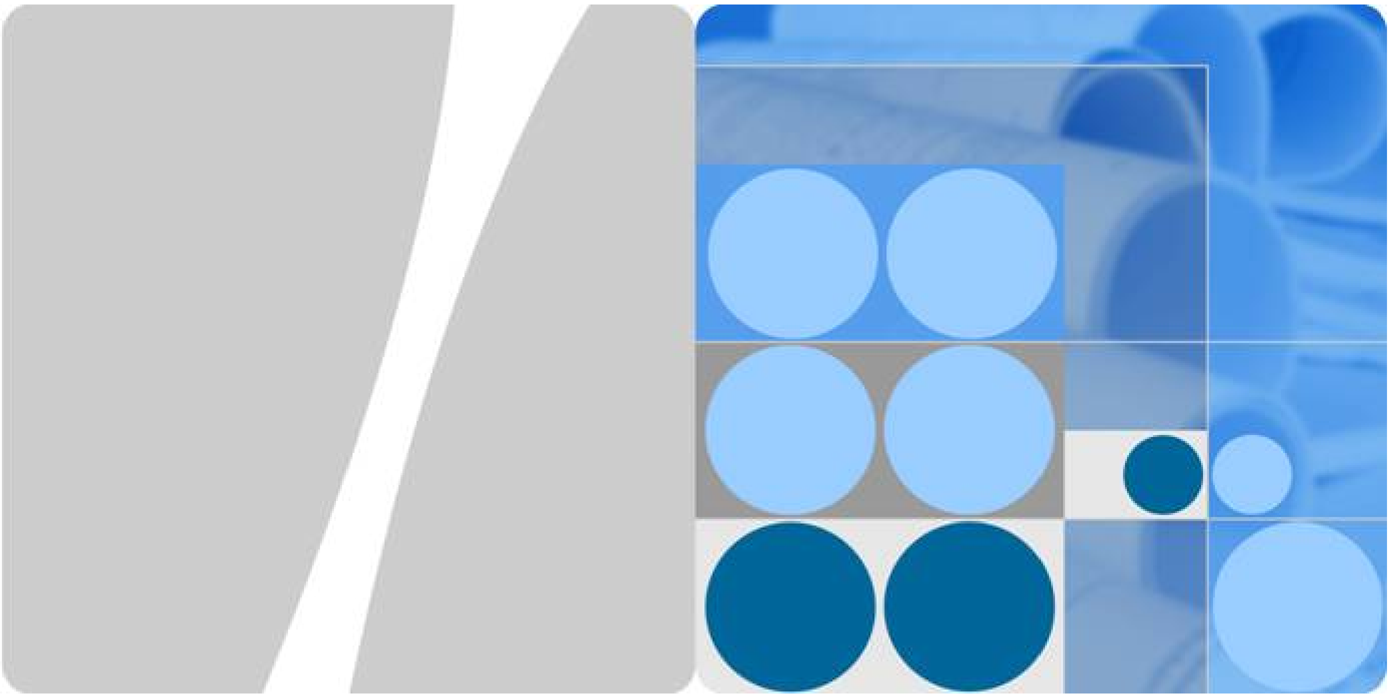


iManager U2000 Unified Network Management System

V200R014C60

Operation Guide for OLT NE Management

Issue 01

Date 2015-02-28

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2015. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Related Version

The following table lists the product version related to this document.

Product Name	Version
iManager U2000	V200R014C60

Intended Audience

This document describes the functions and services provided by the OLT. After you read this document, you should be able to know how to operate the OLT and configure services through the U2000.

The document is intended for:

- Data configuration engineers
- NM administrators
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Symbol	Description
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
⚠ NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
📖 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A maximum of all or none can be selected.

GUI Conventions

The GUI conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue 01 (2015-02-28) Based on Product Version V200R014C60

Initial release for V200R014C60 version.

Contents

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

1 OLT Series NE and Service Overview

NE Overview

OLTs refer to the following NEs: MA5600T, MA5603T, MA5608T, MA5680T, MA5683T, MA5606T, and MA5603U.

As optical-copper access NEs, MA5600Ts, MA5603Ts, and MA5608Ts provide high-rate, wide-bandwidth, high-quality, broadband and narrowband combo, and optical-copper access services. MA5600Ts, MA5603Ts, and MA5608Ts can:

- Function as OLTs in a 10G GPON, GPON, or EPON system and work with ONTs or ONUs to achieve multiservice bearing.
- Function as DSLAM NEs and support different broadband access services (including ADSL2+, VDSL2, and SHDSL) to enhance xDSL line functions.
- Function as MSAN NEs and provide SIP- and H.248-based voice services and POTS ports to support voice services, fax services, narrowband modem services, and a lot of supplementary services.
- Function as MDUs when MA5600Ts, MA5603Ts, or MA5608Ts are cascaded to other upstream OLTs.

As GPON and EPON access products, MA5680Ts and MA5683Ts can function as OLTs in a 10G GPON, GPON, or EPON system and work with ONTs or ONUs to achieve multiservice bearing.

MA5800s are multi-service access devices. They support large-capacity NGPON and NGPON2 and act as head-end aggregation devices on SDN access networks.

- MA5800s support GPON, 10G GPON, and P2P access.
- MA5800s apply to FTTB, FTTC, and FTTD networks and can act as aggregation MDUs.
- MA5800s apply to the FTTH networks based on GPON, 10G GPON, and P2P access.
- In the Distributed Converged Cable Access Platform (D-CCAP) solution, MA5800s can act as D-CCAP office devices and aggregation D-CCAP optical sites.
- As CO head-end aggregation devices, MA5800s support multiple networking modes and any media and serve family, mobile, and enterprise users, thereby realizing heterogeneous access networks.

As small multi-service access NEs, MA5606Ts can:

- Mainly function as mini DSLAM NEs and provide small-capacity subscriber services using ADSL2+, ADSL, G.SHDSL, VDSL2, or P2P FE.
- Function as OLTs in a GPON system and work with ONTs or ONUs to support the fiber to the home (FTTH) solution.
- Function as MDUs in a GPON system, provide GPON-upstream transmission, and work with OLTs to support FTTx solutions.

As middle multi-service access NEs, MA5603Us can:

- Function as OLTs in a GPON system and work with ONTs or ONUs to support the FTTH solution.
- Support VDSL2 and POTS combo access.
- Cascade over IP DSLAM NEs through Ethernet ports.

Service Configuration Description

MA5600Ts, MA5603Ts, MA5608Ts, MA5606Ts, and MA5603Us are multiservice access NEs. They can function as DSLAM and MSAN NEs as well as OLTs.

To learn how to configure GPON, EPON, xDSL, and voice services supported by these series of NEs, see "OLT NE Management."

- If these series of NEs function as OLTs, refer to "FTTx O&M" for E2E service configuration for OLTs and ONUs on an FTTx network.
- To learn configuration for single NEs, see "OLT NE Management."
- If these series of NEs function as DSLAM and MSAN NEs, refer to "OLT NE Management" for xDSL and voice service configuration.

Service Overview

Feature		**MA5600T**	**MA5603T**	**MA5608T**	**MA5680T**	**MA5683T**	**MA5606T**	**MA5603U**	**MA5800**
Upstream transmission mode	GE-upstream	√	√	√	√	√	√	√	√
	10 GE-upstream	√	√	√	√	√	×	√	√
	E1-upstream	√	√	√	×	×	×	×	×
	T1-upstream	√	√	√	×	×	×	×	×
	GPON-upstream	√	√	√	√	√	√	×	×
	EPON-upstream	√	√	√	√	√	√	×	×
	STM-1-upstream	√	√	√	×	×	×	×	×
Access mode	EPON access	√	√	√	√	√	×	×	×

Feature		**MA5600T**	**MA5603T**	**MA5608T**	**MA5680T**	**MA5683T**	**MA5606T**	**MA5603U**	**MA5800**
	10G EPON access	√	√	√	√	√	×	×	×
	GPON access	√	√	√	√	√	×	√	√
	10G GPON access	√	√	√	√	√	×	×	√
	Ethernet access	√	√	√	√	×	√	√	√
	P2P optical access	√	√	√	√	√	√	×	√
	ADSL2+ access	√	√	√	×	×	√	×	×
	VDSL2+ access	√	√	√	×	×	√	√	×
	G.SHDSL access	√	√	√	×	×	√	×	×
	TDM G.SHDSL access	√	√	√	×	×	×	×	×
	Vectoring access	√	√	√	×	×	×	×	×
	POTS access	√	√	√	×	×	√	×	×
	ISDN BRA access	√	√	√	×	×	√	×	×
	ISDN PRA access	√	√	√	×	×	√	×	×
	ATM access	√	√	×	×	×	×	×	×
	VDSL2 and POTS combo access	√	√	√	×	×	×	√	×
	RF access	√	√	√	√	√	×	×	√
Key service feature	D-CMTS management	√	√	√	√	√	×	×	√
	MPLS feature	√	√	√	√	√	×	×	×
	VPLS feature	√	√	√	√	√	×	×	×
	VPWS feature	√	√	√	√	√	×	×	×

Feature		**MA5600T**	**MA5603T**	**MA5608T**	**MA5680T**	**MA5683T**	**MA5606T**	**MA5603U**	**MA5800**
	Multicast feature	√	√	√	√	√	√	√	√
	Voice feature (MGCP)	√	√	√	×	×	√	×	×
	Voice feature (H.248)	√	√	√	×	×	√	×	×
	Voice feature (SIP)	√	√	√	×	×	√	×	×

2 Basic Configurations

About This Chapter

Basic configurations mainly include certain common configurations and public configurations. There is no obvious logical relation between basic configurations. You can perform basic configurations according to actual requirements.

The quality of service (QoS) provides the user services with the end-to-end quality assurance by setting different measurement indicators, such as the service availability, throughput, delay, jitter, and loss rate. The OLT provides the high QoS assurance by supporting the traffic classification, traffic statistics, and schedule policy of the traffic rules.

This topic describes how to specify the clock signals of a port as the system clock source so that the entire system uses a same clock reference. The clock source may be an external BITS clock or a line clock of the upper-level node. The clock module automatically checks the types (BITS, TDM, or SDH) of the specified clock sources, and then locks the clock source with the highest priority as the system clock source.

System security configuration aims to prevent devices from being attacked by unauthorized packets that are transmitted from the network side or the user side. System security configuration ensures that the devices on the network run in the normal state.

This topic introduces the user security function and describes how to configure it in the OLT.

This topic describes how to configure the card with the active/standby switchover for the upstream service so that the stability of the service is guaranteed.

By means of file operations, you can save the records as a file, preview the file printing effect, and print the file. In this case, you can save and analyze the relevant information of the U2000.

This topic describes how to synchronize the NE data, NE time, NE alarms and system parameter profile so that the data of the NE and the data on the U2000 are the same.

2.8 Saving the Data

After saving the data to the flash memory of a device, you can query the data information to maintain and manage the device. Saving the data prevents data loss in case of unexpected restart.

2.9 Detecting the Network

This topic describes how to check the connectivity of a network and whether the host is reachable, and how to check all gateways passed by data packets sent from a source host to the destination host. In addition, this operation helps you to locate network faults and log in to the device through the network remotely to configure and maintain the device.

2.1 Configuring the QoS Policy

The quality of service (QoS) provides the user services with the end-to-end quality assurance by setting different measurement indicators, such as the service availability, throughput, delay, jitter, and loss rate. The OLT provides the high QoS assurance by supporting the traffic classification, traffic statistics, and schedule policy of the traffic rules.

Context

- The access control list (ACL) is used to filter the specific data packets by setting the filter criteria. In this way, the required objects can be displayed. After the required objects are displayed, network devices can permit or refuse the matching data packets to pass with the matching rules.
- The QoS processes the packets filtered by the ACL according to the user requirement, which is the vital function of the ACL.
- In the OLT, the ACL can be classified into the standard ACL, extended ACL, L2 ACL, and customized ACL. **Table 2-1** lists the ACL classification.

Table 2-1 ACL classification

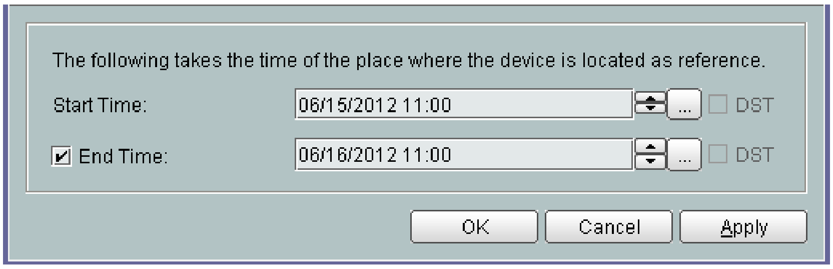
Item	Range	Feature
Standard ACL	2000-2999	Defines ACL rules according to only the L3 source IP address, and analyzes and processes the data packets.
Extended ACL	3000-3999	Defines ACL rules according to the source IP address and destination IP address of the data packets, protocol type carried by the IP network, features of the protocol (such as the source port and destination port of the TCP, ICMP type, and code). With the extended ACL, rules more exact, rich, and flexible can be defined.
L2 ACL	4000-4999	Defines ACL rules according to the information about the link layer, such as the source MAC address, source VLAN ID, L2 protocol type, and destination MAC address, and analyzes and processes the data.
Customized ACL	5000-5999	Performs matching according to the 32 bytes of the former 80 bytes of the L2 data frames at random, and processes the data packets.

Procedure

Step 1 Add the time range.

Copyright © Huawei Technologies Co., Ltd.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **QoS** > **QoS&ACL** from the navigation tree.
3. Click the **Time Segment Management** tab, right-click the list, and then choose **Add**.
4. In the dialog box that is displayed, set the name of the time range.
5. Click **OK**.
6. Select the added time record, click the **One-off Time** tab or the **Periodic Time** tab in the lower pane. In the information list, right-click and choose **Add** from the shortcut menu.
7. In the dialog box that is displayed, set the parameters.
   - In the **Add One-off Time** dialog box, set **Start Time** and **End Time** of the time range.

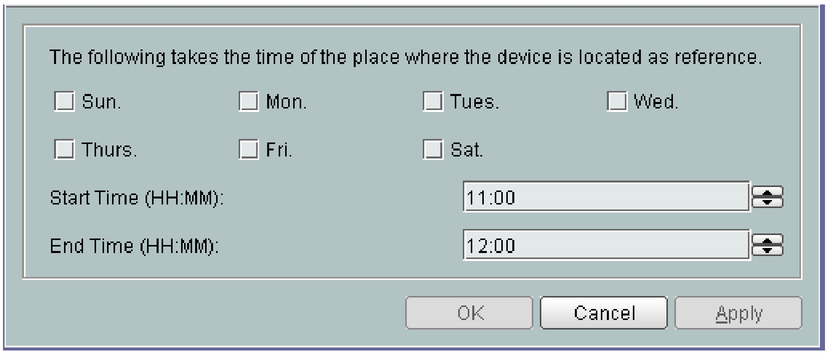


The following takes the time of the place where the device is located as reference.

Start Time: 06/15/2012 11:00 ☐ DST

☑ End Time: 06/16/2012 11:00 ☐ DST

   - In the **Add Periodic Time** dialog box, set the period, **Start Time**, and **End Time** of the time range.



The following takes the time of the place where the device is located as reference.

☐ Sun. ☐ Mon. ☐ Tues. ☐ Wed.

☐ Thurs. ☐ Fri. ☐ Sat.

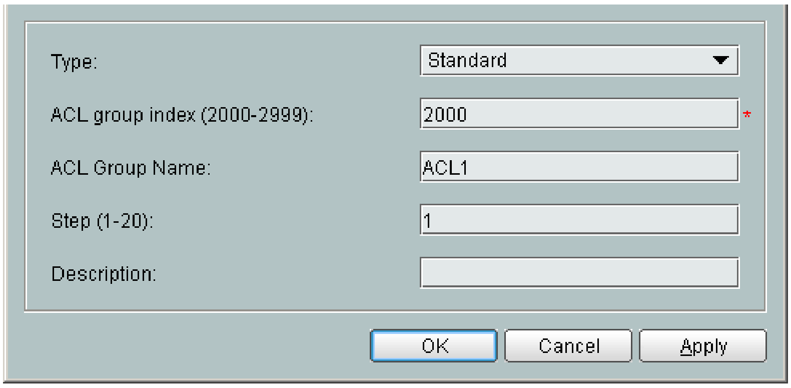
Start Time (HH:MM): 11:00

End Time (HH:MM): 12:00

8. Click **OK**.

Step 2 Add an ACL group. The following uses the standard ACL group as an example.

1. Click the **ACL Management** tab, set the filter criteria to display the records, right-click the list, and then choose **Add**.
2. In the dialog box that is displayed, set the parameters.



Type: Standard

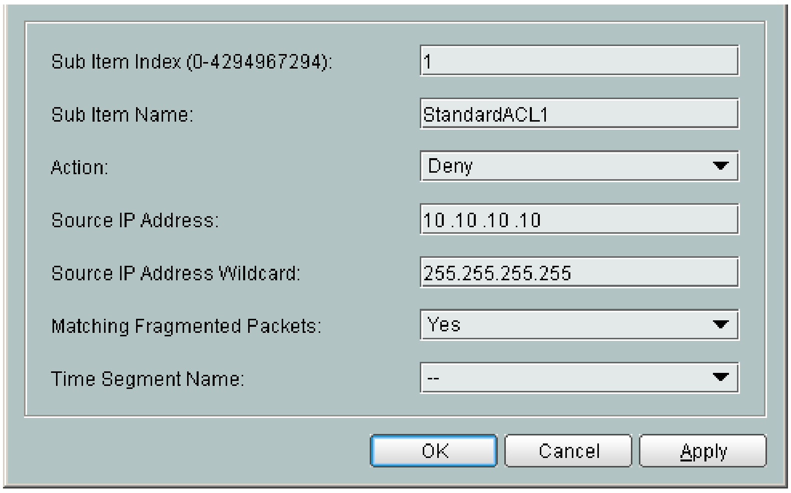
ACL group index (2000-2999): 2000 *

ACL Group Name: ACL1

Step (1-20): 1

Description:

3. Click **OK**.
4. Select the added ACL, and then click the **Standard Sub Item** tab in the lower pane. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



Sub Item Index (0-4294967294): 1
Sub Item Name: StandardACL1
Action: Deny
Source IP Address: 10 .10 .10 .10
Source IP Address Wildcard: 255.255.255.255
Matching Fragmented Packets: Yes
Time Segment Name: --

6. Click **OK**.

Step 3 Add the QoS rule. The following uses adding rules in batches as an example.

1. Click the **QoS Management** tab, set the filter criteria to display the records, right-click the list, and then choose **Batch Add** > **Packet Filtering**.
2. In the dialog box that is displayed, set the parameters.

   There are three steps for adding packets filtering, that is, select the port, select the ACL rule, and fill in the packets filtering parameter. The specific operations are as follows:

   - Select the port to be bound, and then click **Next**.
   - Select the referenced ACL rule, and then click **Next**.
   - Select the packets filtering parameter, that is, the direction for packets filtering.
3. Click **Finish**.

----End

2.2 Setting the System Clock

This topic describes how to specify the clock signals of a port as the system clock source so that the entire system uses a same clock reference. The clock source may be an external BITS clock or a line clock of the upper-level node. The clock module automatically checks the types (BITS, TDM, or SDH) of the specified clock sources, and then locks the clock source with the highest priority as the system clock source.

2.2.1 Introduction to the Clock System

When configuring the system clock, restrict the clock frequency and the phase of each node in a network within the predefined tolerance scope. This prevents transmission performance degradation caused by poor timings at both Tx and Rx ends.

Context

The OLT supports the frequency synchronization and the phase synchronization (also called time synchronization) of the clock.

In the digital network that is composed of the OLT and other devices, clock synchronization is a fundamental requirement. Clock synchronization aims to restrict the clock frequency and the phase of each node in a network within the predefined tolerance scope. This prevents transmission performance degradation caused by poor timings at both Tx and Rx ends.

The methods for clock synchronization on the digital network are as follows: pseudo synchronization and master/slave synchronization.

- Pseudo synchronization: The digital switch offices of a digital switch network have clocks that are independent of one another. These clocks, usually cesium atomic clocks, have high accuracy and stability. Although these clocks are not synchronous (in frequency and phase), the time difference between them is small, that is, they are almost synchronous. Therefore, these clocks are in pseudo synchronization. Pseudo synchronization is mainly used in international digital networks, that is, between the digital networks of different countries.
- Master/slave synchronization: The digital switch network has a master clock configured with a clock of high accuracy. The digital switch offices of the digital switch network are under the control of the master clock. That is, these offices trace the master clock, and use the clock as the clock source. A lower layer office, including the end terminal office, uses the clock of its upper layer office as the clock source.

Generally, the OLT uses master/slave clock synchronization. Clock synchronization is implemented in the following way:

1. The OLT obtains the clock signals of the upper layer device from the line as the system clock sources, and uses the system clock source with the highest priority as the system clock.
2. The OLT sends the system clock signals to the service cards through the backplane.
3. The service cards send the clock signals further to the lower layer network elements (NEs).

2.2.2 Setting the Global Parameters of a Time Clock Source

This topic describes how to specify the clock signals of a specified port as the system clock source. OLT supports a maximum of 10 clock sources.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Clock Management** > **PTP Clock** from the navigation tree.

Step 3 In the information list, set the parameters and then click **Apply**.

----End

2.2.3 Adding a Frequency Clock Source

This topic describes how to specify the clock signals of a specified port as the system clock source. OLT supports a maximum of 10 clock sources.

Procedure

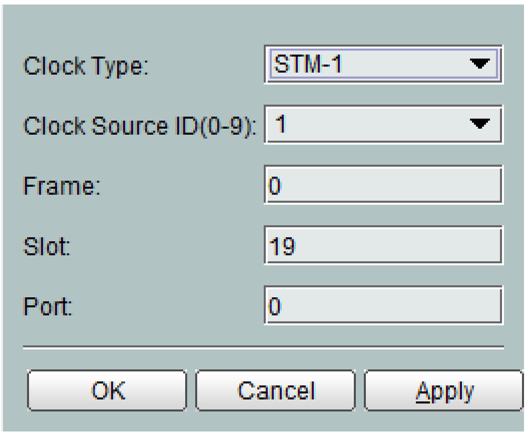
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Clock Management** > **Frequency Clock** from the navigation tree.

