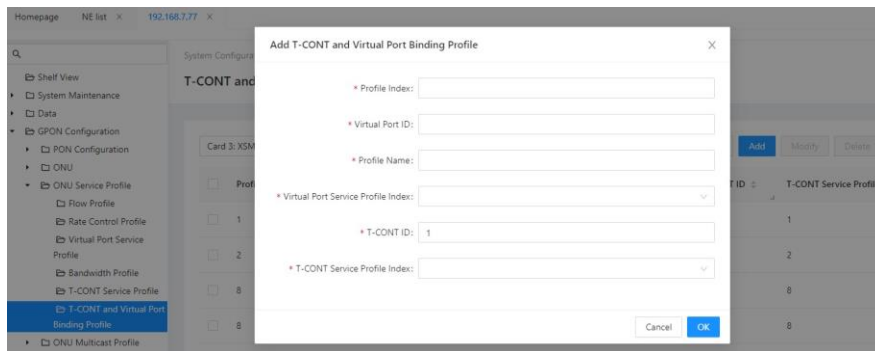
“T-CONT and Virtual Port Binding Profile” for the binding of the virtual port and T- CONT.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration>ONU service profile > T-CONT and Virtual Port Binding Profile”.

In this instance, the virtual port 1 and 2 carry the data and voice services, respectively. There are different requirements for uplink bandwidth, to bind to different T-CONT, The virtual port 1 binds to T-CONT 1 with a fixed bandwidth of 200M. The virtual port 2 binds to T-CONT 2 with a maximum bandwidth of 100M.

- Click on the Add configuration “T-CONT and Virtual Port Binding Profile”, “The virtual port 1” binds “T-CONT 1”, select 200M “T-CONT Business profile”, and click <Apply> Save Configuration.



- Another T-CONT and virtual port binding profile is configured as above.
- View “T-CONT and virtual port binding profile”.

System Configuration > GPON Configuration > ONU Service Profile > T-CONT and Virtual Port Binding Profile

T-CONT and Virtual Port Binding Profile

Card 3: XSM2C

Profile Index	Virtual Port ID	Profile Name	Virtual Port Service Profile Index	T-CONT ID	T-CONT Service Profile
1	1	newprof_tcontbi...	1	1	1
2	1	hgu	1	1	2
8	1	test	8	1	8
8	2	test	8	2	8
100	1	gpon_1	1	1	100

【Parameter Declaration】

Field	Description
Profile Index	Required, Profile Index
Virtual Port ID	Required, Virtual Port index, Corresponding to the Virtual Port Number in the Flow profile
Profile Name	Profile Name
Virtual Port Service Profile Index	Required, corresponding to the Virtual Port service profile index.
T-CONT ID	Required, T-CONT ID, as specified by the user
T-CONT Service Profile Index	Required, corresponding to the T-CONT service profile index

7.3.12 Configure the ONU Virtual Port

When the GPON profile configuration is complete, it is available to all ONU. The configured profile needs to be distributed to ONU. ONU receives profile information and takes effect after completing local setting.

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

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration> ONU > ONU Virtual Port Configuration”.

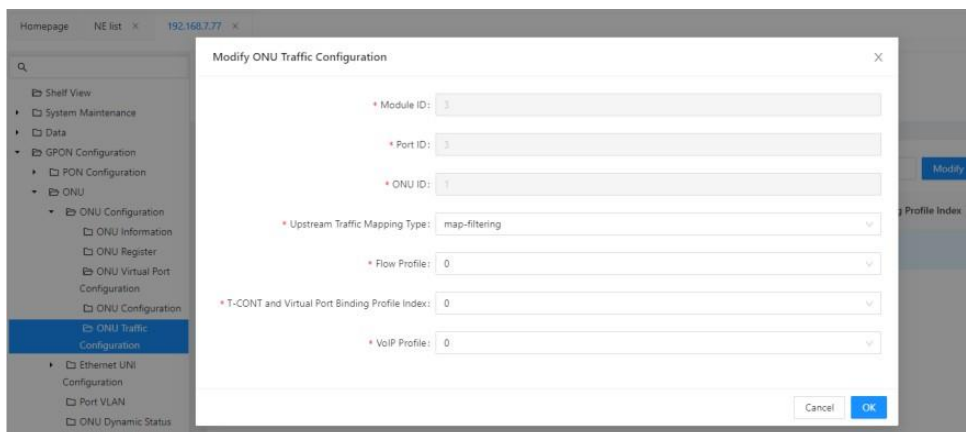
In this case, you need to create two virtual ports 1 and 2 to host data and voice services, respectively.

Note: The virtual port index must coincide with the Virtual Port number in the Flow profile.

- Click Add to configure the virtual port 1, Click <OK> to save the configuration.

- Configure Virtual Port 2 as described above.
- View the ONU Virtual Port Configuration.

- In the Function View navigation tree, click “GPON Configuration> ONU > ONU Configuration> ONU Traffic Configuration”. Select the ONU and click on Modify, Configure the flow profile and T-CONT with the virtual port binding profile, click <OK>.



【Parameter Declaration】

ONU Virtual Port Configuration Parameters

Field	Description
Module ID	Slot number
Port ID	port number
ONU ID	ONU ID
Virtual Port ID	The ONU virtual port identification
Admin State	With a virtual port management status, you can set either On or Off
T-CONT index	Identifies the T-CONT for the virtual port binding
OLT VLAN Translate Profile	The OLT vlan translate profile
GEM Port	The GEM Port ID that identifies the virtual port
Alloc-ID	Identifies the Alloc-ID of the virtual port binding
MAC Filter Profile	MAC Filter template number
MAC Filter Preassign	Mac Filters the pre-configuration template
Encryption Mode	Set whether to downlink encryption
Downstream Rate limit(kbps)	Downdownndirection is based on rate limits of virtual ports
Upstream Rate limit(kbps)	The upward direction is based on the rate limit of the virtual ports
Downstream Brust Size	Downside-direction burst size
Upstream Brust Size	uplink burst size

ONU Service Configuration Parameters

Field	Description
Module ID	Identify the slot number
Port ID	PON port number
ONU ID	ONU ID
Upstream Traffic Mapping Type	The ONU service mapping

Field	Description
Flow Profile	Identifies the Flow Template index
T-CONT and Virtual Port Binding Profile Index	Identifies the T-CONT and Virtual Port Binding Template Index
VoIP Profile	Identifies the "VOIP Template"

7.3.13 Configure the VLAN Translation

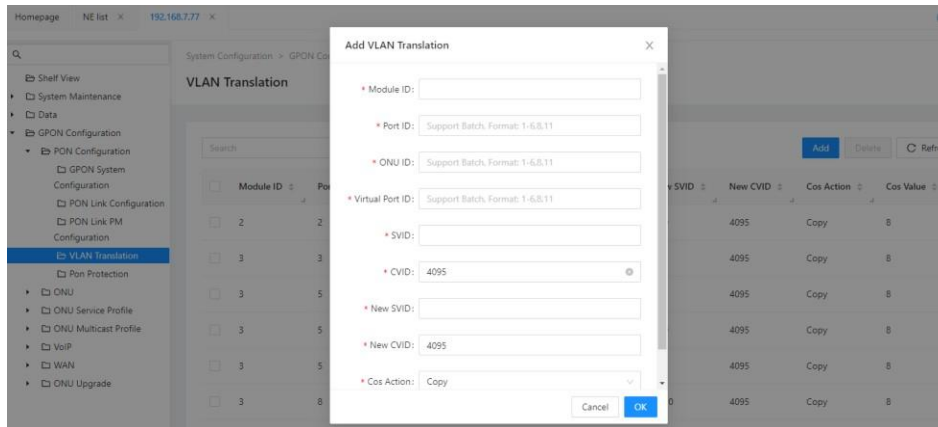
The flow on the GPON system is identified as GEM Port, map GEM Port to the corresponding VLAN on the switch, OLT supports the VLAN conversion table to complete the corresponding mapping.

【Operating Steps】

- In the Function View navigation tree, click "GPON Configuration > PON Configuration> VLAN Translation".

In this example, the data VLAN 101 and voice VLAN 1001 do not change and are configured as follows.

- Click Add to configure the VLAN translation, configure the virtual port 1, VLAN 101 conversion to VLAN 101,Click <OK> to save the configuration.



- Configure VLAN conversion according to the above steps, configure virtual port 2, and VLAN 1001 conversion to VLAN1001, Click <OK> to save the configuration.

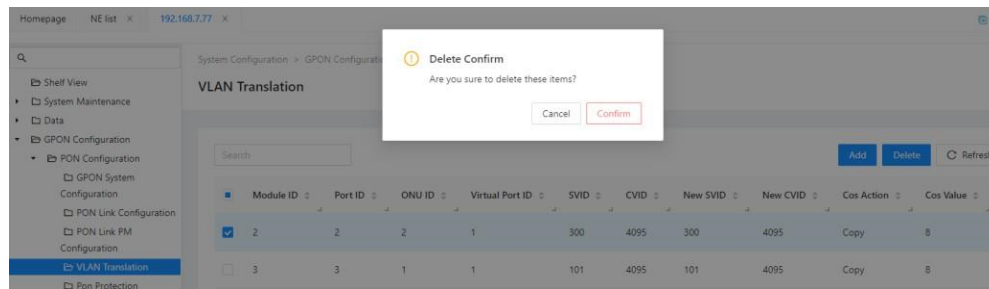
【Parameter Declaration】

Field	Description
Module ID	Identify the slot number
Port ID	PON port number
ONU ID	ONU ID
Virtual Port ID	Required,the ONU ID / virtual port number, which identifies the virtual port of the ONU
SVID	Required, user VLAN ID. span: 1-4095, "4095" express Untagged
C-VID	Required, user VLAN ID. span: 1-4095, "4095" express Untagged

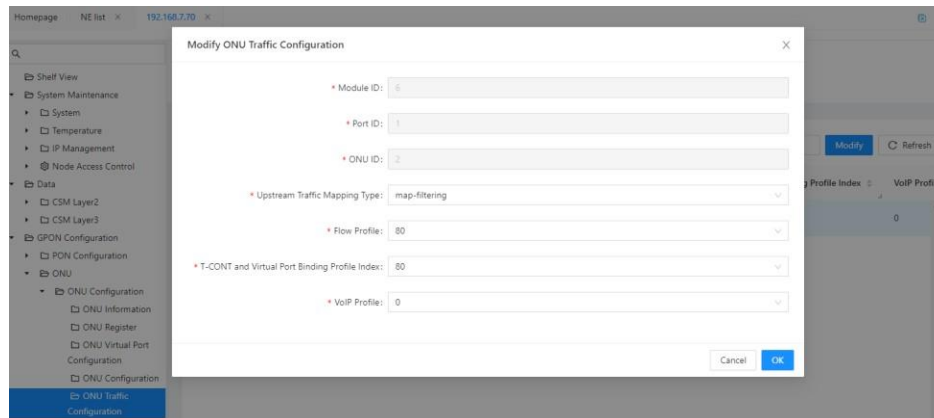
Field	Description
New S-VID	Required, New outer layer of VLAN ID. Span: 1-4095, "4095" Represents no outer VLAN.
New C-VID	Optional, new inner layer VLAN ID, span: 1-4095, "4095" Represents no inner layer of VLAN.
CoS Action	Optional, 802.1p priority processing mode. Copy / Replace
CoS	Optionally, take effect when the CoS Action is replace, setting the 802.1p priority. Value range: 0-7.

7.3.14 Delete this Instance of the ONU Service Configuration

- Note:** Due to the relevance of the ONU configuration, it is recommended that the configuration be deleted in a specific order, otherwise it may fail. Delete the VLAN transformation.



- Delete the ONU service Configuration. Click to set the template index to 0.



- Delete the Virtual Port Configuration.
- Delete the GPON profile.

Since the template is not deleted when it is referenced, when the deletion fails, see if the template is used.

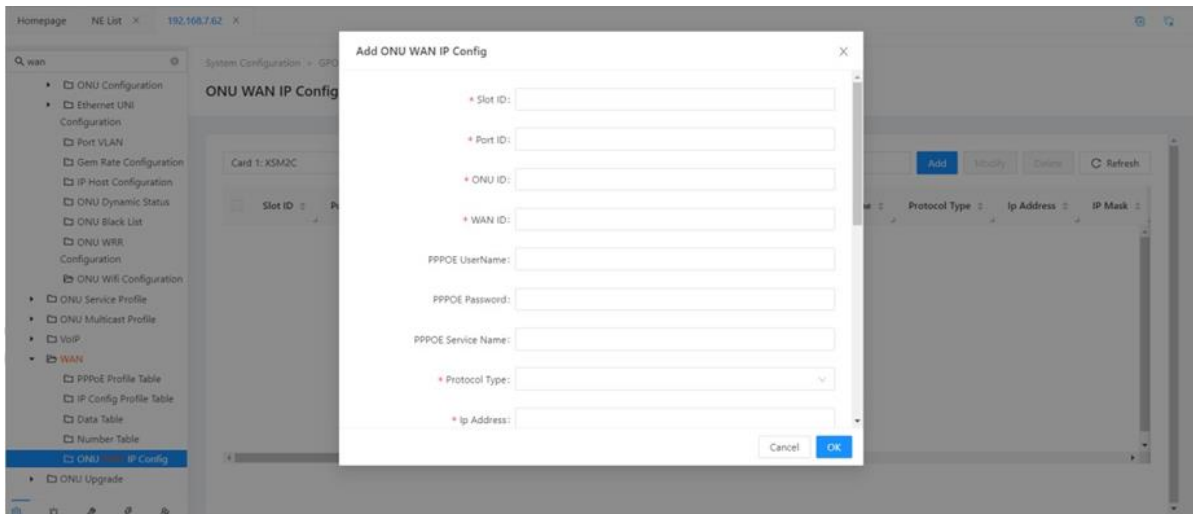
- Note:** The GPON template "1" is the system default template, and deletion is not supported.

7.3.15 ONU WAN Port Configuration

Configure WAN IP.

【Operating Steps】

1. In the Function View navigation tree, click [GPON Configuration\WAN\ONU WAN IP Config].
2. Click add,configure slot 1 port 1 ONU ID 1 WAN ID 1,protocol type ipv4,ip address 1.2.3.4,IP mask 255.255.255.0,Gateway 0.0.0.0,IP Option disable DHCP,WAN mode bridge,service type internet,port bind 0x1,dhcp server disable,dhcp transparent transmission disable,vlan id 101,vlan priority 0,multicast vlan 3330.



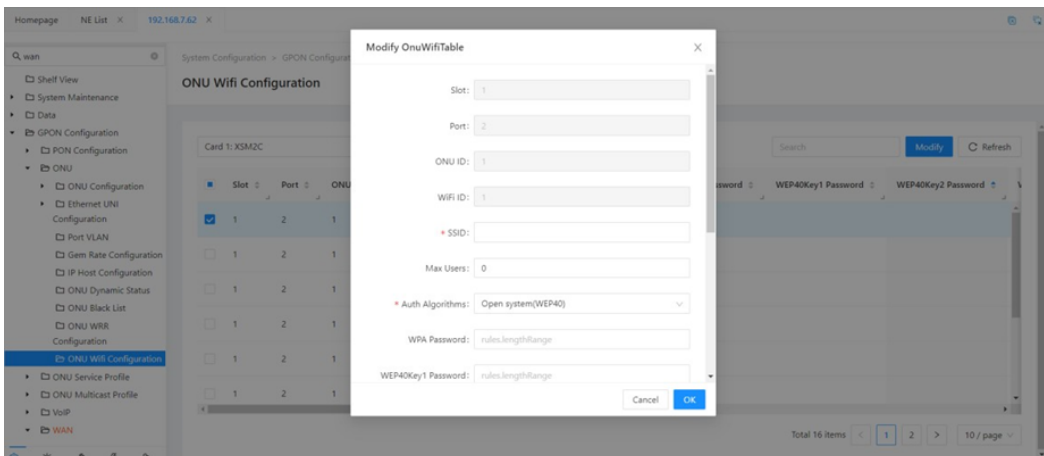
7.3.16 ONU Wi-Fi Configuration

Configure the onu WIFI service.

【Operating Steps】

1. In the Function View navigation tree, click [GPON Configuration\ONU Wifi Configuration].
2. Then select the onu you want to configure and click Modify.

In this example, select slot 1 port 2 ont 1,WiFi id 1.



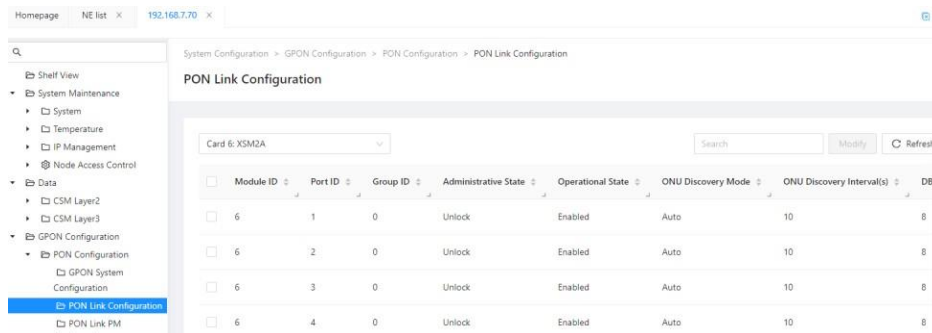
7.4 OLT Management

7.4.1 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 status is on.

【Operating Steps】

The PON port can be turned on or off by setting the administrative status of the port. The PON port management status is turned on by default.



【Parameter Declaration】

Field	Description
Module ID	Identify the slot number
Port ID	PON port number
Group ID	The PON protection group number, effective only when the PON protection is configured
Administrative State	Port management status
Operational State	Port running status
ONU Discovery Mode	System-supported ONU discovery mode, automatic discover
ONU Discovery Interval(s)	OLT periodically issues ONU discovery messages, in seconds
DBA Cycle Time(ms)	DBA algorithm cycle
Broadcast GEM Port ID	broadcast GEM Port ID
LOS Threshold	Threshold for LOS
LOF Threshold	Threshold for LOF
Auto Upgrade Enable	Whether to upgrade automatically, and keep it for future use
Key Exchange	Whether to turn on encryption
Key Exchange Interval(ms)	When encryption is turned on, the key exchange timer is used to automatically reset the key, with the key exchange interval time, in milliseconds
FEC Tx Enable	Whether enable tx FEC

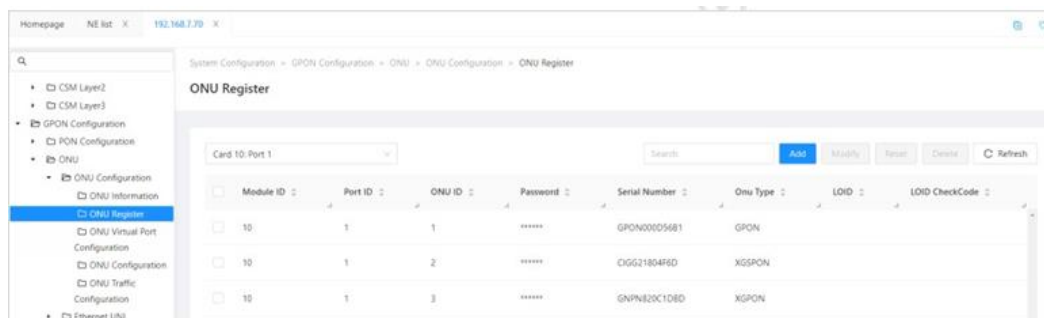
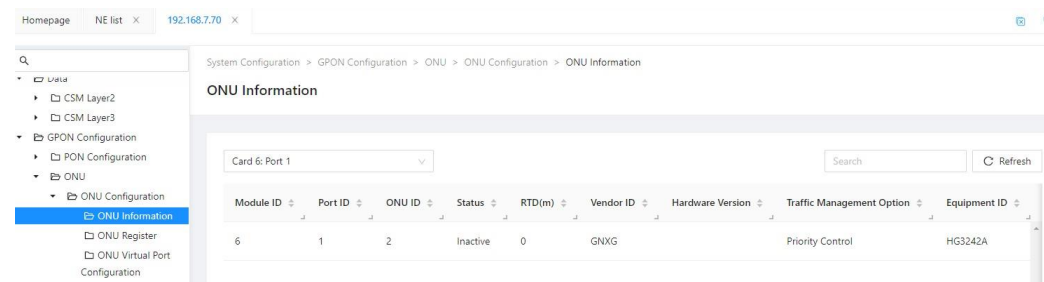
Field	Description
Rogue ONU Detect	Whether to open the rogue ONU detection
Rogue ONU Detect Mode	Processing mode after the rogue ONU is detected
Max Distance(KM)	Optical module maximum distance setting

7.5 ONU Management

ONU usually located on the user side. For convenient management, OLT telemanages ONU.

7.5.1 Get the ONU Basic Information

OLT get basic ONU information through network management. In the Function View navigation tree, click “GPON configuration> ONU > ONU configuration> ONU information” View the ONU status information, Including hardware and software version information, optical module information, etc. See for specific parameters.



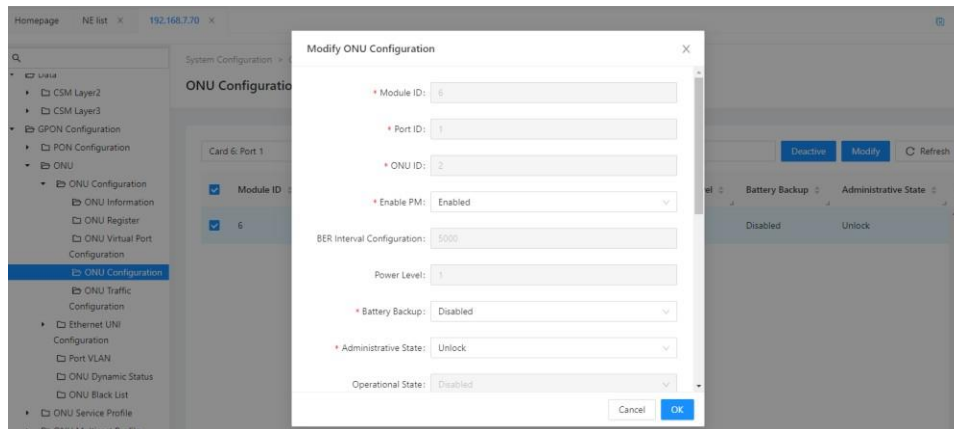
7.5.2 Unlock/Lock ONU

“lock” Status indicates that the ONU is prohibited. Can “unlock” activate ONU. The default status of the ONU is Unlocked.

【Operating Steps】

- Click GPON configuration> ONU > ONU configuration> ONU configuration.

- Select the ONU to need to modify, and click Modify.



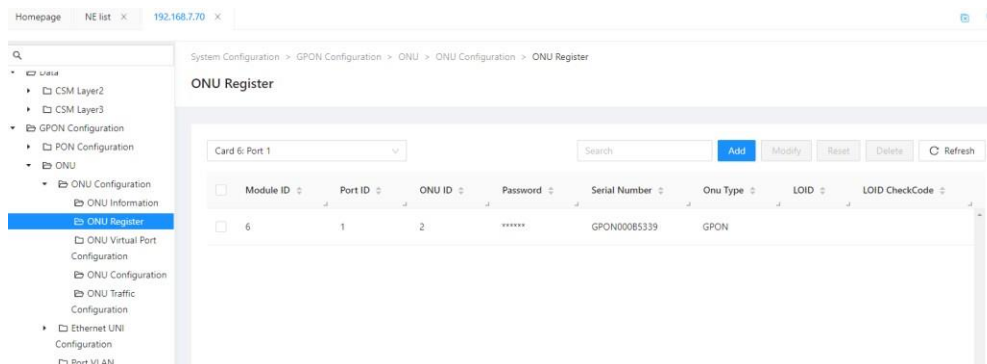
- Set up the "administrative state", click <OK>.

7.5.3 ONU Reset

OLT support to reset a particular ONU.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration> ONU > ONU configuration > ONU register”.
- Select the ONU UNI port that you need to modify, and click Modify.

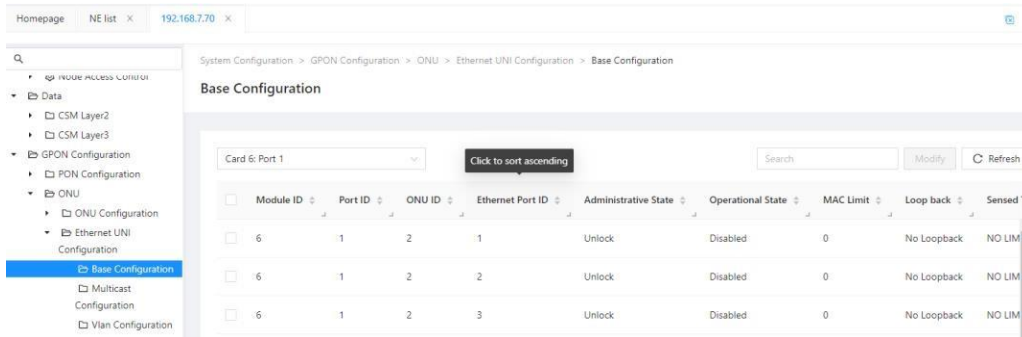


7.5.4 UNI Port Management

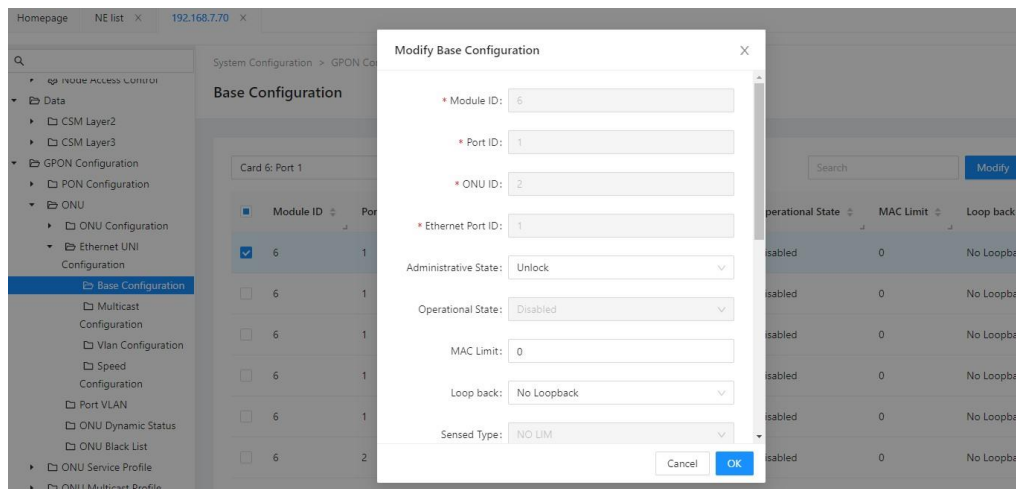
OLT Support user ports that manage a particular ONU.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration> ONU > Ethernet UNI configuration > base configuration”.



- Select the ONU UNI port that you need to modify, and click Modify.

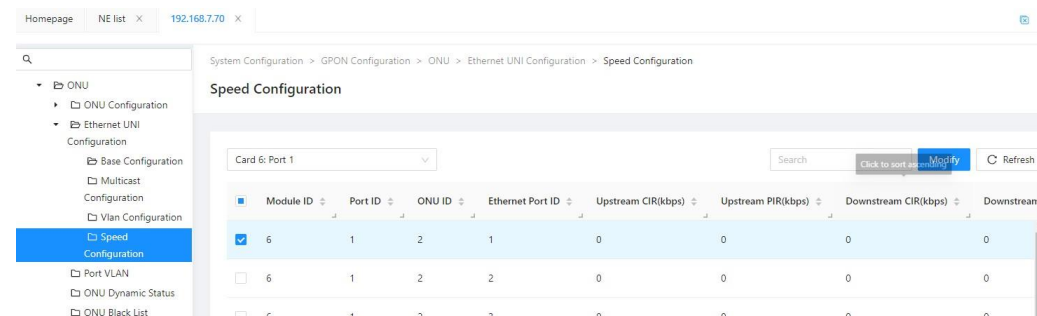


- Set up the "administrative status", click <OK>.