Step 3 In the right pane, click the **Clock Source** tab.

Step 4 In the information list, right-click, and then choose **Add Clock Source**.

Step 5 In the dialog box that is displayed, set the parameters.



Clock Type: STM-1
Clock Source ID(0-9): 1
Frame: 0
Slot: 19
Port: 0

Step 6 Click **OK**.

----End

2.2.4 Adding a Time Clock Source

Since the system supports multiple clock sources, you need to set a priority level for each clock source. The clock source without a priority is unavailable. The options for the clock source priority are 0-9. The higher the value is, the lower the priority is.

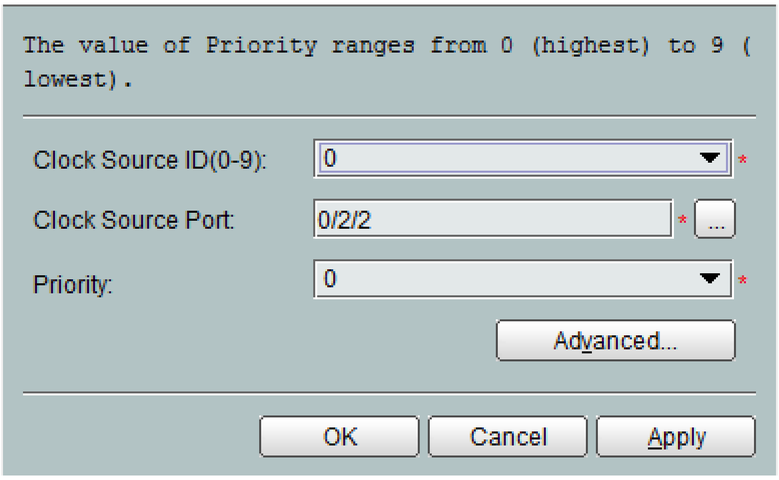
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Clock Management** > **PTP Clock** from the navigation tree.

Step 3 In the right pane, click the **Time Clock Source PTP/IEEE1588** tab.

Step 4 In the information list, right-click, and then choose **Add Clock Source**.


The value of Priority ranges from 0 (highest) to 9 (lowest).

Clock Source ID(0-9): 0 *

Clock Source Port: 0/2/2 *

Priority: 0 *

Step 5 In the dialog box that is displayed, set the parameters.

Step 6 Click **OK**.

----End

2.2.5 Adding an Adaptive Clock Source

This topic describes how to specify the clock signals of a specified port as the system clock source. OLT supports a maximum of 10 clock sources.

Procedure

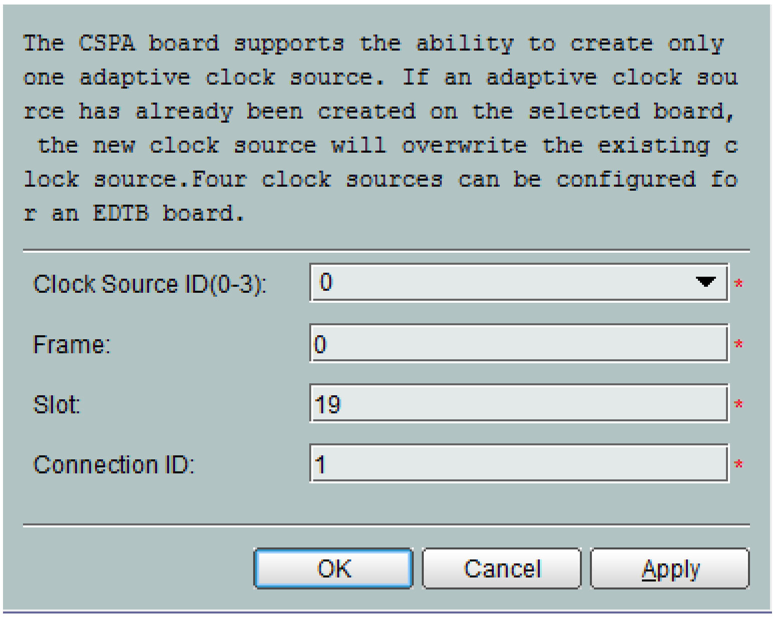
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Clock Management** > **Adaptive Clock** from the navigation tree.

Step 3 In the right pane, click the **Packet Based (Adaptive) Clock Source** tab.

Step 4 In the information list, right-click, and then choose **Add Clock Source**.

Step 5 In the dialog box that is displayed, set the parameters.



The CSPA board supports the ability to create only one adaptive clock source. If an adaptive clock source has already been created on the selected board, the new clock source will overwrite the existing clock source.Four clock sources can be configured for an EDTB board.

Clock Source ID(0-3): 0 *

Frame: 0 *

Slot: 19 *

Connection ID: 1 *

Step 6 Click **OK**.

----End

2.2.6 Setting the Time Zone and the Daylight Saving Time

This topic describes how to set the time zone of the device location as the time zone of the system, and how to set the start time, the end time, and the offset of the daylight saving time (DST).

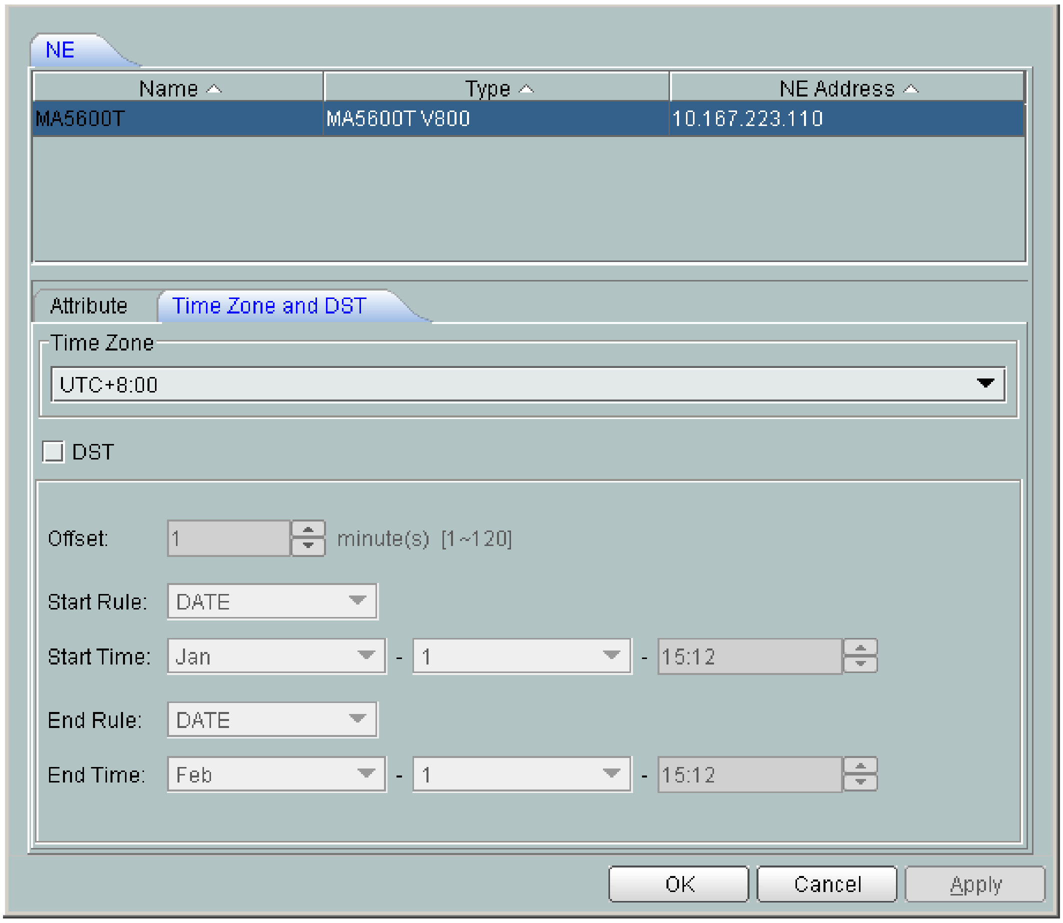
Context

- If the preset time zone of the system is incorrect, the backup operation timed at 04:00 am (the time when the traffic on the network is small) may be performed in the daytime (the time when the traffic on the network is heavy). As a result, the CPU is overloaded, and it is also difficult to locate problems. Therefore, we need to use the time zone of the device location as the time zone of the system.
- The daylight saving time (DST) is ahead of or behind the standard time. If the country or the region of the carrier uses the DST, synchronize the system time with the DST, and adjust, based on the DST, the time-sensitive services to ensure that time information of the accounting, the billing, the alarm, and the log records is correct.

Procedure

Step 1 In the Main Topology, choose the required **OLT** from the **Physical Root** navigation tree, right-click, and then choose **Properties** from the shortcut menu.

Step 2 In the dialog box that is displayed, click the **Time Zone and DST** tab, and set **Time Zone** and **DST**.



Name	Type	NE Address
MA5600T	MA5600T V800	10.167.223.110

Time Zone: UTC+8:00

☐ DST

Offset: 1 minute(s) [1~120]

Start Rule: DATE

Start Time: Jan - 1 - 15:12

End Rule: DATE

End Time: Feb - 1 - 15:12

Step 3 Click **OK**.

----End

2.3 Configuring the System Security Policy

System security configuration aims to prevent devices from being attacked by unauthorized packets that are transmitted from the network side or the user side. System security configuration ensures that the devices on the network run in the normal state.

Context

System security features tighten the network security and protect the OLT, and prevent users' attacks on the system to the utmost extent. In this case, the security of the OLT is guaranteed.

2.3.1 Querying the Blacklist

The system can filter out all of the service packets whose source IP addresses are included in a firewall blacklist. In this case, the system security and the network security are guaranteed. The purpose of setting the firewall blacklist is to prevent system attacks by malicious users. The user packets are discarded if their source IP addresses are included in the firewall blacklist.

Prerequisites

- Before querying the system blacklist, enable the firewall blacklist function and add the entries to the blacklist.
- Before querying the blacklist records on the U2000, set **Anti DOS attack function** to **Enabled** in the system parameter profile.

Context

- Currently, the devices support the functions of enabling the firewall blacklist and adding blacklist entries, while the U2000 supports only the blacklist query.
- By taking the anti-denial of service (DoS) attack measures, the system receives the control packets sent from users in a restrictive manner. The DoS attack means that malicious users send a large number of control packets to attack the system, which makes the system unable to process normal service requests, that is, the normal services are denied. The system the malicious users who initiate DoS attacks to the blacklist. Then, the control packets sent by these users will not be sent to the control module. For the users listed in the blacklist, the system administrator can force them to go offline.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **Security** > **Query Blacklist** from the navigation tree.

Step 3 On the **Blacklist Query** interface, view **Attack Port Index**, **Message Type**, and **Attack Time**.

----End

2.3.2 Setting the DHCP Offline Time-Out Time

This topic describes how to set the time to detect the abnormal disconnection of a DHCP user. The entry that is bound with the MAC address is aged to release the resource of the MAC address binding table when the following conditions are met: The anti-MAC spoofing function is enabled, the user becomes offline abnormally, and the preset offline detection time-out time is over.

Prerequisites

The anti-MAC spoofing function must be enabled. For the settings of anti-MAC spoofing function, see **2.4.2 Configuring the Security Enabling or Disabling**.

Context

When the accumulated offline time of a user is longer than the total time-out time, the system considers the user offline.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Security** > **DHCP parameter config** from the navigation tree.

Step 3 Configure **Total time of the DHCP abnormal offline timeouts**.

Step 4 Click **Apply**.

----End

2.3.3 Adding a Filter Condition Based on the Source MAC Address

To prevent malicious users from attacking the carrier's network by spoofing the MAC address of the network device, you can filter out the packets whose MAC addresses are included in the source MAC address filtering list. In this case, these filtered packets cannot be transmitted upstream through the OLT.

Context

- Up to four source MAC addresses can be filtered out.
- When the MAC address filtering function and the anti-MAC spoofing function are used at the same time, the MAC address filtering function has a higher priority than the anti-MAC spoofing function.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **Security** > **Source MAC Address Filter** from the navigation tree.

Step 3 On the **Source MAC Address Filter** interface, right-click, and then choose **Add MAC Address**.

Step 4 In the dialog box that is displayed, set **Index** and **MAC Address**.

NOTE

The system supports filtering of up to 4 MAC addresses and the **Index** ranges from 1 to 4.

Step 5 Click **OK**.

----End

2.3.4 Adding a Filter Condition Based on the Destination MAC Address

To prevent malicious users from attacking the carrier's network by spoofing the MAC address of the network device, you can filter out the packets whose MAC addresses are included in the destination MAC address filtering list. In this case, these filtered packets cannot be transmitted upstream through the OLT.

Context

- Up to four destination MAC addresses can be filtered.

- When the MAC address filtering function and the anti-MAC spoofing function are used at the same time, the MAC address filtering function has a higher priority than the anti-MAC spoofing function.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Security** > **Destination MAC Address Filter** from the navigation tree.

Step 3 On the **Destination MAC Address Filter** tab page, right-click, and then choose **Add MAC Address**.

Step 4 In the dialog box that is displayed, set **Index** and **MAC Address**.

NOTE

Up to four MAC addresses can be filtered. The index of the MAC addresses ranges from 1 to 4.

Step 5 Click **OK**. The new MAC addresses are displayed in the list.

----End

2.4 Configuring the User Security Policy

This topic introduces the user security function and describes how to configure it in the OLT.

Context

The OLT supports a series of the user security authentication functions that comply with the security standards. With these functions, the OLT performs the binding authentication between the user account and the access port to prevent theft and roaming of the user account.

2.4.1 Setting PITP Management Parameters

By setting PITP management parameters, you can implement the PITP user authentication function. In this case, the device provides the upper layer BRAS with the location information of the access user. After the BRAS obtains the information about the service port, it performs the binding authentication between the user account and the access port to avoid theft and roaming of the user account.

Prerequisites

- There are two choices to enable the PITP user authentication function: Enable it globally, and enable it on the service virtual port. The device provides the BRAS with the location information of the access user only when the PITP function is enabled globally and enabled on the service virtual port at the same time.
- In PITP V mode, the protocol type to be set cannot conflict with the existing protocol type. The existing protocol types are as follows:
  - The IP protocol type is 2048 (0x0800).
  - The ARP protocol type is 2054 (0x0806).

  - The RARP protocol type is 32821 (0x8035).
  - The 802.1Q protocol is 33024 (0x8100).
  - The PPPoE protocol types are 34915 (0x8863) and 34916 (0x8864).
- In the PITP V mode, the **Vmode Ethernet protocol type** parameter cannot be set.

Context

There are two PITP modes: PPPoE+ mode (P mode), and virtual broadband access server (V mode). In terms of implementation principles, these two modes have the similar functions, that is, binding the user account with the information about the physical port. The differences of these two modes are as follows.

- In PITP P mode, the OLT sends the service port information actively, and adds tags to the PPPoE packets. The OLT identifies the user based on the service port information carried in the PPPoE authentication request packet, and transmits the service port information to the BRAS.
- In PITP V mode, the BRAS initiates the request for querying the service port actively. The OLT is required to report the information about the physical port of the access user. OLT sends the port information to the BRAS through a response packet.

Procedure

Step 1 Configure global PITP parameters.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. On the tab page that is displayed, choose **NE Properties** > **Protocol** > **PITP mode** from the navigation tree.
3. Set the parameters such as **PITP Administrative status**, **PITP mode of RAIO**, **PITP Sub Option81**, **PITP Sub Option82**, and **PITP Sub Option90**.
4. Click **Apply**.

Step 2 Set the PITP parameters at the service virtual port level.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **Connection** > **Service Port** from the navigation tree.
3. On the **Service Port** tab page, set the filter criteria to display the required service virtual ports.
4. Select a record, right-click, and choose **Configure Extend Properties**. In the dialog box that is displayed, select the **PITP Function** check box to enable the PITP function at the service virtual port level.
5. Click **OK**.

----End

2.4.2 Configuring the Security Enabling or Disabling

You can configure the security enabling or disabling in the system parameter profile to guarantee the security of the operators and access users.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Security** > **Security** from the navigation tree.

Step 3 Configure **Anti ICMP attack function**, **Anti IP attack function**, **Anti IP spoofing function**, **Anti MAC spoofing function**, **Anti DOS attack function**, and **MAC mode of PPPoE**, etc.

Step 4 Click **Apply**.

----End

2.4.3 Querying the Information About Mapping Between UMAC and VMAC

Querying the information about the mapping between UMAC and VMAC is to query the mapping table of the user MAC address (UMAC) and the virtual MAC address (VMAC).

Prerequisites

- The device must be online and its software version must be MA5600 V800R006 or later versions.
- The port must be in the activated state and it must bear access services.

Context

NOTE

This operation is supported by only the ADSL, VDSL2, and OPFA ports. This topic considers ADSL ports as an example to describe how to query the information about the mapping between UMAC and VMAC.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ⏬ to display the ADSL ports.

Step 4 Select a record from the ADSL port list, and click the **UMAC-VMAC Info** tab. You can view the information about the mapping about between UMAN and VMAC.

----End

2.4.4 Configuring the VMAC Information About a Device

The virtual MAC address (VMAC) is converted by access devices. In the IP network, the user MAC address (UMAC) passes through the OLT, is converted into the virtual MAC address (VMAC) that is unique in the network and is planned officially. After that, the VMAC travels upstream to the network side. The returned VMAC is also converted into the corresponding UMAC by the OLT.

Prerequisites

- The device must be online.
- The software version of the device must be MA5600 V800R006 or later versions.

Context

In the IP network, the source address and the destination address of Ethernet packets between the terminals and the aggregation devices refer to the MAC address of the user home gateway and the MAC address of the aggregation device respectively. Hence, an MAC address must be unique in the network-wide platform domain. The MAC address of an aggregation device must be unique. The MAC address of a user-end terminal, however, may be configured incorrectly and causes the conflict of MAC addresses. Hence, the VMAC scheme ensures that the MAC address of a user-end terminal is unique.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **Security** > **VMAC** from the navigation tree.

Step 3 Set the **VMAC Switch**, **IPv6oE VMAC Switch**, **DSLAM ID**, **Reserved Bits**, and **Address Count Per Port** parameters, etc.

Step 4 Click **Apply**.

----End

2.4.5 Enabling PPPoE

This topic describes how to enable the PPPoE function of the xDSL port and Ethernet port to avoid theft and roaming of the user account.

Context

- If the PPPoE function of the xDSL port and Ethernet port is enabled, the device adds a tag that contains service port information to a captured PPPoE packet to generate a PPPoE Plus packet.
- If the PPPoE function of the xDSL port and Ethernet port is disabled, the system transparently transmits the PPPoE packets.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Select the xDSL port or the Ethernet port. The methods vary with the types of xDSL ports, including ADSL ports, VDSL2 ports, and ATM G.SHDSL ports.

- Choose **ETH Port** from the navigation tree. Click the **Ethernet Port** tab, and set the filter criteria or click ︾ to display the Ethernet ports. Select an Ethernet port.

- Choose **DSL** > **ADSL Port** from the navigation tree. On the **ADSL** tab page, set the filter criteria or click ⌄ to display the ADSL ports. Select an ADSL port.
- Choose **DSL** > **VDSL2 Port** from the navigation tree. On the **VDSL2** tab page, set the filter criteria or click ⌄ to display the VDSL2 ports. Select a VDSL2 port.
- Choose **DSL** > **(ATM) G.SHDSL Port** from the navigation tree. On the **(ATM) G.SHDSL Port** tab page, set the filter criteria or click ⌄ to display the G.SHDSL ports. Select an ATM G.SHDSL port.

Step 3 Click the **Ethernet Port** tab, and set the filter criteria or click ⌄ to display the Ethernet ports. Select an Ethernet port.

Step 4 Right-click, and then choose **PPPoE Switch**.

Step 5 In the dialog box that is displayed, select **Open**, and then click **OK**.

----End

2.4.6 Configuring DHCP Option 82

Dynamic Host Configuration Protocol (DHCP) option 82 is a type of user security mechanism. A user initiates a DHCP request packet, and the device adds the location information of the access user to the option 82 field of the DHCP request packet. This helps the upper layer authentication server authenticate the user.

Prerequisites

- There are three choices to enable the DHCP option 82 function: Enable it globally, enable it on the port, and enable it on the service virtual port. The device adds the option 82 information to the upstream DHCP packets only when the DHCP option 82 function is enabled globally, enabled on the port, and enabled on the service virtual port at the same time. See **2.4.7 Enabling DHCP Option 82 on Ports** for the method of enabling the DHCP option 82 function on the port and the service virtual port.
- Before enabling the DHCP option 82 function, make sure that the upper layer authentication device has completed the authentication configuration.
- After the DHCP option 82 function is enabled, you can set the maximum length of the DHCP packet. If the length of a DHCP packet that is added with the option 82 field exceeds the maximum length of the DHCP packet, or exceeds the maximum transmission unit (MTU) of the VLAN L3 interface, the system transparently transmits the packet directly, without adding the option 82 field to the DHCP packet. If you do not set the maximum length of the DHCP packet, the system uses the MTU of the VLAN L3 interface as the maximum length of the DHCP packet.

Context

- Currently, the widely used DHCP function has no authentication and security mechanism, especially for the independent DHCP server. In the actual network applications, compared with the Point-to-Point Protocol (PPP), DHCP has some security problems, such as too much DHCP broadcast, DHCP IP address use-up attack, IP address spoofing, MAC address spoofing, and user ID spoofing. In addition, DHCP clients cannot be managed in a centralized manner.
- To enhance the security when the user obtains IP address through DHCP and enhance the user access security, the OLT adds a reliable option that is used to identify the user ports

and terminal information to the DHCP packets. The DHCP server uses this option as a valid basis and reference when allocating the IP address and setting the other parameters. This option is called DHCP Relay Agent Information Option. Because its serial number is 82, it is shortened as DHCP option 82.

- The DHCP option 82 field includes the CID (circuit ID), RID (remote ID), and optional sub-option90 fields, which provide the user's shelf ID, slot ID, port ID, VPI, and VCI. The formats and contents of CID and RID vary with the RAIO working modes. The sub-option90 field contains the line encapsulation information. You can determine whether to add this field by enabling or disabling setting.
- The OLT adds the option 82 field to or removes the option 82 field from the DHCP packet only when the DHCP option 82 function is enabled.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Protocol** > **DHCP Option82** from the navigation tree.

Step 3 Set the parameters such as **DHCP Option82** and **Max length of the DHCP packet after being attached with the Option82 option**.

Step 4 Click **Apply**.

----End

2.4.7 Enabling DHCP Option 82 on Ports

This topic describes how to enable the DHCP option 82 function on the xDSL port and Ethernet port. In this case, the security of the DHCP function is improved.

Prerequisites

When you enable or disable the DHCP option 82 function on a physical port of a card, make sure that the card is in the normal state, or in the offline configuration state. In addition, the card must not be a control card.

Context

- When you enable the DHCP option 82 function on the xDSL port and Ethernet port, the device adds/removes the DHCP information to/from the captured DHCP packet.
- When you disable the DHCP option 82 function on the xDSL port and Ethernet port, the system transparently transmits or directly forwards the DHCP packet.
- There are three choices to enable the DHCP option 82 function: Enable it globally, enable it on the port, and enable it on the service virtual port. The device adds the option 82 information to the upstream DHCP packets only when the DHCP option 82 function is enabled globally, enabled on the port, and enabled on the service virtual port at the same time. See **2.4.6 Configuring DHCP Option 82** for how to configure DHCP option 82 globally.
- By default, the DHCP option 82 function is disabled globally, and enabled on a port. When the DHCP option 82 function is disabled globally, no vendor tag is added to the DHCP

packets that are transmitted from the port, no matter whether the DHCP option 82 function is enabled or disabled on the port. Vendor tags are added to the DHCP packets that are transmitted from the port only when the DHCP option 82 function is enabled globally and enabled on the port.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Enable the DHCP option 82 function on ports.

1. Select the xDSL port or the Ethernet port. The methods vary with the types of xDSL ports, including ADSL ports, VDSL2 ports, and ATM G.SHDSL ports.
   - Choose **ETH Port** from the navigation tree. Click the **Ethernet Port** tab, and set the filter criteria or click ︾ to display the Ethernet ports. Select an Ethernet port.
   - Choose **DSL** > **ADSL Port** from the navigation tree. On the **ADSL** tab page, set the filter criteria or click ︾ to display the ADSL ports. Select an ADSL port.
   - Choose **DSL** > **VDSL2 Port** from the navigation tree. On the **VDSL2** tab page, set the filter criteria or click ︾ to display the VDSL2 ports. Select a VDSL2 port.
   - Choose **DSL** > **(ATM) G.SHDSL Port** from the navigation tree. On the **(ATM) G.SHDSL Port** tab page, set the filter criteria or click ︾ to display the G.SHDSL ports. Select an ATM G.SHDSL port.
2. Right-click, and then choose **DHCP Option82 Switch**.
3. In the dialog box that is displayed, select **Open**, and then click **OK**.

Step 3 Enable the DHCP option 82 function on service virtual ports.

1. Choose **Connection** > **Service Port** from the navigation tree.
2. On the **Service Port** tab page, set the filter criteria to display the required service virtual ports.
3. Select a record from the service virtual port list, right-click, and then choose **Configure Extended Properties**. Select **DHCP Option82 Function** and **Allow DHCP Option82 forwarding**.
4. Click **OK**.

----End

2.5 Configuring the Active/Standby Switchover for the Upstream Service

This topic describes how to configure the card with the active/standby switchover for the upstream service so that the stability of the service is guaranteed.

Context

The DSLAM provides two levels of active/standby switchover guarantee, the SCU active/standby switchover and the ISU active/standby switchover. The following factors affect the service recovery after the active/standby switchover occurs:

- The duration of switching the upper layer router.
- The duration for the user terminal to determine the link interruption and to re-dial.
- The switchover duration of the SCU card and the ISU card.

2.5.1 Configuring the Active/Standby Switchover for the GIU Upstream

This topic describes how to configure the active/standby upstream ports for the GIU card, so that active/standby switchover can be performed when the active control card is faulty and the standby control card works in the normal state. In this way, services are not interrupted.

Context

Only the GE upstream interface card of the OLT supports this operation.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Panel** from the navigation tree.

Step 3 Right-click a card in the list and choose **GIU Protect Group** from the shortcut menu.

Step 4 In the dialog box that is displayed, click **Add**.

Step 5 In the dialog box that is displayed, set the parameters.

Step 6 Click **OK**.

----End

2.6 File Operations

By means of file operations, you can save the records as a file, preview the file printing effect, and print the file. In this case, you can save and analyze the relevant information of the U2000.

2.6.1 Saving Records as a File

This topic describes how to save records as a CSV file, a text file, an xls file, or an HTML file. In this case, you can use the records in different file formats.

Context

This topic considers VLAN as an example. For other subjects, the steps are the same but the navigation path is different.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

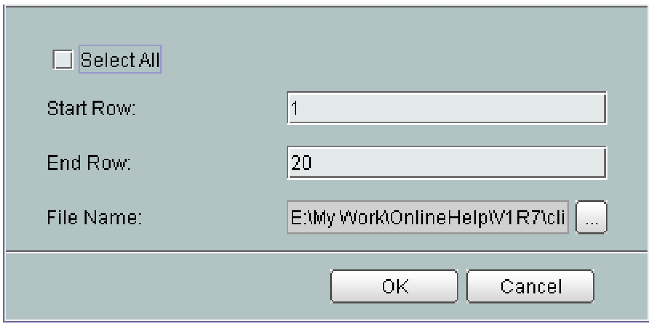
Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.

Step 4 In the information list, right-click and choose **File** > **Save As** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.

- Set **Start Row** and **End Row**.
- Click ... next to **File Name** and set the path (client\report by default) for saving the file, the filename, the file type and encoding.



☐ Select All
Start Row: 1
End Row: 20
File Name: E:\My Work\OnlineHelp\V1R7\cli

Step 6 Click **OK**.

Step 7 In the dialog box that is displayed, click **Yes** to open the folder to view related files or click **No** to close the dialog box.

----End

2.6.2 Previewing the File Printing Effect

This topic describes how to preview the file printing effect so that you can adjust the page settings before printing.

Context

This topic considers VLAN as an example. For other subjects, the steps are the same but the navigation path is different.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.

Step 4 Right-click in the list and choose **File** > **Print Preview** from the shortcut menu.

Step 5 In the dialog box that is displayed, set **Start Row** and **End Row**, click **OK**.

Step 6 In the dialog box that is displayed, preview the file printing effect, or adjust the page settings according to the requirements. Click **Close** to close the current dialog box, or click **Print** to print the file.

----End

2.6.3 Printing

You can print out the records in the U2000 information list to keep the related information of the U2000 and analyze it.

Context

This topic considers VLAN as an example. For other subjects, the steps are the same but the navigation path is different.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⏬ to display the VLANs.

Step 4 Right-click in the list and choose **File** > **Print** from the shortcut menu.

Step 5 In the dialog box that is displayed, set **Start Row** and **End Row**, click **OK**.

Step 6 Click **OK**.

----End

2.7 Synchronization

This topic describes how to synchronize the NE data, NE time, NE alarms and system parameter profile so that the data of the NE and the data on the U2000 are the same.

2.7.1 Synchronizing the NE Data

This topic describes how to synchronize the device panel data and service data on the U2000 with that of the NE, which facilitates the centralized maintenance and management.

Prerequisites

Related xFTP settings have been configured. To obtain the configuration instructions, choose **Administration** > **NMS Commissioning Wizard** from the main menu and then select **NMS Communication with NEs** from the navigation tree.

Context

- Data must be consistent between the U2000 and NEs.

  If data is not consistent between the U2000 and NEs, the following problems may arise:

  - The U2000 cannot properly display the resource information for NEs,such as the board,port lists,optics module info.and the port lists for boards are empty.
  - The U2000 cannot display all ONU information for OLTs. For example, software versions are not displayed.

  - The U2000 cannot display icons for the MDUs under OLTs.
  - The U2000 cannot obtain ONU versions.
  - During service application to OLTs, the U2000 displays an error message indicating invalid parameter names or values.
  - Port status is inconsistent between the U2000 and third-party NMSs.
- After the data of the NE is configured and the NE works in the normal state, synchronize the data on the U2000 with that of the NE manually. When an error occurs to the NE data, check whether the NE data saved on the U2000 is correct. If it is correct, download the data from the U2000 to the NE. In this case, the data of the NE is restored.
- How long it takes to synchronize NE data depends on the performance of the U2000 server and the number of NEs.

Procedure

- Path one: In the Main Topology, choose the required **OLT** from the **Physical Root** navigation tree, right-click, and then choose **Synchronize NE Data** from the shortcut menu.
- Path two: Choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (application style). In the **Synchronize NE Data** window, select the desired NE and click **Synchronize**.
- Path three: In the Main Topology, double-click the required NE in the **Physical Root** navigation tree; or right-click the required NE and choose **NE Explorer** from the shortcut menu. Select a module from the navigation tree, right-click on the right pane, and then choose **Synchronize** or **Refresh**.

----End

Subsequent Handling

You can stop synchronizing an NE that is being synchronized or waiting to be synchronized. The path is as follows:

Choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Configuration** > **Synchronize NE Configuration Data** from the main menu (application style). In the **Synchronize NE Data** window, select the desired NE and click **Cancel**.

NOTE

- A user that is logged in to another client using the same user name can also stop the NE synchronization process.
- The administrator can stop NE synchronization processes on different clients.

2.7.2 Synchronizing the NE Time

This topic describes how to synchronize the NE time with the U2000 time to ensure that the time when the NE reports the information is correct.

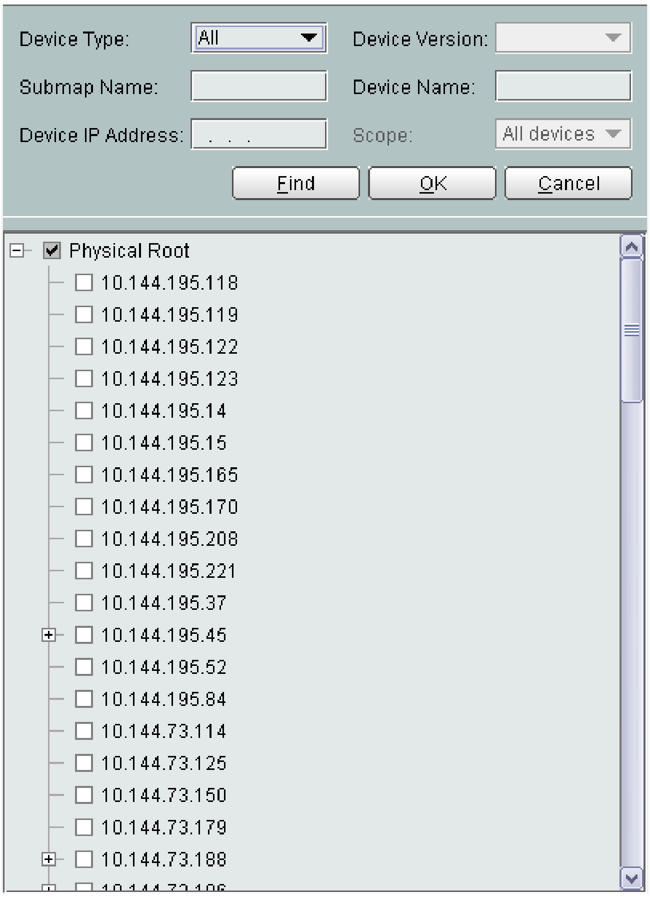
Context

- The U2000 delivers the system time automatically when a device goes online.
- By default, the U2000 automatically synchronizes NE time every morning.
- After synchronizing the NE time, do not change the system time of the U2000 frequently.
- NE time can be set in batches.

Procedure

Step 1 In the Main Topology, select the required **OLT** from the **Physical Root** navigation tree, right-click, and then choose **Set NE Time** from the shortcut menu.

Step 2 In the dialog box that is displayed, set parameters and click **Find**.



Device Type: All
Scope: All devices

Step 3 Click **OK**.

----End

2.7.3 Synchronizing NE Alarms

This topic describes how to synchronize NE alarms. After the communication between the U2000 and the device recovers or the U2000 restarts, the alarms generated on the device are not reported to the U2000 in time. This results in the inconsistency of the alarm status between the U2000 and the device. In this case, you need to synchronize the alarms. You can synchronize the alarms manually, or enable the automatic synchronization. This ensures that the U2000 monitors the actual running status of the device.

Context

By manual alarm synchronization, all alarms generated by NE are synchronized.

Procedure

- In the Main Topology, choose the required **OLT** from the **Physical Root** navigation tree, right-click, and then choose **Synchronize Current Alarms** from the shortcut menu.

----End

2.7.4 Synchronizing the System Parameter Profile

You can perform this operation to synchronize the system parameter profile that is modified at the device to the U2000 to maintain the consistency of the parameters in the system parameter profile.

Context

To synchronize the system parameter profile, perform this operation.

Procedure

- Synchronizing the System Parameter Profile
  1. Choose **View** > **Main Topology** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** and choose **Topology** > **Main Topology** from the main menu (application style).
  2. On the **Physical Root** navigation tree on the **Main Topology** tab page, select the required **OLT**, right-click, and then choose **Synchronize System Parameter Profile**.

----End

2.7.5 Synchronizing the Port

This topic describes how to synchronize port information from an NE to the U2000 to maintain consistency in port information.

Context

To synchronize port information, perform this operation. The synchronization procedures for different types of ports are similar. The Ethernet port is used as an example in this topic.

To avoid port data inconsistency between the U2000 and NE, you are advised to synchronize port data before configuring port data on the U2000.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ETH Port** from the navigation tree.

Step 3 Right-click and choose **Synchronize** from the shortcut menu.

----End

2.8 Saving the Data

After saving the data to the flash memory of a device, you can query the data information to maintain and manage the device. Saving the data prevents data loss in case of unexpected restart.

2.8.1 Setting the Parameters for Saving the Data

You can configure the auto save period of the data through enabling the auto save function of the device. The U2000 automatically saves the data to the flash memory of the device according to the configured period. Through the U2000, you can periodically maintain and manage the device according to the saved data information.

Context

Saving the data frequently affects the system performance. It is recommended that you set the auto-save interval to 1440 minutes or longer.

NOTE

The automatic data saving function must be enabled on NEs. Otherwise, configuration data will be lost. For example, an ONU is added to a PON port of an OLT but fails to be displayed if the ONU data is not saved automatically.

The absolute period and relative period of the device are based on the time of the site where the device is located.

Procedure

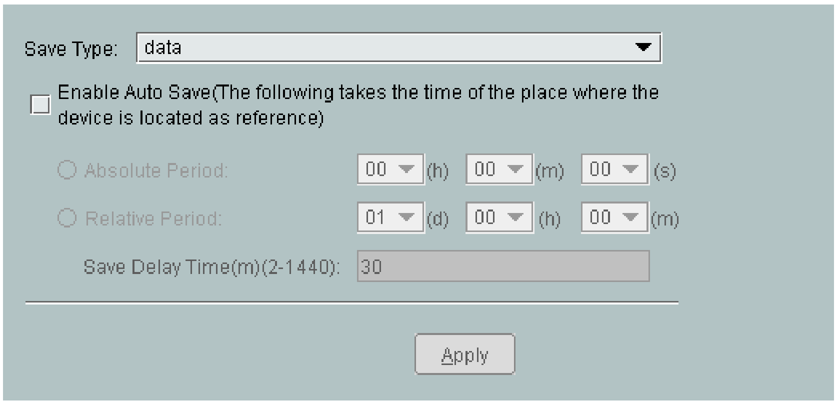
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Auto Save Configuration** from the navigation tree.

Step 3 In the right pane, select the **Enable Auto Save** check box, and then set the **Absolute Period** or **Relative Period** parameter for saving the data.

NOTE

- Absolute Period: The data is automatically saved at a specified time. For example, if the **Absolute Period** parameter is set to **01h 05m 31s**, the data is automatically saved at the preset time.
- Relative Period: The data is automatically saved at an interval. For example, if the **Relative Period** parameter is set to **00d 05h 31m**, the data is automatically saved every other 331 minutes.



Save Type: data

☐ Enable Auto Save(The following takes the time of the place where the device is located as reference)

○ Absolute Period: 00 (h) 00 (m) 00 (s)

○ Relative Period: 01 (d) 00 (h) 00 (m)

Save Delay Time(m)(2-1440): 30

Step 4 Click **Apply**.

----End

2.8.2 Immediately Enabling Data Saving Function

This topic describes how to immediately enable the auto save function of a device to save the current data of the device in time.

Context

NOTICE

- This operation is applicable to only the device that supports the SNMP protocol.
- After being enabled immediately, the automatic saving function cannot be manually stopped. Do not power off or reset the device before the data is saved. Otherwise, the data saved to the flash memory is damaged.

Procedure

Step 1 In the Main Topology, choose the required **OLT** from the **Physical Root** navigation tree, right-click, and then choose **Save Data Immediately** from the shortcut menu.

Step 2 In the dialog box that is displayed, click **OK**.

----End

2.9 Detecting the Network

This topic describes how to check the connectivity of a network and whether the host is reachable, and how to check all gateways passed by data packets sent from a source host to the destination host. In addition, this operation helps you to locate network faults and log in to the device through the network remotely to configure and maintain the device.

2.9.1 Telnet

This topic describes how to log in to the device through the network remotely to configure and maintain the device.

Prerequisites

Before telneting to a device, ensure that port 31035 is enabled between the U2000 client and server.

Ensure that client ACL rules have been configured.

Context

Clients access NEs using a proxy. To keep network users secure, you need to set the proxy service ACL to allow specified clients to access NEs. Before using the telnet function to connect to a device, ensure that port 31035 is enabled between the U2000 server and clients and client ACL rules have been configured. If no client ACL rule is configured, Choose **Administration** > **NMS Security** > **Proxy Service ACL** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **Settings** > **Proxy Service ACL** from the main menu (application style).For details, see **Working with the NMS** > **Security Management** > **User Security Policy Management** > **Security Policy Management** > **Setting the Proxy Service ACL**.

Procedure

Step 1 In the navigation tree or the topology view, select a required device.

Step 2 Right-click and choose **Tool** > **Telnet** from the shortcut menu. In the CLI displayed, enter the user name and password for the NE. After you successfully telnet to the remote server or device in the network, you can operate the device in command lines.

----End

2.9.2 Ping

This topic describes how to send ping packets to a remote host to check whether it is reachable. To check the network connectivity or the line quality, perform this operation.

Prerequisites

Before sending ping packets to a remote host, disable firewall that runs on the U2000 server, because it blocks ICMP packets, which consequently causes communication interruption between the U2000 and ICMP NEs.

Context

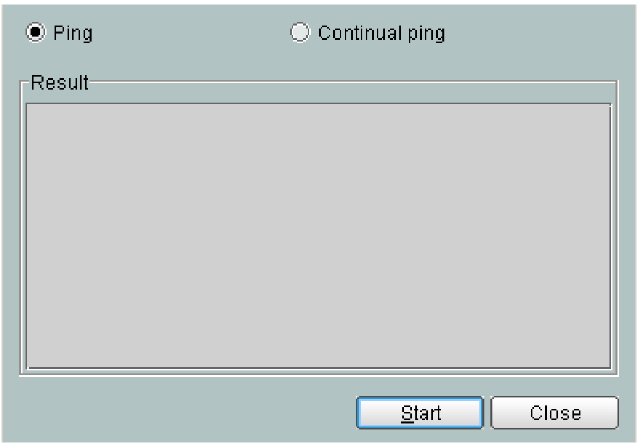
During the ping process, the source host sends the ICMP ECHO-REQUEST packets to the destination host. If the network connection between the source host and the destination host is normal, after receiving the ICMP ECHO-REQUEST packets, the destination host responds to the source host with the ICMP ECHO-REPLY packets.

Procedure

Step 1 In the navigation tree or the topology view, select a required device.

Step 2 Right-click and choose **Tool** > **Ping** from the shortcut menu.

Step 3 In the dialog box that is displayed, select **Ping** or **Continual Ping** and click **Start**.



NOTE

- If the operation is successful, it indicates that the destination host is reachable. In the **Result** area, the system displays the information indicating that the network connectivity is in the normal state. The displayed information includes the number of sent packets, number of received response packets, packet loss ratio, and minimum, maximum, and average values of the response time.
- If the operation fails, it indicates that the destination host is not reachable. The system fails to check the network connectivity or line failure. The system displays the message **Request time out**.

----End

2.9.3 Tracert

This topic descries how to test the route that is passed by data packets sent from a source host to the destination host. To track the route that is passed by data packets and locate the network fault, perform this operation. After running the ping command to test the network and detect a fault, you can run the tracert command to locate the fault on the network.

Context

The execution process of the tracert command is as follows:

- The source host sends a packet with TTL 1. TTL times out. The first hop sends back an ICMP error message to indicate that this packet cannot be sent.
- The source host sends a packet with TTL 2. TTL times out. The second hop sends back an ICMP error message to indicate that this packet cannot be sent.
- The source host sends a packet with TTL 3. TTL times out. The third hop sends back an ICMP error message to indicate that this packet cannot be sent.
- The process continues in this manner until the packet reaches the destination host.
- The purpose of performing these operations is to record the source address of each ICMP TTL time-out message, so as to provide the route that an IP packet passes to reach the destination host.

Procedure

Step 1 In the navigation tree or the topology view, select a required device.

Step 2 Right-click and choose **Tool** > **Tracert** from the shortcut menu.