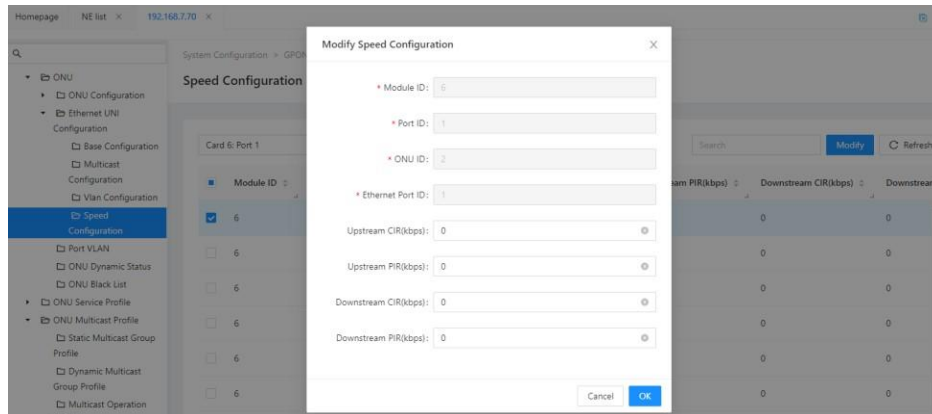
7.5.5 Port Speed Limit

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration > ONU > Ethernet UNI configuration > Speed configuration”.



- Select the ONU UNI port that you need to modify, Click Modify.



- Set the relevant parameter values, click <OK>.

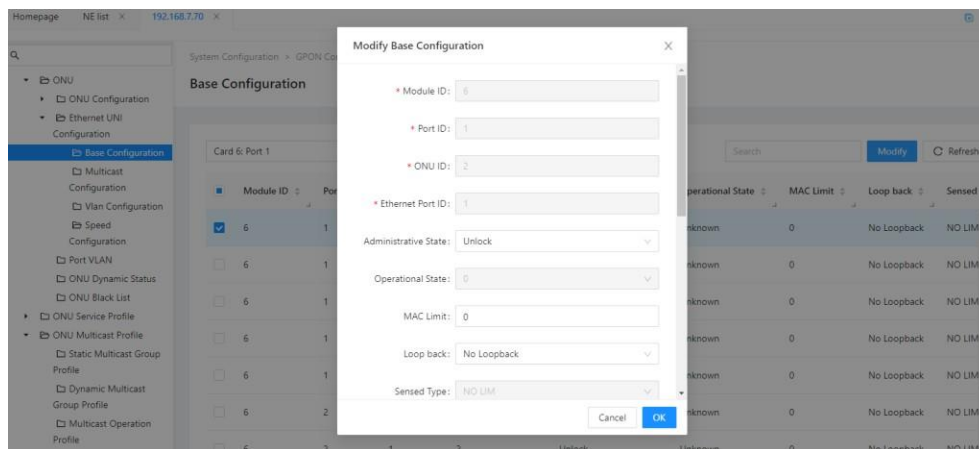
7.5.6 MAC Address Limit

The user can configuration MAC address Number Limits.

7.5.6.1 Limit on the Number of MAC Address Based on the UNI Ports

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration > ONU > Ethernet UNI configuration > base configuration”.
- Select the ONU UNI port that you need to modify, and click "Modify".

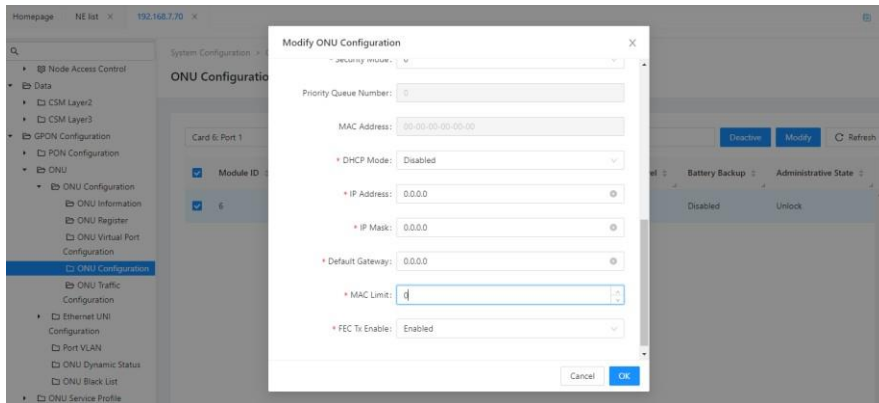


- Set the MAC Limits parameter, and click <OK>.

7.5.6.2 The ONU Bridge Service-based MAC Address Quantity Limit

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration > ONU > ONU configuration > ONU configuration”.
- Select the ONU to need to modify and click Modify.



- Set the MAC Limits parameter, and click <OK>.

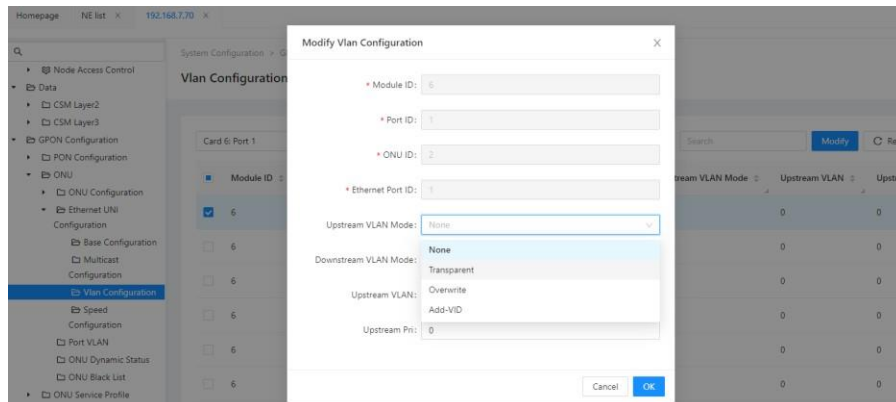
7.5.7 VLAN Configuration

The user can configure UNI port-based VLAN operations and message-based VLAN operations.

7.5.7.1 UNI-Port-Based VLAN Operation

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration > ONU > Ethernet UNI configuration > VLAN configuration”.
- Select the ONU UNI port that you need to modify, and click Modify.



- Set the relevant parameter values, click <OK>.

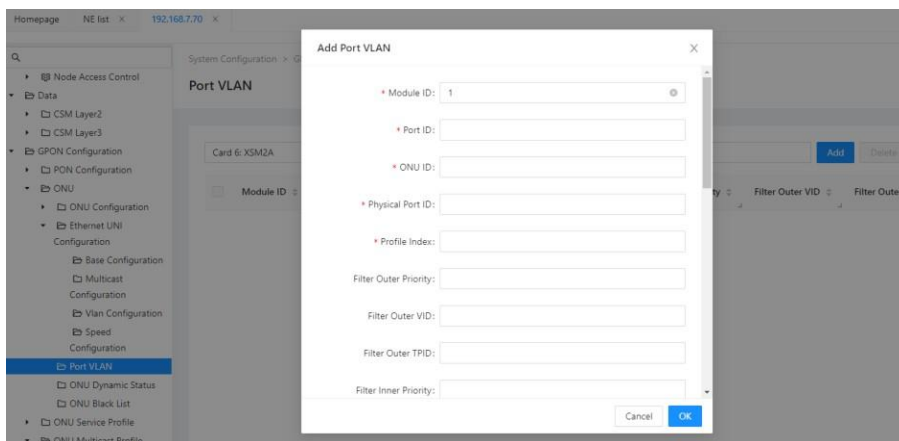
【Parameter Declaration】

Field	Description
Module ID	Slot number
Port ID	PON port number
ONU ID	ONU ID
Ethernet Port ID	ONU user port number
Upstream VLAN Mode	Upstream VLAN mode: Transparent, Over Write, Add-VID
Downstream VLAN Mode	Downstream VLAN mode: Transparent, Remove VID.
Upstream VLAN	The Upstream VLAN ID works only if the Upstream VLAN mode is Over Write or Add-VID.
Upstream Pri	Upstream VLAN priority is only valid if the "upstream VLAN mode" is "Over Write" or "Add-VID".

7.5.7.2 Message-based VLAN Operation

【Operating Steps】

- In the Function View navigation tree, click “GPON Configuration > ONU >Port VLAN”, and click Add.



- Set relevant parameters, click “OK”.

【Parameter Declaration】

Field	Description
Module ID	Slot number
Port ID	PON port number
ONU ID	ONU ID
Physical Port ID	ONU user port number
Profile Index	Rule index number
Filter Outer Priority	Is the outer priority filtered and the corresponding values
Filter Outer VID	Is the outer layer VLAN ID filtered and the corresponding values

Field	Description
Filter Outer TPID	Is the outer TPID filtered and the corresponding values
Filter Inner Priority	Whether the inner layer priority is filtered and the corresponding values
Filter Inner VID	Is the inner layer VLAN ID filtered and the corresponding values
Filter Inner TPID	Is the inner TPID filtered and the corresponding values
Filter Ether Type	Is the Ethernet type filtered and the corresponding values
Treatment Outer Priority	Processing outer priority
Treatment Outer VID	The processed outer layer, the VLAN ID
Treatment Outer TPID	The treated outer layer, the TPID
Treatment Inner Priority	Inner layer priority after processing
Treatment Inner VID	The VLAN ID of the treated inner layer
Treatment Inner TPID	Treated inner layer, TPID
Upstream Packet Format	The upstream received message VLAN mode: Untagged, Single-tagged, Double-tagged
Action	Operation processing mode of the message: Add-VID, QinQ, Transparent, Discard.

7.5.8 ONU Upgrade

OLT Support for a remote upgrade of the ONU. Two upgrade methods are supported:

- Manual upgrade
- Auto upgrade

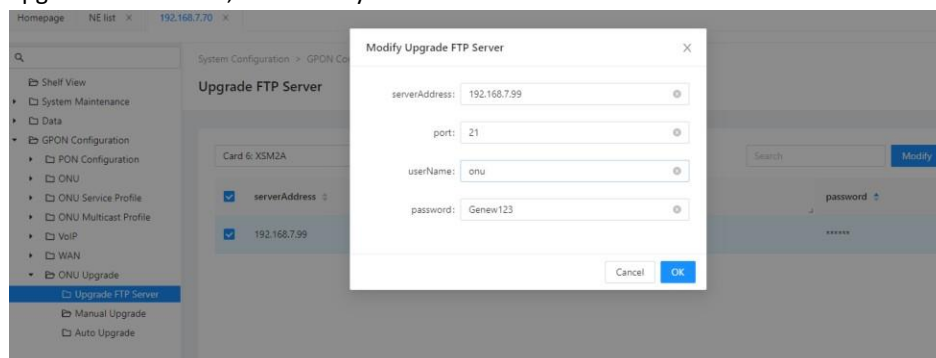
7.5.8.1 Manual Upgrade

【Configuration Precondition】

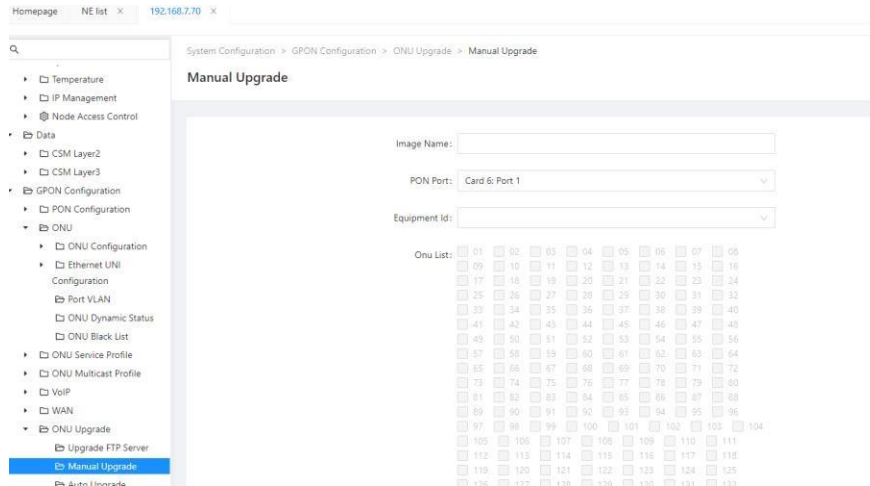
- Verify that the FTP server is started, can ping OLT success.
- The user name and password of the login FTP server is already configured.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration > ONU upgrade > upgrade FTP server”, Click Modify.



- Configuration FTP Server information, click “OK”.
- Click “GPON configuration > ONU upgrade> manual upgrade”. Enter the ONU firmware name, device ID, and hardware type, and select the ONU that require to upgrade.



- Click “node upgrade”.

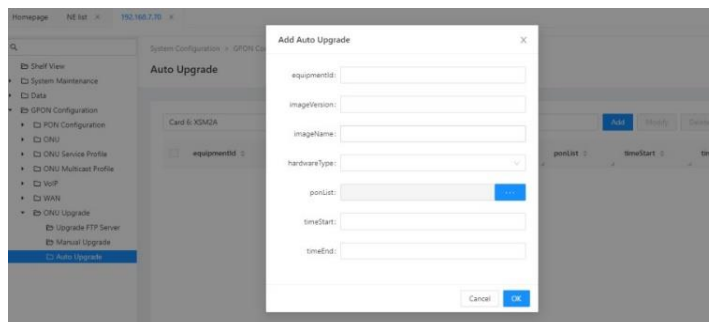
7.5.8.2 Auto Upgrade

【Configuration Precondition】

- Verify that the FTP server is started. And can OLT Ping success.
- The user name and password of the login FTP server is already configuration.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration > ONU upgrade> upgrade FTP server”, Click Modify.
- Configuration FTP Server information, click <OK>.
- Select “auto upgrade”. Enter the ONU firmware version, firmware name, device ID, and hardware type, Select the PON port that requires the upgrade, Sets the upgrade start time and the end time. Click <OK>.

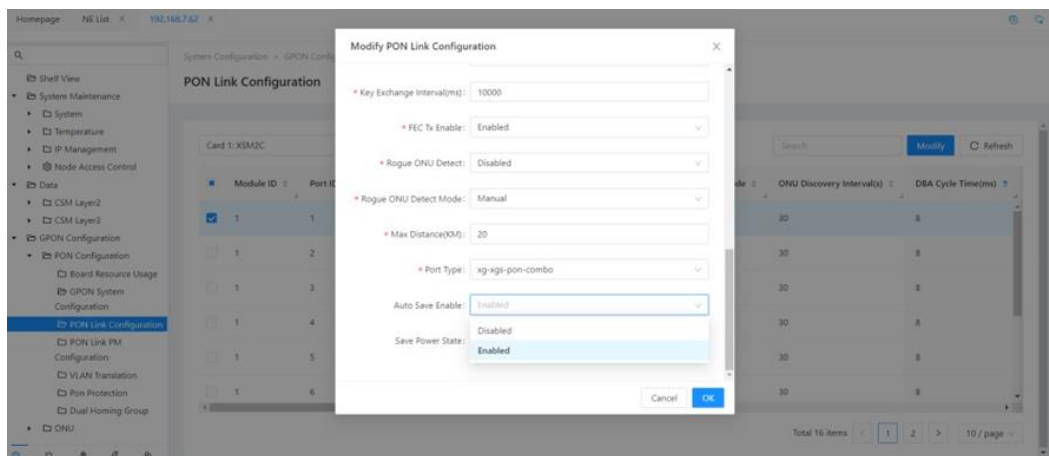


7.6 PON Energy Saving

The OLT supports the automatic energy saving of the PON port, and will decide whether to shutdown the port according to whether there is service.

【Operating Steps】

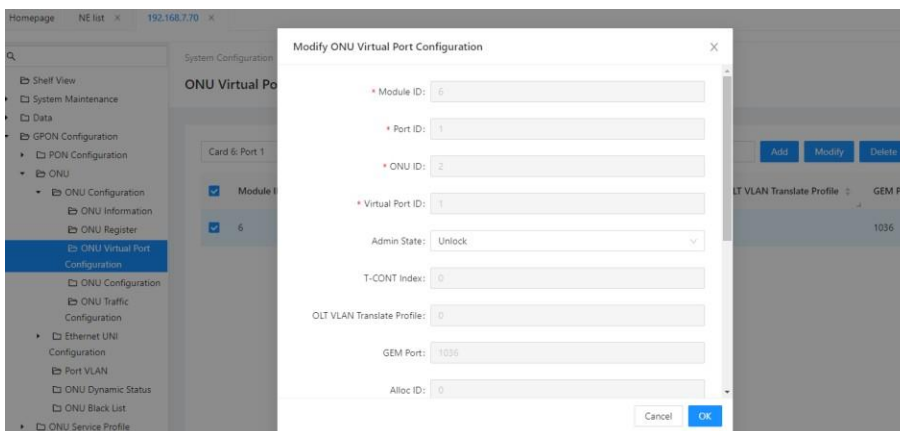
- In the Feature View navigation tree, click “GPON configuration > ONU > ONU configuration > ONU virtual port configuration”.
- Select the virtual port that requires the configuration, Click Modify.
- Change the automatic energy saving option to enable.



7.7 Based on Flow Speed Limit

OLT system shall support a virtual port-based rate restriction. [Operating Steps]

- In the Function View navigation tree, click [GPON configuration\ONU \ ONU configuration \ ONU virtual port configuration].
- Select the virtual port that requires the configuration, Click Modify.



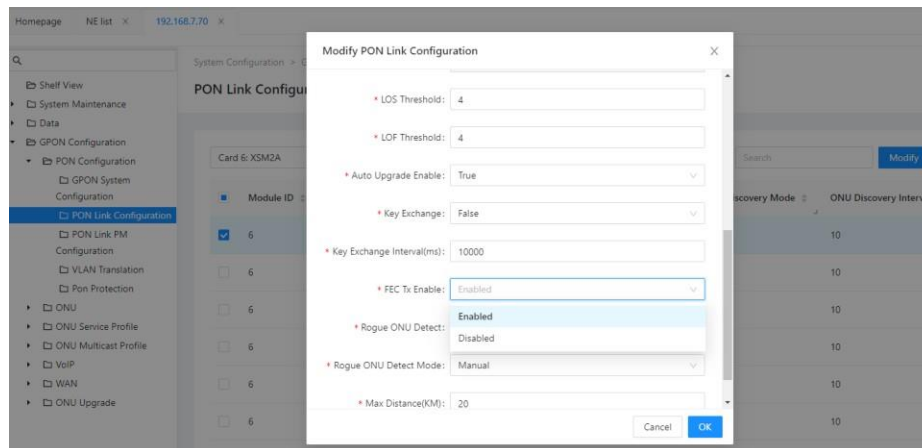
Note: The GPON template "1" is the system default template, and deletion is not supported.

7.8 FEC

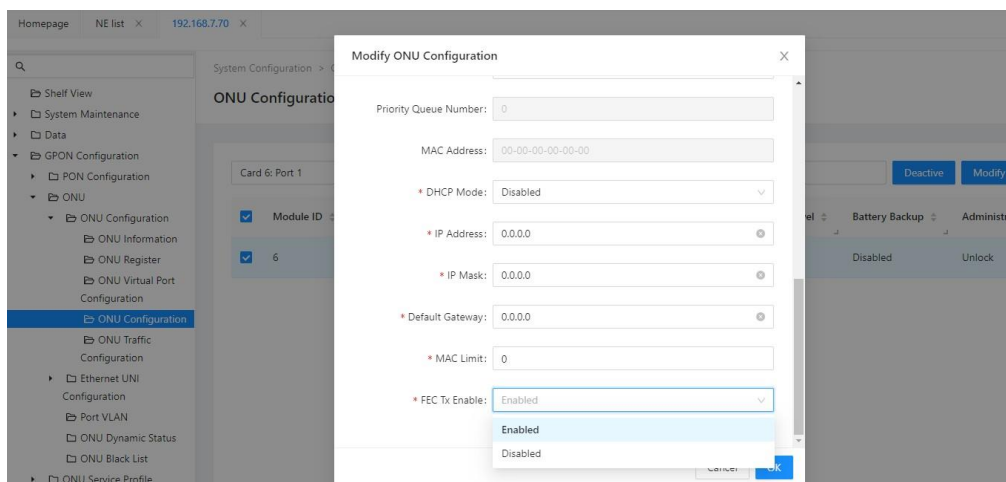
The PON system shall support a two-way forward error correction (FEC). By default, the FEC is not activated. By default, the ONU supports downlink adaptations and reception.

【Operating Steps】

- In the Function View navigation tree, click “GPON configuration > PON configuration > PON link configuration”.
- On the PON link configuration's page, Select the PON port, Click Modify configure downstream FEC.



- In the Function View navigation tree, click “GPON Configuration > ONU > ONU Configuration>ONU Configuration”.
- Select the ONU that requires the configuration, Click Modify configure upstream FEC.



7.9 Downstream Encryption

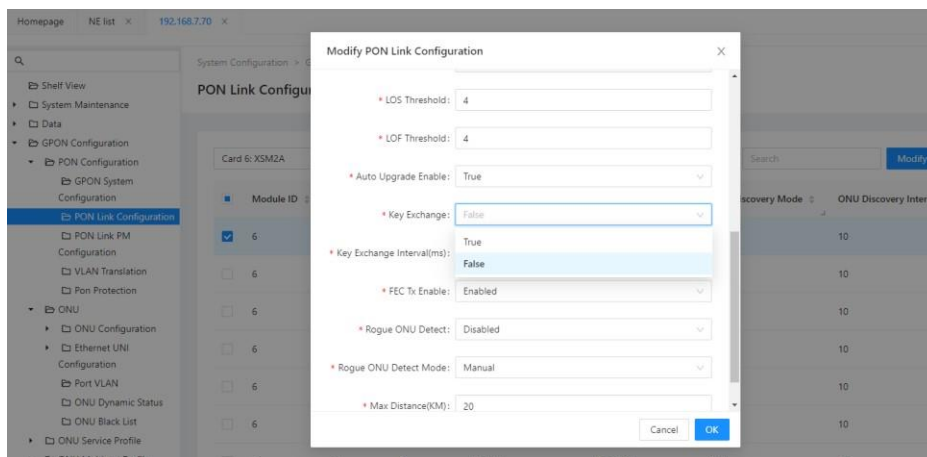
The GPON system supports the broadcast transmission of the downlink services, Malicious users can easily capture information from other users. This leads to two major security issues for the GPON network system: user information is overheard (user issues) and service theft(service provider issues). To prevent the downlink transmission from being overheard, OLT system provides the downlink AES algorithm for encryption.

Advanced Encryption Standard, AES

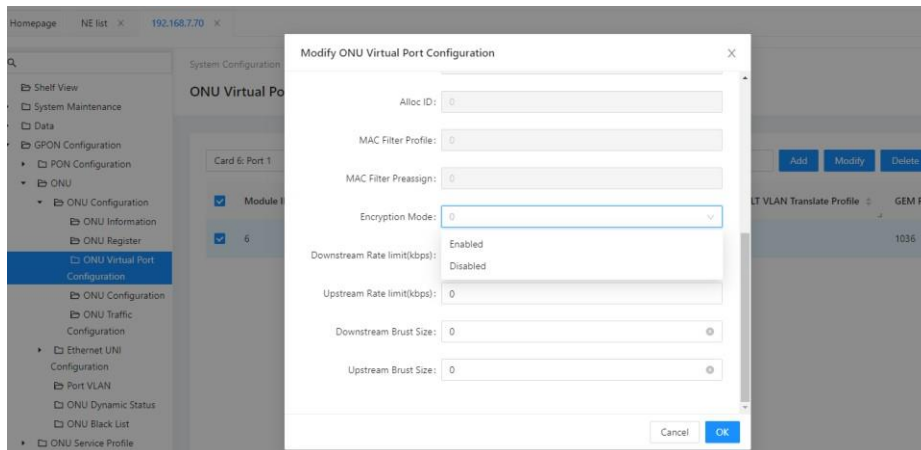
According to the user's request, the communication between the ONU and the OLT can be an encrypted communication.

【Operating Steps】

- In the Function View navigation tree, click “GPON Configuration > PON Configuration > PON Configuration”.



- In the Function View navigation tree, click “GPON configuration > ONU > ONU configuration > ONU Virtual port configuration”.
- Click Modify “Enabled” or “Disabled” Virtual port downstream encryption.



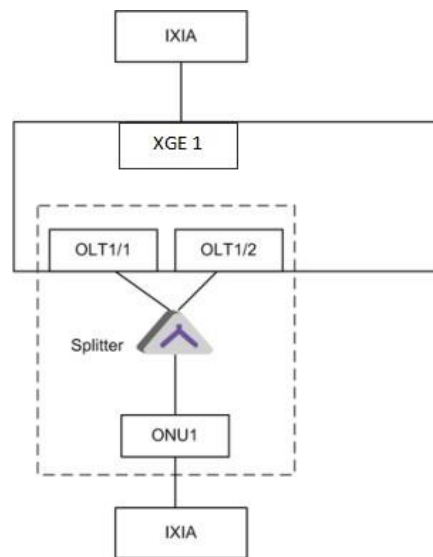
7.10 PON Protection

To protect network connections from fiber failures between the PON ports and the PON ports to the separator, OLT realize pon protection.

7.10.1 Application Description

Realize OLT OLT 1/1and OLT 1/2 Group protection.

7.10.2 Topology Instance



In the topological instance of the face, PON 1/1 and PON 1/2 are the protection groups. Use the 2: N optical separator (which has two uplink ports and N downlink ports).

7.10.3 The Task List of Configuration

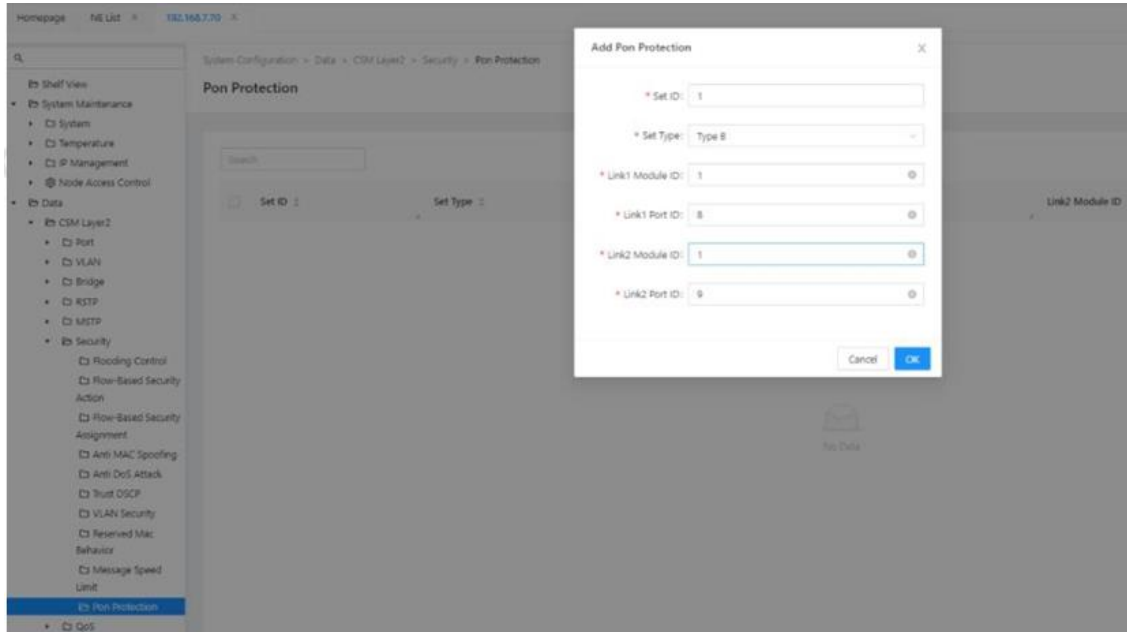
Configuration PON protection tasks are listed below:

- Configuration PON protection tasks are listed below: Configuration PON protection
- Configuration ONU Registration and service
- Manual conversion between the active and redundant ports

7.10.4 Configuration PON Protection

【Operating Steps】

In the Function View navigation tree, click “GPON Configuration > PON Configuration > PON Protection”, click Add.