----End

2.9.4 SSH

The secure shell (SSH) guarantees the security of the network communications by providing authentication, encryption, and authorization. When users telnet the router through an insecure network, SSH offers secure information guarantee and powerful authentication to protect the device against attacks such as IP address spoofing and interception of the plain text password.

Prerequisites

Ensure that client ACL rules have been configured.

Context

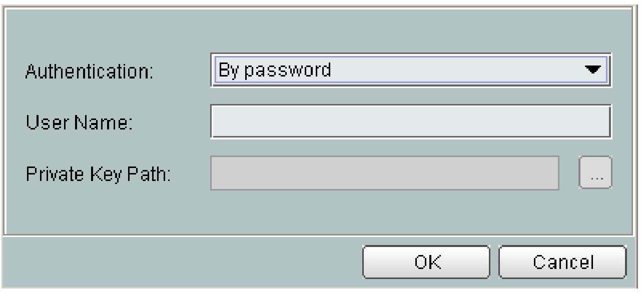
Clients access NEs using a proxy. To keep network users secure, you need to set the proxy service ACL to allow specified clients to access NEs. Before using the telnet function to connect to a device, ensure that port 31035 is enabled between the U2000 server and clients and client ACL rules have been configured. If no client ACL rule is configured, Choose **Administration** > **NMS Security** > **Proxy Service ACL** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **Settings** > **Proxy Service ACL** from the main menu (application style). For details, see the nodes **Working with the NMSSecurity Management** > **Managing U2000 Users** > **Setting Security Policies of U2000 Users** > **Setting the Proxy Service ACL**.

Procedure

Step 1 In the navigation tree or the topology view, select a required device.

Step 2 Right-click and choose **Tool** > **SSH** from the shortcut menu.

Step 3 In the dialog box that is displayed, set the parameters.



Authentication: By password

Step 4 Click **OK**.

----End

3 Managing Devices

About This Chapter

The U2000 provides the graphical management function for devices. After the NEs are added to the topology view, the U2000 can display the physical status of the devices through the device panel, and can maintain and manage the devices.

3.1 Setting the Communication Parameters

This topic describes how to set the handshake parameters and SNMP trap port ID for an NE to communicate with the U2000. The device automatically sends the trap packet to the U2000 periodically to report the exception event and error alarm to the U2000. The U2000 determines whether the device is running in the normal state and manages the device.

3.2 Adding an NE to the U2000

This topic describes how to add an NE to the U2000. You can manage NEs in a centralized manner on the U2000.

3.3 Bulk Adding NEs to the U2000

This topic describes how to bulk add NEs to the U2000 to manage the NEs in a centralized manner.

3.4 Adding a Shelf

To increase the access capacity of the OLT and reduce costs, you need to add a local slave shelf on the U2000 and the device. For UA5000(IPMB), after you add the slave shelf successfully, the control card in the slave shelf works in the normal state. The service cards in the slave shelf, however, work in the normal state only after you confirm them. For UA5000(PVM), when you add the shelf on both the U2000 and the device, the shelf works in the normal state only after you confirm it on the U2000. After adding the shelf successfully, you can configure and query the shelf.

3.1 Setting the Communication Parameters

This topic describes how to set the handshake parameters and SNMP trap port ID for an NE to communicate with the U2000. The device automatically sends the trap packet to the U2000 periodically to report the exception event and error alarm to the U2000. The U2000 determines whether the device is running in the normal state and manages the device.

3.1.1 Setting the SNMP Parameters

This topic describes how to set the SNMP parameters. The set SNMP parameters need to be consistent with the parameters on the device. You can directly use the set SNMP parameter profile when adding a device. Using SNMPv3 is recommended because of its higher security than SNMPv1 and SNMPv2c.

Context

Currently, the SNMP protocol is most widely applied in computer networks. The SNMP protocol ensures that the management information is transmitted between any two nodes. This facilitates the operations of the network administrator in terms of retrieving information, modifying information, locating faults, diagnosing faults, planning capacities, and generating reports on any node in the network. The SNMP protocol uses the polling mechanism and provides the most basic function set to implement the User Datagram Protocol (UDP) that runs on the transmission layer and is based on the connectionless mode. Hence, the SNMP protocol can implement obstacle-free connections with multiple products.

NOTE

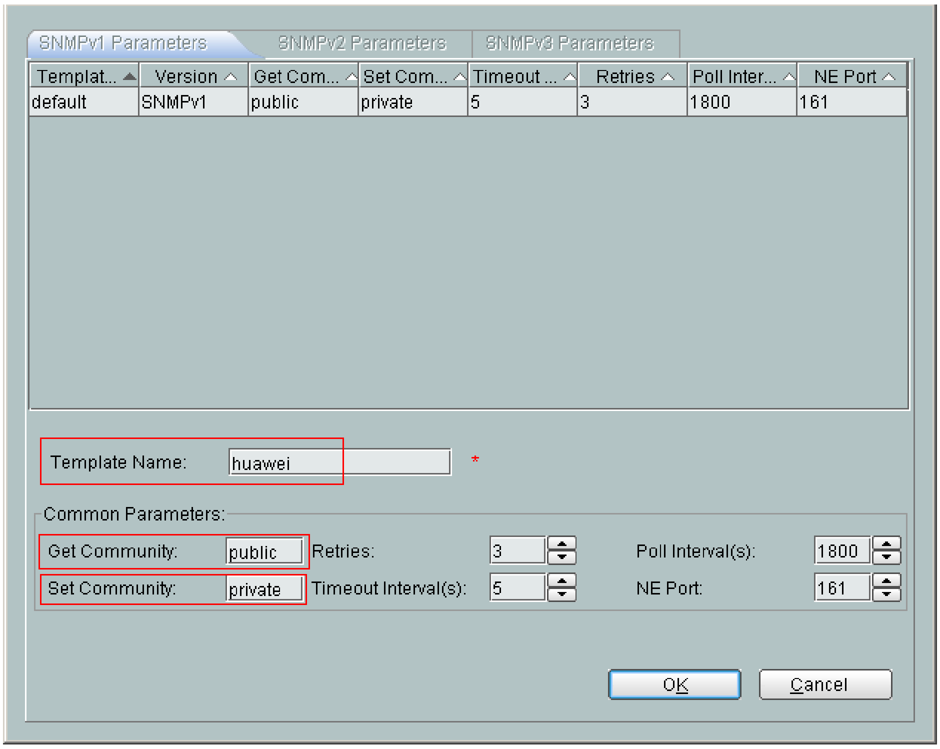
- The profile name must be unique.
- Currently, the default name of the get community is public and the default name of the set community is private.
- To ensure the device security, sometimes you need to change the get community name and set community name. Then, when adding a device, you need to set **NE Access Protocol Parameters** to choose the corresponding the get community name and set community name. Otherwise, the adding may fail.
- After setting the SNMP parameters, you can test whether the SNMP parameters on the U2000 are consistent with the SNMP parameters on the device by performing Step 6 to Step 7.
- If the Simple Network Management Protocol version 3 (SNMPv3) is used, plan NE communication parameters in a unified manner. Group NEs and ensure that NEs within the same group use the same communication parameters and different NE groups use different user names. The communication parameters include the user name, private protocol, encryption password, authentication protocol, and authentication password.
- For all SNMPv3 NEs that are managed by the same NMS, if different NEs need to use the same user name, ensure that the private protocol, encryption password, authentication protocol, and authentication password are consistent on these NEs.

Procedure

Step 1 Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu (application style).

Step 2 On the tab page that is displayed, click **Reset**. In the dialog box that is displayed, click the corresponding tab, and then click **Add**.

Step 3 In the dialog box that is displayed, set the **Template Name**, **Get Community**, and **Set Community** parameters.



Templat...	Version	Get Com...	Set Com...	Timeout ...	Retries	Poll Inter...	NE Port
default	SNMPv1	public	private	5	3	1800	161

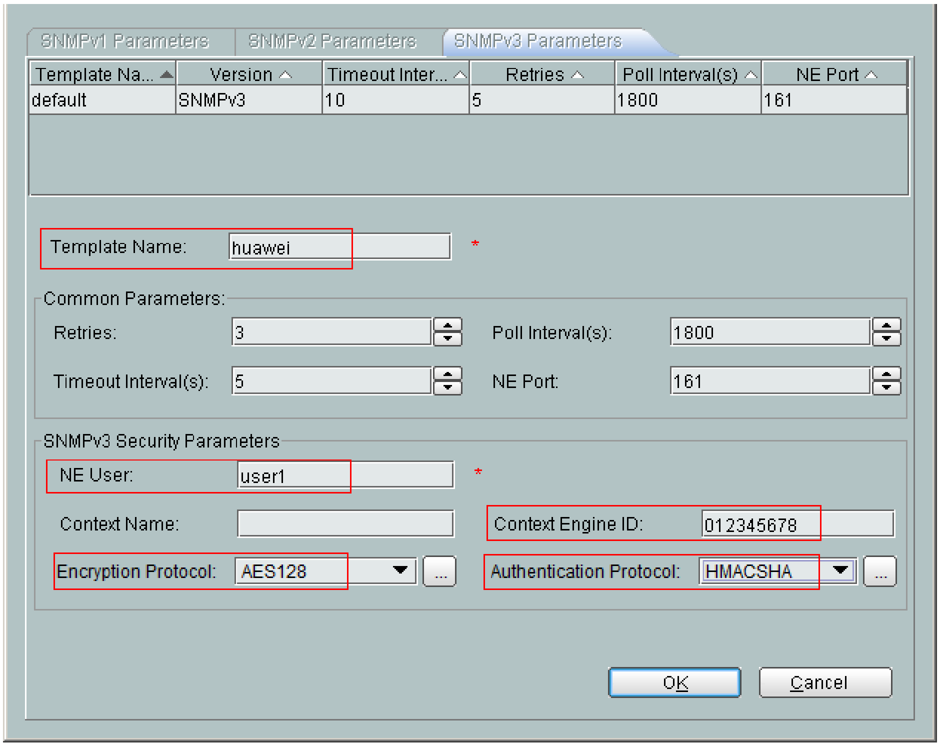
Template Name: huawei *

Common Parameters:

Get Community: public
Retries: 3
Poll Interval(s): 1800
Set Community: private
Timeout Interval(s): 5
NE Port: 161

NOTE

When clicking the **SNMPv3 Parameters** tab, you can configure the related parameters.



Template Na...	Version	Timeout Inter...	Retries	Poll Interval(s)	NE Port
default	SNMPv3	10	5	1800	161

Template Name: huawei *

Common Parameters:

Retries: 3
Poll Interval(s): 1800
Timeout Interval(s): 5
NE Port: 161

SNMPv3 Security Parameters

NE User: user1 *
Context Name:
Context Engine ID: 012345678
Encryption Protocol: AES128
Authentication Protocol: HMACSHA

Step 4 Click **OK**.

Step 5 Select the added SNMP parameters. Click **OK**.

Step 6 In the dialog box that is displayed, click **Yes** to test the set SNMP parameters.

Step 7 The U2000 displays the **Loading** dialog box. After the testing is complete, click **OK**.

----End

3.1.2 Setting the NE Handshake Parameters

By setting the device handshake parameters, you can learn the communication status between the device and the U2000. The device initiates the handshake request actively, and sends the handshake packets on a timed basis. If the U2000 receives the handshake packets on a timed basis, the system considers that the current communication is in the normal state.

Context

The handshake duration between the device and the U2000 determines the handshake frequency. If the duration is too short, the U2000 may face a heavy burden when managing too many devices and processing too many handshake packets. If the duration is too long, the U2000 cannot immediately detect the disconnection between the device and U2000. You can set proper handshake duration as required. The default value 300s is recommended.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Properties** > **Configure NE Handshake Parameter** from the navigation tree on the tab page that is displayed.

Step 3 Select the **Device Handshake Switch** check box in the view on the right side, and set the device handshake duration.

Step 4 Click **Apply**.

----End

3.1.3 Setting the SNMP Trap Port Number

The agent generates the trap packet and reports the exception event of the managed device to the U2000. When an error occurs on the device and an alarm is generated, or the important data of the device is changed by the user, console, or other NMSs, the agent sends the trap packet to the U2000.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Properties** > **SNMP Trap Port** from the navigation tree on the tab page that is displayed.

Step 3 Set the **SNMP Trap Port** in the view on the right side.

Step 4 Click **Apply**.

----End

3.2 Adding an NE to the U2000

This topic describes how to add an NE to the U2000. You can manage NEs in a centralized manner on the U2000.

Prerequisites

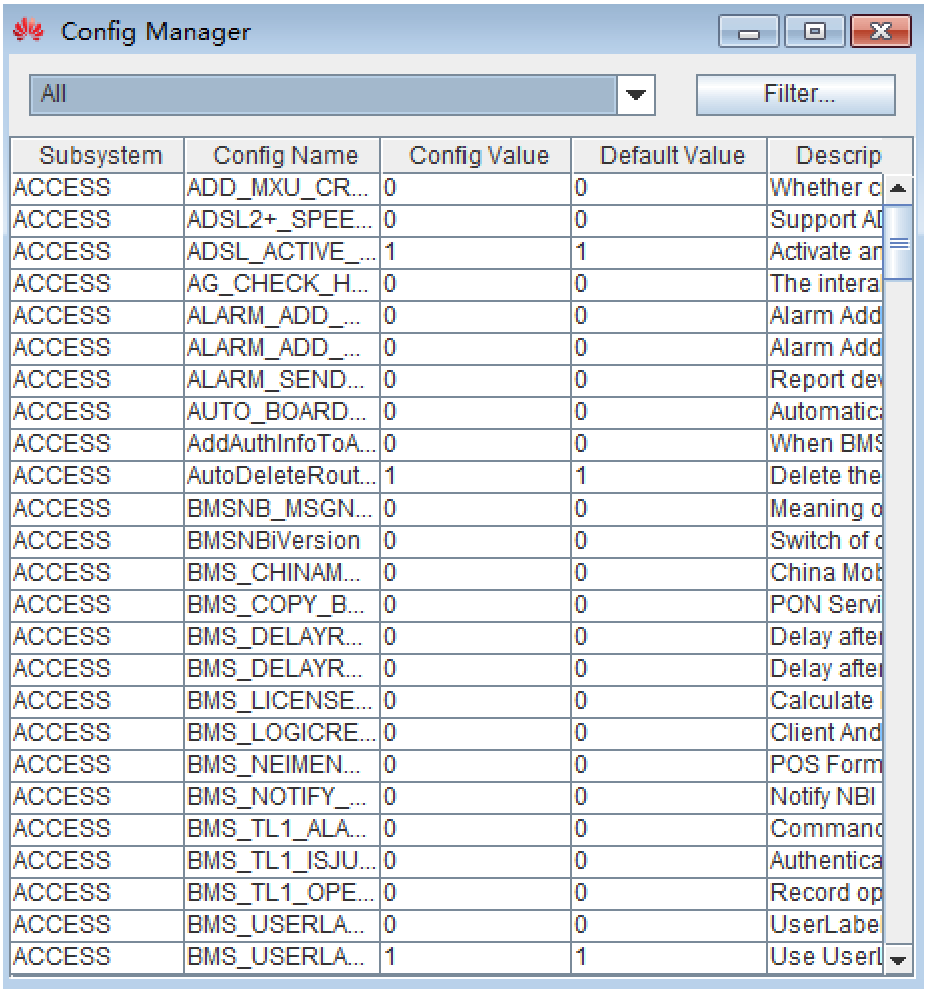
Related xFTP settings have been configured. To obtain the configuration instructions, choose **Administration** > **NMS Commissioning Wizard** from the main menu and then select **NMS Communication with NEs** from the navigation tree.

Context

SNMP parameters on the U2000 must be the same as those on NEs. These parameters include the protocol version, read community name, and write community name. If an NE fails to be added, check whether the settings of the SNMP parameters are consistent between the U2000 and the NE and whether the SNMP parameters are activated. For details, see **3.1.1 Setting the SNMP Parameters**.

One NE can be managed by multiple sets of U2000.

- If the NE version is earlier than V800R012, the NE can be managed by a set of U2000 whose version is V100R008 or later versions and a set of U2000 whose version is earlier than V100R008. On the U2000 of V100R008 or later version, you need to set MULTI_NMS_SCENE to **1**.
- If the NE version is later than V800R012, the NE can be managed by multiple sets of U2000 whose version is V100R008 or later. On all sets of U2000, MULTI_NMS_SCENE must be set to **1** and NE_FTP_SYNC_EMS_FLAG must be set to the same.
- Set MULTI_NMS_SCENE and NE_FTP_SYNC_EMS_FLAG as follows:
  1. Log in to the MSuite client.
  2. Choose **Tools** > **Config Manager** from the main menu. The **Config Manager** dialog box is displayed, and all configuration items are displayed by default.



Subsystem	Config Name	Config Value	Default Value	Descrip
ACCESS	ADD_MXU_CR...	0	0	Whether c
ACCESS	ADSL2+_SPEE...	0	0	Support AI
ACCESS	ADSL_ACTIVE_...	1	1	Activate ar
ACCESS	AG_CHECK_H...	0	0	The intera
ACCESS	ALARM_ADD_...	0	0	Alarm Add
ACCESS	ALARM_ADD_...	0	0	Alarm Add
ACCESS	ALARM_SEND...	0	0	Report dev
ACCESS	AUTO_BOARD...	0	0	Automatic
ACCESS	AddAuthInfoToA...	0	0	When BMS
ACCESS	AutoDeleteRout...	1	1	Delete the
ACCESS	BMSNB_MSGN...	0	0	Meaning o
ACCESS	BMSNBiVersion	0	0	Switch of c
ACCESS	BMS_CHINAM...	0	0	China Mob
ACCESS	BMS_COPY_B...	0	0	PON Servi
ACCESS	BMS_DELAYR...	0	0	Delay after
ACCESS	BMS_DELAYR...	0	0	Delay after
ACCESS	BMS_LICENSE...	0	0	Calculate
ACCESS	BMS_LOGICRE...	0	0	Client And
ACCESS	BMS_NEIMEN...	0	0	POS Form
ACCESS	BMS_NOTIFY_...	0	0	Notify NBI
ACCESS	BMS_TL1_ALA...	0	0	Command
ACCESS	BMS_TL1_ISJU...	0	0	Authentica
ACCESS	BMS_TL1_OPE...	0	0	Record op
ACCESS	BMS_USERLA...	0	0	UserLabe
ACCESS	BMS_USERLA...	1	1	Use UserL

3. In the **Config Manager** dialog box, filter **MULTI_NMS_SCENE** out of other configuration items. Double-click the item and set **Config Value** to **1**.
4. In the **Config Manager** dialog box, filter **NE_FTP_SYNC_EMS_FLAG** out of other configuration items. Double-click the item and set **Config Value**.

Procedure

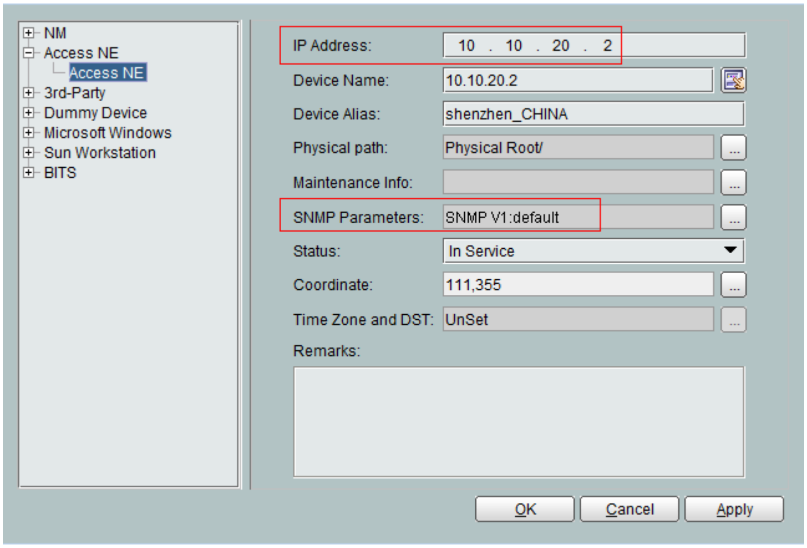
- Add an NE to the U2000.

NOTE

When the **Management Status** of an NE is **Being deployed**, the U2000 does not receive alarms from the NE. If the U2000 needs to receive alarms from the NE, set **Management Status** to **In Service** as follows:

In the physical root view, right-click the NE and choose **Configure Management Status** from the shortcut menu. In the dialog box that is displayed, set **Management Status** to **In Service**.

1. Right-click in the Main Topology and choose **New** > **NE** from the shortcut menu.
2. In the dialog box that is displayed, set the parameters.



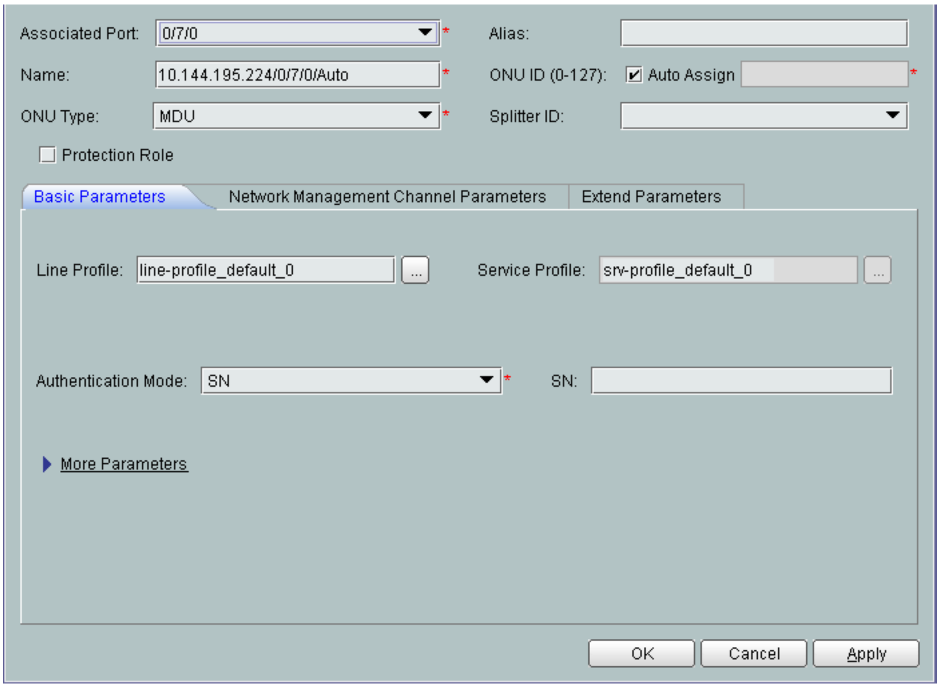
IP Address: 10 . 10 . 20 . 2
Device Name: 10.10.20.2
Device Alias: shenzhen_CHINA
Physical path: Physical Root/
Maintenance Info:
SNMP Parameters: SNMP V1:default
Status: In Service
Coordinate: 111,355
Time Zone and DST: UnSet
Remarks:

3. Click **OK**.

NOTE

In the dialog box that is displayed, the system displays a message indicating that it takes several seconds or dozens of minutes to load the device data. After the device data is loaded and read successfully, the system automatically refreshes the device icon.

- Add the MA5606T, MA5600T or MA5603T that functions as an MDU.
  1. Right-click the OLT to which the MA5606T, MA5600T or MA5603T is connected and choose **NE Explorer** from the shortcut menu.
  2. Choose **GPON** > **GPON Management** from the navigation tree.
  3. On the **GPON ONU** tab page, set the filter criteria or click ¥ to display the required GPON ONUs.
  4. In the information list, right-click and choose **Add** from the shortcut menu.
  5. In the dialog box that is displayed, set the parameters.



Associated Port: 0/7/0 *
Alias:
Name: 10.144.195.224/0/7/0/Auto *
ONU ID (0-127): ☑ Auto Assign *
ONU Type: MDU *
Splitter ID:
☐ Protection Role
Line Profile: line-profile_default_0
Service Profile: srv-profile_default_0
Authentication Mode: SN *
SN:

NOTE

Set the SNMP profile and SNMP parameters in **Network Management Channel Parameters**. The **IP Address** parameter is usually set to the IP address of the Layer 3 interface of the VLAN.

----End

Result

NE data is synchronized to the U2000 if the NE icon turns green in the Main Topology. That is, the NE is successfully added to the U2000.

Follow-up Procedure

If the NE icon is gray or has a sign like a gear in the upper left corner in the Main Topology, right-click the NE and choose **Synchronize NE Data** from the shortcut menu.

3.3 Bulk Adding NEs to the U2000

This topic describes how to bulk add NEs to the U2000 to manage the NEs in a centralized manner.

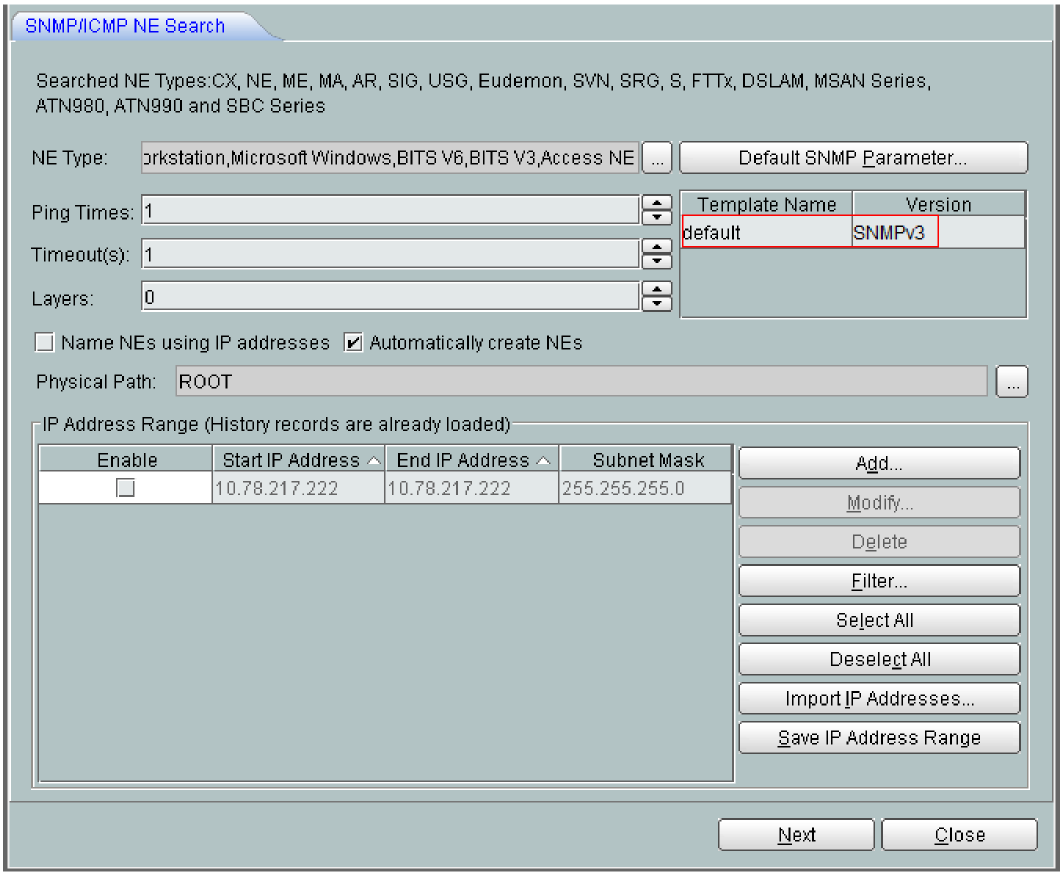
Prerequisites

- Related xFTP settings have been configured. To obtain the configuration instructions, choose **Administration** > **NMS Commissioning Wizard** from the main menu and then select **NMS Communication with NEs** from the navigation tree.
- The SNMP parameters on the U2000 must be the same as the SNMP parameters on the NEs. These parameters include the protocol version, get community name, and set community name. For details, see **3.1.1 Setting the SNMP Parameters**.

Procedure

Step 1 Choose **File** > **Discovery** > **NE** from the main menu (traditional style); alternatively, double-click **Topo View** in **Application Center** and choose **File** > **Discovery** > **NE** from the main menu (application style).

Step 2 In the dialog box that is displayed, click the **SNMP/ICMP NE Search** tab and set the parameters.



Searched NE Types:CX, NE, ME, MA, AR, SIG, USG, Eudemon, SVN, SRG, S, FTTx, DSLAM, MSAN Series, ATN980, ATN990 and SBC Series

NE Type: orkstation,Microsoft Windows,BITS V6,BITS V3,Access NE

Ping Times: 1

Timeout(s): 1

Layers: 0

Template Name	Version
default	SNMPv3

☐ Name NEs using IP addresses ☑ Automatically create NEs

Physical Path: ROOT

IP Address Range (History records are already loaded)

Enable	Start IP Address	End IP Address	Subnet Mask
☐	10.78.217.222	10.78.217.222	255.255.255.0

NOTE

- In the **NE Type** field, select the required device type. By default, the value is **All Device Types**.
- Click **Default SNMP Parameter** to set the SNMP parameters on the U2000 for successful communications between the U2000 and NEs.
- Click **Add** to configure the range of IP addresses of automatically discovered NEs in the **IP address Range** area.

Step 3 Click **Next**. The U2000 starts searching for NEs and reading the data of the NEs in real time.

----End

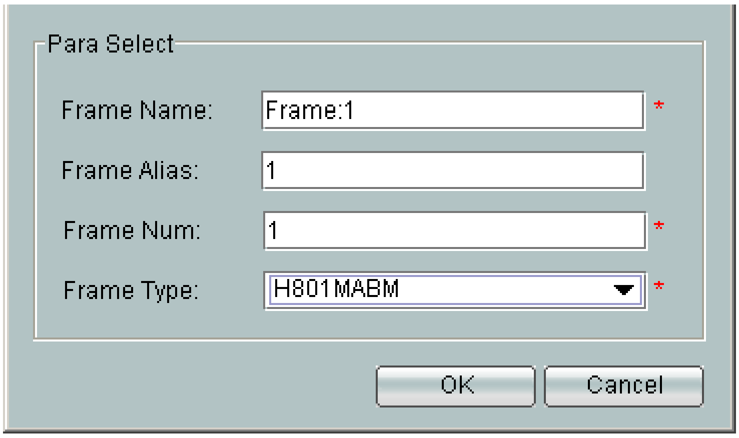
3.4 Adding a Shelf

To increase the access capacity of the OLT and reduce costs, you need to add a local slave shelf on the U2000 and the device. For UA5000(IPMB), after you add the slave shelf successfully, the control card in the slave shelf works in the normal state. The service cards in the slave shelf, however, work in the normal state only after you confirm them. For UA5000(PVM), when you add the shelf on both the U2000 and the device, the shelf works in the normal state only after you confirm it on the U2000. After adding the shelf successfully, you can configure and query the shelf.

Procedure

Step 1 In the **Physical Root** navigation tree, right-click the required device and choose **Add Frame** from the shortcut menu.

Step 2 In the dialog box that is displayed, set the parameters such as **Name**, **Number**, and **Type**.



Frame Name: Frame:1

Frame Alias: 1

Frame Num: 1

Frame Type: H801MABM

Step 3 Click **OK**.

Step 4 In the **Physical Root** navigation tree, right-click the slave shelf to be confirmed and choose **Confirm Frame** from the shortcut menu.

----End

Copyright © Huawei Technologies Co., Ltd.

4 Configuring the Protocol

About This Chapter

Protocol configurations mainly include protocol common configurations. There is no obvious logical relationship between protocol configurations. You can perform protocol configurations according to actual requirements.

4.1 Configuring the DHCP Relay
The DHCP relay enables the OLT to function as a bridge between the DHCP clients and servers that are located in different subnets. With this function, the DHCP packets can be relayed to the destination DHCP server (or client) across different subnets. As a result, the DHCP clients in different networks can share the same DHCP server. In this case, it saves the cost and realizes the uniform management.

4.2 Configuring the MSTP
The Multiple Spanning Tree Protocol (MSTP) is a new spanning tree protocol defined in IEEE 802.1s. MSTP prunes a loop network to a tree network without loops to prevent proliferation and infinite loops of packets. In addition, MSTP provides redundant paths for forwarding packets, thus allowing load balancing between VLANs.

Copyright © Huawei Technologies Co., Ltd.

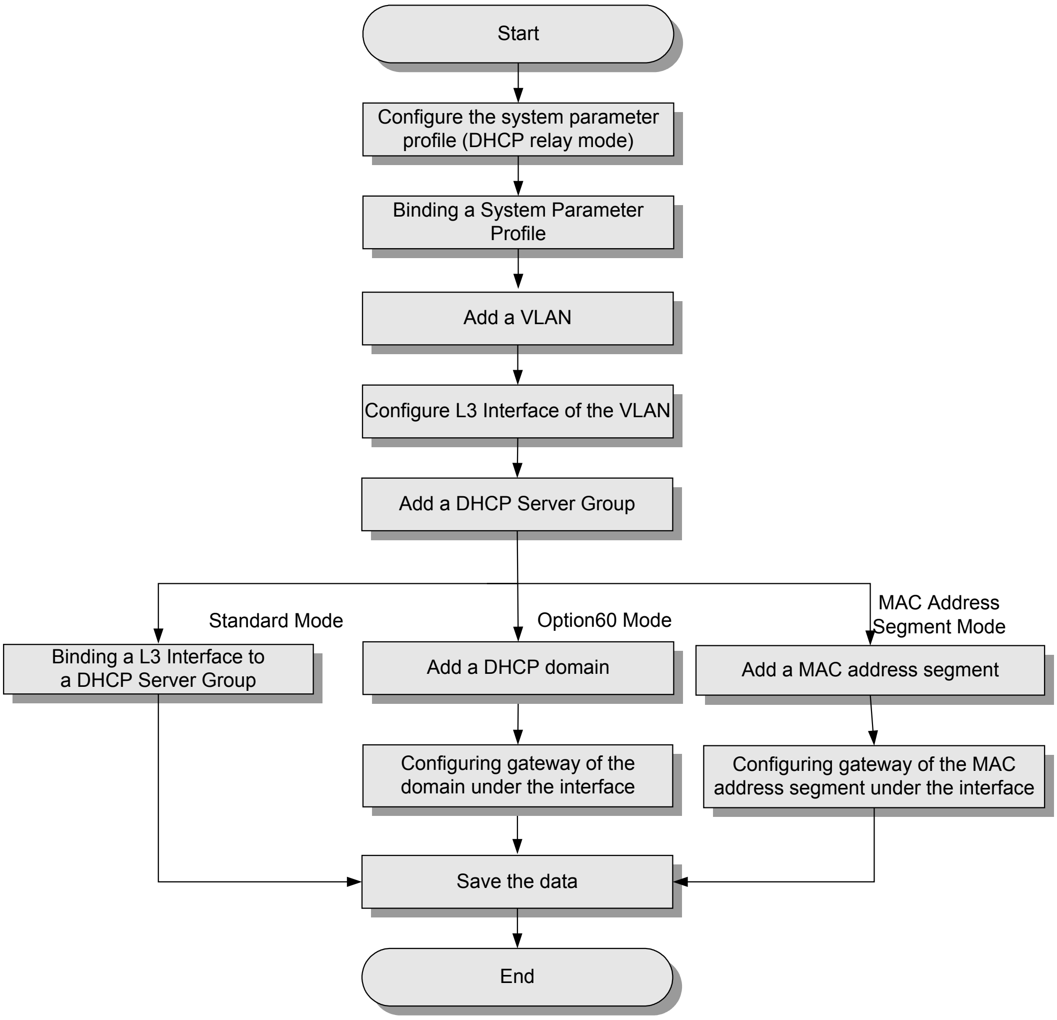
4.1 Configuring the DHCP Relay

The DHCP relay enables the OLT to function as a bridge between the DHCP clients and servers that are located in different subnets. With this function, the DHCP packets can be relayed to the destination DHCP server (or client) across different subnets. As a result, the DHCP clients in different networks can share the same DHCP server. In this case, it saves the cost and realizes the uniform management.

Context

Figure 4-1 shows the flowchart for configuring the DHCP relay function.

Figure 4-1 Flowchart for configuring the DHCP relay function


Start
Configure the system parameter profile (DHCP relay mode)
Binding a System Parameter Profile
Add a VLAN
Configure L3 Interface of the VLAN
Add a DHCP Server Group
Standard Mode
Option60 Mode
MAC Address Segment Mode
Binding a L3 Interface to a DHCP Server Group
Add a DHCP domain
Add a MAC address segment
Configuring gateway of the domain under the interface
Configuring gateway of the MAC address segment under the interface
Save the data
End

4.1.1 Introduction to the DHCP Relay

This topic describes the technical principles and service specifications of the dynamic host configuration protocol (DHCP) relay.

Context

DHCP is a solution for dynamic IP address allocation based on the TCP/IP protocol suite.

DHCP is only applicable to the case that the DHCP client and the DHCP server are in the same subnet, and the client and the server cannot work across the subnet. In this case, each subnet needs to be set with a DHCP server, which wastes resources.

The DHCP relay functions as a bridge between the DHCP clients and servers that are located in different subnets. With this function, the DHCP packets can be relayed to the destination DHCP server (or client) across different subnets. As a result, the DHCP clients on different networks can share the same DHCP server. In this way, it saves cost and realizes uniform management.

The OLT supports L2 and L3 forwarding. L3 forwarding includes the standard mode, Option60 (DHCP domain) mode, and MAC address segment mode.

- In the L2 mode, the OLT only transparently transmits packets and does not process the packets.
- When the OLT is in the L3 forwarding mode, the DHCP packets are forwarded by the DHCP client according to the forwarding mode (standard, Option60, or MAC address segment) that is selected by the DHCP relay module. **Table 4-1** describes the features of DHCP relay modes.

Table 4-1 L3 forwarding mode

Parameter	Description
MAC address segment mode	Selects a DHCP server group based on the source MAC address segment of DHCP packets. The OLT forwards the DHCP packets that match a certain MAC address segment to the DHCP server group that is bound to the MAC address segment. A MAC address segment can be bound to only one DHCP server group. The device finds the MAC address segment according to the source MAC address of a user, and forwards DHCP packets based on the DHCP server bound to the MAC address segment. The system supports up to 128 MAC address segments.
DHCP standard mode	Selects a DHCP server based on the IP address of the VLAN L3 interface to forward DHCP packets. The OLT selects a DHCP server based on the DHCP server group that is bound to the VLAN L3 interface for receiving DHCP packets from the client. A VLAN L3 interface can be bound to only one DHCP server group. Therefore, all the DHCP packets to be sent upstream through the VLAN L3 interface are forwarded to the DHCP server group bound to the VLAN L3 interface.

Parameter	Description
Option60 (DHCP domain) mode	Selects a DHCP server based on the DHCP Option60 domain. The OLT differentiates service types according to terminal types, thus forwarding DHCP packets to different DHCP server groups. Option60 is an option in the DHCP packet. It identifies the terminal type. You can select the gateway connected to the interface for the DHCP domain according to different terminal types.

The DHCP relay of the OLT can be configured as only one forwarding mode in the same period. For details about how to set the forwarding mode, see **4.1.2.1 Configuring the DHCP Relay Mode**.

The OLT enhances the security of the DHCP function through the DHCP option 82 feature.

The actual applications over the network may encounter various security problems, because the DHCP function is without the authentication and security mechanism. The OLT can solve these problems by using the DHCP option 82 option. When the DHCP option 82 function is enabled, the BRAS can authenticate the user. When the DHCP option 82 feature is enabled, the BRAS can authenticate the user. When the DHCP option 82 feature is disabled, the device only transparently transmits the DHCP packets and does not process the packets. For details about how to configure the DHCP option 82 feature, see Setting DHCP Option 82 Parameters.

4.1.2 Configuring the DHCP Standard Mode

In the DHCP standard mode, the OLT selects a DHCP server according to the DHCP server group that is bound to the VLAN L3 interface where the DHCP packets of the client are received.

4.1.2.1 Configuring the DHCP Relay Mode

The DHCP Relay serves as a bridge between a DHCP client and a server that are located on different subnets. With this function, the DHCP packets can be relayed to the destination DHCP server (or client) across different subnets. As a result, the DHCP clients on different subnets can share the same DHCP server. In this way, it saves cost and realizes uniform management.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.

Step 3 On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the name of the system parameter profile. Choose **Protocol** > **DHCP Relay forward mode** from the **Parameters for Selection**, click > to add the parameters to the **Selected Parameters**, and then click **Next**.

Step 6 In the dialogue box, set the **DHCP Relay forward mode** to **Layer-3 mode**, set the **DHCPv6 Relay Mode** to **layer-3**.

Step 7 Click **Finish**.

Step 8 Select the system parameter profile, right-click, and then choose **Download to NE**.

Step 9 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

4.1.2.2 Adding a VLAN

Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

Context

Table 4-2 describes VLAN types and their applications.

Table 4-2 VLAN types and their applications

VLAN Type	Description	Application
Standard VLAN	Ethernet ports in a standard VLAN are interconnected with each other. Ethernet ports in different standard VLANs are isolated from each other.	Only available for Ethernet ports. Applied to network management and subtending.
Smart VLAN	A smart VLAN contains multiple service virtual ports. In addition, traffic streams on these ports are isolated from each other and traffic streams on different VLANs are isolated from each other. A smart VLAN provides access for multiple users, saving the VLAN resources.	Applied to the access service, such as the residential community access.
MUX VLAN	A MUX VLAN contains only one service virtual port. In addition, traffic streams on different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. In this case, a MUX VLAN can uniquely identify an access user.	Applied to the access service, such as scenarios where users are distinguished based on VLANs.

VLAN Type	Description	Application
Super VLAN	The super VLAN is a L3-based VLAN. It consists of multiple sub VLANs. Through ARP proxy, a super VLAN realizes L3 interconnection for these sub VLANs. A sub VLAN can be a standard VLAN, smart VLAN, or a MUX VLAN.	Applied to save IP address resources so that the utilization of the IP address is improved.

Table 4-3 describes the VLAN attributes.

Table 4-3 VLAN attributes

VLAN Attribute	Application
Common	A VLAN with the common attribute can be used as a L2 VLAN or to create a L3 interface.
QinQ	A QinQ VLAN packet contains two layers of VLAN tags: inner VLAN tag from the private network and outer VLAN tag from the OLT. Through the outer VLAN, a L2 VPN tunnel can be set up to transparently transmit the service between private networks.
Stacking	A stacking VLAN packet contains two layers of VLAN tags: inner VLAN tag and outer VLAN tag from the OLT. With this attribute, the upper layer BRAS device authenticates users based on the two VLAN tags, thus increasing the number of access users. In an upper network in the L2 working mode, you can forward packets according to the "VLAN + MAC", thus providing the wholesale service provisioning function for ISPs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

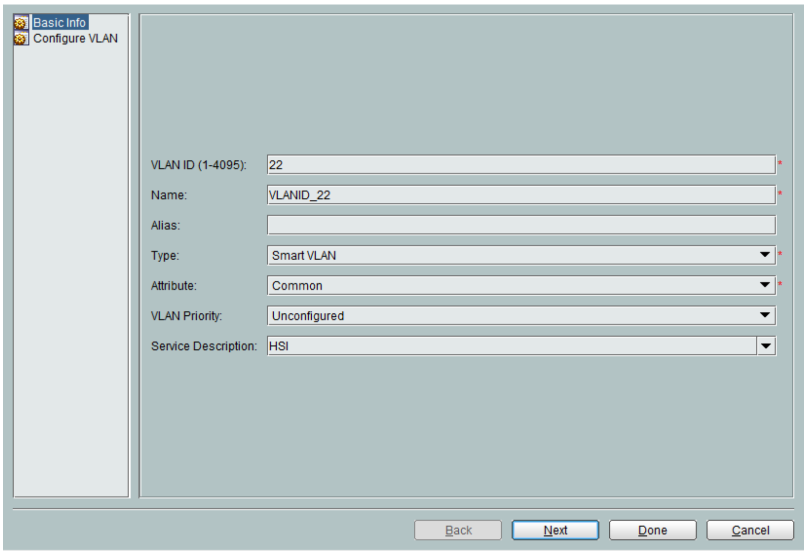
Step 3 On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.