7.10.5 Configuration ONU Registration and Service

Note: After the protection group takes effect, the active port is operational and is required at the active port configure ONU. See for the specific ONU service configuration GPON Configuration.

7.10.6 Manual Conversion between the Active and Redundant Ports

In the Function View navigation tree, click “GPON Configuration>PON Configuration>Pon Protection”. Click Modify to set Force Turn Down to Yes, Click <Apply> Save configuration.

7.10.7 Delete PON Protection Group

Select the PON protection group that you need to delete. Click Delete.

【Parameter Declaration】

Field	Description
Protection group id	PON protection group group number
Name	PON protection name
Type	PON protection type. Type-B is Main dry fiber protection
Switch Over Timeout	Replace the timeout time
Force Switch	Is it mandatory to switch
Link1 Module ID	Protection group Link1 Module ID
Link1 Port ID	Protection group Link1 port ID
Link2 Module ID	Protection group Link2 Module ID
Link2 Port ID	Protection group Link2 port ID
Active Module ID	Protection group Running link slot bit number
Active Port ID	Protection group Running link port number

7.11 PON Optical Power Detection

The optical power measurement of the OLT port can be performed when an optical module with the optical power measurement function is inserted into the AX3516. When the optical module with optical power measurement is configuration on the ONU, the optical power measurement on the ONU end can be performed.

The OLT supports the measurement function of the upward average optical power it receives from each ONU. When the uplink optical power received from the OLT from an ONU is too low (below the standard OLT sensitivity upper limit) or too high (above the OLT overload optical power lower limit specified in the standard), the OLT shall generate the corresponding optical power more limit alarm.

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

Based on the measurement of the uplink optical power of the ONU under the PON interface, the OLT can realize the fault diagnosis of the optical link. Fault diagnosis refers to whether the optical power analysis and attenuation of the optical link according to the ONU received on the PON interface is normal, and provides certain link fault judgment function. OLT provides the monitoring of its own optical module operating temperature (operating temperature), power supply voltage (supply voltage), bias current (bias current), transmitting optical power (transmitted power) and other parameters.

7.11.1 OLT optical power

【Operating Steps】

- In the Optical Transceiver Diagnostics navigation tree, click “OLT Optical Transceiver Diagnosis”.

Module ID	Port ID	Working Voltage(V)	Tx Optical Power(dBm)	Bias Current(mA)	Temperature(°C)	Xg Voltage(V)	Xg Tx Power(dBm)
6	1	3.26	3.8532	16.376	28.00	3.26	3.8937
6	8	3.28	3.5177	17.548	28.00	3.28	4.0986

- Click Refresh to get the optical power that the OLT receives to the ONU.

7.11.2 ONU optical power

【Operating Steps】

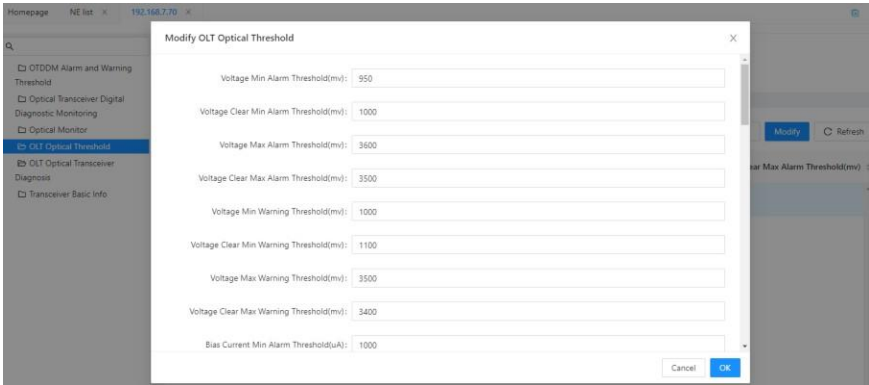
- In the Function View navigation tree, click “GPON configuration > ONU > ONU configuration > ONU base information”.
- Slide to the right to view the optical power information for the ONU.

Port	Whole ONU DBA Report	Working Voltage(V)	Rx Optical Power(dBm)	Tx Optical Power(dBm)	Bias Current(mA)	Temperature(°C)
Unsupport	0	0	0	0	0	0

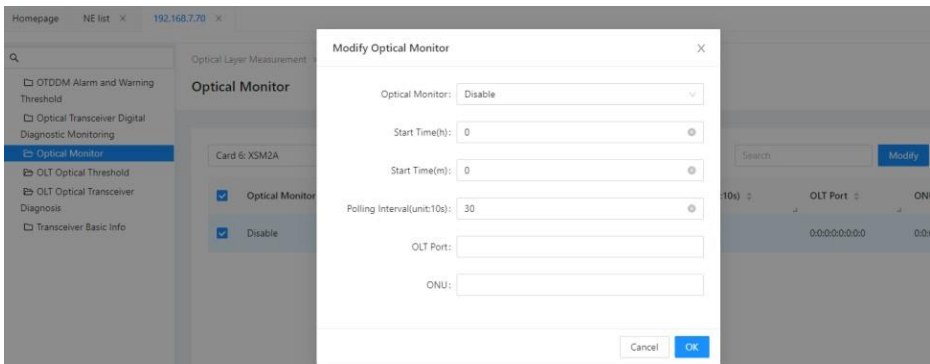
7.11.3 Optical power monitoring

【Operating Steps】

- In the Optical Transceiver Diagnostics navigation tree, Click Select “OLT Optical Threshold”, Click on Modify to set the alarm threshold.



- Select the Optical Monitoring, Click Modify, Select the OLT / ONU required to be monitored, set up to turn on light power monitoring.



【Parameter Declaration】

Field

Description

Optical Power Monitoring

Optical power monitoring on / off

Start Time

Optical power monitoring start time

Start Time

Optical power monitoring start time is in minutes

Polling Interval(10s)

Monitor the polling interval in 10 seconds, set the appropriate value, polling too fast may make the system busy

OLT port

The PON port being monitored

ONU

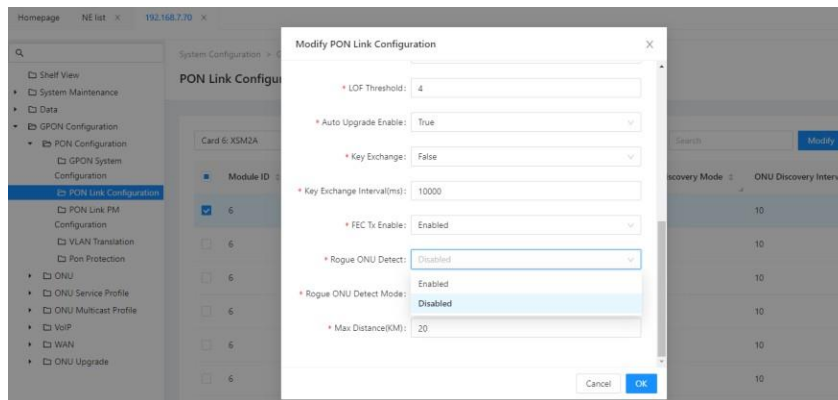
ONU ID

7.12 Rogue ONU Detection

Because the GPON system adopts time division multiplexing technology in the upward direction, all ONU must be in the OLT specified time slot in order to make the GPON system work normally, ONU not in the OLT specified time slot ONU, such as long luminous, luminous, light leakage ONU will cause uplink signal conflict, irregular influence of other ONU under the same PON port cannot be registered, or repeated offline. Such ONU is collectively referred to as rogue ONU. The system supports the detection of a rogue ONU in the system, and performs the positioning and isolation. Help with the troubleshooting.

【Operating Steps】

- In the Function View navigation tree, click “GPON Configuration>PON Configuration >PON Configuration”.
- Select the PON port, click “Modify” configure Rogue ONU detection.



Note: After "manual" mode reaches the rogue ONU, report the alarm, and the user decides whether to turn off the ONU luminator. After "automatic" mode reaches the rogue ONU, report the alarm and automatically turn off the ONU luminator. Due to the complexity of the optical road environment, the ONU localization has some misjudgment rate, so manual operation is recommended.

8 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.

OLT supports layer 2 using the following protocol:

IGMP snooping (layer 2)

8.1 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.

8.2 IGMP Snooping Introduction

OLT can use IGMP (Internet Group Management Protocol) snooping to suppress the flooding of multicast services, which dynamically configure ports only to ports related to IP multicast devices.

The IGMP snooping requires the LAN switch to monitor the IGMP transfers between the host and the router, and to track the multicast groups and member ports.

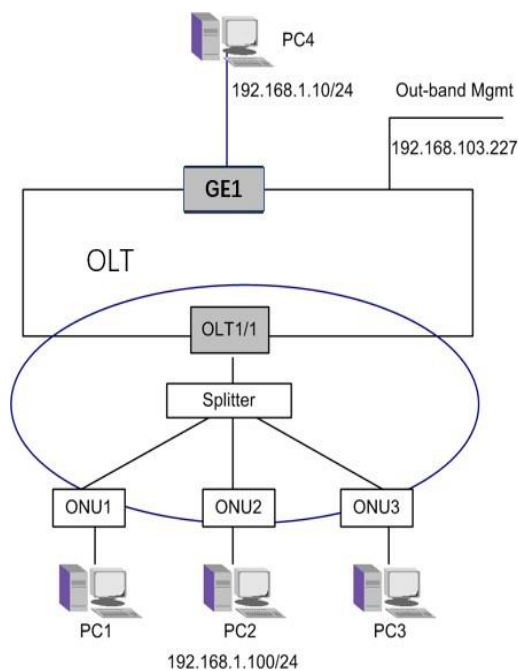
The layer 2 multicast table items were learned by IGMP snooping.

8.3 Standard IGMP Snooping Configuration Instance

8.3.1 Application Description

In the application instance shown in Figure8-1, the PC connected to the ONU1, ONU2, and ONU3 all receive the multicast traffic. Explain the IGMP snooping configuration by using the following example.

8.3.2 Topological Instances



In the above figure, the OLT is connected to the multicast source PC4 via the XGE1 uplink port. The downlink port OLT 1/1 is connected to ONU1, ONU2, and ONU3 via an optical distributor. Ports XGE1, IS 1/1, and all ONU belong to VLAN10. PC1, PC2, and PC3 are respectively connected to their corresponding ONU1-3. PC1- 3 are all members of the multicast groups and receive the multicast services from OLT.

When connecting a new downlink user to a group, the user sends an IGMP member report message. The report message is received and snooping by OLT. After adding the table item, the IGMP report message is forwarded to the uplink device.

In this case, the PC4 sends a multicast service. Three PC1-3 receive the multicast service.

8.3.3 Configuration Requirements

- Take home gateway ONU as an example, the WAN configuration of ONU1, ONU2 and ONU3 is bridging mode, VLAN ID 10. See “ONU Configuration Manual”.
- ONU1, ONU2, and ONU3 bind to the corresponding ONU ID, respectively.
- Multicast source application of multicast source PC4 is installed.

8.3.4 The task list of configuration

The list of the configuration IGMP snooping tasks is as follows:

- Create multicast VLAN
- Enable IGMP Snooping
- Configure ONU multicast profile
- View OLT IGMP snooping

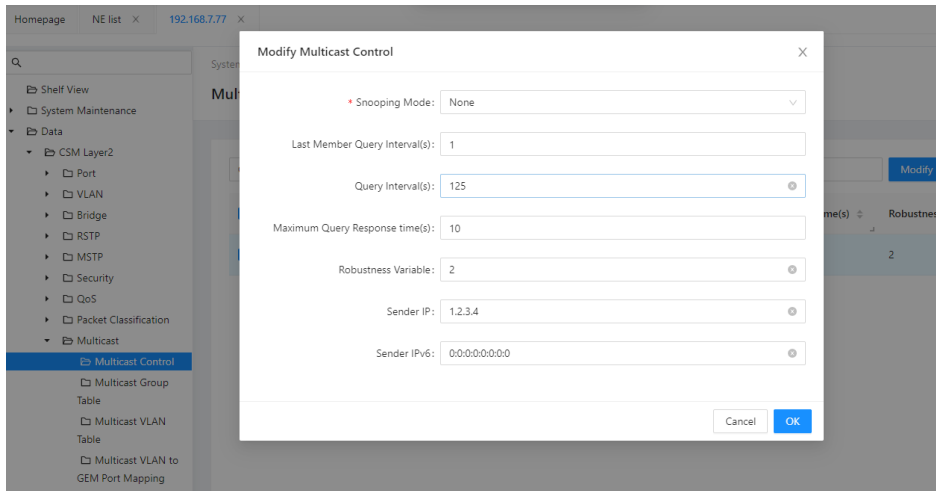
The detailed steps of each task are described below as an example of the topology in Topological Instances.

8.3.5 Create multicast VLAN

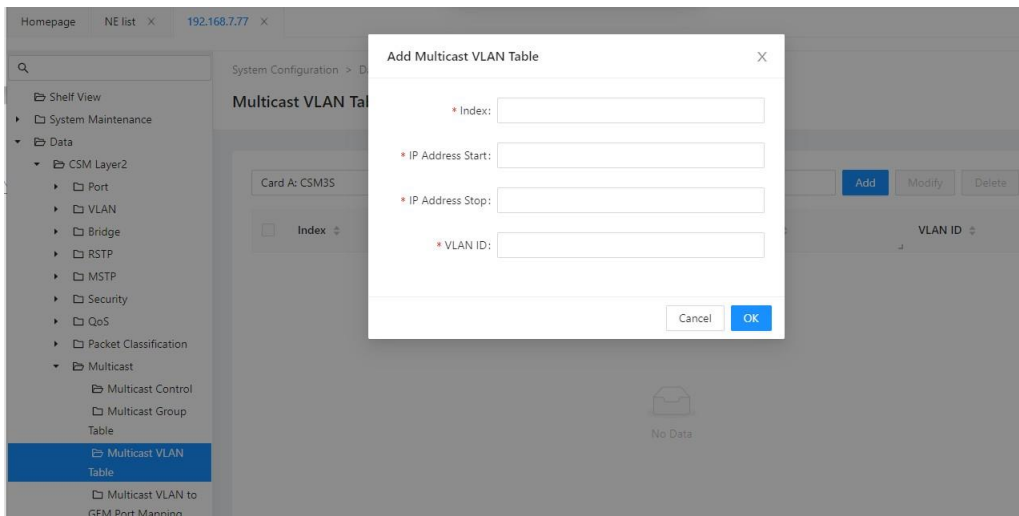
1. Create a multicast VLAN 4000, configure IS 1/1 as Tagged member port, XGE1 as tagged member port, and XGE 1 PVID set to 4000.
2. Create a unicast VLAN 101 and add IS 1/1 as the tagged member of that VLAN.
3. Create a VLAN 3800 for mapping to a multicast GEM port, and IS 1 / 1 is the tagged member of that VLAN. Refer to VLAN Configuration.

8.3.6 Enable IGMP Snooping

1. In the Function View navigation tree, click “Data> CSM Layer 2> multicast> multicast Control”. Click Modify to modify configuration.

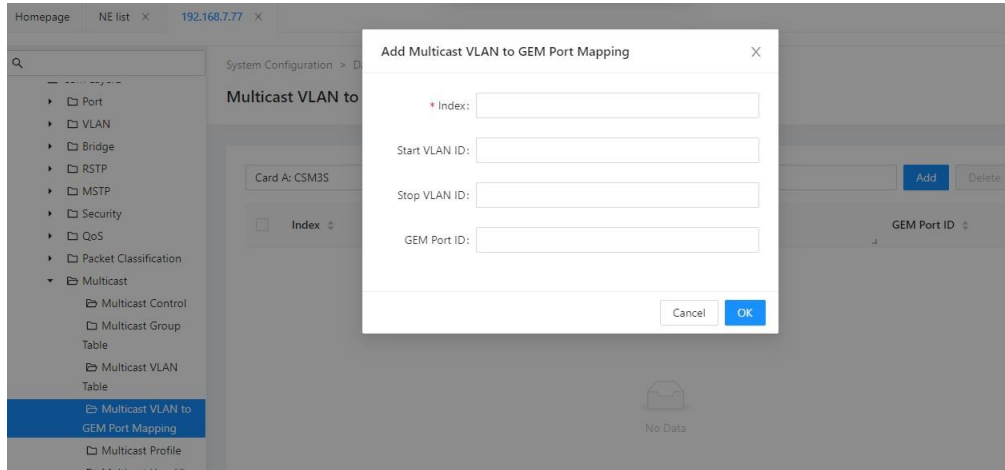


2. In the Function View navigation tree, click Data> CSM Layer 2> multicast> multicast VLAN Table.
3. Click “Add” to configure multicast VLAN 4000, with the group address of 225.0.0.1- 225.0.0.10.



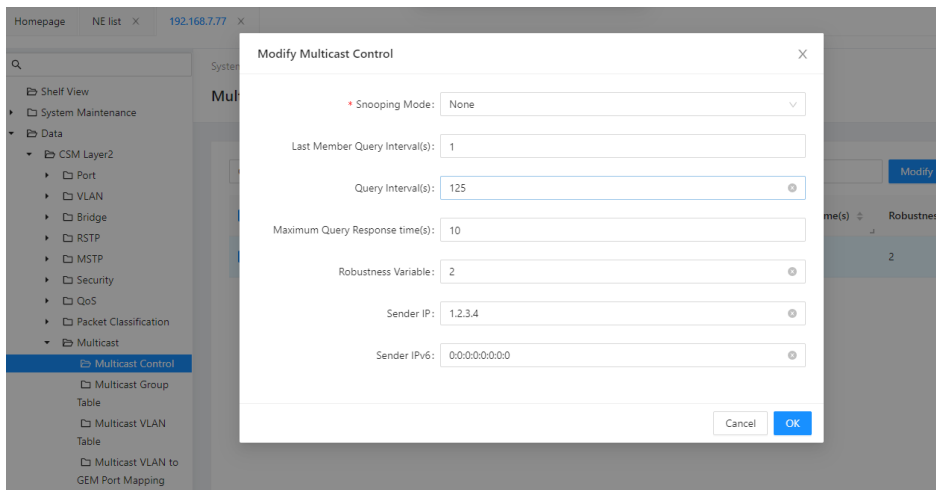
4. In the Functional View navigation tree, click “Data> CSM Layer 2> multicast> multicast VLAN to GEM Port Mapping”.

- Click “Add” to configure multicast VLAN 4000 mapping to GEM Port 3800.

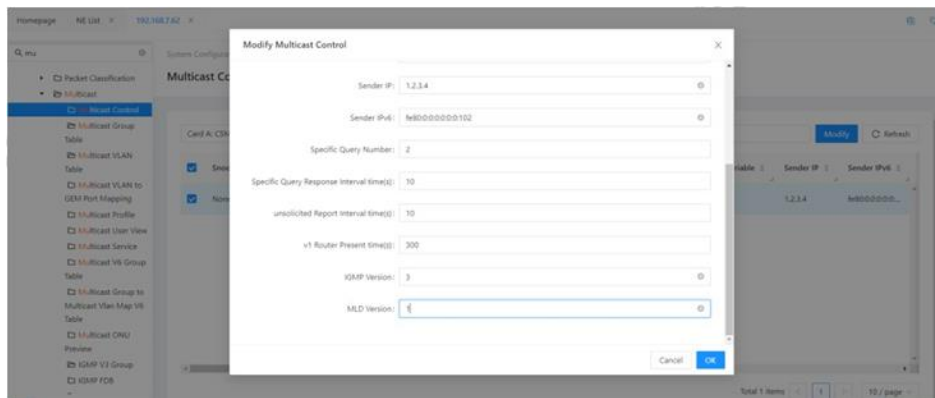


8.3.7 Enable IGMPv3 Snooping

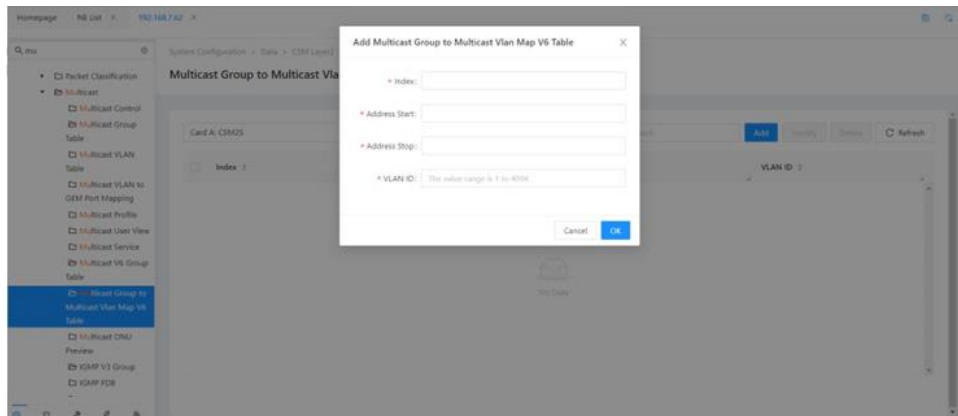
- In the Function View navigation tree, click “Data> CSM Layer 2> multicast> multicast Control”. Click Modify to modify configuration.



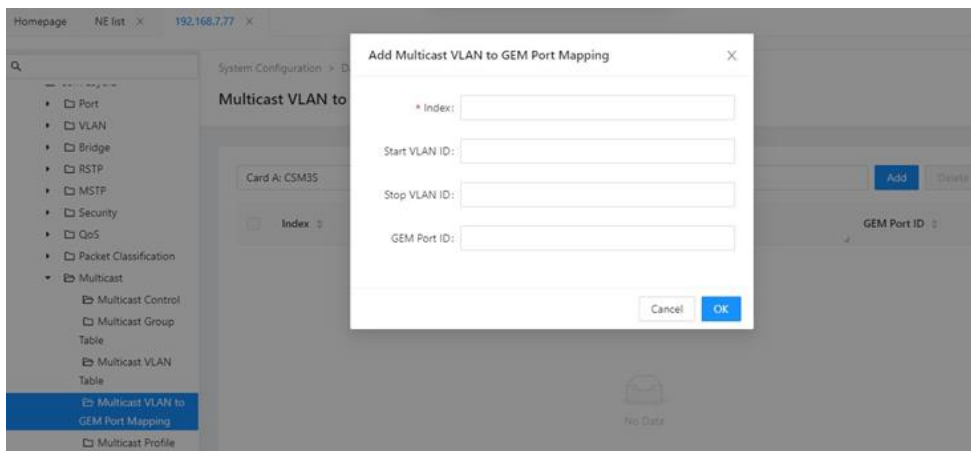
- Then modify the IGMP version to 3.



3. In the Function View navigation tree, click [Data\ CSM Layer 2\ multicast\ multicast VLAN Table]. Click “Add” to configure multicast VLAN 4000, with the group address of ff1e::1-ff1e::10.

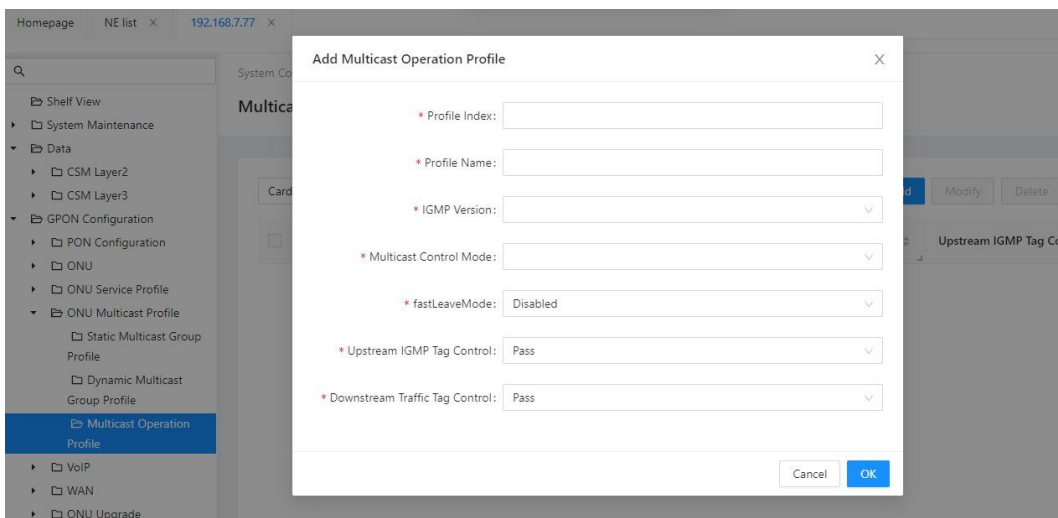


4. In the Functional View navigation tree, click [Data\CSM Layer 2\ multicas\ multicast VLAN to GEM Port Mapping]. Click “Add” to configure multicast VLAN 4000 mapping to GEM Port 3800.

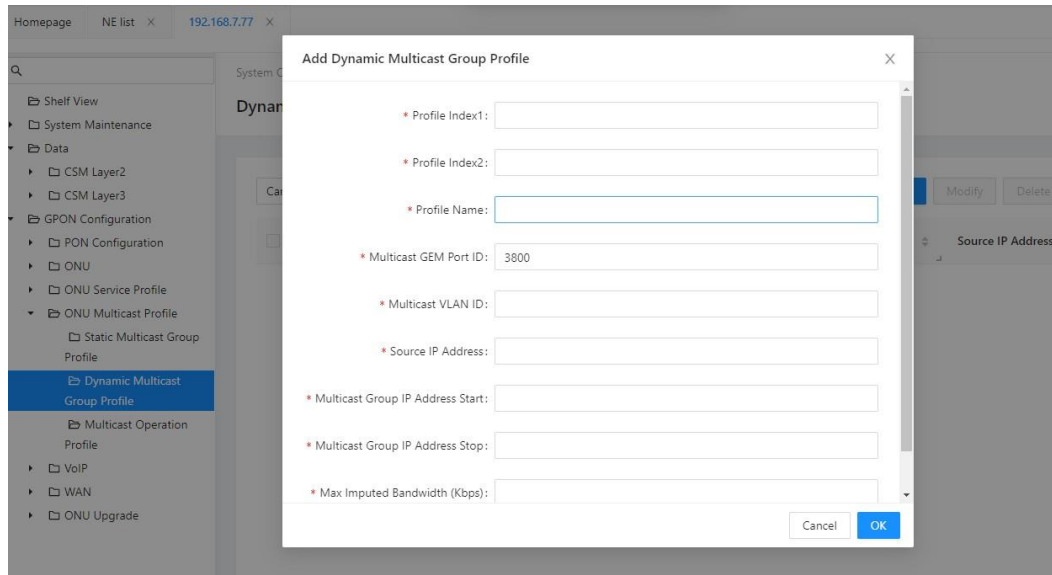


8.3.8 Configure ONU Multicast Profile

1. In the Function View navigation tree, click “GPON Configuration> Hipcast profiles> multicast Configuration profiles”. Click Add to configure a multicast profile.