Step 4 Right-click the list, and then choose **Add** or **Batch Add**.

Step 5 In the dialog box that is displayed, set the parameters.

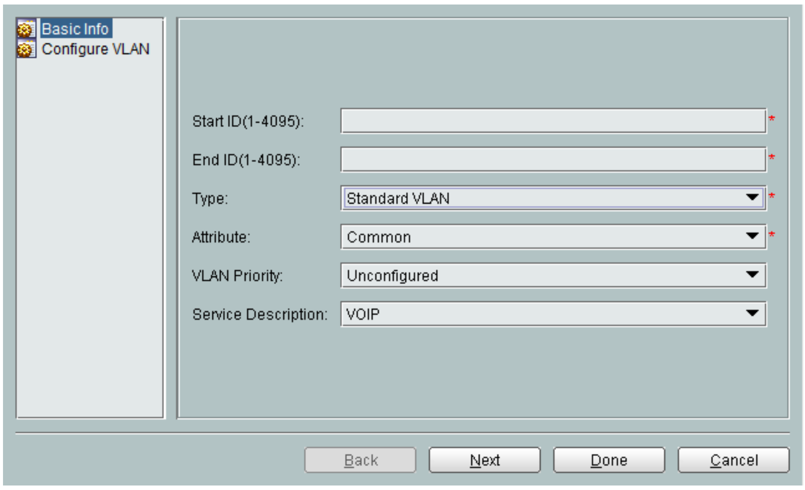
- When you add a VLAN, and then set the parameters as follows:
  - **VLAN ID**
  - **Name**
  - **Alias**

  - **Type**
  - **VLAN Priority**



VLAN ID (1-4095): 22 *
Name: VLANID_22 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI

- When you add VLANs in batches, and then set the parameters as follows:
  - **Start ID**
  - **End ID**
  - **Type**
  - **VLAN Priority**



Start ID(1-4095): *
End ID(1-4095): *
Type: Standard VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: VOIP

Step 6 Click **Done**.

----End

4.1.2.3 Configuring a VLAN L3 Interface

The functions of a L3 interface that is based on the VLAN are similar to a L3 switch. Through L3 forwarding, the L3 interface forwards data between different VLANs.

Context

You can configure the L3 interfaces of common VLANs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

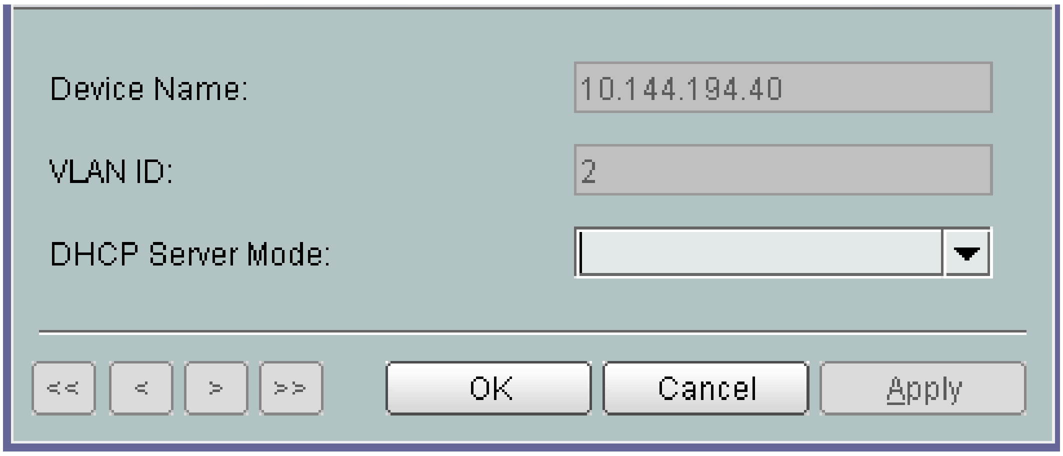
Step 3 Select **VLAN L3 Interface** tab.

Step 4 Right-click a record and choose **Modify** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the proper parameters.

You can set the **DHCP Server Mode** parameter as you need. The options are as follows:

- Standard
- Option-60
- MAC-range



Device Name: 10.144.194.40

VLAN ID: 2

DHCP Server Mode:

Step 6 Click **Done**.

----End

4.1.2.4 Adding a DHCP Server Group

To add a DHCP server group to provide the DHCP services for the DHCP clients in the local network, perform this operation.

Context

- The system supports up to 20 server groups. The IP addresses of the active and standby servers in each server group must be unique.
- A server group must contain at least the IP address of an active server.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

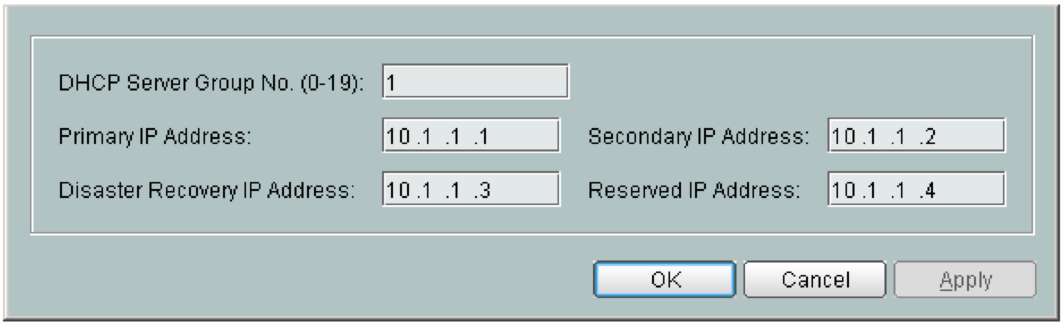
Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Select **DHCP Server Group** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the proper parameters.



DHCP Server Group No. (0-19): 1
Primary IP Address: 10 .1 .1 .1
Secondary IP Address: 10 .1 .1 .2
Disaster Recovery IP Address: 10 .1 .1 .3
Reserved IP Address: 10 .1 .1 .4

Step 6 Click **OK**.

----End

4.1.2.5 Adding a DHCPv6 Server Group

To add a DHCPv6 server group to provide the DHCPv6 services for the DHCPv6 clients in the local network, perform this operation.

Context

- The system supports up to 20 server groups. The IP addresses of the active and standby servers in each server group must be unique.
- A server group must contain at least the IP address of an active server.

Procedure

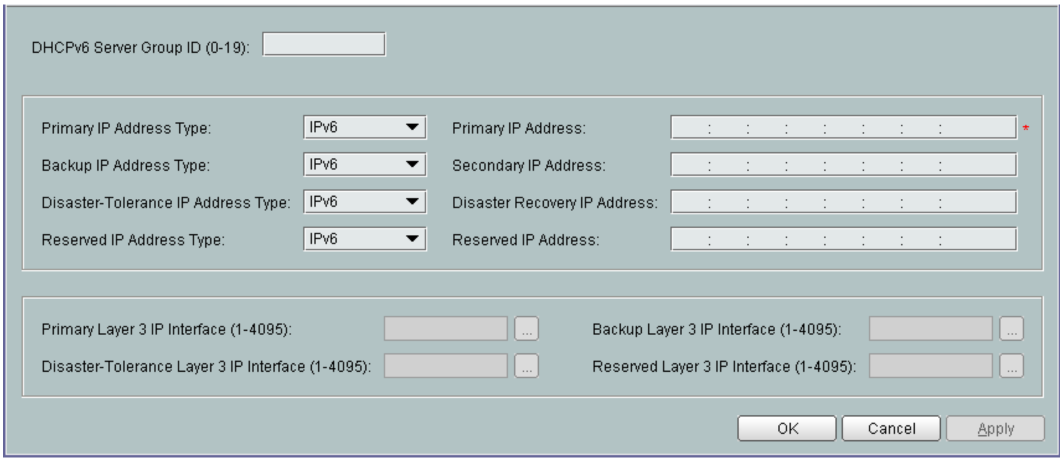
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 Select **DHCPv6 Server Group** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the proper parameters.



Primary IP Address Type: IPv6

Backup IP Address Type: IPv6

Disaster-Tolerance IP Address Type: IPv6

Reserved IP Address Type: IPv6

DHCPv6 Server Group ID (0-19):
Primary IP Address:
Secondary IP Address:
Disaster Recovery IP Address:
Reserved IP Address:
Primary Layer 3 IP Interface (1-4095):
Backup Layer 3 IP Interface (1-4095):
Disaster-Tolerance Layer 3 IP Interface (1-4095):
Reserved Layer 3 IP Interface (1-4095):
OK
Cancel
Apply

Step 6 Click **OK**.

----End

4.1.2.6 Binding an L3 Interface to a DHCP Server Group

To bind a VLAN L3 interface to a DHCP server group, perform this operation. When the DHCP relay function uses the standard mode to forward DHCP packets, you need to configure the VLAN L3 interface of the DHCP server group. After the configuration is successful, all packets received on the VLAN L3 interface are forwarded to the corresponding DHCP server group.

Context

If the VLAN L3 interface is already bound to a DHCP server group, the new value overwrites the original value.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 On the **Standard Mode** tab page, set the querying criteria to display the required records.

Step 4 Right-click a record and choose **Modify** from the shortcut menu.

Step 5 In the dialog box that is displayed, select **DHCP Server Group No.**.

Step 6 Click **OK**.

----End

4.1.2.7 Binding an L3 Interface to a DHCPv6 Server Group

To bind a VLAN L3 interface to a DHCPv6 server group, perform this operation. When the DHCP relay function uses the standard mode to forward DHCP packets, you need to configure the VLAN L3 interface of the DHCPv6 server group. After the configuration is successful, all packets received on the VLAN L3 interface are forwarded to the corresponding DHCPv6 server group.

Context

If the VLAN L3 interface is already bound to a DHCPv6 server group, the new value overwrites the original value.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 On the VLAN L3 interface tab page, set the querying criteria to display the required records.

Step 4 Select a record from the VLAN L3 list, and then click the **Bind DHCPv6 Server Group** tab in the lower pane.

Step 5 In the information list, right-click and choose **Add** from the shortcut menu.

Step 6 In the dialog box that is displayed, select DHCPv6 server group.

Step 7 Click **OK**.

----End

4.1.3 Configuring the DHCP Option60 Mode

In the DHCP option60 mode, the OLT differentiates the service types according to terminal types, thus forwarding DHCP packets to different DHCP server groups.

Prerequisites

- The DHCP relay mode must be set in the system parameter profile and must be applied to the device. For details about the operations, see **4.1.2.1 Configuring the DHCP Relay Mode** and Adding the System Parameter Profile to a Device.
- The corresponding VLAN must be added. For details about the operations, see **4.1.2.2 Adding a VLAN**.

4.1.3.1 Adding a DHCP Server Group

To add a DHCP server group to provide the DHCP services for the DHCP clients in the local network, perform this operation.

Context

- The system supports up to 20 server groups. The IP addresses of the active and standby servers in each server group must be unique.
- A server group must contain at least the IP address of an active server.

Procedure

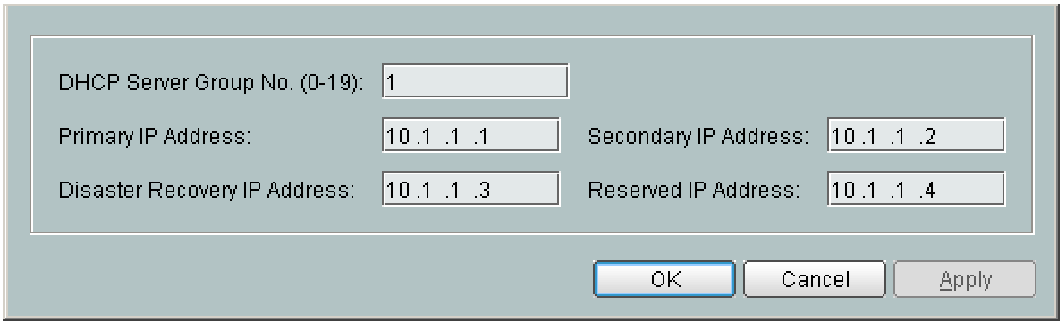
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 Select **DHCP Server Group** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the proper parameters.



DHCP Server Group No. (0-19): 1

Primary IP Address: 10 .1 .1 .1

Secondary IP Address: 10 .1 .1 .2

Disaster Recovery IP Address: 10 .1 .1 .3

Reserved IP Address: 10 .1 .1 .4

Step 6 Click **OK**.

----End

4.1.3.2 Adding a DHCP Domain

To create a DHCP domain when the OLT enables the DHCP relay function and the forwarding mode is the Option60 (DHCP domain) mode, perform this operation.

Context

After receiving the DHCP packets containing the Option60 information from a service port, the OLT checks whether the information matches the domain names by the packets. The matching rule is from long to short, and from start to end. If the DHCP packet does not contain the Option60 information or does not match a proper domain name after the matching process ends, the device matches the default domain for the DHCP relay.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 Click the **DHCP Domain** tab, and set the filter criteria to display the required DHCP domains. In the information list, right-click and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters.

Step 5 Click **OK**.

----End

4.1.3.3 Configuring a VLAN L3 Interface

The functions of a L3 interface that is based on the VLAN are similar to a L3 switch. Through L3 forwarding, the L3 interface forwards data between different VLANs.

Context

You can configure the L3 interfaces of common VLANs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

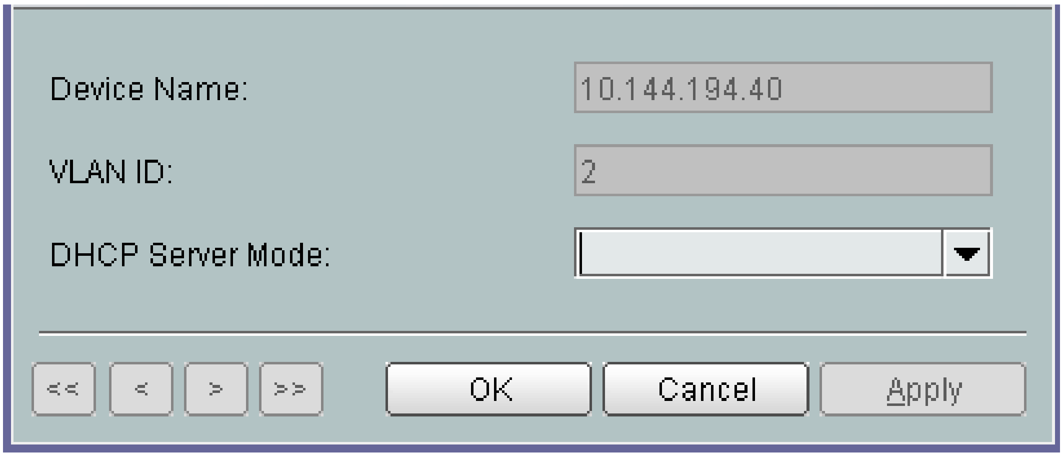
Step 3 Select **VLAN L3 Interface** tab.

Step 4 Right-click a record and choose **Modify** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the proper parameters.

You can set the **DHCP Server Mode** parameter as you need. The options are as follows:

- Standard
- Option-60
- MAC-range



Device Name: 10.144.194.40

VLAN ID: 2

DHCP Server Mode:

Step 6 Click **Done**.

----End

4.1.3.4 Configuring the Gateway IP Address of the Domain Under an Interface

When the DHCP relay working mode is the DHCP domain forwarding mode, you need to configure the gateway IP address corresponding to the DHCP domain. After the gateway IP address is configured successfully, the OLT can forward packets to the corresponding server through the gateway IP address.

Context

On a VLAN interface, a DHCP domain can be configured with only one gateway IP address, and this gateway IP address must be the IP address already configured on the VLAN interface.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

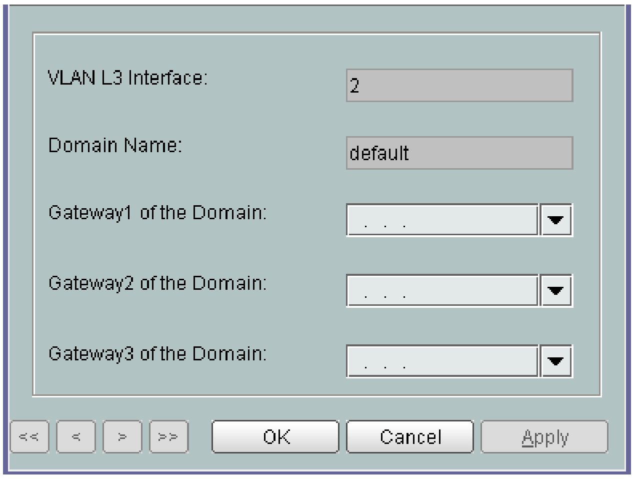
Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 Click the **DHCP Domain** tab, and set the filter criteria to display the required DHCP domains.

Step 4 Select a record from the DHCP domain list, right-click, and then click the **Gateway of the Domain under the Interface** tab in the lower pane.

Step 5 Right-click a record and choose **Modify** from the shortcut menu.

Step 6 In the dialog box that is displayed, set the parameters.



VLAN L3 Interface: 2

Domain Name: default

Gateway1 of the Domain: . . .

Gateway2 of the Domain: . . .

Gateway3 of the Domain: . . .

Step 7 Click **OK**.

----End

4.1.4 Configuring the DHCP MAC Address Segment Mode

In the DHCP MAC address segment mode, the OLT forwards the DHCP packets matching a certain MAC address segment to the DHCP server group to which the MAC address segment is bound.

Prerequisites

- The DHCP relay mode must be set in the system parameter profile and the system parameter profile must be applied to the device. For details about the operations, see **4.1.2.1 Configuring the DHCP Relay Mode** and Adding the System Parameter Profile to a Device.
- The corresponding VLAN must be added. For details about the operations, see **4.1.2.2 Adding a VLAN**.

4.1.4.1 Adding a DHCP Server Group

To add a DHCP server group to provide the DHCP services for the DHCP clients in the local network, perform this operation.

Context

- The system supports up to 20 server groups. The IP addresses of the active and standby servers in each server group must be unique.
- A server group must contain at least the IP address of an active server.

Procedure

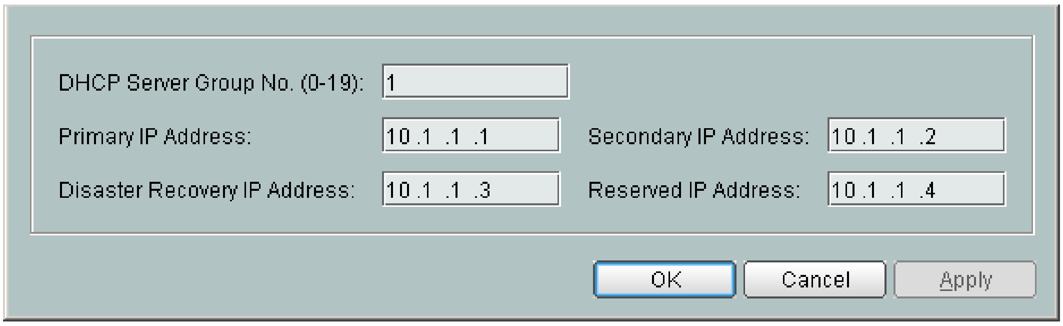
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 Select **DHCP Server Group** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the proper parameters.



DHCP Server Group No. (0-19): 1

Primary IP Address: 10 .1 .1 .1

Secondary IP Address: 10 .1 .1 .2

Disaster Recovery IP Address: 10 .1 .1 .3

Reserved IP Address: 10 .1 .1 .4

Step 6 Click **OK**.

----End

4.1.4.2 Adding a MAC Address Segment

To add a DHCP MAC address segment when the OLT enables the DHCP relay function and the forwarding mode is the MAC address segment mode, perform this operation.

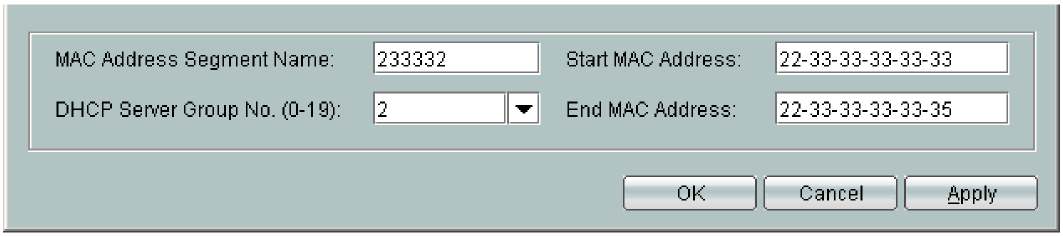
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 Click the **MAC Address Segment** tab, and set the filter criteria to display the required MAC address segments. In the information list, right-click and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters.



MAC Address Segment Name: 233332

Start MAC Address: 22-33-33-33-33-33

DHCP Server Group No. (0-19): 2

End MAC Address: 22-33-33-33-33-35

Step 5 Click **OK**.

----End

4.1.4.3 Configuring a VLAN L3 Interface

The functions of a L3 interface that is based on the VLAN are similar to a L3 switch. Through L3 forwarding, the L3 interface forwards data between different VLANs.