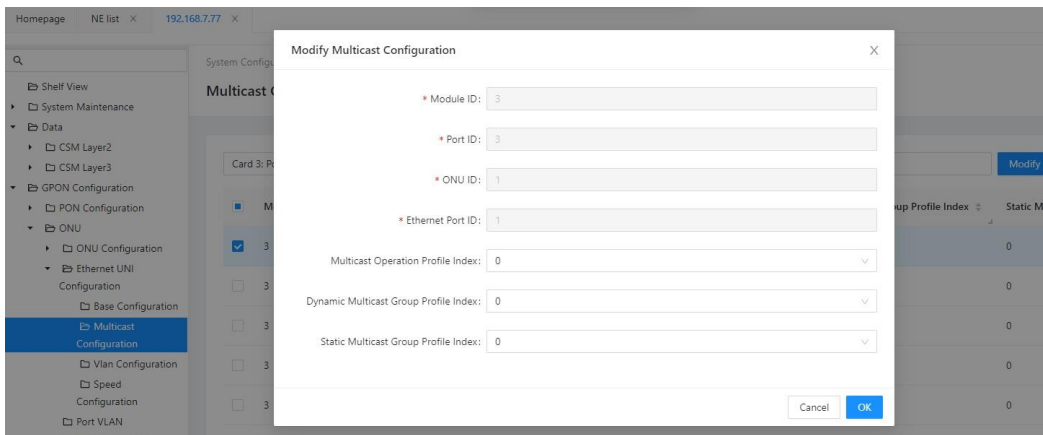
2. In the Function View navigation tree, click “GPON Configuration> Multicast profiles> Dynamic multicast profile”. Click “Add” to configure a multicast profile.



3. Configure the ONU service stream, uplink VLAN101, refer to ONU.
4. Apply the profile to ONU 1, apply it to ONU 2, and ONU 3 operates similarly.

In the Function View navigation tree, click “GPON Configuration> ONU> Ether UNI Configuration> Multicast Configuration”.

Select the ONU, and click “Modify” to perform the multicast profile configuration.



8.3.9 View OLT IGMP Snooping

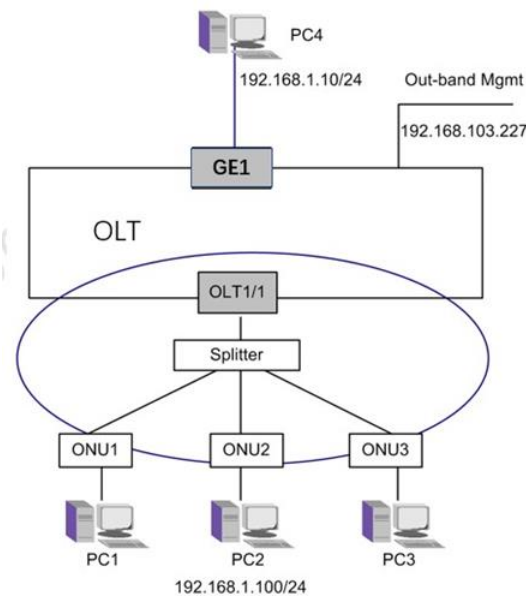
Send a multicast member report on PC1 and start multicast source service on PC4. If PC1 receives a normal multicast stream, it indicates that IGMP snooping on AX3516 is working.

8.4 Standard MLD proxy Configuration Instance

8.4.1 Application Description

In the application instance shown in Figure MLD proxy configuration, the PC connected to the ONU1, ONU2, and ONU3 all receive the multicast traffic. The MLD proxy configuration is illustrated using the following example.

8.4.2 Topological Instances



In the above figure, the OLT is connected to the multicast source PC4 via the XGE1 uplink port. The downlink port OLT 1/1 is connected to ONU1, ONU2, and ONU3 via an optical distributor. Ports XGE1, IS 1/1, and all ONU belong to VLAN10. PC1, PC2, and PC3 are respectively connected to their corresponding ONU1-3. PC1-3 are all members of the multicast groups and receive the multicast services from AX3517/AX3508/AX3502.

When connecting a new downlink user to a group, the user sends an IGMP member report message. The report message is received and snooping by OLT. After adding the table item, the IGMP report message is forwarded to the uplink device.

In this case, the PC4 sends a multicast service. Three PC1-3 receive the multicast service.

8.4.3 Configuration Requirements

- Take home gateway ONU as an example, the WAN configuration of ONU1, ONU2 and ONU3 is bridging mode, VLAN ID 10. See **ONU Configuration Manual**.
- ONU1, ONU2, and ONU3 bind to the corresponding ONU ID, respectively.
- Multicast source application of multicast source PC4 is installed.

8.4.4 Configuration Requirements

The list of the configuration IGMP snooping tasks is as follows:

- Create multicast VLAN
- Enable MLD proxy
- Configure ONU multicast profile
- View MLD proxy

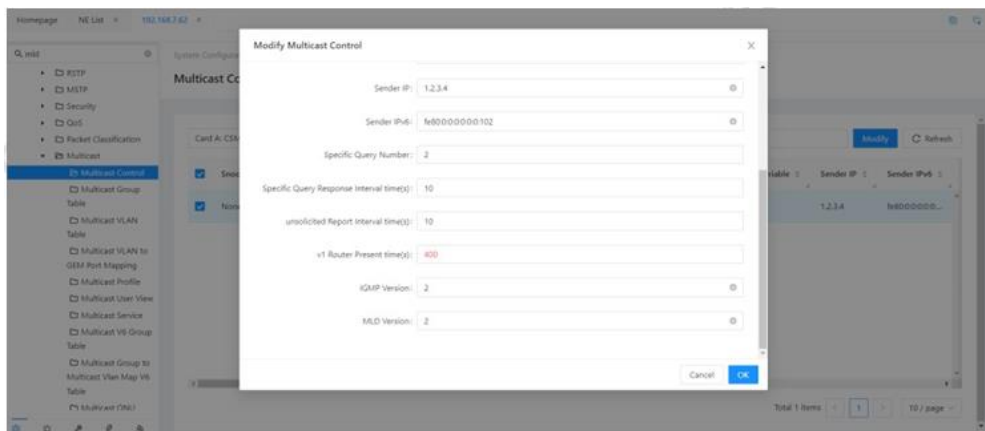
The detailed steps of each task are described below as an example of the topology in MLD Proxy Configuration figure.

8.4.5 Create Multicast VLAN

1. Create a multicast VLAN 4000, configure IS 1/1 as Tagged member port, XGE1 as tagged member port, and XGE 1 PVID set to 4000.
2. Create a unicast VLAN 101 and add IS 1/1 as the tagged member of that VLAN.
3. Create a VLAN 3800 for mapping to a multicast GEM port, and IS 1 / 1 is the tagged member of that VLAN. Refer to VLAN configuration.

8.4.6 Enable MLDv2 Proxy

1. In the Function View navigation tree, click [Data\ CSM Layer 2\ multicast\ multicast Control]. Click Modify to modify configuration.
2. Then modify the mld version to 2.

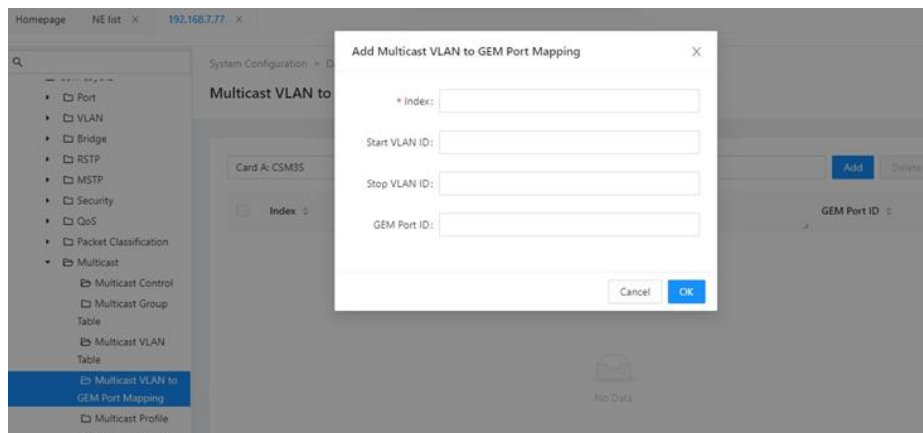


3. In the Function View navigation tree, click [Data\ CSM Layer 2\ multicast\ Multicast Group to Multicast Vlan Map V6 Table]. Click “Add” to configure multicast VLAN 4000, with the group address of ff1e::1-ff1e::10.



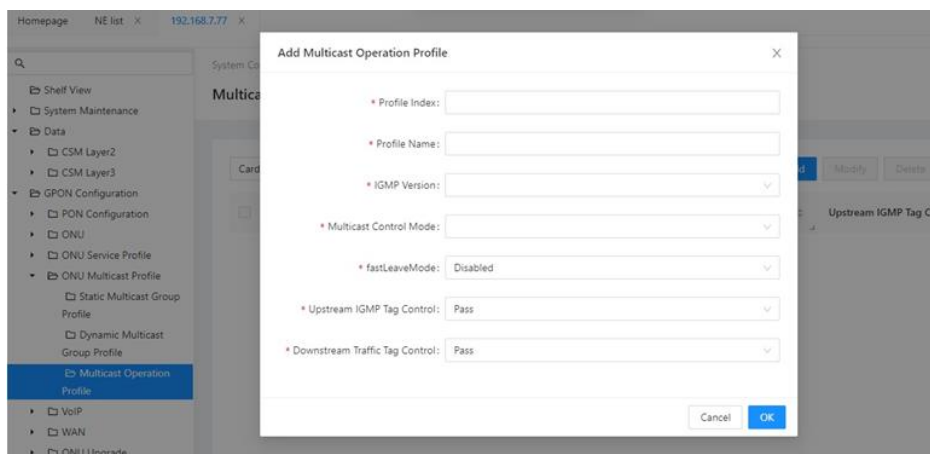
4. In the Functional View navigation tree, click [Data\CSM Layer 2\ multicas\ multicast VLAN to GEM Port Mapping].

Click “Add” to configure multicast VLAN 4000 mapping to GEM Port 3800.

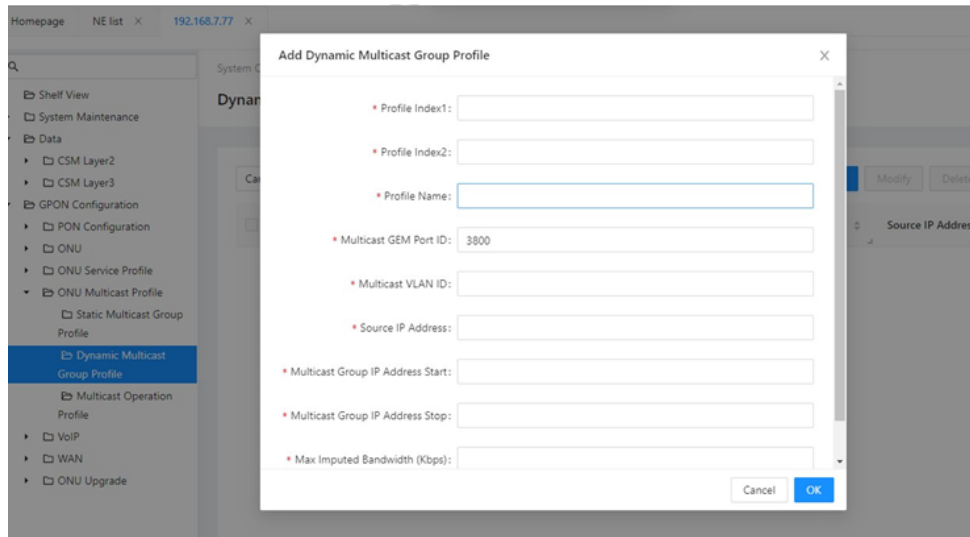


8.4.7 Configure ONU Multicast Profile

1. In the Function View navigation tree, click [GPON Configuration\Multicast profiles\ multicast operation profiles]. Click Add to configure a multicast profile.



2. In the Function View navigation tree, click “GPON Configuration> Multicast profiles> Dynamic multicast profile”. Click “Add” to configure a multicast profile.



3. Configure the ONU service stream, uplink VLAN101, refer to ONU.
4. Apply the profile to ONU 1, apply it to ONU 2, and ONU 3 operates similarly.
5. In the Function View navigation tree, click [GPON Configuration\ ONU\ Ether UNI Configuration\ Multicast Configuration].
6. Select the ONU, and click “Modify” to perform the multicast profile configuration.



8.4.8 View MLD proxy

Send a multicast member report on PC1 and start multicast source service on PC4. If PC1 receives a normal multicast stream, it indicates that MLD proxy on OLT is working.

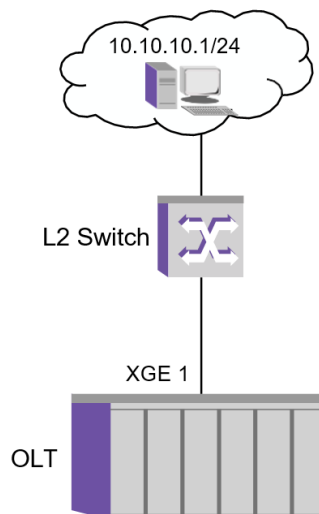
9 Multicast Configuration

ACL (Access Control List) is used to filter data packets to limit network traffic and to restrict network access to specific users or devices. Specific rules are defined in the ACL that allow or deny packet access to the OLT CPU or its specified interface. ACL is a range of allowed and rejected conditions applied to incoming packets. When the interface receives a packet, the packet field is compared to the applied ACL to verify that the packet is allowed to be forwarded. The packets were tested item by item against the list of filter conditions in the ACL.

9.1 ACL Instance

9.1.1 Application Description

In the application instance shown in Figure9-1, OLT connects to the network via XGE1, configure ACL to reject PC(10.10.10.1/24) Access OLT via XGE1. Explain the ACL configuration by using the following examples.



9.1.2 Configuration Tasks

The list of the configuration ACL tasks is as follows:

- Create a Package Classification-Matching Pattern
- Create a Packet Classification Rule
- Create a Flow-Based Security Control
- Create a Flow-Based Security Assignment

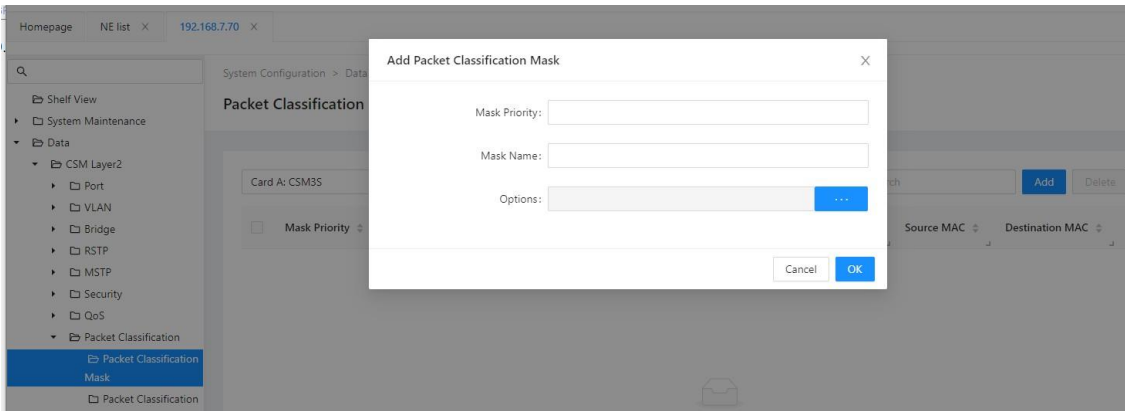
The detailed steps of each task are described below as an example of the topology in IP multicast introduction.

9.1.3 Create a Package Classification-Matching Mask

【Operating Steps】

In the Functional View navigation tree, click “Data> CSM Layer 2> Package Classification> Package Classification Mask”.

- Click “Add” to add a new stream classification matching mode, Source UDP Port.



- Click <OK> to save configuration.

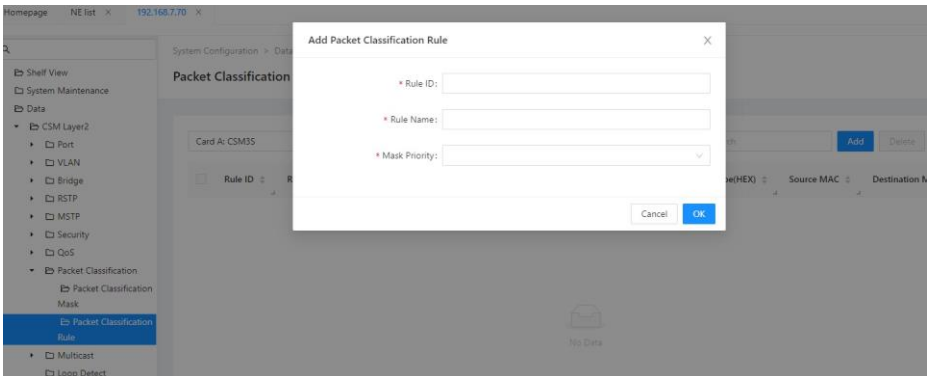
【Parameter Declaration】

Field	Description
Mask Priority	Priority of the mask
Mask Name	Mask name
Option	Match mode options
Source or ARP Sender IP	Source IP address
Destination ARP or IP Address	Destination IP address
Source MAC	Source MAC
Destination MAC	Destination MAC
ARP Sender MAC	The Source MAC in the ARP packet
ARP Target MAC	The Target MAC in the ARP packet
Source Ipv6 Mask	Source Ipv6 mask
Destination Ipv6 Mask	Target Ipv6 mask

9.1.4 Create a Packet Classification Rule

【Operating Steps】

- In the Functional View navigation tree, click Data> CSM Layer 2> Package Classification> Packet Classification Rule.
- Click Add to add a new flow classification rule with the source UDP port of 10.



- Click <OK> to save the configuration.

【Parameter Declaration】

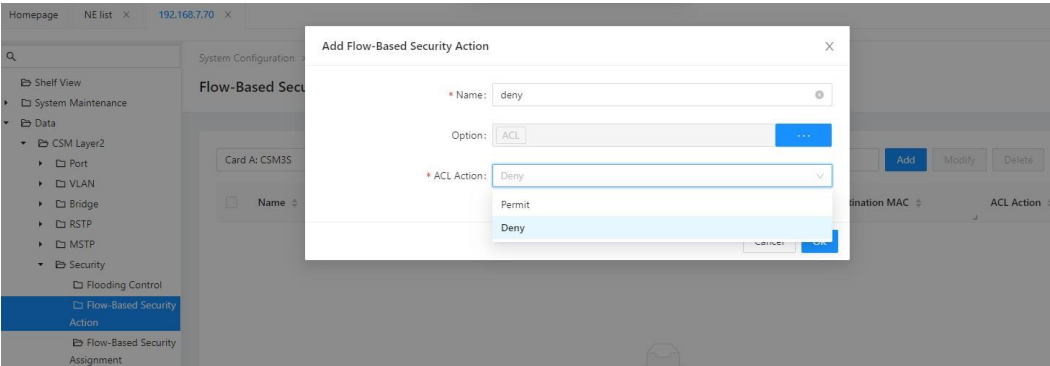
Field	Description
Rule ID	Identify the rule number
Rule Name	Rule name
Mask Priority	Match mode priority
S-VID	S-VID
S-PRI	S-PRI
C-VID	C-VID
C-PRI	C-PRI
Ethernet Type(HEX)	Ethernet type
Source MAC	Source MAC
Destination MAC	Destination MAC
IP Protocol Type	IP Protocol Type
Source or ARP Sender IP	Source or ARP Sender IP
Destination ARP or Target IP	Destination ARP or Target IP
DSCP	DSCP
ToS	ToS
Source TCP or UDP Port	Source TCP or UDP Port

Field	Description
Destination TCP or UDP Port	Destination TCP or UDP Port
ARP Sender MAC	ARP Sender MAC
ARP Target MAC	ARP Target MAC
Egress Port	Egress Port
Source IPv6 Address	Source IPv6 Address
Destination IPv6 Address	Destination IPv6 Address

9.1.5 Create a Flow-Based Security Control

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> Security> Flow- Based Security Action”.
- Click “Add” to add a new flow security action, Deny.



- Click <OK> to save the configuration.

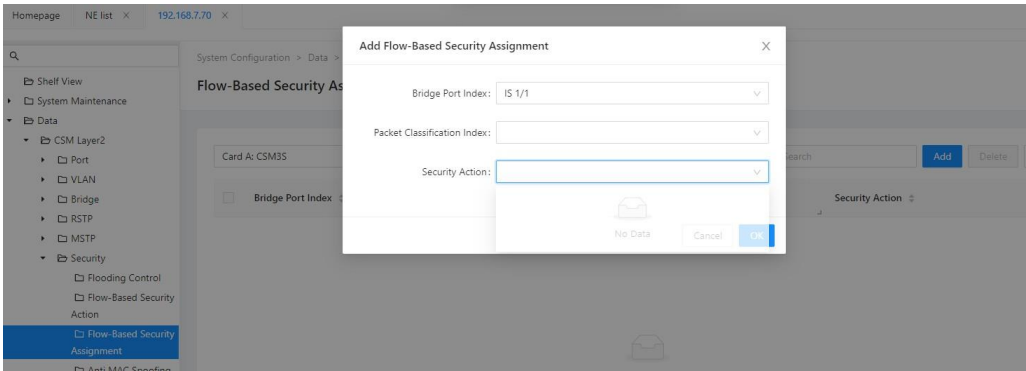
【Parameter Declaration】

Field	Description
Bridge Port Index	Port ID
Package Classification Index	Package classification rule profile.
Security Action	Security control profile.
VLAN ID	VLAN ID
Destination MAC	Destination MAC
ACL Action	ACL action: permit or Deny

9.1.6 Create a Flow-Based Security Assignment

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> Security> flow- based security assignment”.
- Click “Add” to apply the acl deny profile to the port.



- Click <OK> to save configuration.

【Parameter Declaration】

Field	Description
Bridge Port Index	Port ID
Package classification Index	Package classification rule profile.
Security Action	Security control profile.

10 QoS Configuration

10.1 QoS Introduction

This section describes how to configure the Business Quality (QoS) of OLT to select specific network services and prioritize their relative importance. QoS is implemented in the equipment to avoid bottleneck congestion and improve the predictability of network performance and bandwidth utilization.

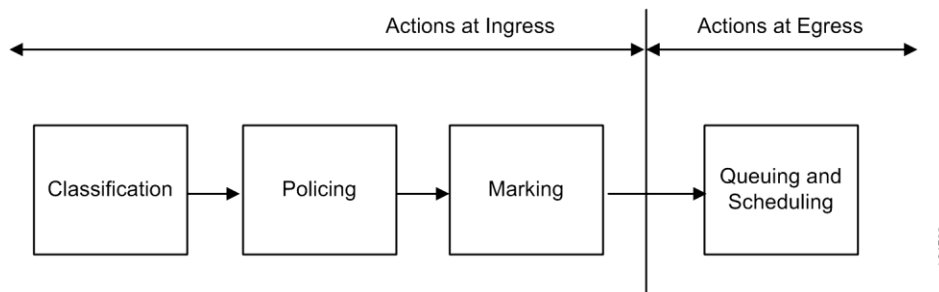
Implementing QoS in OLT provides different priorities to different users and ensures a certain level of performance to ensure that higher priority services (such as voice and video services) are prioritized.

The OLT 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 incoming port include classification, policing, and marking. Operations at the destination port are queuing and scheduling.

All these features work together to provide QoS guarantees and fair allocation of excess bandwidth and prioritize (both up and downside) user services for GE switches and PON systems.



With business flow classification, user frames can be marked in the DSCP field of an IP packet or in the 802.1p priority field of Ethernet frames.

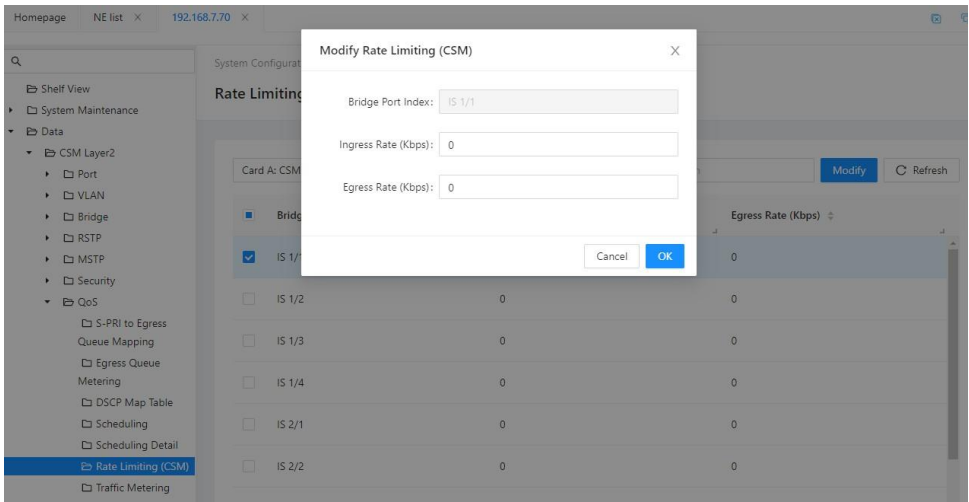
10.2 Rate Limit

The OLT provides rate limiting functionality for uplink and downlink traffic of the XGE ports.

【Operating Steps】

- In the Functional View navigation tree, click “Data> CSM Layer 2> QoS> Rate Limiting (CSM)”.

- Select a port and click “Modify” to modify the rate configuration.



- Click <OK> to save the configuration.

【Parameter Declaration】

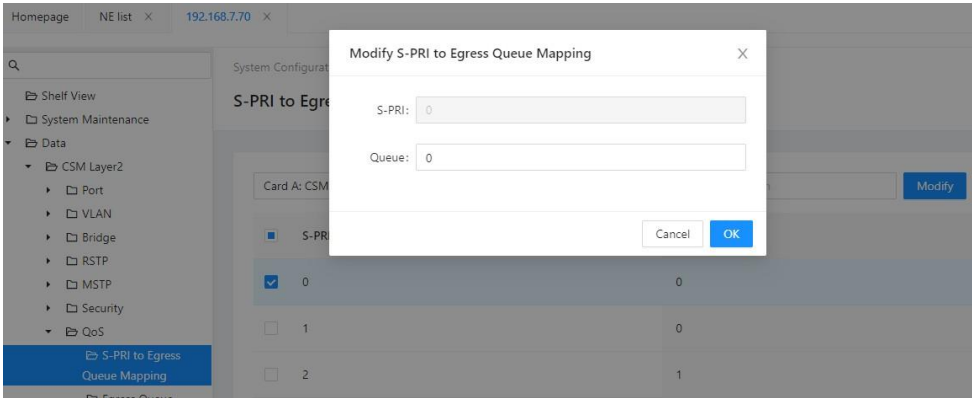
Field	Description
Bridge Port Index	Identify the port number.
Ingress Rate(Kbps)	Ingress rate, unit in Kbps.
Egress Rate (Kbps)	Egress rate, per unit in Kbps.

10.3 Queue Mapping

Priority to-exit queue mapping.

【Operating Steps】

- Click Data> CSM Layer 2> QoS> S-PRI to Egress Queue Mapping.
- Select a map that you need to modify, and click Modify.



- Click <OK> to save the configuration.