Context

You can configure the L3 interfaces of common VLANs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

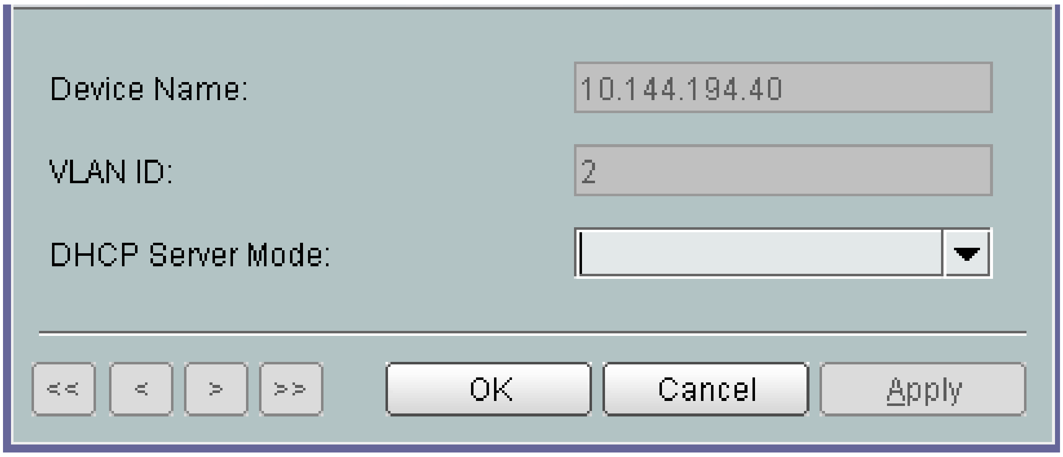
Step 3 Select **VLAN L3 Interface** tab.

Step 4 Right-click a record and choose **Modify** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the proper parameters.

You can set the **DHCP Server Mode** parameter as you need. The options are as follows:

- Standard
- Option-60
- MAC-range



Device Name: 10.144.194.40

VLAN ID: 2

DHCP Server Mode:

Step 6 Click **Done**.

----End

4.1.4.4 Configuring the Gateway IP Address Corresponding to the MAC Address Segment Under an Interface

To configure the gateway IP address corresponding to the MAC address segment under a VLAN interface, perform this operation. When the DHCP relay mode is the MAC address segment forwarding mode, you need to configure the gateway IP address corresponding to the MAC address segment. After the gateway IP address is configured successfully, the OLT can forward packets to the corresponding server through the gateway IP address.

Context

On a VLAN interface, a MAC address segment can be configured with only one gateway IP address, and this gateway IP address must be the IP address already configured on the VLAN interface.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **DHCP** from the navigation tree.

Step 3 Click the **MAC Address Segment** tab, and set the filter criteria to display the required MAC address segments.

Step 4 Select a MAC address segment, and then click the **Gateway of the MAC Address Segment Under the Interface** tab in the lower pane.

Step 5 Right-click a record and choose **Modify** from the shortcut menu.

Step 6 In the dialog box that is displayed, select **Gateway of the MAC Address Segment Under the Interface**.

Step 7 Click **OK**.

----End

4.2 Configuring the MSTP

The Multiple Spanning Tree Protocol (MSTP) is a new spanning tree protocol defined in IEEE 802.1s. MSTP prunes a loop network to a tree network without loops to prevent proliferation and infinite loops of packets. In addition, MSTP provides redundant paths for forwarding packets, thus allowing load balancing between VLANs.

Context

- MSTP sets VLAN mapping tables (relationship tables between VLANs and spanning trees) to associate VLANs and spanning trees so that packets of different VLANs can be forwarded on different spanning trees. In addition, MSTP divides the entire L2 network into multiple MST regions. In each region, multiple spanning trees are generated through calculation, and each spanning tree is called a multiple spanning-tree instance (MSTI). The MSTIs are independent from each other.

- MSTP is applicable to the redundant network, which remedies the drawback of Spanning Tree Protocol (STP) and (Rapid Spanning Tree Protocol) RSTP. MSTP implements fast convergence. In addition, MSTP allocates the traffic of different VLANs to their respective paths, thus providing a better load-balancing mechanism for redundant links.
- MSTP is compatible with STP and supports the MSTP loop networking, which meets the requirement for the flexible networking.

4.2.1 Configuring the MSTP Global Parameters

The Multiple Spanning Tree Protocol (MSTP) prunes a loop network to a tree network without loops to avoid proliferation and infinite loops of the packets. In addition, MSTP provides redundant paths for forwarding packets, thus allowing load balancing between VLANs. MSTP also supports the ring network to meet various networking requirements.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.

Step 3 On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the name of the system parameter profile. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters** navigation tree, and then click **Next**.

Step 6 In the dialog box that is displayed, and choose **Protocol** > **MSTP** on the **System Parameter Settings** navigation tree.

Step 7 In the right pane, set **MSTP Switch** to **Open**, and then set other related parameters according to the plan.

Step 8 Click **Finish**.

Step 9 Select the system parameter profile, right-click, and then choose **Download to NE**.

Step 10 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

4.2.2 Modifying the MST Region Information

After the device is added successfully, the system concurrently adds an MST region named the first MAC address of the device. You can assign multiple devices to one MST region by modifying the MST region information. After the operation is successful, the system recalculates the spanning tree according to the modified information.

Context

The region name, revision level, and operation key in one MST region must be consistent.

Procedure

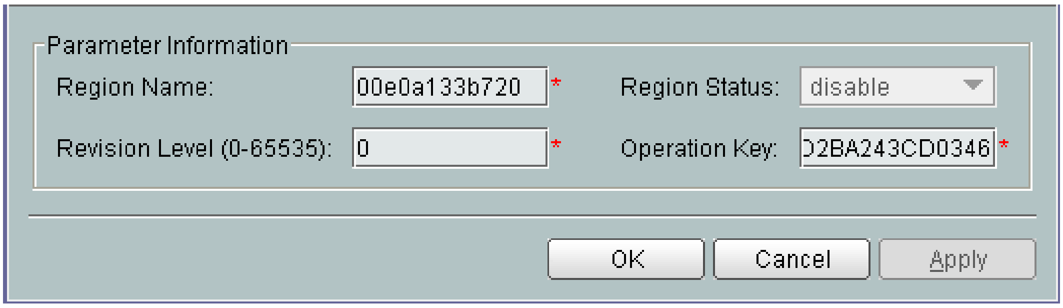
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **MSTP** from the navigation tree.

Step 3 Click the **Region Management** tab, and set the filter criteria to display the required MST regions.

Step 4 Right-click a record and choose **Modify** from the shortcut menu.

Step 5 In the dialog box that is displayed, modify the parameters of **Region Name**, **Revision Level**, and **Operation Key** in the MST region.



Region Name: 00e0a133b720 *
Region Status: disable
Revision Level (0-65535): 0 *
Operation Key: 2BA243CD0346 *

Step 6 Click **OK**.

----End

4.2.3 Adding an MSTI

The system maps different VLANs of the device to the corresponding multiple spanning tree instance (MSTI), elects the root bridge of the spanning tree according to the priority of the bridge, and then generates the spanning tree according to the spanning tree algorithm.

Context

CAUTION

This operation may interrupt services. Excise caution when performing this operation.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **MSTP** from the navigation tree.

Step 3 Click the **Instance Management** tab, right-click, and then choose **Add**.

Step 4 In the dialog box that is displayed, set **Bridge Type**, **Instance ID**, and **VLAN ID** of the port.

Step 5 Click **OK**.

----End

4.2.4 Modifying an MST Port

After an MSTP instance is configured, the related port is generated automatically. You can modify the parameters of the MST port to meet customer requirements.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

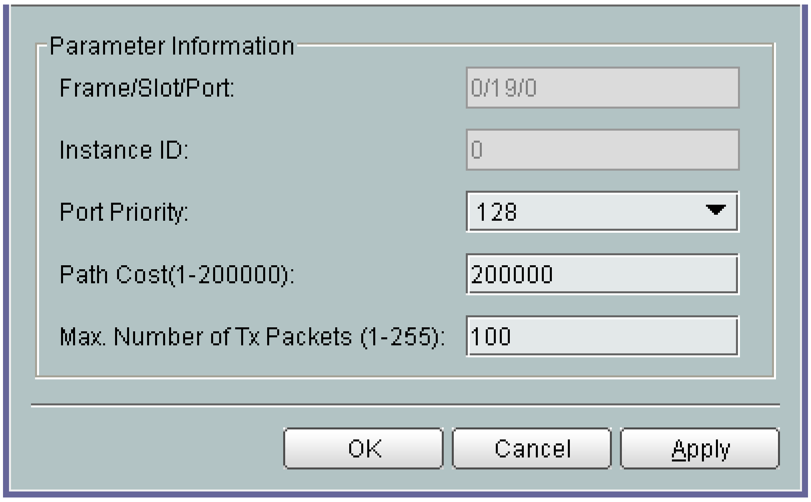
Step 2 Choose **Protocol** > **MSTP** from the navigation tree.

Step 3 Click the **Instance Management** tab, and set the filter criteria to display the required instances.

Step 4 Select an instance and click the **Port and Instance** tab.

Step 5 Right-click a record and choose **Modify** from the shortcut menu.

Step 6 In the dialog box that is displayed, set the parameters.



Parameter Information
Frame/Slot/Port: 0/19/0
Instance ID: 0
Port Priority: 128
Path Cost(1-200000): 200000
Max. Number of Tx Packets (1-255): 100

Step 7 Click **OK**.

----End

5 Configuring the Ethernet Access

About This Chapter

The Ethernet port on the OLT is used in upstream data transmission, slave shelf subtending, and user access.

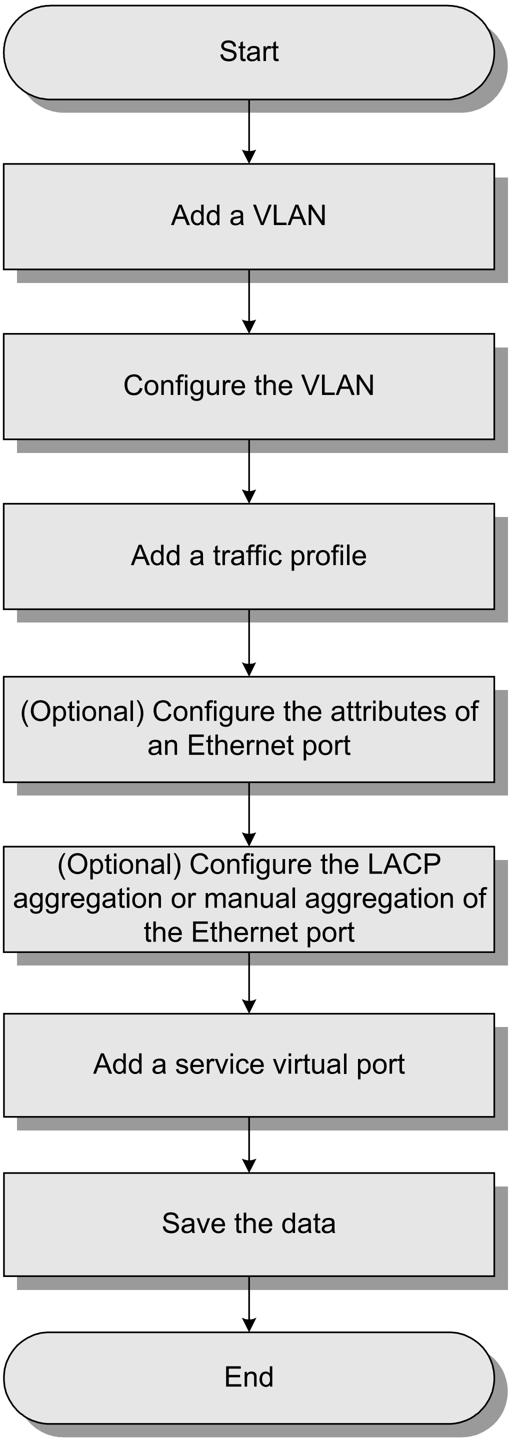
Prerequisites

The corresponding VLAN must exist. For details, see **4.1.2.2 Adding a VLAN**.

Context

Figure 5-1 shows the flowchart for configuring the Ethernet access service on the OLT.

Figure 5-1 Flowchart for configuring the Ethernet access service


Start
Add a VLAN
Configure the VLAN
Add a traffic profile
(Optional) Configure the attributes of an Ethernet port
(Optional) Configure the LACP aggregation or manual aggregation of the Ethernet port
Add a service virtual port
Save the data
End

1. 5.2 Configuring an MEF IP Traffic Profile
   The MEF IP traffic profile defines a series of traffic parameters. It is used to configure the parameters of the traffic streams by being bound to the service port so that the rate of the traffic stream can be limited. When configuring a service port, bind the service port to a MEF IP traffic profile.

2. 5.3 Configuring the Upstream Port of a VLAN
   To enable the user packets with a VLAN tag to be forwarded through an upstream port, perform this operation to add the upstream port to the VLAN. After the upstream port is successfully added, the user packets with this VLAN tag can be forwarded through the corresponding port.
3. 5.4 (Optional) Configuring the Attributes of an Ethernet Port
   This topic describes how to configure the attributes of an Ethernet port, such as the self-negotiation mode, working mode, port rate, and traffic suppression. After successful configuration, the Ethernet port performs communications according to the configured attributes.
4. 5.5 (Optional) Configuring Ethernet Port Aggregation Through the LACP Protocol
   This topic describes how to add an Ethernet port to an LACP static aggregation group and manage the aggregated Ethernet ports through the LACP protocol. Aggregated Ethernet ports share incoming and outgoing loads, and link reliability is enhanced.
5. 5.6 (Optional) Configuring an Aggregated Ethernet Port Manually
   This topic describes how to add an Ethernet port to an aggregation group manually. Aggregated Ethernet ports share incoming and outgoing loads, and link reliability is enhanced.
6. 5.7 Configuring the Service Port
   A service virtual port is used to bear the service streams formed between the user device and the OLT so that the user can access different types of services. Before configuring the services, configure the service virtual ports that bear these services.

5.1 Introduction to the Ethernet Access Service

The Ethernet port on the OLT is used in the upstream data transmission, slave shelf subtending, and user access. You can manage the Ethernet port by configuring the physical attributes, traffic suppression, port aggregation, and port protection for the Ethernet port.

Context

The Ethernet is a LAN standard. It uses a matrix or star topology and adopts the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. The Ethernet supports data transmission rates of 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s. The Ethernet is suitable for the burst services that do not have strict requirements for delays. The IEEE802.3 protocol family specifies detailed standards for the media access control (MAC) sublayer and physical layer of the Ethernet.

The Ethernet access service has the following features:

- High bandwidth: The Ethernet supports the access rates of 10 Mbit/s, 100 Mbit/s, and 1000 Mbit/s.
- Low cost: The Ethernet uses the unshielded twisted-pair cables and fibers as the access media.
- Simple network structure: The Ethernet adopts a topology that is similar to the star topology of an enterprise network. This simple network structure facilitates troubleshooting.

The PC is connected to the service port of the OPFA card on the OLT through the optical modem. In this way, the point-to-point fiber connection is established. The user data packets are sent to the OLT through the optical modem, and then sent upstream to the upper layer network through the upstream port of the control card.

5.2 Configuring an MEF IP Traffic Profile

The MEF IP traffic profile defines a series of traffic parameters. It is used to configure the parameters of the traffic streams by being bound to the service port so that the rate of the traffic stream can be limited. When configuring a service port, bind the service port to a MEF IP traffic profile.

Context

When an MEF IP traffic profile is added through the U2000, the MEF IP traffic profile is added to only the database of the U2000, but is not applied to the device. This MEF IP traffic profile is created on a device only when the device references the MEF IP traffic profile to create a service port or the MEF IP traffic profile is manually applied to the device.

Procedure

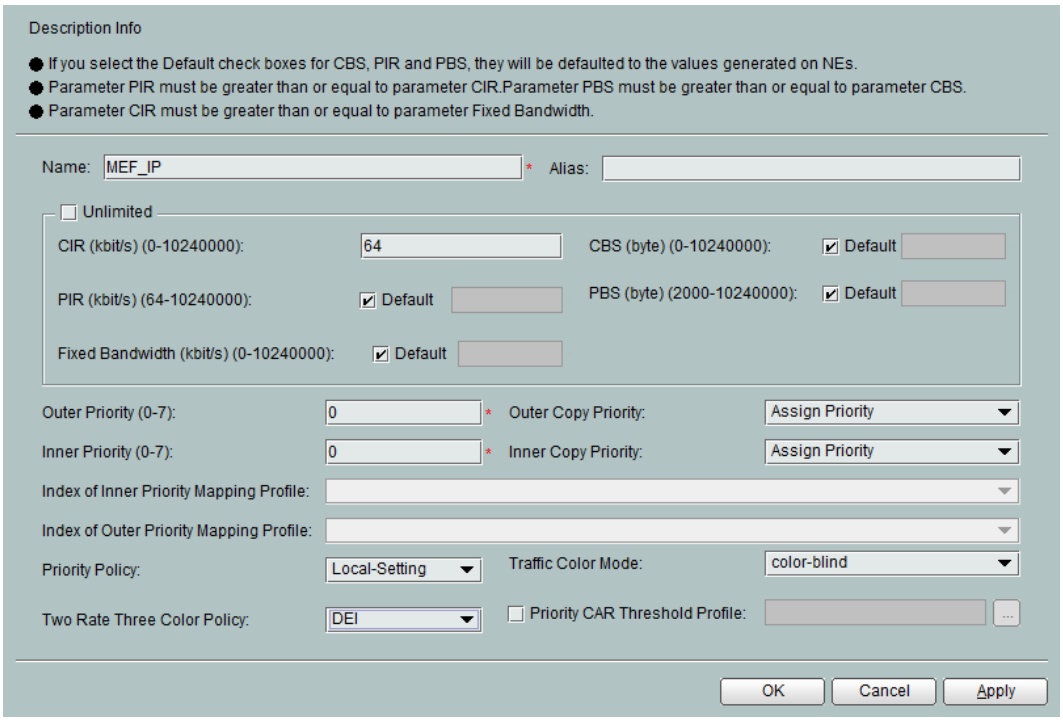
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.

Step 3 Click the **MEF IP Traffic Profile** tab.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Description Info

- If you select the Default check boxes for CBS, PIR and PBS, they will be defaulted to the values generated on NEs.
- Parameter PIR must be greater than or equal to parameter CIR.Parameter PBS must be greater than or equal to parameter CBS.
- Parameter CIR must be greater than or equal to parameter Fixed Bandwidth.

Name: MEF_IP * Alias:

☐ Unlimited

CIR (kbit/s) (0-10240000): 64
CBS (byte) (0-10240000): ☑ Default
PIR (kbit/s) (64-10240000): ☑ Default
PBS (byte) (2000-10240000): ☑ Default
Fixed Bandwidth (kbit/s) (0-10240000): ☑ Default

Outer Priority (0-7): 0 *
Outer Copy Priority: Assign Priority
Inner Priority (0-7): 0 *
Inner Copy Priority: Assign Priority
Index of Inner Priority Mapping Profile:
Index of Outer Priority Mapping Profile:
Priority Policy: Local-Setting
Traffic Color Mode: color-blind
Two Rate Three Color Policy: DEI
☐ Priority CAR Threshold Profile:

Step 6 Click **OK**.

Step 7 Select the traffic profile, right-click, and then choose **Download to NE**.

Step 8 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

5.3 Configuring the Upstream Port of a VLAN

To enable the user packets with a VLAN tag to be forwarded through an upstream port, perform this operation to add the upstream port to the VLAN. After the upstream port is successfully added, the user packets with this VLAN tag can be forwarded through the corresponding port.

Prerequisites

The corresponding VLAN must exist. For details about adding a VLAN, see **4.1.2.2 Adding a VLAN**.

Procedure

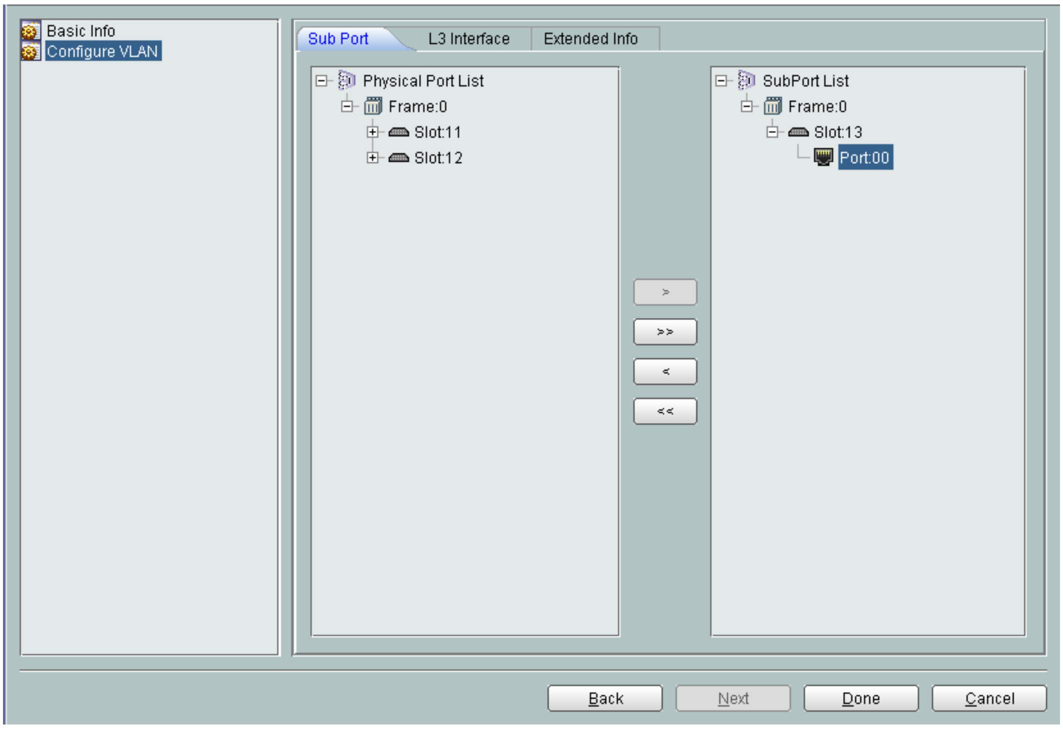
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.

Step 4 Select the VLAN to be configured, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, choose **Configure VLAN** from the navigation tree. Click the **Sub Port** tab, and then set the upstream port of the VLAN.