【Parameter Declaration】

Field	Description
S-PRI	Priority identification
Queue	Queue number, queue 7 is the highest priority

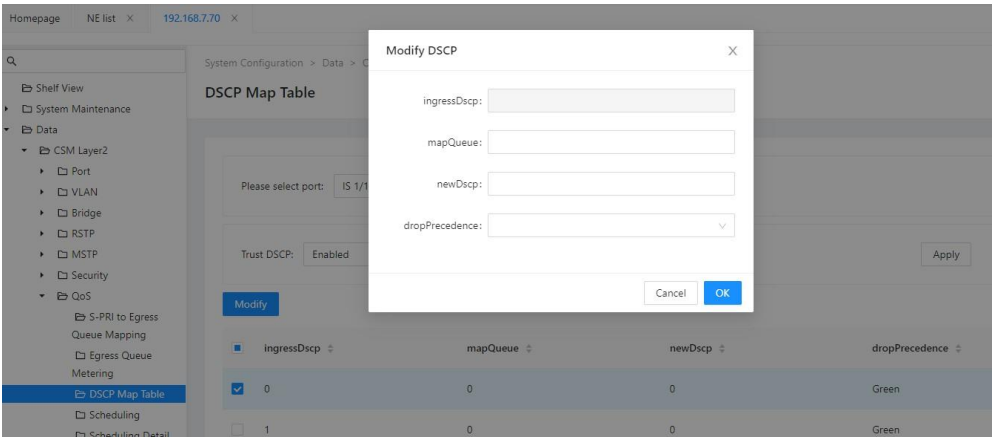
10.4 DSCP Mapping Table

If a trusted DSCP is set, the DSCP values in the incoming packets from this interface are always trusted to classify the packet QoS.

- By default, the trust DSCP is disabled.
- If a trusted DSCP is configured, the portal transforms the DSCP value in the incoming packet to the new DSCP value against the DSCP mapping queue.

【Operating Steps】

- Click “Data> CSM Layer 2> QoS> DSCP Map Table”.
- Select the port to Enable the trust DSCP.
- Click “Modify”.



- Click <OK> to save the configuration.

【Parameter Declaration】

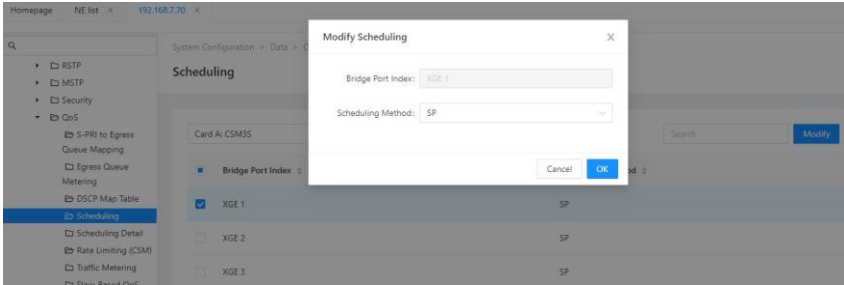
Field	Description
Trust DSCP	Do you trust DSCP and queue as DSCP.
Ingress DSCP	Message DSCP value received at the entry.
MapQueue	The mapped queue number.
NewDSCP	New DSCP value.
Dropprecedence	Drop precedence

10.5 Schedule Mode

Each port supports 8 egress queue. After packets are assigned to each queue according to QoS priority, the system will schedule depending on scheduling mode and queue weights.

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> QoS> Scheduling”.
- Select a port, and click “Modify” to modify the port scheduling mode.



- Click <OK> to save the configuration.

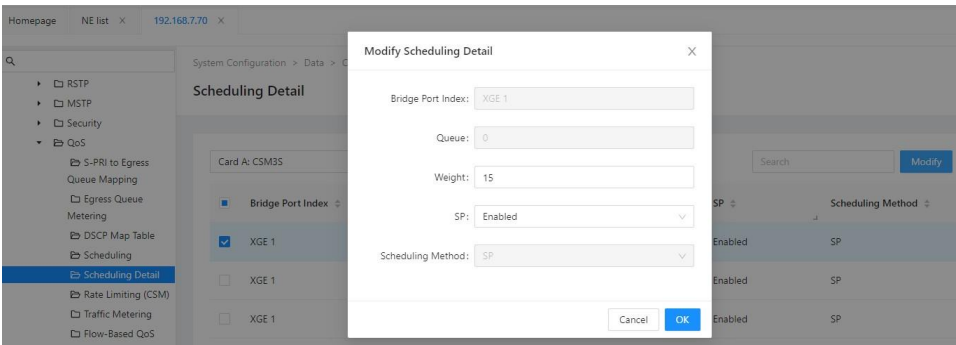
【Parameter Declaration】

Field	Description
Egress Port Index	Port ID
Scheduling Method	Egress scheduling method: SP, WRR, SP + WRR

10.6 Weight Configuration

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> QoS> Schedule Detail”.
- Select a port, and click “Modify”, to modify the scheduling weight value (WRR or WRR + SP scheduling).



- Click <OK> to save the configuration.

【Parameter Declaration】

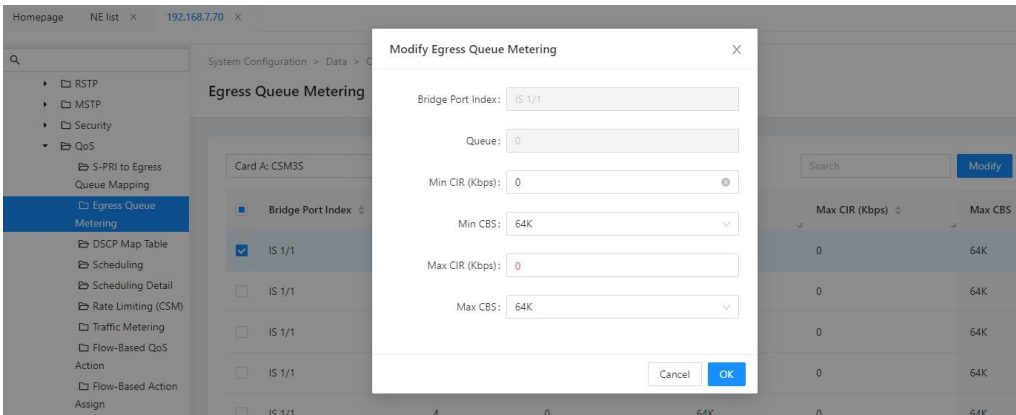
Field	Description
Bridge Port Index	Port ID
Queue	Queue ID
Weight	Set the WRR weight value.
SP	Enable / Disable

10.7 Egress Queue Metering

【Operating Steps】

In the Function View navigation tree, click “Data> CSM Layer 2> QoS> Egress Queue Metering”.

Select a port, and click Modify, to modify the egress queue metering parameter.



Click <OK> to save the configuration.

【Parameter Declaration】

Field	Description
Bridge Port Index	Port ID
Queue	Queue ID
Min CIR (Kbps)	Sets the queue minimum CIR value.
Min CBS	Sets the queue minimum CBS value.
Max CIR (Kbps)	Sets the queue maximum CIR value.
Max CBS	Set the queue maximum CBS value.

10.8 Flow-Based QoS

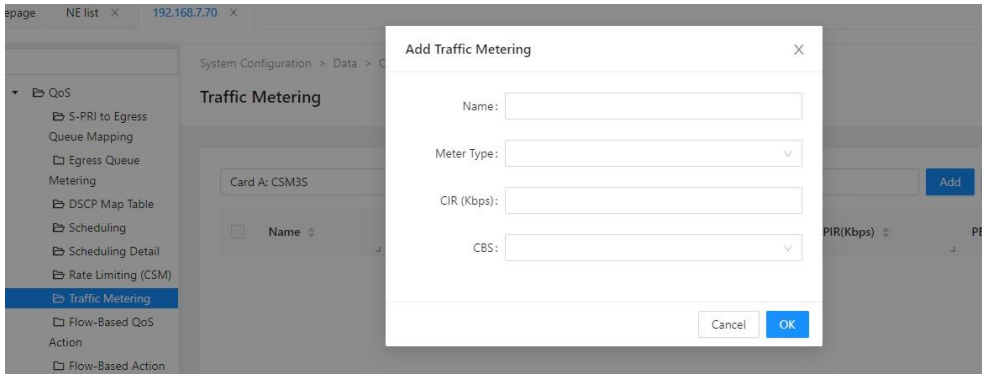
The task list of configuration is following:

- Traffic Metering Profile
- Flow-based QoS Action
- Flow-based QoS Assign

10.8.1 Traffic Metering Profile

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> QoS> Traffic Metering”.
- Click “Add” to add a new traffic metering.



- Click <OK> to save the configuration.

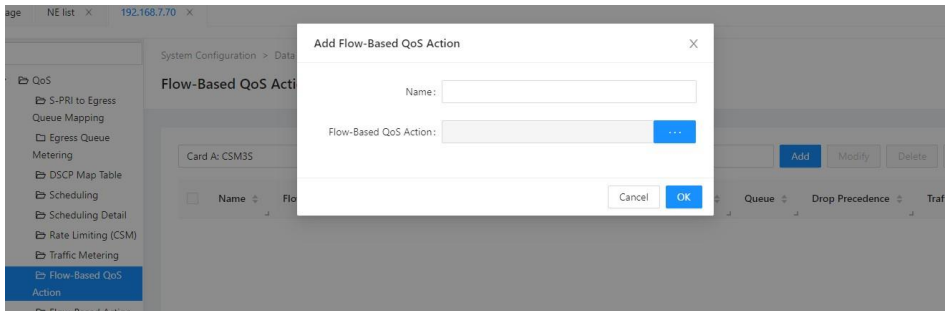
【Parameter Declaration】

Field	Description
Name	Rule name
Meter Type	The discarding priority colors
CIR	CIR values, in the unit of Kbps
CBS	CBS values
PIR	PIR values, in the unit of Kbps
PBS	PBS values
EBS	EBS values

10.8.2 Flow-based QoS Action

【Operating Steps】

- In the Function View navigation tree, click “Data> CSM Layer 2> QoS> Flow-Based QoS Action”.
- Click “Add” to add a new flow-based operation rule.
- Click <OK> to save the configuration.



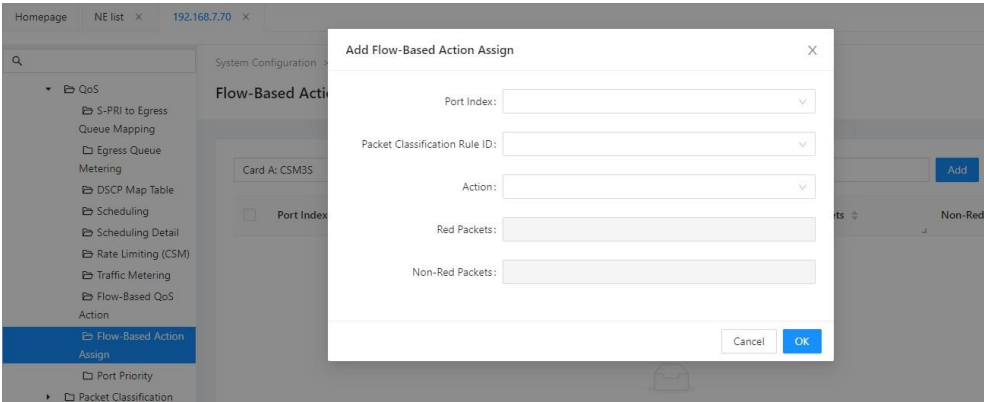
【Parameter Declaration】

Field	Description
Name	Rule name
Flow-Based QoS Action	Select a flow-based QoS action
Traffic Metering Name	Select the traffic metering profile
New Priority	New priority identification
New DSCP	The New DSCP ID
Queue	Queue ID
Drop Precedence	Discarding priority
Traffic Class	0-255

10.8.3 Flow-based QoS Assign

【Operating Steps】

- In the Function View navigation tree, click“Data > CSM layer2 > QoS > Flow-based Action Assign”.
- Click Add to apply the flow action rule to the port.



- Click <Apply> to save the configuration.

【Parameter Declaration】

Field	Description
Port Index	Port ID
Package Classification Rule ID	Select a flow-based QoS action.
Action	Select traffic metering profile

11 SyncE

11.1 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.

11.2 SyncE Configuration Instance

11.2.1 Operating Steps

- Check the uplink port status
- Configure SyncE
- Check the SyncE status of the uplink port

11.2.1.1 Check the Uplink Port Status

- Check the uplink port status, the port needs to be UP.

【Operating Steps】

- In the Function View navigation tree, click “System Configuration>Data>CSM Layer2>Port>Port Active”.

The screenshot shows the 'Port Active' configuration page in the AX3500 OLT web interface. The page title is 'Port Active' and it is under the path 'System Configuration > Data > CSM Layer2 > Port > Port Active'. The table below lists the status of various ports.

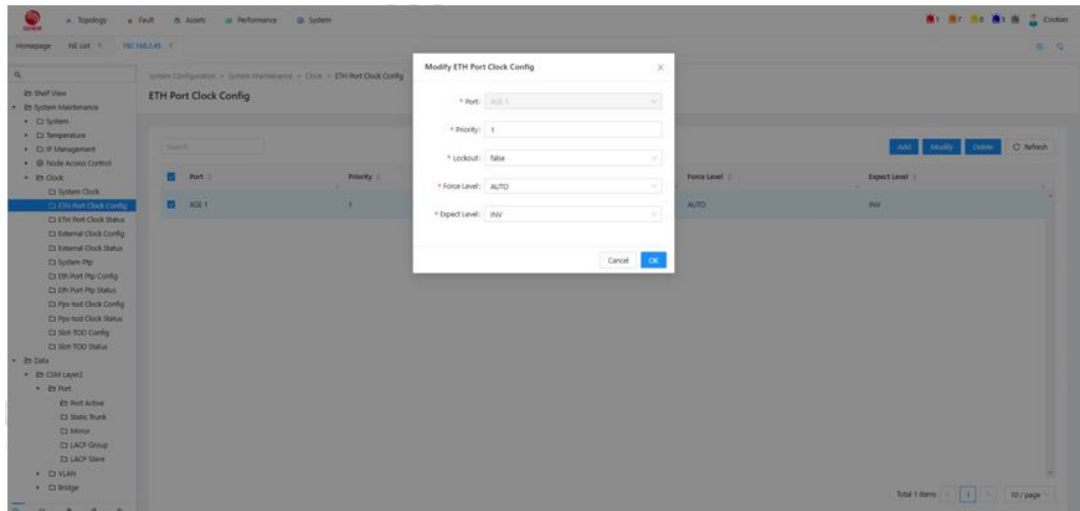
Port Index	Administrative State	Operational State	Configured Speed	Configured Duplex	Configured Flow Control	Actual Speed	Actual Duplex	Actual Flow Control	Orientation	SFP Type	Auto
IS S/1	Enabled	Disabled	25G	Full	On	100	Full	On	Subscriber	Abvent	D
IS S/8	Enabled	Disabled	25G	Full	On	100	Full	On	Subscriber	Abvent	D
XGE 1	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	100GBASE-LR	D
XGE 2	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	Abvent	D
XGE 3	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	Abvent	D
XGE 4	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	Abvent	D
XGE 5	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	Abvent	D
XGE 6	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	Abvent	D
XGE 7	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	Abvent	D
XGE 8	Enabled	Disabled	Auto Negotiation	Auto Negotiation	Auto Negotiation	100	Full	On	Network	Abvent	D

11.2.1.2 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.

【Operating Steps】

- In the Function View navigation tree, click “System Configuration>System Maintenance>Clock>ETH Port Clock Config”.

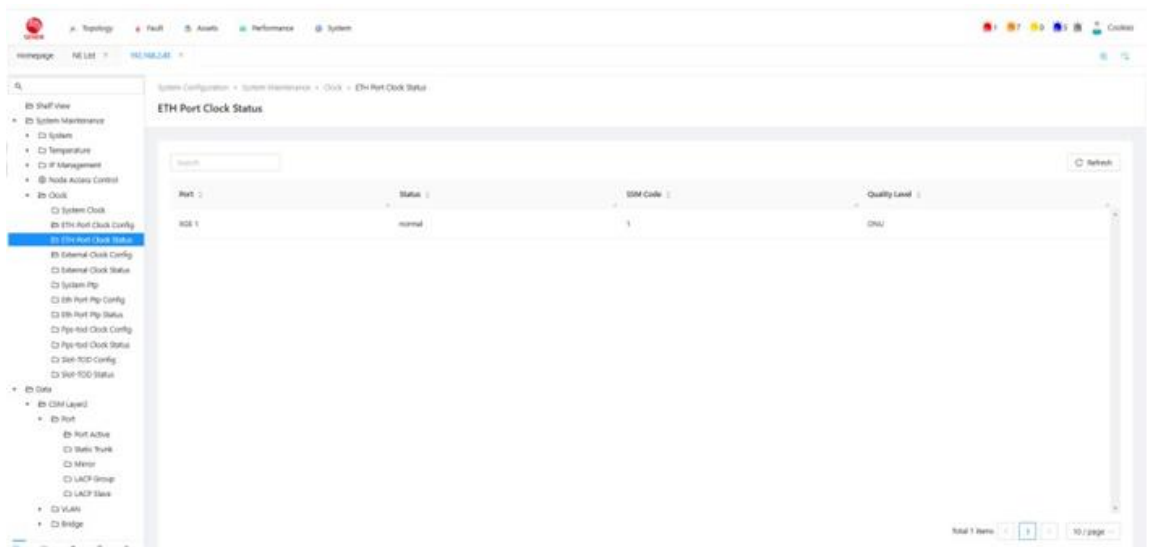


11.2.1.3 Check the SyncE status of the uplink port

- Check the SyncE status; "normal" indicates that the frequency has been successfully locked.

【Operating Steps】

- In the Function View navigation tree, click “System Configuration>System Maintenance>Clock>ETH Port Clock Status”.



12 PTP

12.1 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.

12.1.1 Basic Concepts of PTP

12.1.1.1 PTP Protocol Standards

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.

12.1.1.2 PTP Domain

A 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.

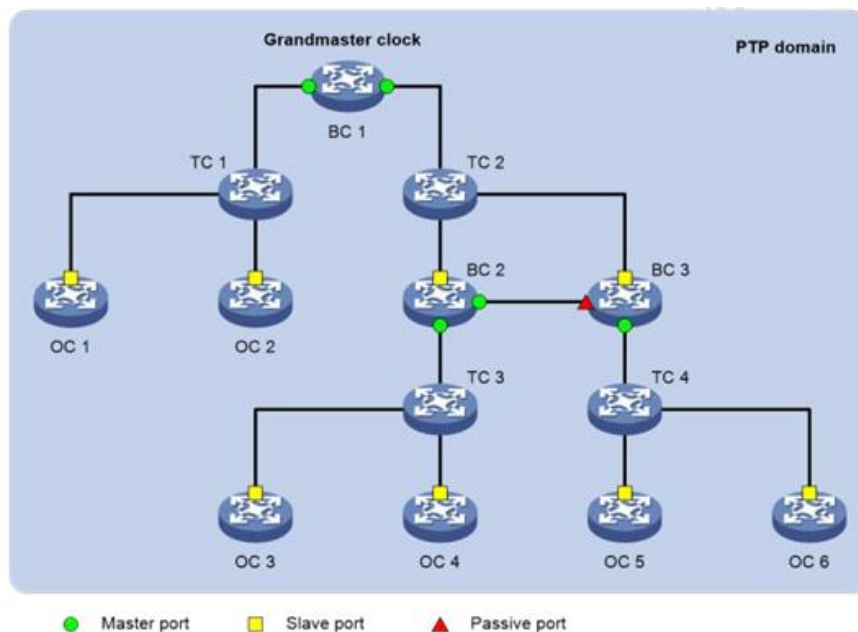
12.1.1.3 PTP Instances

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.

12.1.1.4 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 Figure NuMax Cloud 4000 topological management 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.



12.1.2 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.

12.1.3 Optimal Clock

As shown in Figure Diagram of Basic Clock Nodes, 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.

12.1.4 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.

12.1.5 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.

12.1.6 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 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 Figure 10-2, the Sync message's sending timestamp t_1 is carried by the Follow_Up message.
- In one-step mode, the Sync message's sending timestamp t_1 is carried by the Sync message itself, and no Follow_Up message is sent.

Below figure explains the implementation process of the Request-Response mechanism in two-step mode:

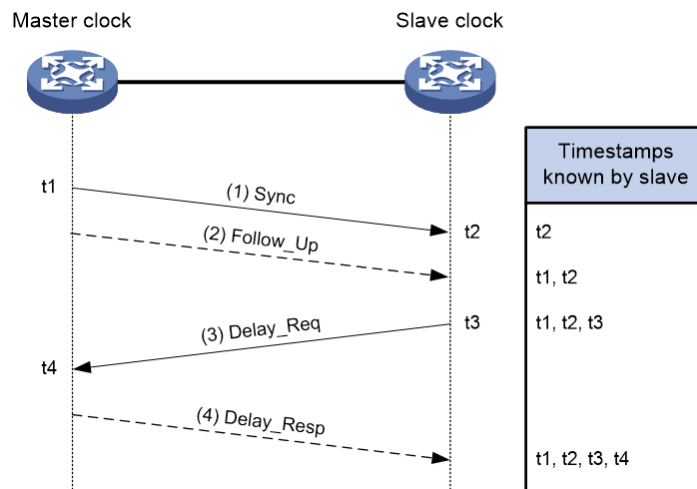
The slave clock sends a Delay_Req message to the master clock to initiate the calculation of the reverse transmission delay and records the sending time t_3 . The master clock records the receiving time t_4 after receiving this message.

1. The master clock sends a Sync message to the slave clock and records the sending time t_1 . The slave clock records the receiving time t_2 .
2. After sending the Sync message, the master clock immediately sends a Follow_Up message carrying t_1 .
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 t_3 . The master clock records the receiving time t_4 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 = $(t2 - t1) - [(t2 - t1) + (t4 - t3)] / 2 = [(t2 - t1) - (t4 - t3)] / 2$



12.2 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.

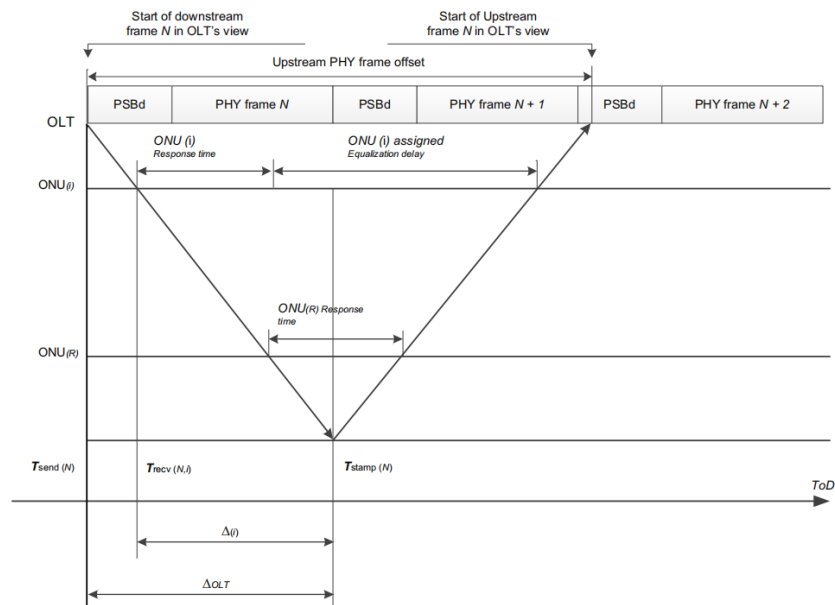
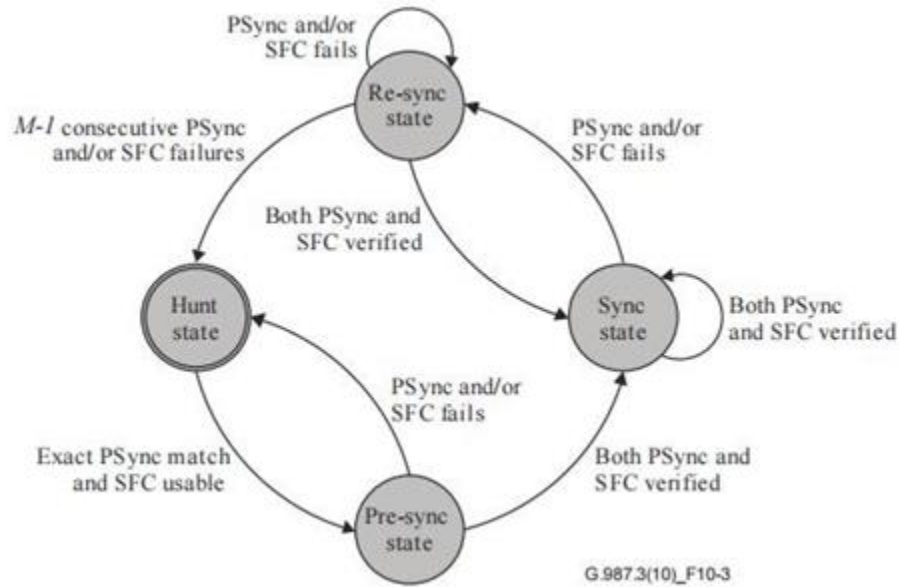
The principle of operation assumes that the OLT has an accurate real-time clock (RTC), obtained through means beyond the scope of these specifications. The OLT informs the ONU of the time of day when a certain downstream GTC/XGTC frame will arrive at a hypothetical ONU that has zero equalization delay 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 Tsend(N), which is the time of transmission of frame number N at the OLT, and Teqd, 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 Tsend(N) in the OLT. It is assumed that the quantity Teqd is known by configuration, and does not change frequently throughout the link activation period. ONU frequency synchronization with the OLT during registration.



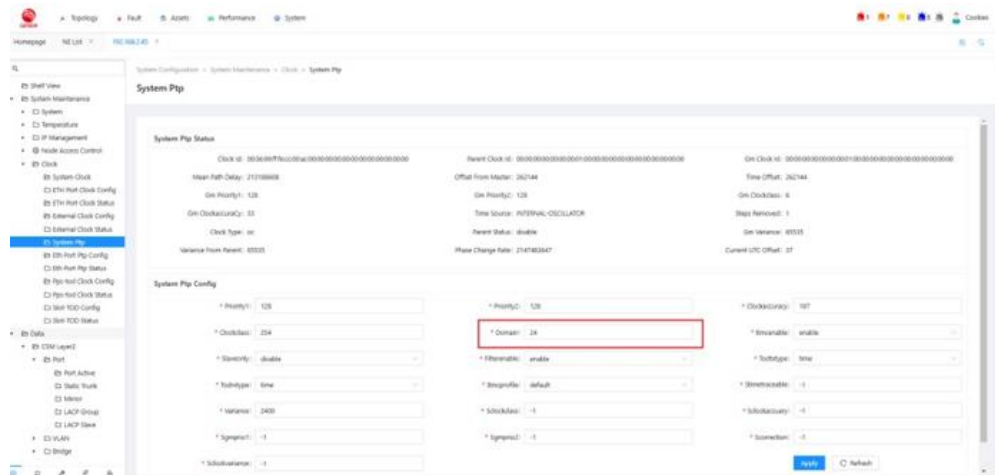
12.3.3.2 Configure Port PTP Parameters

Configure the uplink port XGE1 SyncE function, see Chapter 9 for details.

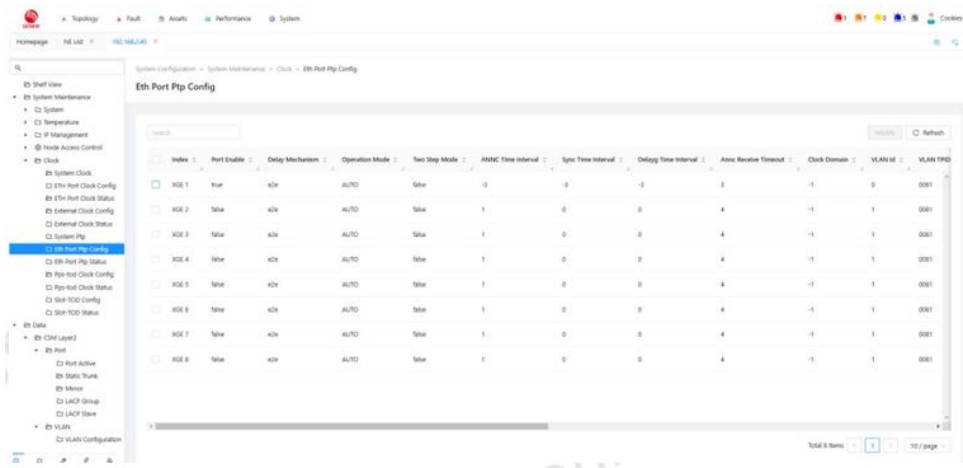
- Set the OLT PTP domain to 24. [Operating Steps]

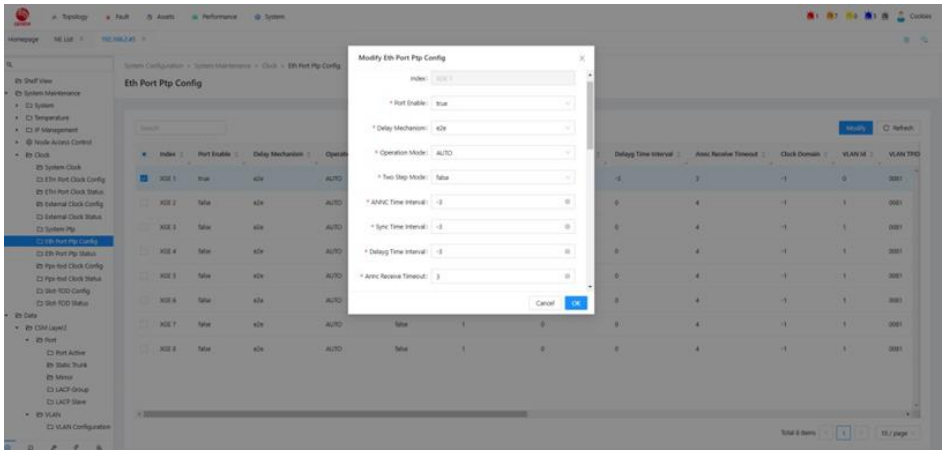
【Operating Steps】

- In the Function View navigation tree, click “System Configuration>System Maintenance>Clock>System Ptp”.



- In the Function View navigation tree, click “System Configuration>System Maintenance>Clock>Eth Port Ptp Config”.
- Enable PTP function on the uplink port XGE1.
- Set the local priority of the uplink port XGE1 PTP to 128.
- Set the uplink port XGE1 PTP message to untagged.
- Configure the uplink port XGE1 PTP Announce message to 8 per second with a timeout of 3 seconds.
- Set the uplink port XGE1 PTP Sync message to 8 per second (no Sync messages are sent when the port role is Slave).





【Parameter Declaration】

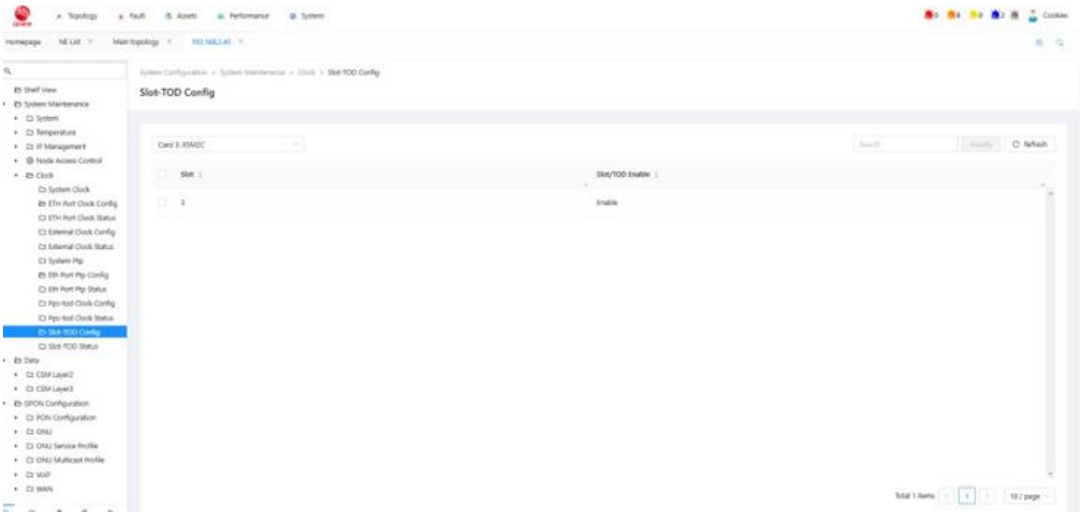
Field	Description
Domain	Configure PTP clock domain.
ANNC/Sync/DelayReq Interval	The transmission interval is from 2 ⁻⁴ to 2 ⁴ , i.e., 0.0625 seconds to 16 seconds.2 ⁻³ means the interval is 1/8 of a second, or 0.125 seconds.
Local Port Priority	Configure the local Ethernet port's PTP priority.
Two-Step Mode	Enable/Disable Two-Step Timestamp Mode
VLAN ID	Configure the VLAN for PTP messages, default VLAN ID=0 is untagged.

12.3.3.3 Enable ToD to Slot

Enable the main control to send ToD to Slot card.

【Operating Steps】

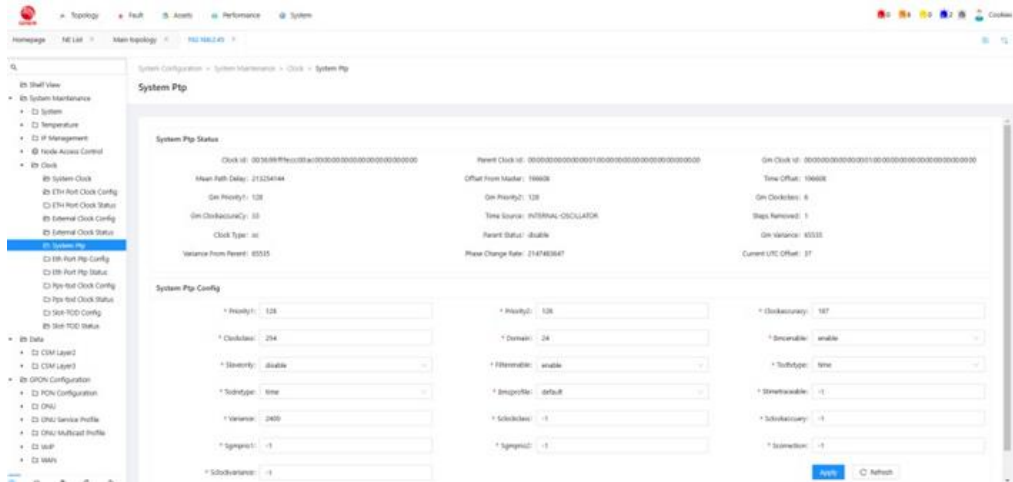
In the Function View navigation tree, click “System Configuration>System Maintenance>Clock>Slot-TOD Config”.



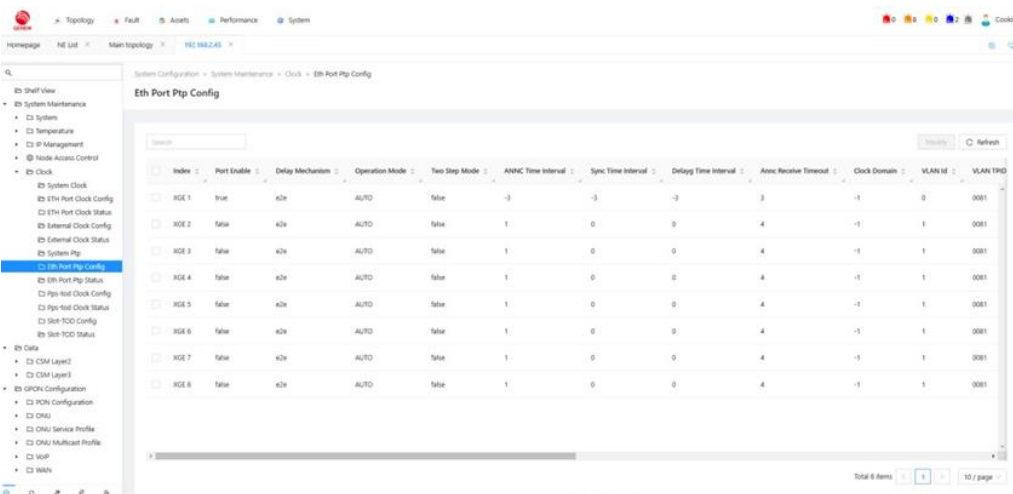
12.3.3.4 View PTP Configuration

【Operating Steps】

In the Function View navigation tree, click “System Configuration>System Maintenance>Clock>System Ptp”.



In the Function View navigation tree, click “System Configuration>System Maintenance>Clock>Eth Port Ptp Config”.

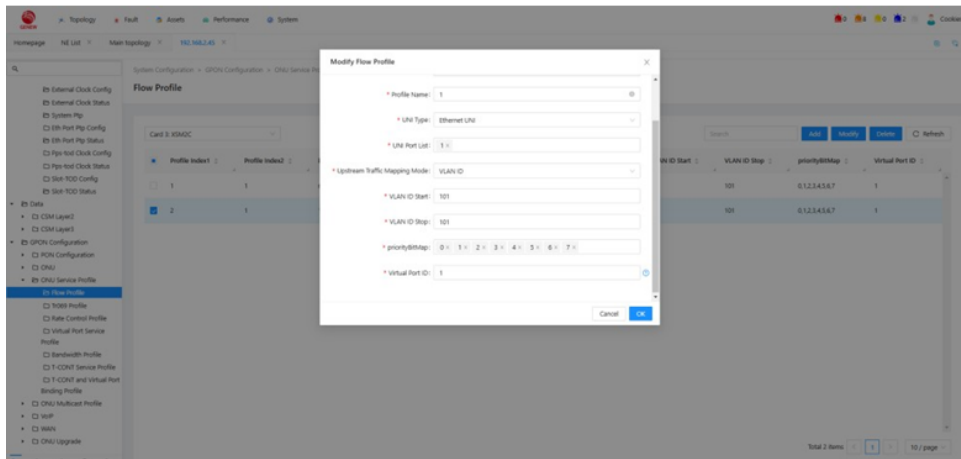
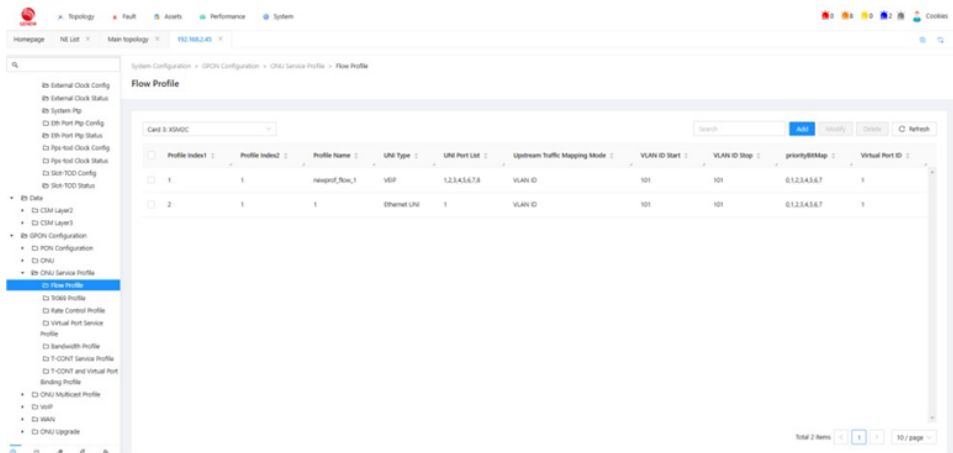


12.3.4 Application Description

Create an ONU service template.

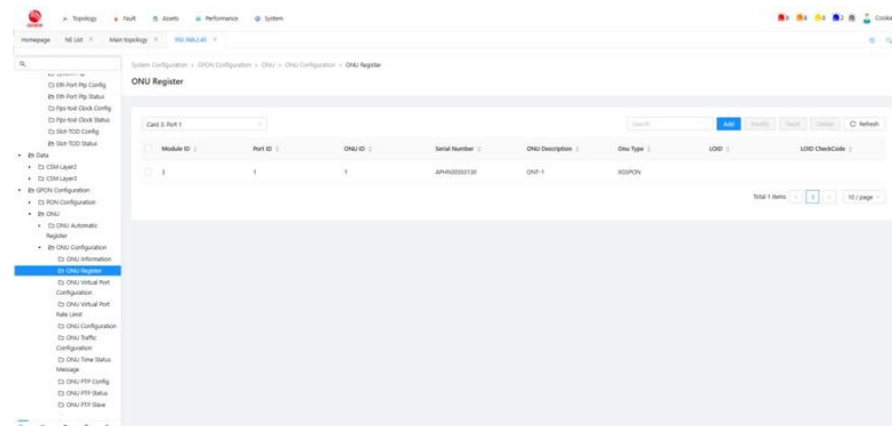
【Operating Steps】

In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU Service Profile>Flow Profile”.

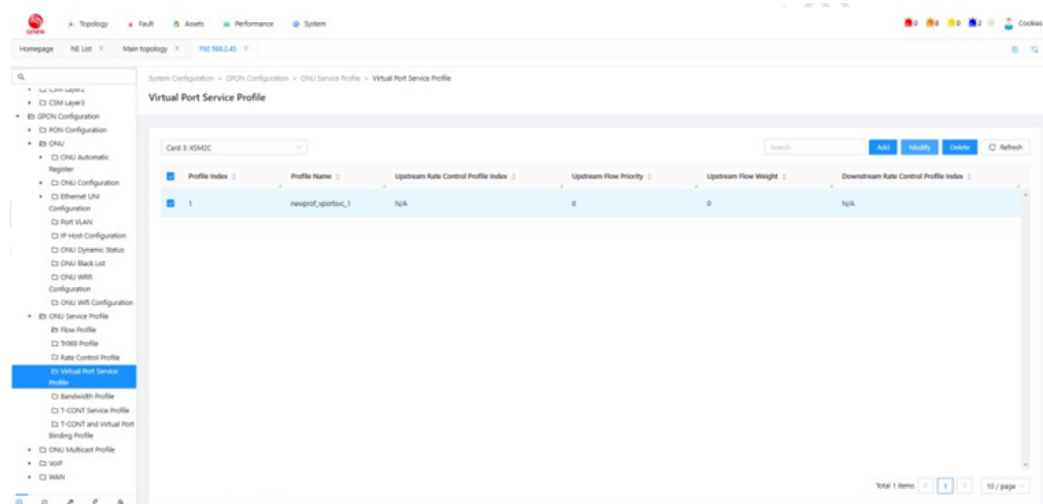


Register the ONU and configure the basic services for the ONU.

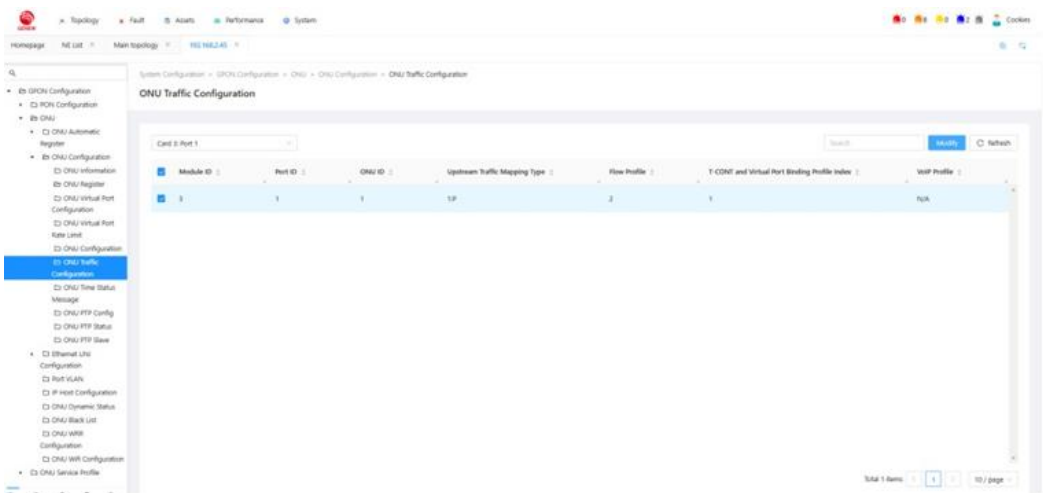
In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU>ONU Configuration>ONU Register”.



In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU Service Profile>Virtual Port Service Profile”.

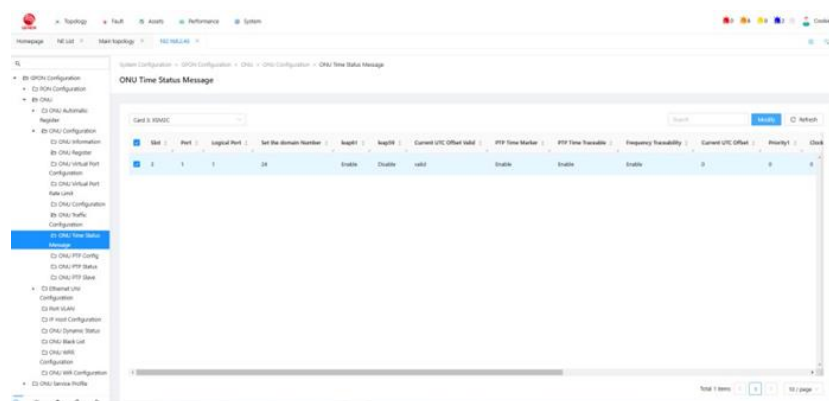


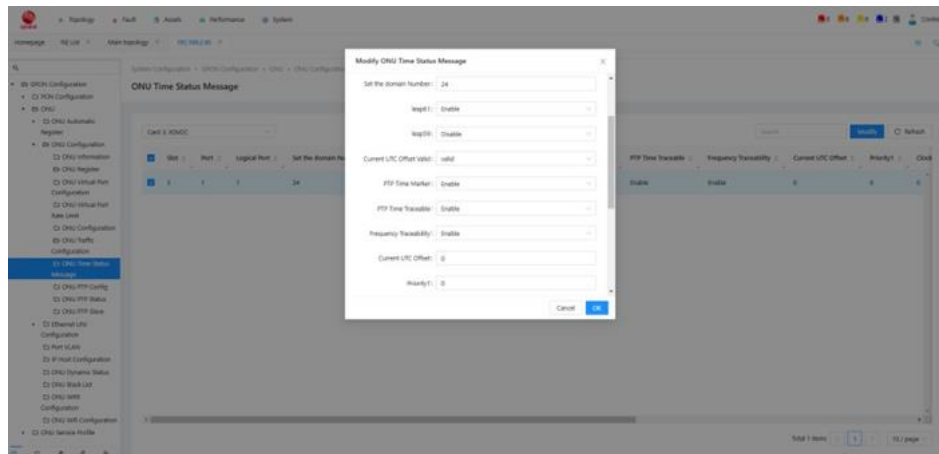
In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU>ONU Configuration>ONU Traffic Configuration”.



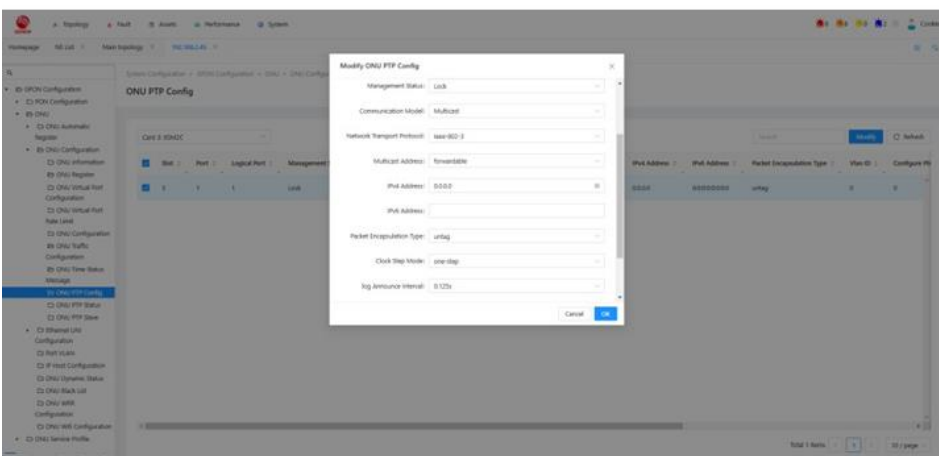
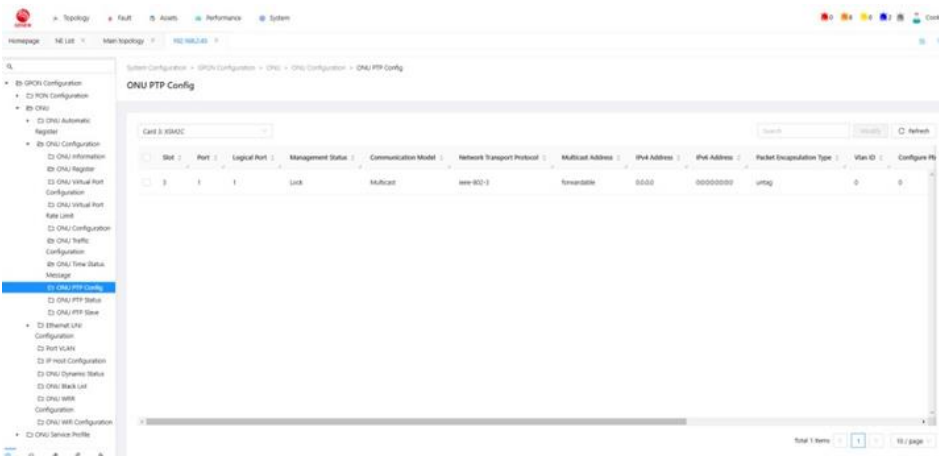
Configure the ONU 1588-related parameters, such as setting the domain to 24, mode to one-step, message format to multicast, and setting message intervals, etc.

In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU>ONU Configuration>ONU Time Status Message”.

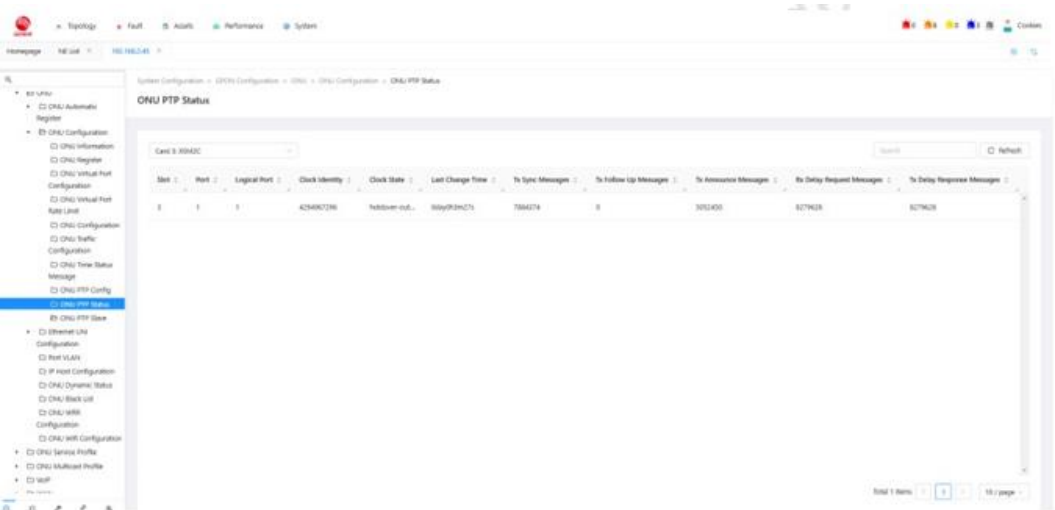




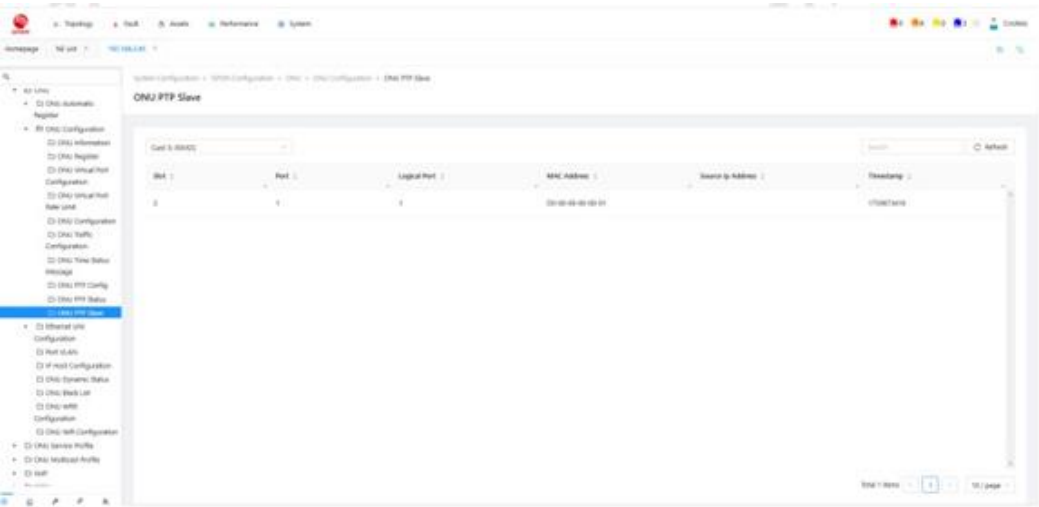
In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU>ONU Configuration>ONU PTP Config”.



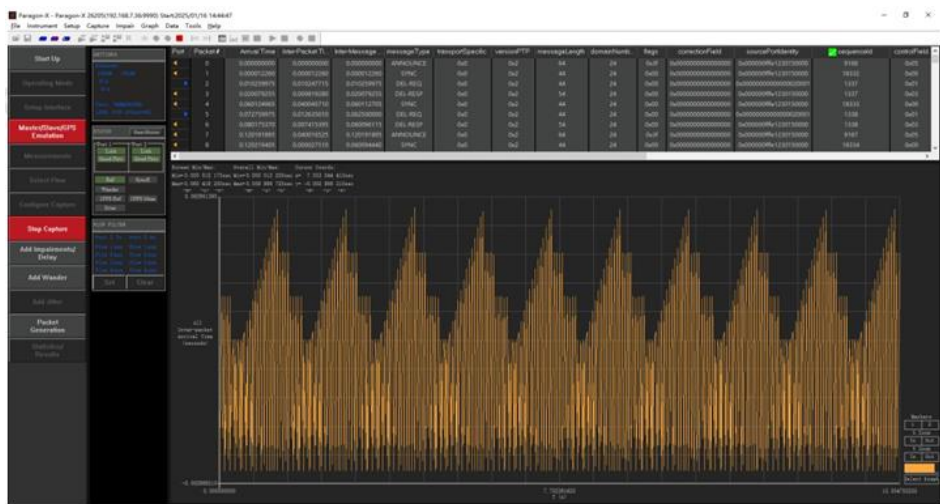
In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU>ONU Configuration>ONU PTP Status”.

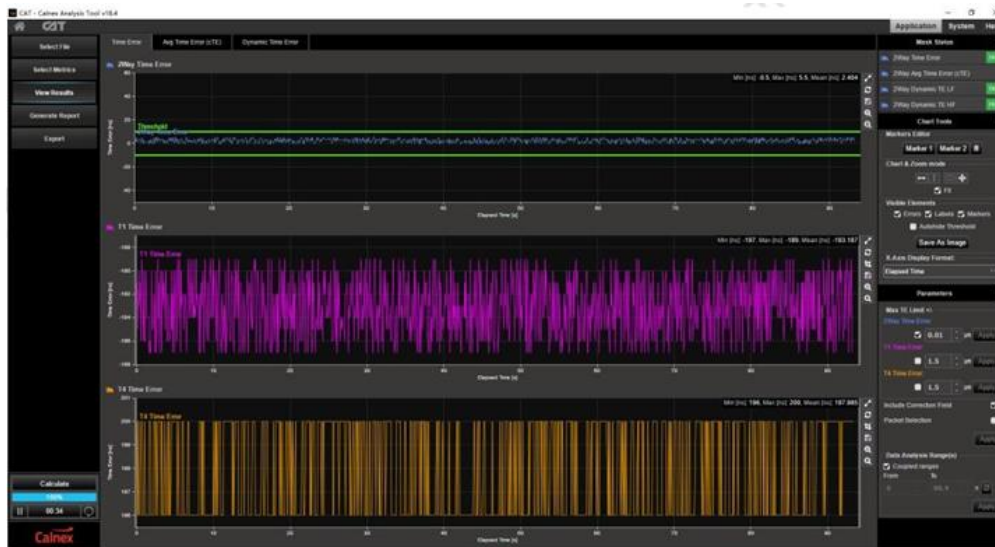


In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU>ONU Configuration>ONU PTP Status”.

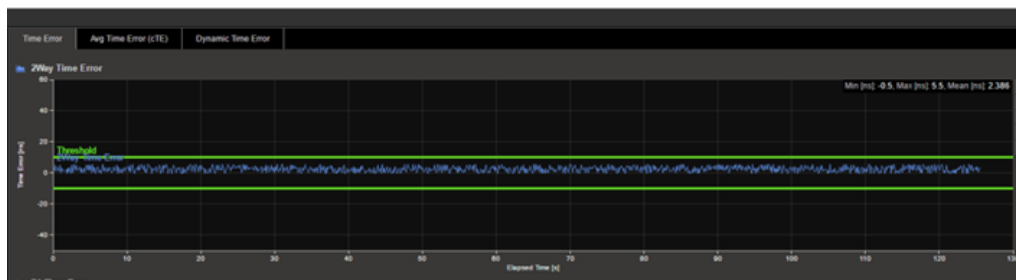


Result.





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).



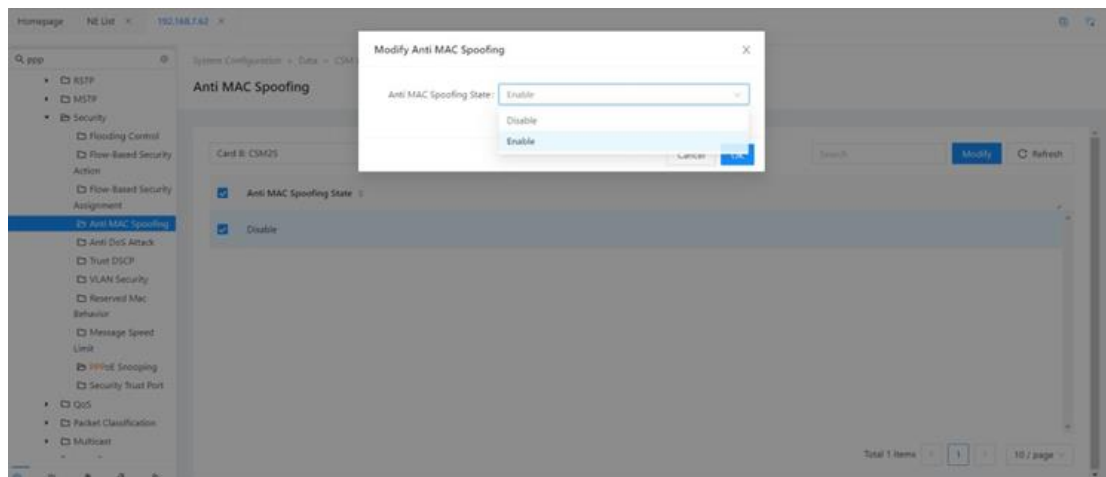
13 Security Management

This section describes how to configure system security options to ensure that data in the OLT is protected from external attacks.

13.1 Anti-MAC Spoofing

【Operating Steps】

1. In the Function View navigation tree, click “System Configuration>GPON Configuration>ONU Service Profile>Flow Profile”.
2. Click Modify to enable Anti MAC Spoofing.



13.2 ARP Snooping Scalars

【Operating Steps】

1. In the Function View navigation tree, click[Data \ CSM layer3\ARP\ Arp Snooping Scalars].
2. Click Modify to enable ARP snooping Scalars.



13.3 MACFF (MAC-Forced 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.

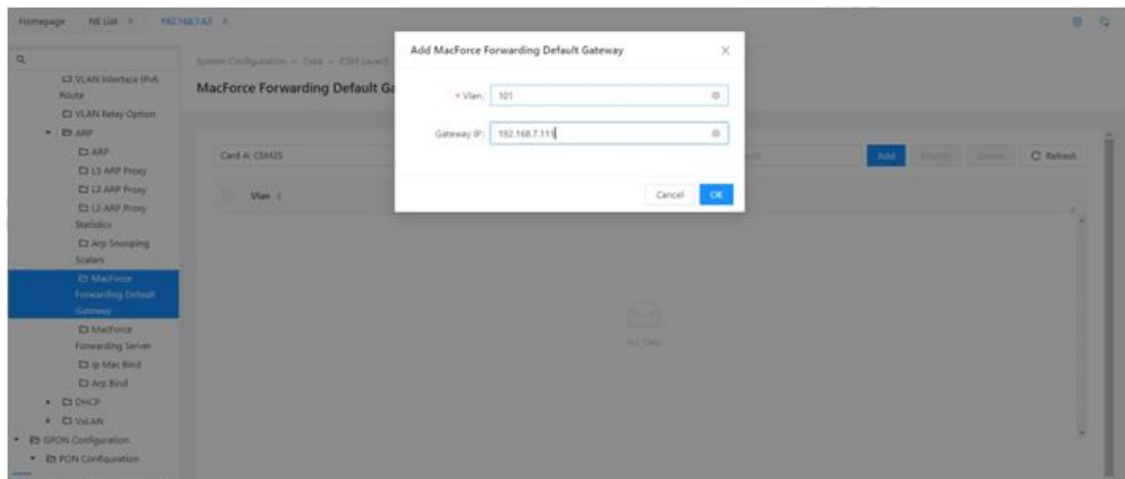


Note: ARP snooping must be enabled in advance.

13.3.1 MAC Forced Forwarding Default Gateway

【Operating Steps】

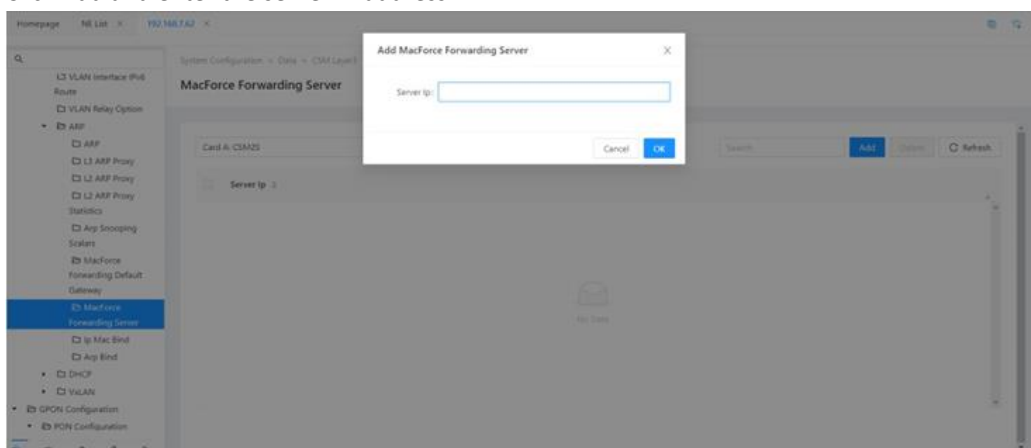
1. In the Device Manager main menu, click Data > ARP > Force Forwarding Default Gateway.
2. Click Add and enter the vlan and gateway IP address.



13.3.2 MAC Force Forwarding Server

【Operating Steps】

1. In the Device Manager main menu, click Data > ARP > Force Forwarding Default Server.
2. Click Add and enter the server IP address.

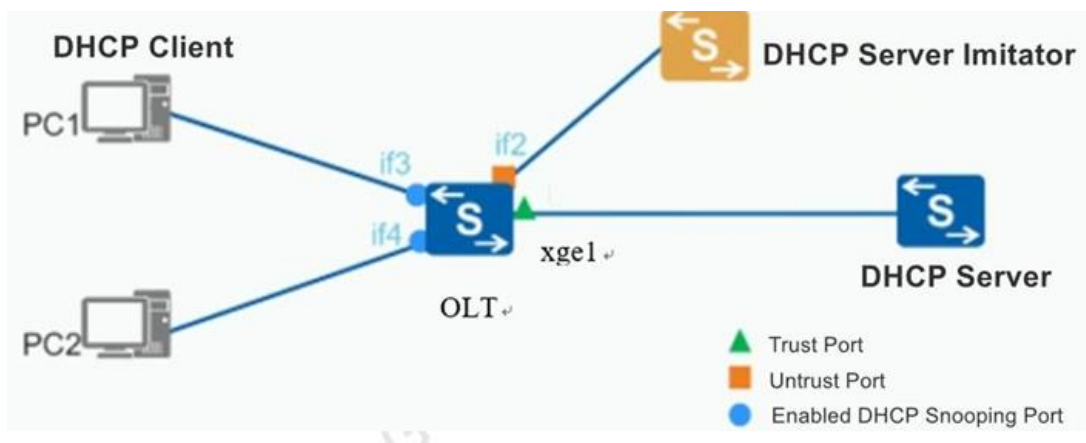


13.4 DHCP Snooping

DHCP Snooping is a security feature of DHCP, which can shield illegal DHCP servers in the access network. That is, when DHCP Snooping is enabled, clients in the network can only obtain IP addresses from DHCP servers specified by administrators. Due to the lack of authentication mechanism in DHCP packets, if there is an illegal DHCP server in the network, the administrator will not be able to ensure that the client gets the legal address from the DHCP server specified by the administrator, and the client may get the wrong IP address and other configuration information from the illegal DHCP server, resulting in the client can not use the network normally.

When DHCP Snooping is enabled, the ports on the device must be set to Trust and Untrust states, and the switch only forwards DHCP OFFER/ACK/NAK.

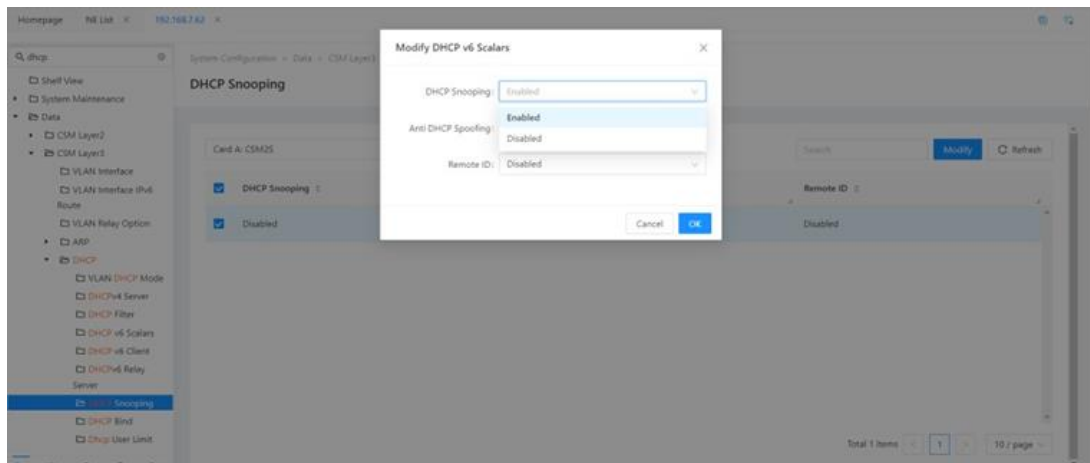
13.4.1 Topology Instances



13.4.2 Configuration Instance

【Operating Steps】

1. In the Device Manager main menu, click “Configuration Management > Data > CSM Layer 3 > DHCP > DHCP Snooping”.
2. Click “Modify”.
3. Enable DHCP Snooping.



14 System Management

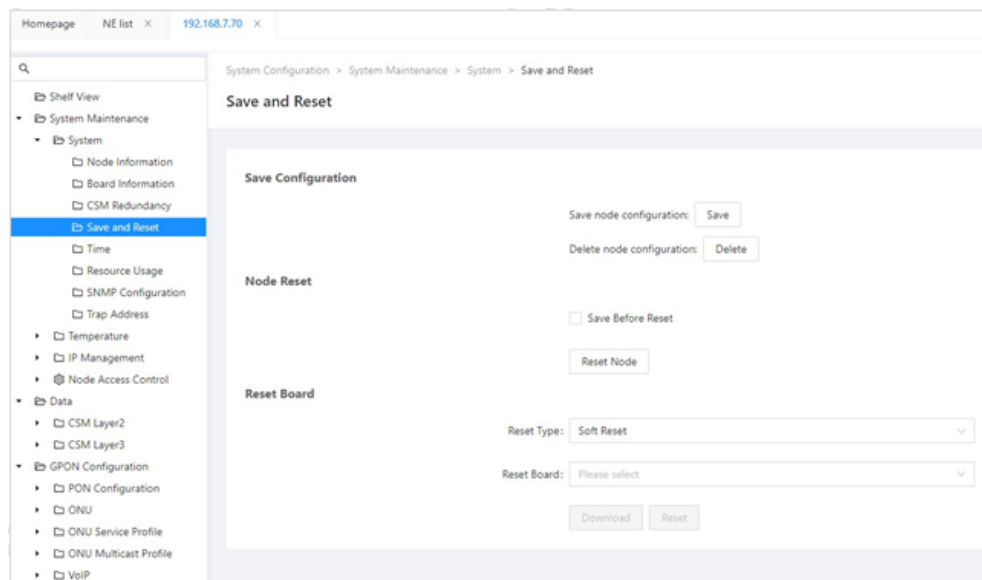
The following sections detail how to perform system management tasks:

- Save system configuration
- Reset the system
- Reset the line card
- Upgrade the system
- Active/standby switchover

14.1 Save System Configuration

Save the current system configuration to memory so that these configurations remain valid after the system reset. Otherwise, and all user configurations will fail after system reset.

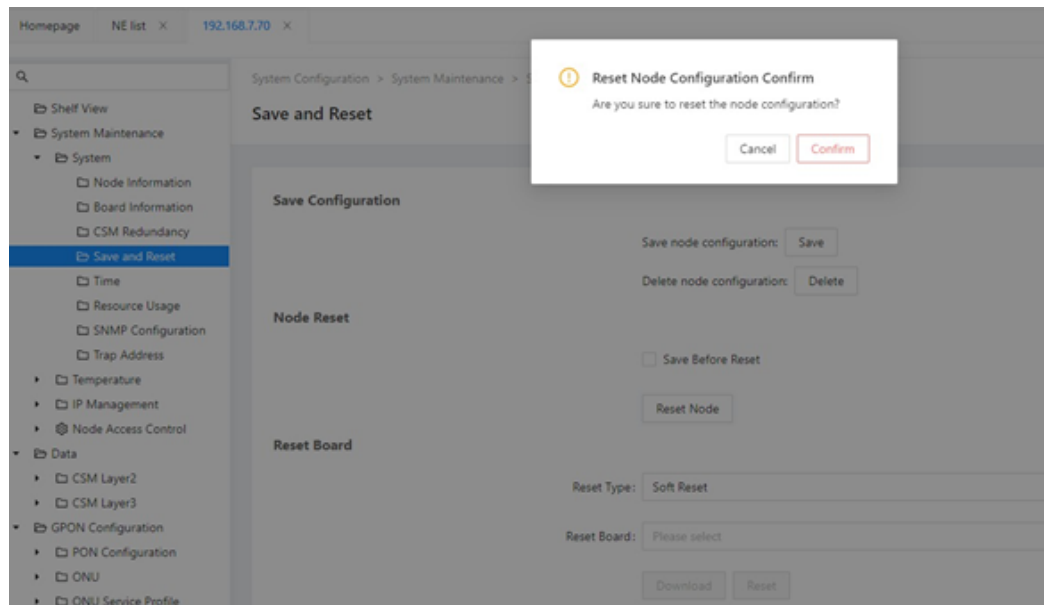
On the Device Manager main menu, click [System Maintenance\ System\ Save and Reset].



14.2 Reset System

【Operating Steps】

- Click [System Maintenance\System\Save and Reset] in the Function View navigation tree.
- Click <Reset Node>.

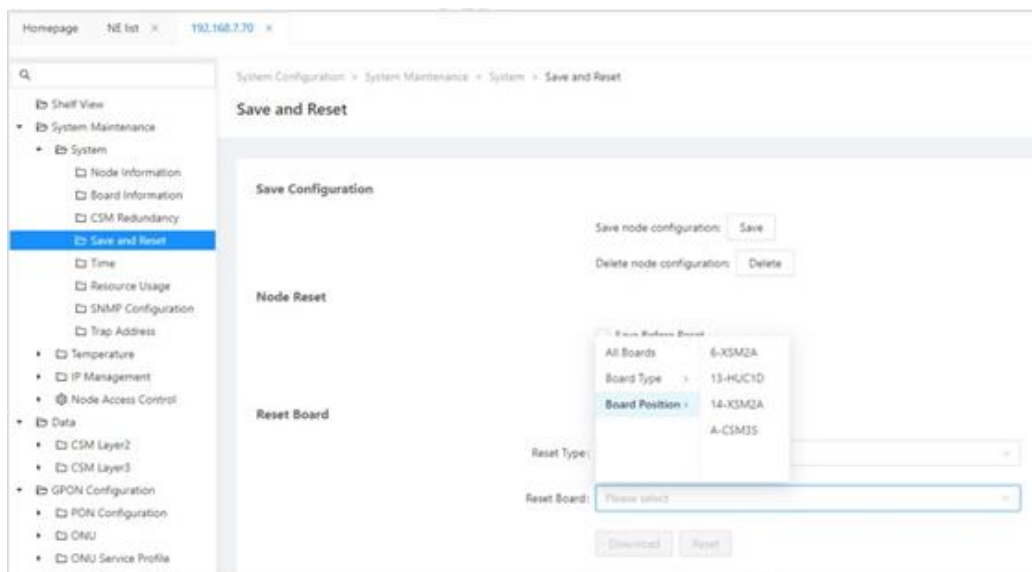


- Click <Submit> Restart the NE.

14.3 Reset Line Card

【Operating Steps】

In the Function View navigation tree, click [System Maintenance\ System\ Save and Reset]. Select the line card and click <Back>.

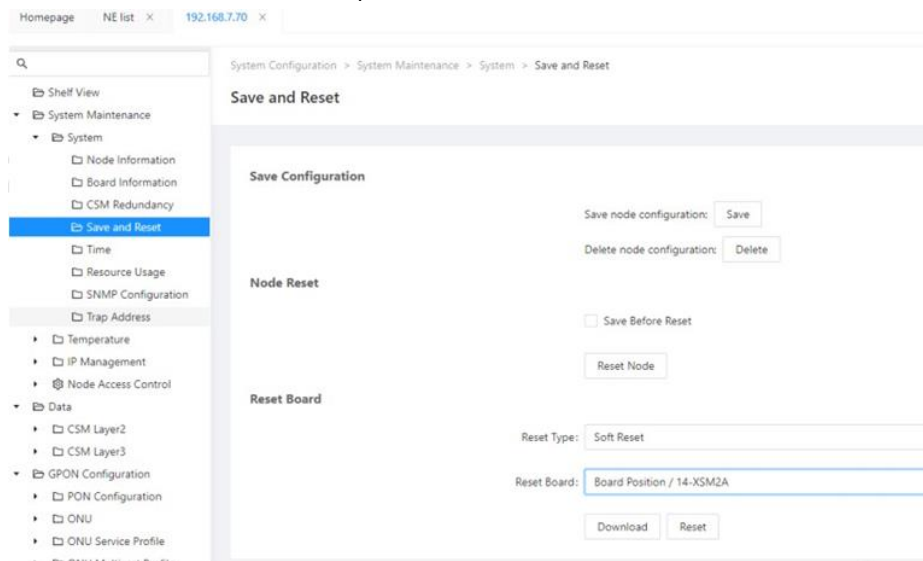


14.4 Upgrade System

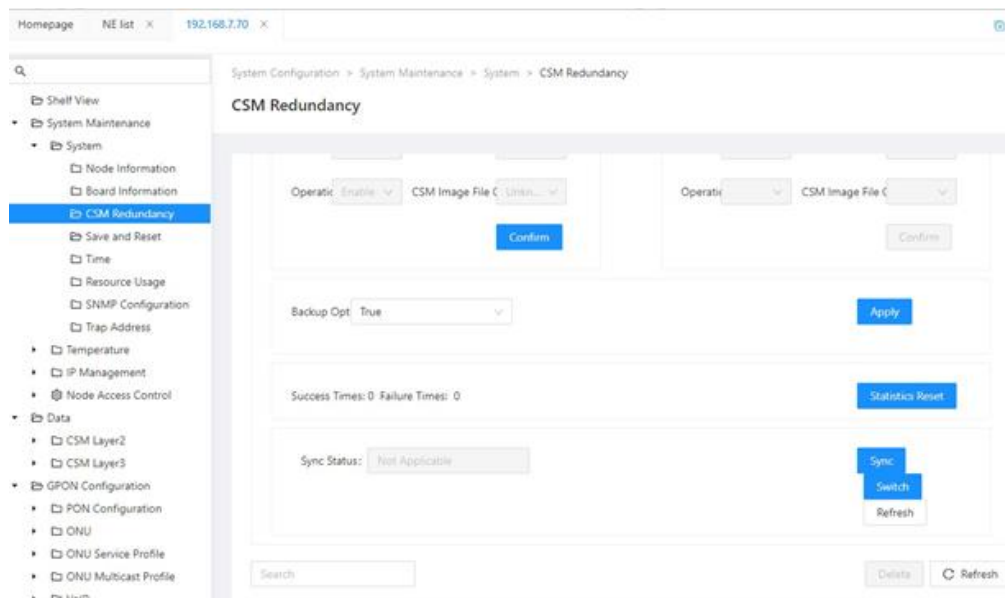
【Operating Steps】

- Backup the profile, sysconfig.gz.
- Download the image file "csm1g.gz".
- Download the line card image file, such as "gpn2.img".
- Upgrade line card.

In the Function View navigation tree, click [System Maintenance\System\Save and Reset]. Select the line card and click <Download>.Wait for the download to complete.



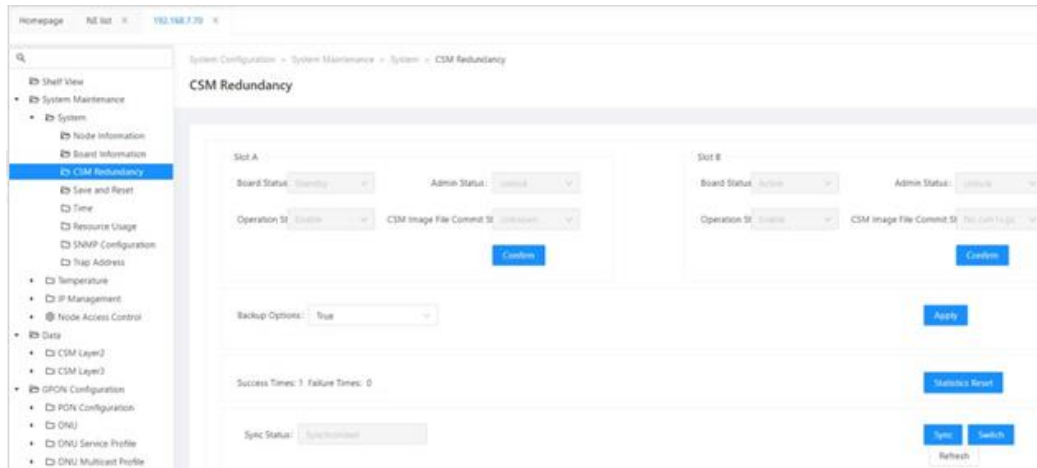
- Upgrade the master control, click [System Maintenance\ System\ CSM Backup], click <Confirm> to confirm Image File.Wait for the submission to complete.



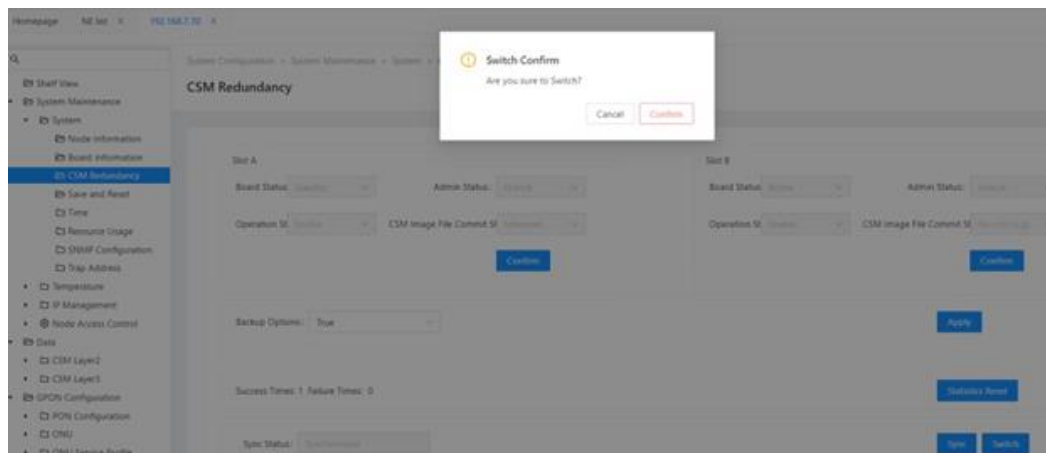
14.5 Active/Standby Switchover

【Operating Steps】

- In the Function View navigation tree, click [System Maintenance\ System\ CSM Redundancy].
- Click <Switch>.



- Click <Confirm>.



15 Alarm Management

This chapter describes how to configure an alarm and an alarm server:

- Configure TCA
- View the alarms and events

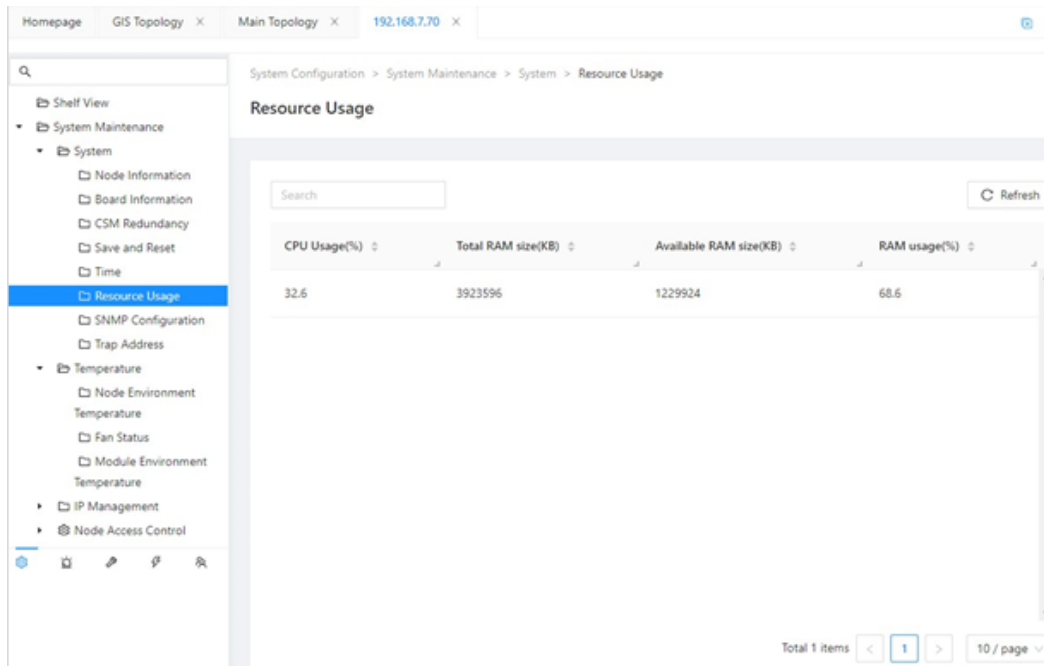
15.1 Configure TCA

The following threshold values for the OLT system are configurable:

- System resource management
- Temperature monitoring
- Uplink port optical module monitoring

15.1.1 System Resource Management

In the navigation tree, click [System Maintenance\ System\ Resource Usage].



The screenshot shows the 'Resource Usage' page in the AX3500 OLT web interface. The left navigation tree is expanded to 'System Maintenance' > 'System' > 'Resource Usage'. The main content area displays a table with resource usage statistics. The table has four columns: CPU Usage(%), Total RAM size(KB), Available RAM size(KB), and RAM usage(%). The values shown are 32.6, 3923596, 1229924, and 68.6 respectively. There is a search bar and a refresh button at the top of the table. At the bottom, it shows 'Total 1 items' and a pagination control for '10 / page'.

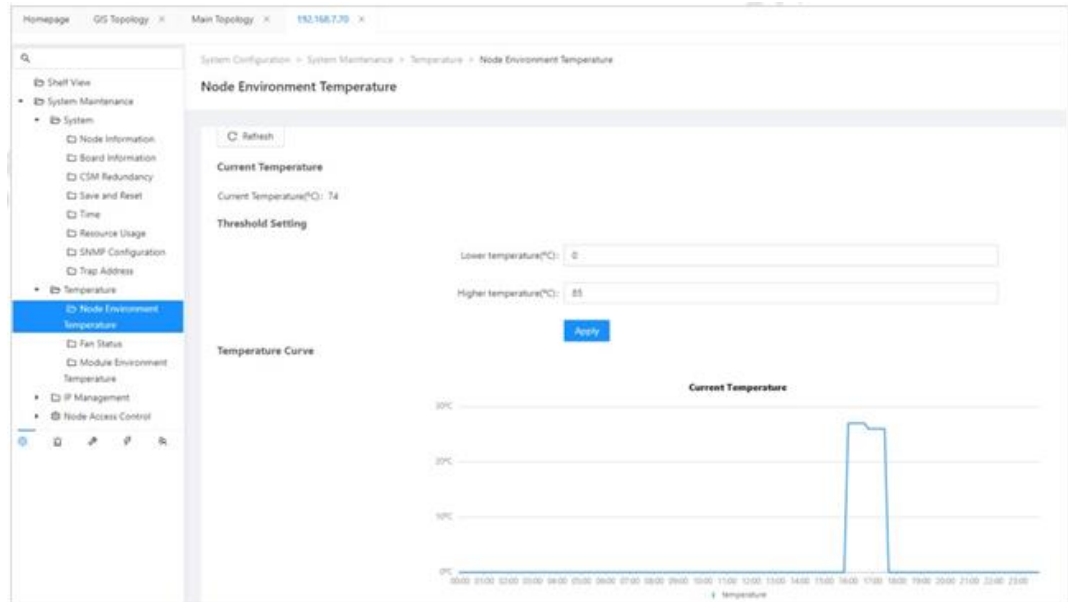
CPU Usage(%)	Total RAM size(KB)	Available RAM size(KB)	RAM usage(%)
32.6	3923596	1229924	68.6

15.1.2 Temperature Monitoring

15.1.2.1 Node Environment Temperature

【Operating Steps】

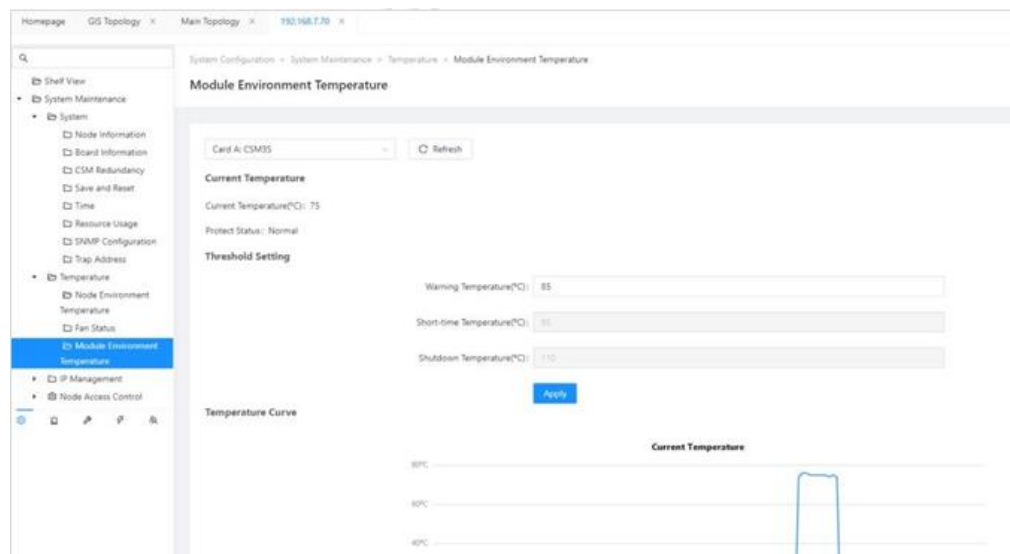
- Click [System Maintenance\Temperature\ Node Environment Temperature] in the Function View navigation tree.
- Modify the alarm threshold required to be changed, click <Apply>.



15.1.2.2 Module Temperature Management

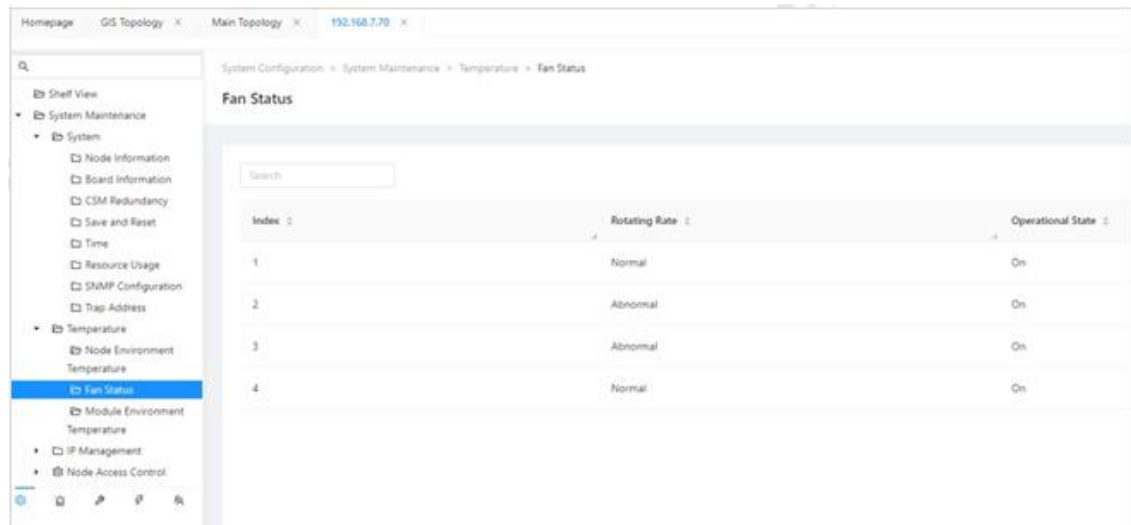
【Operating Steps】

- Here, click [System Maintenance/Temperature/Mouldle Temperature Management] in the Function View navigation tree.



15.1.2.3 Fan Temperature Management

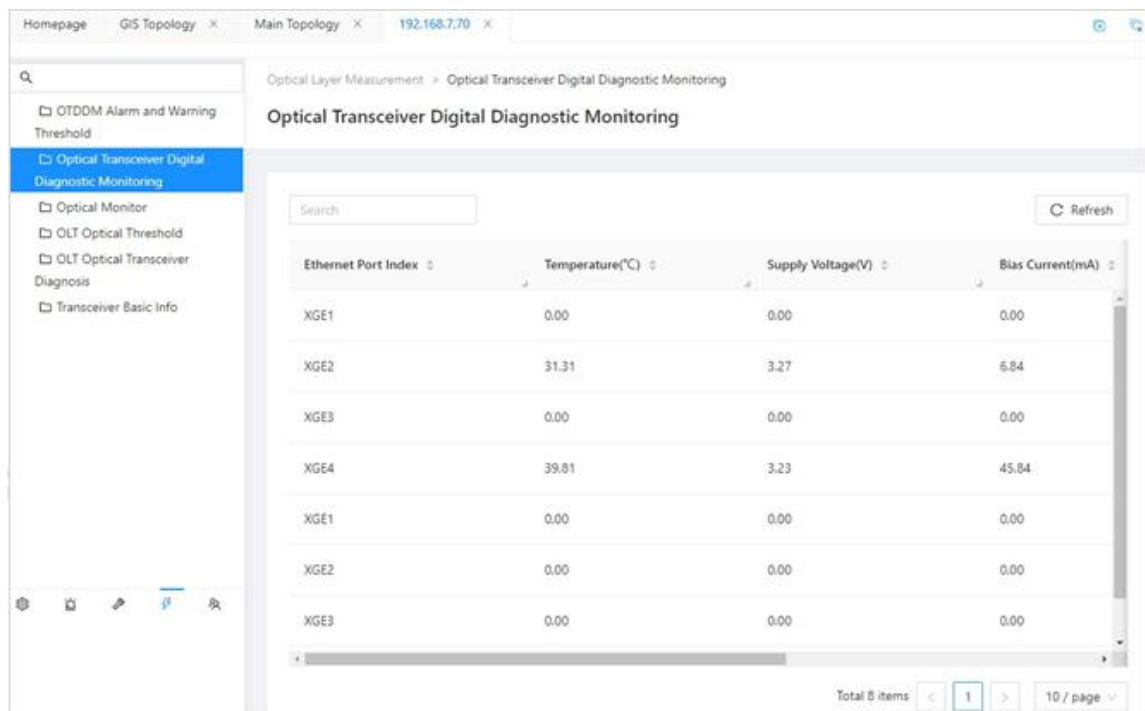
In the Function View navigation tree, click [System Maintenance\ Temperature\ Fan Status].



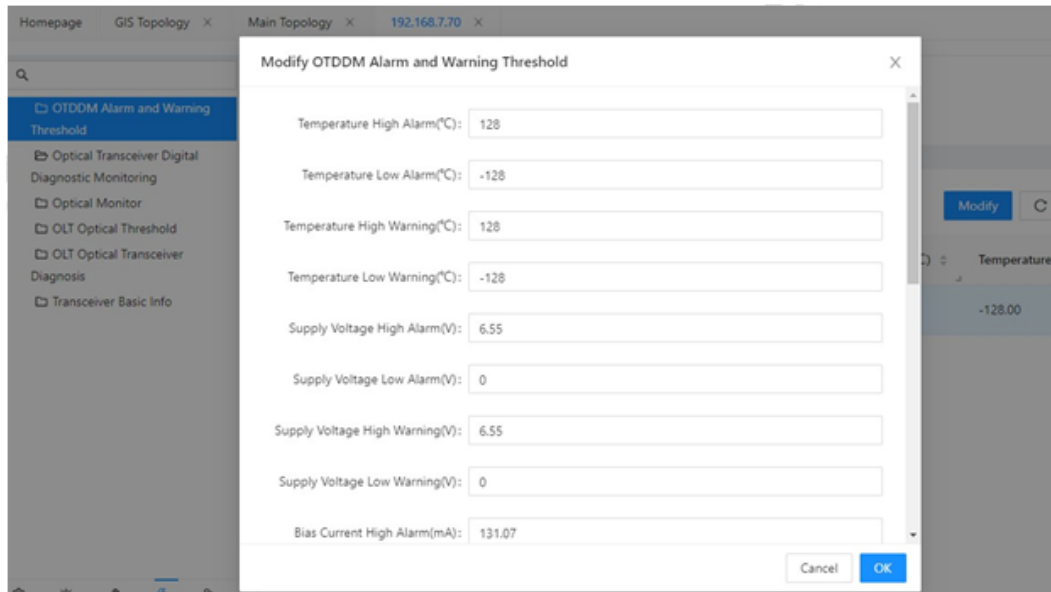
15.1.3 Uplink Port Optical Module Monitoring

【Operating Steps】

- Click [Optical Transceiver Digital Diagnostic Monitoring] in the Optical Layer Measurement navigation tree. View the uplink port optical module parameter information.



- Click [OTDDM Alarm and Warning Threshold] in the Function View navigation tree.



- Modify the alarm threshold required to be changed, click <OK>.

15.2 View Alarms and Events

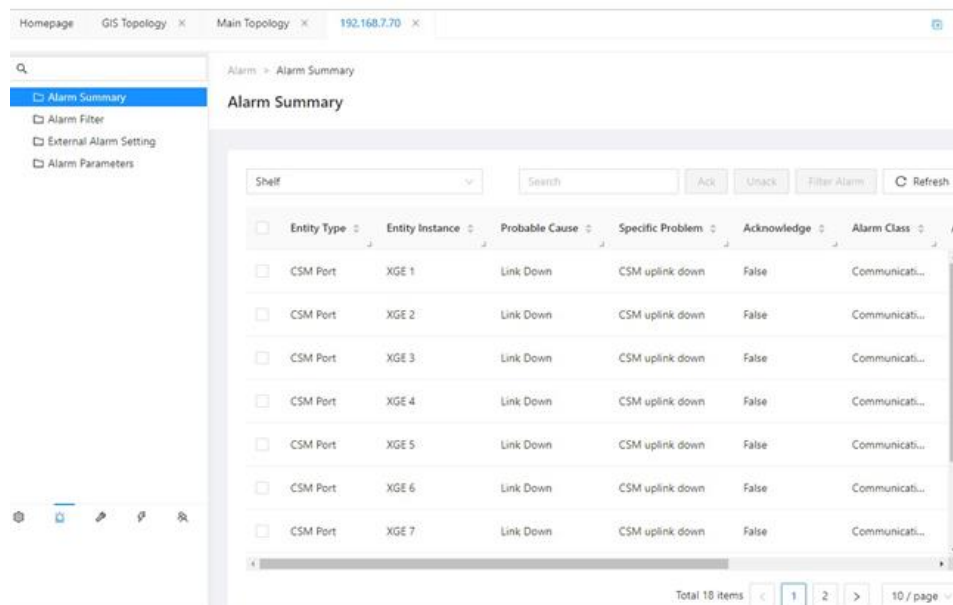
Users can view the current, historical, and event logs of the OLT.

15.2.1 View Current Alarm

An alarm is a notification generated by the system for detecting a fault. The alarm exists at some point until the fault is fixed, or the alarm is removed manually. Through this task view the current alarm information, and you can confirm the current alarm.

【Operating Steps】

- In the Alarm navigation tree, click [Alarm Summary].

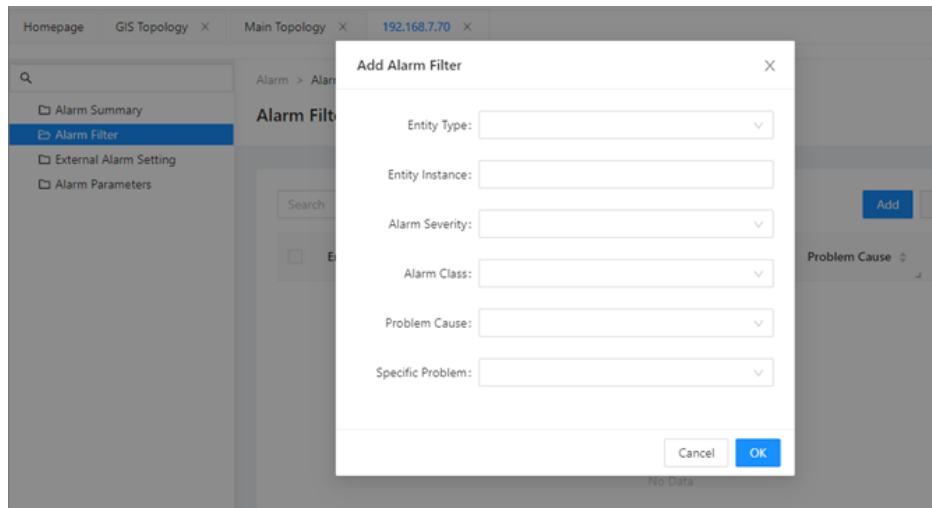


- On the “Alarm Summary” interface, you can browse the current alarm.
- Select an alarm, and click “Alarm Filter”, to set up the alarm filtering.

15.2.2 Configure Alarm Filtering

Set the filter conditions to view the alarms you pay close attention to. [Operating Steps].

- In the “Alarm” navigation tree, click [Alarm Filter].
- Click “Add” to add the alarm filtering parameter.



- Click <OK> to save configuration.

16 External Alarm Input/Output

16.1 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.

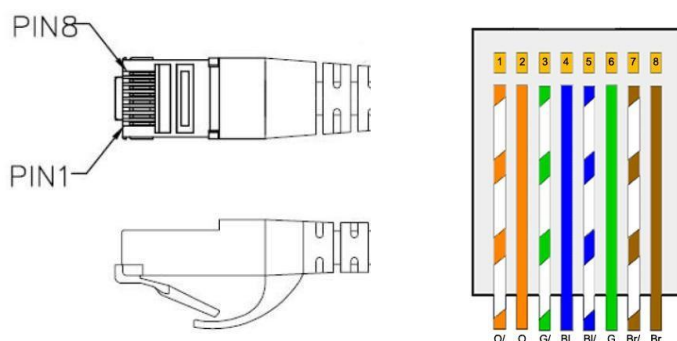
16.2 Product Specifications

- The AX3508/AX3515/AX3517 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.

16.3 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)



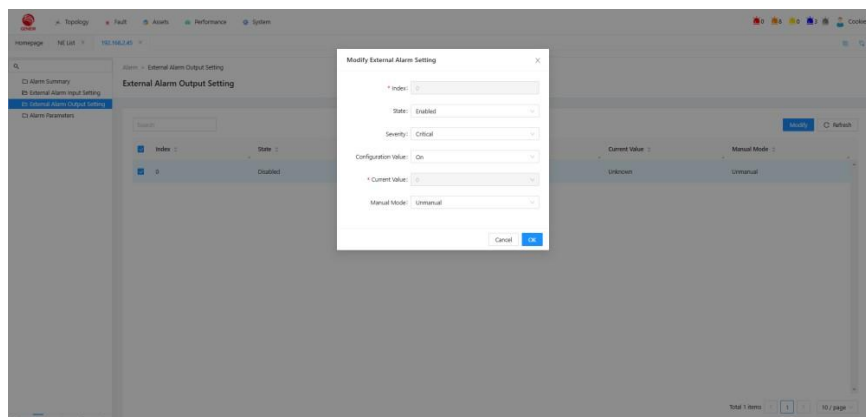
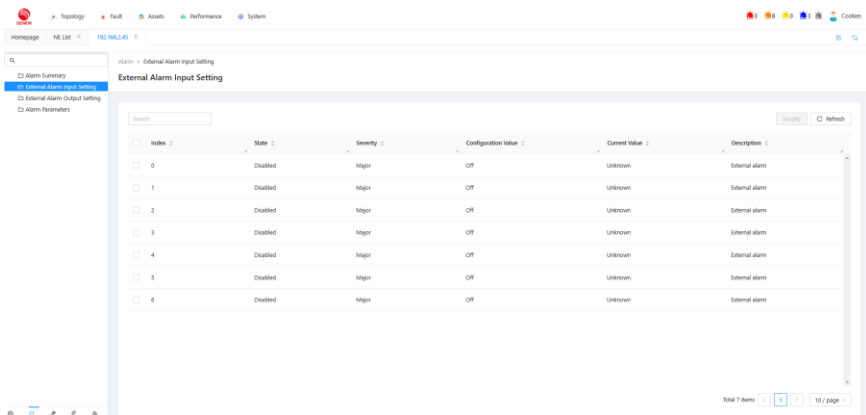
16.3.1 Configure Alarm Input

【Operating Steps】

- Click the alarm in the bottom left corner of the main page.



- Click the alarm in the bottom left corner of the main page.

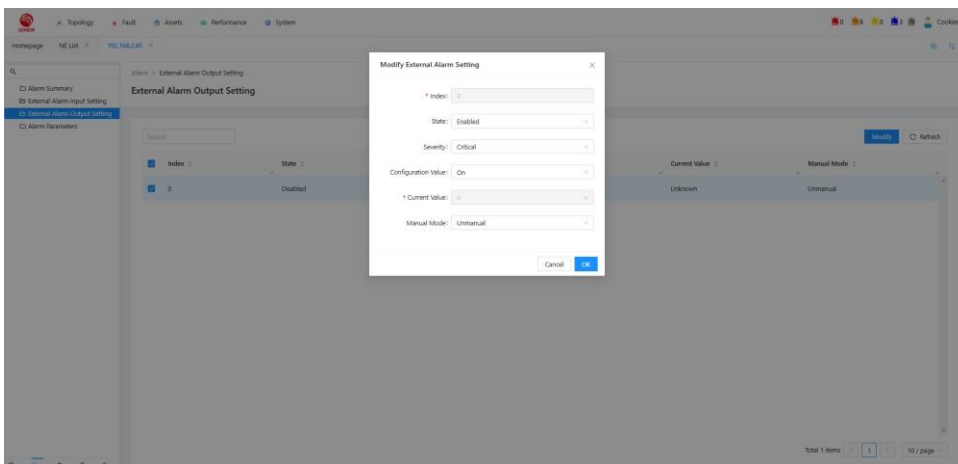
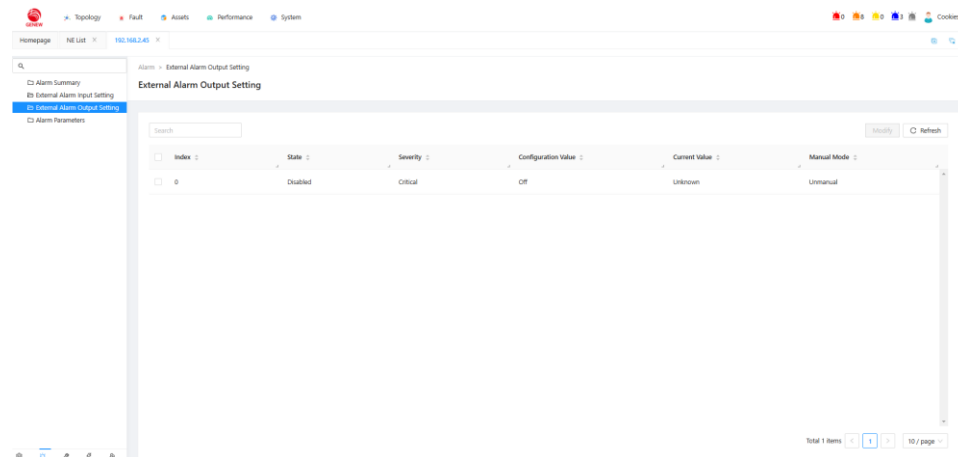


16.3.2 Configure Alarm Output

【Operating Steps】

Click “Alarm>External Alarm Output Setting”.

The input and output ports will be monitored every minute, and alarms will be reported or cleared Accordingly.



16.3.3 Querying Alarms

- Query alarm information.
- Click “Alarm>Alarm Summary”.

Entity Type	Entity Instance	Probable Cause	Specific Problem	Acknowledge	Alarm Class	Alarm Severity	Occur Time	Addition Text	Slave Name
CSM Port	1-A-RGE 2	Link down	CSM uplink down	False	Communication	Major	2000-05-25 08:48:17		
CSM Port	1-A-RGE 3	Link down	CSM uplink down	False	Communication	Major	2000-05-25 08:48:17		
CSM Port	1-A-RGE 4	Link down	CSM uplink down	False	Communication	Major	2000-05-25 08:48:17		
CSM Port	1-A-RGE 5	Link down	CSM uplink down	False	Communication	Major	2000-05-25 08:48:17		
CSM Port	1-A-RGE 6	Link down	CSM uplink down	False	Communication	Major	2000-05-25 08:48:17		
CSM Port	1-A-RGE 7	Link down	CSM uplink down	False	Communication	Major	2000-05-25 08:48:17		
CSM Port	1-A-RGE 8	Link down	CSM uplink down	False	Communication	Major	2000-05-25 08:48:18		
Module	1-P1	Module renewal	Assigned module is miss...	False	Equipment	Major	2000-05-25 08:49:50		

17 Performance Statistics

All types of data received and sent on Ethernet ports, OLT ports, and ONU ports are counted through the following three performance counters.

- Ethernet port counter
- The OLT port counter

These 2 counters count the number of frames or packets accumulated to the current period since the previous system restart. The counter takes a 64-bit integer (counter 64) with a maximum value of 264, and resets back to 0 once the counter reaches the maximum value.

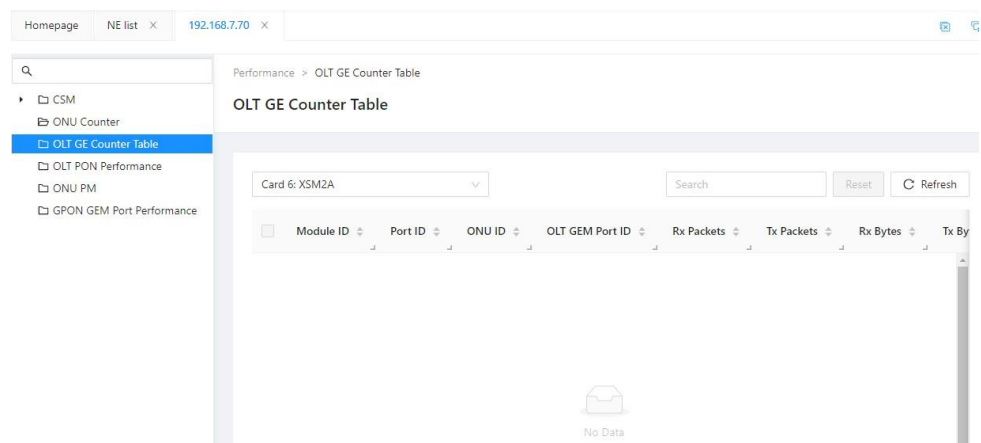
17.1 Ethernet Port Performance Statistics

In the Performance Monitoring navigation tree, click [CSM/Statistics].

Port Index	Rx Total Octets	Rx Total Frames	Rx Multicast Frames	Rx Broadcast Frames	Rx Pause Frames
IS 1/1	0	0	0	0	0
IS 1/2	0	0	0	0	0
IS 1/3	0	0	0	0	0
IS 1/4	0	0	0	0	0
IS 2/1	0	0	0	0	0
IS 2/2	0	0	0	0	0
IS 2/3	0	0	0	0	0

17.2 OLT Port Performance Statistics

In the Performance Monitoring Navigation tree, click [OLT GE Counter Table].





Ascent Communication Technology Ltd

AUSTRALIA

140 William Street, Melbourne
Victoria 3000, AUSTRALIA
Phone: +61-3-8691 2902

Hong Kong SAR

Room 1210, 12th Floor, Wing Tuck Commercial Centre
181 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_Device_Operation_QRG_V1b_Jun_2024