Step 6 Click **Done**.

----End

5.4 (Optional) Configuring the Attributes of an Ethernet Port

This topic describes how to configure the attributes of an Ethernet port, such as the self-negotiation mode, working mode, port rate, and traffic suppression. After successful configuration, the Ethernet port performs communications according to the configured attributes.

Context

- The basic principle for setting the working mode and rate of an Ethernet port is to keep the consistency of the port settings between two connected devices.
- When the Ethernet port is in the self-negotiation mode, you need to disable the self-negotiation mode first before modifying the port rate or working mode of the Ethernet port.
- By default, the duplex state of an FE electrical port is set to the auto (self-negotiation) mode. The working mode of the FE/GE optical port is set to the full duplex mode by the system, and it cannot be changed.

- The traffic control function takes effect only when the function is supported by the remote device and the OLT. If the remote device supports the traffic control function, enable the traffic control function on the OLT. If the remote device does not support the traffic control function, disable the traffic control function on the OLT.
- The native VLAN attribute (PVID) of an Ethernet port determines whether VLAN tags are added to the packets of the upstream Ethernet port.
  - If the ID of the VLAN to which the Ethernet port belongs and the ID of the native VLAN are the same, no VLAN tags are added to the packets of the upstream Ethernet port.
  - If the ID of the VLAN to which the Ethernet port belongs and the ID of the native VLAN are different, VLAN tags are added to the packets of the upstream Ethernet port.

Procedure

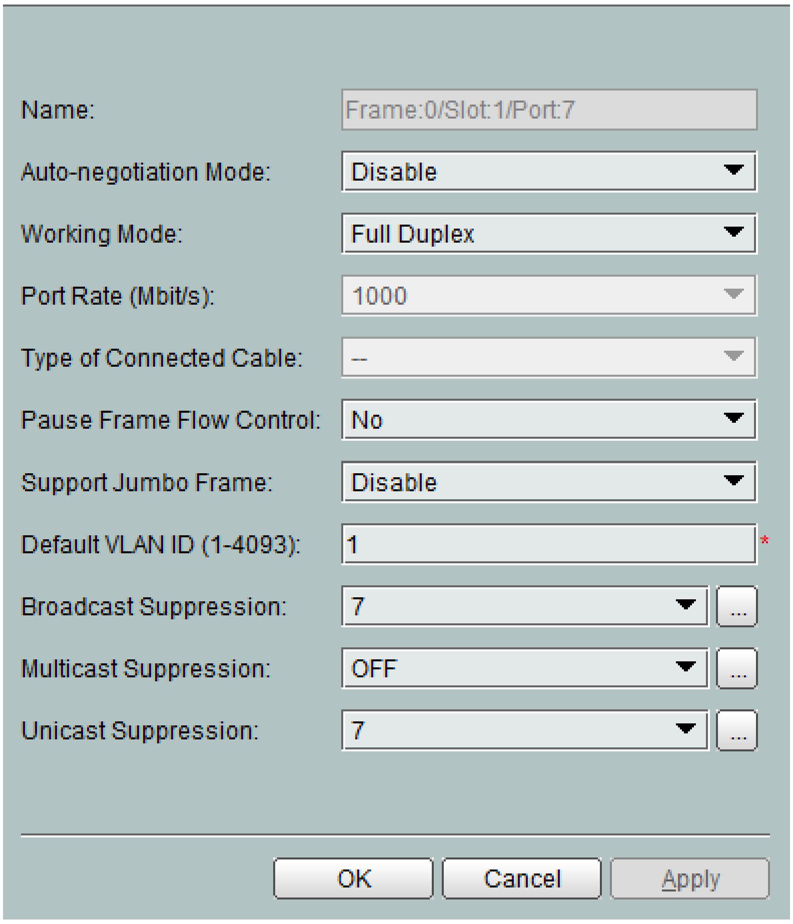
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ETH Port** from the navigation tree.

Step 3 Click the **Ethernet Port** tab, and set the filter criteria or click ⌄ to display the Ethernet ports.

Step 4 Select a record from the Ethernet port list, right-click, and then choose **Configure Attributes**.

Step 5 In the dialog box that is displayed, set the parameters.



Name: Frame:0/Slot:1/Port:7
Auto-negotiation Mode: Disable
Working Mode: Full Duplex
Port Rate (Mbit/s): 1000
Type of Connected Cable: --
Pause Frame Flow Control: No
Support Jumbo Frame: Disable
Default VLAN ID (1-4093): 1 *
Broadcast Suppression: 7
Multicast Suppression: OFF
Unicast Suppression: 7

Step 6 Click **OK**.

NOTE

- The interfaces of port attribute configuration may vary with the values of the parameters. Configure the port attributes according to the data plan.
- Before enabling the self-negotiation mode of an Ethernet port, make sure that the interconnected devices both support the self-negotiation mode.
- The type of the cable connected to the port must match the configured cable negotiation mode.

----End

5.5 (Optional) Configuring Ethernet Port Aggregation Through the LACP Protocol

This topic describes how to add an Ethernet port to an LACP static aggregation group and manage the aggregated Ethernet ports through the LACP protocol. Aggregated Ethernet ports share incoming and outgoing loads, and link reliability is enhanced.

Context

Configure Ethernet port mirroring and flow mirroring. In this manner, the product does not resolve or process the captured data.

The Link Aggregation Control Protocol (LACP) is part of the IEEE 802.3ad standard. A device on which the LACP runs exchanges information with the peer device through the link aggregation control protocol data units (LACPDU). Through the LACP, the ports of the devices are aggregated automatically without manual operation. The LACP can also be used to detect link-layer failures and faulty ports, control link aggregation, and trigger protection switching.

The Ethernet ports to be aggregated must meet the following conditions:

- For UA5000(IPMB)/MA5680T/MA5800, MA5606T/MA5600:
  - Destination ports for mirroring, ports configured with a MUX VLAN, and ports that have been added to an aggregation group cannot be aggregated.
  - Ports on the boards in two different slots cannot be aggregated.
  - An optical port and an electrical port can be added to an aggregation group.
- For MA5600T and MA5608T, information about boards that can be aggregated are as follows:
  - H801ETHA, H801ETHB, SCU series ontrol boards, and GIU series upstream interface boards support port aggregation.
  - GIU series upstream interface boards and H801ETHB boards support inter-board aggregation but H801ETHA and SCU series ontrol boards do not.
- The following ports cannot to be configured with port aggregation:
  - Destination ports and ports that have been added to an aggregation group
  - GPON uplink ports or MPLS ports
  - Ports on a link configured with an MEP
  - Ethernet ports working in half duplex mode
  - Ports configured with static MAC addresses
  - Ports configured with protection pairs

  - Ports configured with static ARPs
  - Ports configured with ACL rules
  - IP cascading ports configured with static programs
- The slave ports must meet the following conditions:
  - The master port is not configured with a protection group.
  - The native VLAN ID and the VLAN ID of the slave ports must be the default value or be the same with those of the master port.
  - Their network role and isolation status must be consistent with the master port.
  - MEPs are not configured on slave ports.
- The configurations of all ports in an aggregation group must be the same, and a forced port and an auto negotiation port can be in an aggregation group.

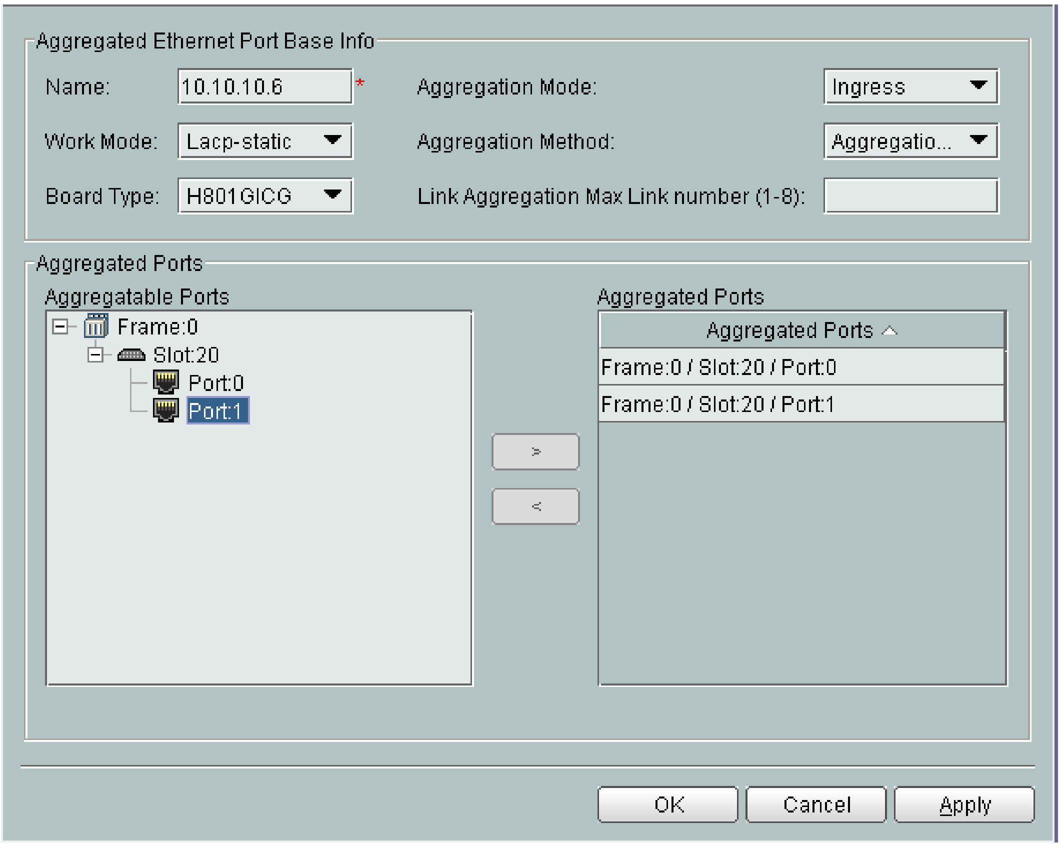
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ETH Port** from the navigation tree.

Step 3 On the **Aggregation Group** tab, right-click and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set **Work Mode** to **LACP-static**, and then set **Name**, **Board Type**, **Aggregation Mode**, and **Aggregated Ports** as follows.



Aggregated Ethernet Port Base Info

Name: 10.10.10.6 *

Work Mode: Lacp-static

Board Type: H801GICG

Aggregation Mode: Ingress

Aggregation Method: Aggregatio...

Link Aggregation Max Link number (1-8):

Aggregated Ports

Aggregatable Ports

Aggregated Ports

Aggregated Ports
Frame:0 / Slot:20 / Port:0
Frame:0 / Slot:20 / Port:1

Step 5 Click **OK**.

NOTE

The interfaces of aggregated Ethernet port configuration may vary with the values of the parameters. Configure the aggregated Ethernet ports according to the data plan.

----End

5.6 (Optional) Configuring an Aggregated Ethernet Port Manually

This topic describes how to add an Ethernet port to an aggregation group manually. Aggregated Ethernet ports share incoming and outgoing loads, and link reliability is enhanced.

Context

Configure Ethernet port mirroring and flow mirroring. In this manner, the product does not resolve or process the captured data.

In manual aggregation, the aggregation group is configured manually without using the LACP. The member links in the aggregation group are fixed. These links can only be modified manually. The system cannot add a link to or delete a link from the aggregation group. Because the aggregation group and member links are fixed and managed manually, aggregation management is performed conveniently.

During manual link aggregation, however, the LACP is not used and the systems at both ends of the link do not negotiate the aggregation. As a result, the aggregation control may be inaccurate and ineffective. For example, if a physical link is incorrectly connected to a port that does not support link aggregation, the system cannot detect this incorrect connection.

The Ethernet ports to be aggregated must meet the following conditions:

- For UA5000(IPMB)/MA5680T/MA5800/MA5606T/MA5600:
  - Destination ports for mirroring, ports configured with a MUX VLAN, and ports that have been added to an aggregation group cannot be aggregated.
  - Ports on the boards in two different slots cannot be aggregated.
  - An optical port and an electrical port can be added to an aggregation group.
- For MA5600T and MA5608T, information about boards that can be aggregated are as follows:
  - H801ETHA, H801ETHB, SCU series ontrol boards, and GIU series upstream interface boards support port aggregation.
  - GIU series upstream interface boards and H801ETHB boards support inter-board aggregation but H801ETHA and SCU series ontrol boards do not.
- The following ports cannot to be configured with port aggregation:
  - Destination ports and ports that have been added to an aggregation group
  - GPON uplink ports or MPLS ports
  - Ports on a link configured with an MEP
  - Ethernet ports working in half duplex mode
  - Ports configured with static MAC addresses
  - Ports configured with protection pairs

  - Ports configured with static ARPs
  - Ports configured with ACL rules
  - IP cascading ports configured with static programs
- The slave ports must meet the following conditions:
  - The master port is not configured with a protection group.
  - The native VLAN ID and the VLAN ID of the slave ports must be the default value or be the same with those of the master port.
  - Their network role and isolation status must be consistent with the master port.
  - MEPs are not configured on slave ports.
- The configurations of all ports in an aggregation group must be the same, and a forced port and an auto negotiation port can be in an aggregation group.

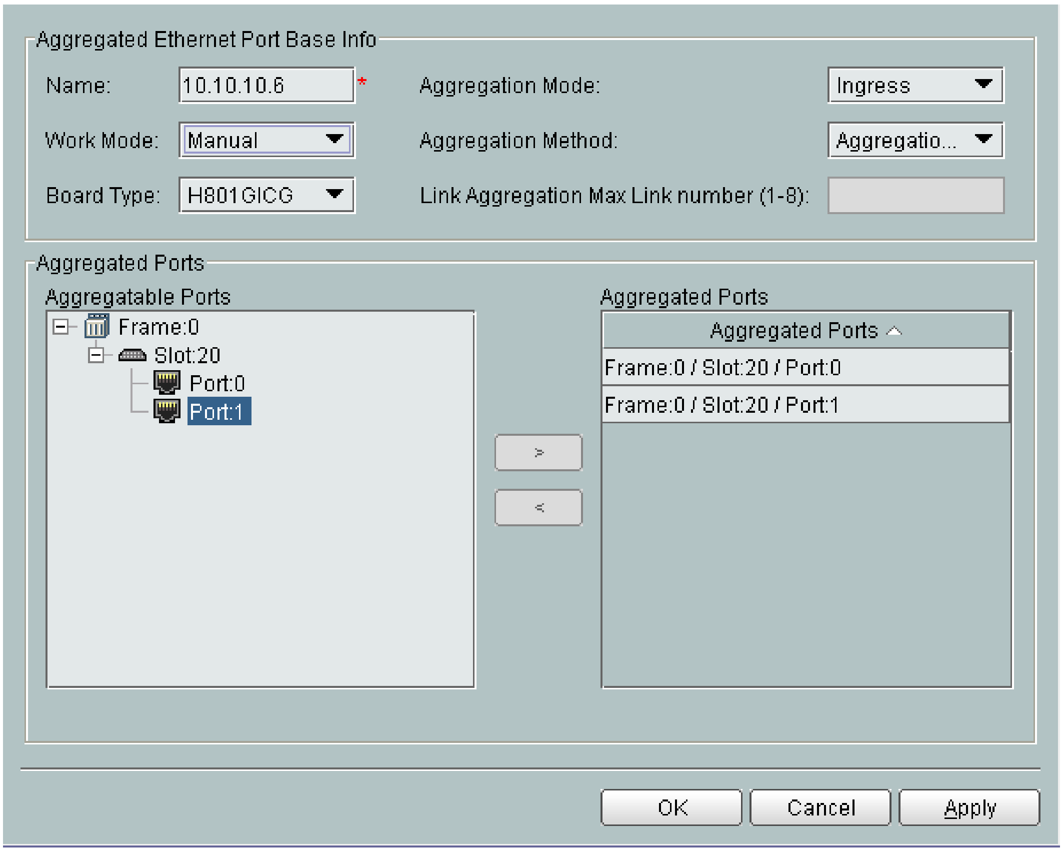
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ETH Port** from the navigation tree.

Step 3 On the **Aggregation Group** tab page, right-click and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set **Work Mode** to **Manual**, and then set **Aggregation Name**, **Aggregation Mode**, **Board Type**, and **Aggregated Ports** as follows.



Aggregated Ethernet Port Base Info

Name: 10.10.10.6 *
Aggregation Mode: Ingress
Work Mode: Manual
Aggregation Method: Aggregatio...
Board Type: H801GICG
Link Aggregation Max Link number (1-8):

Aggregated Ports

Aggregatable Ports
Frame:0
  Slot:20
    Port:0
    Port:1

Aggregated Ports

Aggregated Ports
Frame:0 / Slot:20 / Port:0
Frame:0 / Slot:20 / Port:1

Step 5 Click **OK**.

NOTE

The interfaces of aggregated Ethernet port configuration may vary with the values of the parameters. Configure the aggregated Ethernet ports according to the data plan.

----End

5.7 Configuring the Service Port

A service virtual port is used to bear the service streams formed between the user device and the OLT so that the user can access different types of services. Before configuring the services, configure the service virtual ports that bear these services.

Prerequisites

- The VLAN to which the service virtual port belongs must be configured. For details, see **4.1.2.2 Adding a VLAN**.
- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- The traffic profile must be configured. For details, see **5.2 Configuring an MEF IP Traffic Profile** (where the configuration of an MEF IP traffic profile is provided as an example).

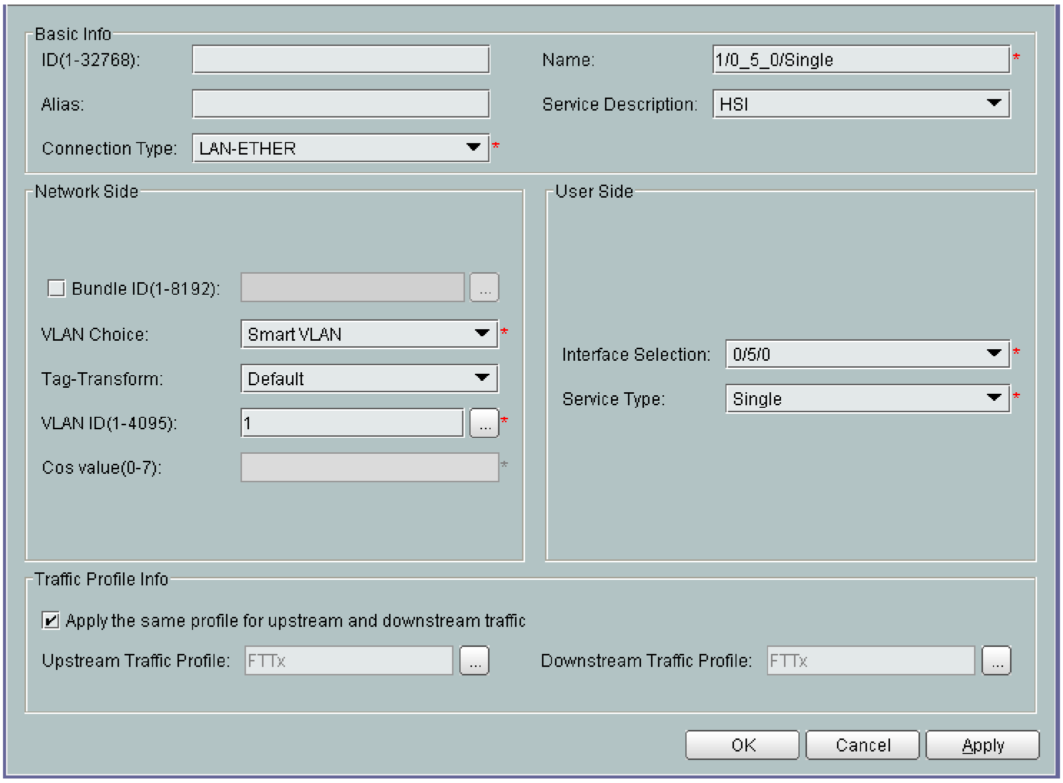
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Connection** > **Service Port** from the navigation tree.

Step 3 On the **Service Port** table page, right-click, and then choose **Add**.

Step 4 In the dialog box that is displayed, set the parameters.



Name: 1/0_5_0/Single

Service Description: HSI

Connection Type: LAN-ETHER

☐ Bundle ID(1-8192):

VLAN Choice: Smart VLAN

Tag-Transform: Default

VLAN ID(1-4095): 1

Cos value(0-7):

Interface Selection: 0/5/0

Service Type: Single

☑ Apply the same profile for upstream and downstream traffic

Upstream Traffic Profile: FTTx

Downstream Traffic Profile: FTTx

Step 5 Click **OK**.

NOTE

The interfaces of adding service virtual ports may vary with the values of the parameters. Configure the service virtual ports according to the data plan.

----End

6 Configuring the xDSL Access

About This Chapter

This topic describes the VDSL2 in the xDSL technology and how to configure the IPoA, PPPoA, and bridge access services on the OLT.

6.1 Introduction to the xDSL Access
Using the existing twisted pair and high frequency (higher than 4 kHz) data compress method, the xDSL technology is a modulation technology providing users with a high rate and high frequency Internet service. Because the xDSL have a higher frequency spectrum than common communication signal, the twisted pair can transmit the voice signal when providing the Internet service with the xDSL technology.

6.2 Configuring the xDSL-Related Profiles
Before you provision services for network elements, you can configure the xDSL-related profiles according to the global data plan. The xDSL-related profiles can improve the service quality by limiting the port rate and noise margin, and can monitor the performance of the port by configuring the related thresholds.

6.3 Configuring the xDSL Access Services
This topic describes how to configure the IPoA, PPPoA, and bridge access services based on the xDSL technology on the OLT.

6.4 Configuration Example of a VDSL2 Access Service in Bridging Mode
This topic describes how to configure a VDSL2 access service in bridging mode in an example network. Configure the access service by referring to this example when the service streams on the modem is activated in bridging mode. After the configuration, you can access the Internet in PPPoE mode over VDSL2 lines.

6.5 Configuration Example of the ADSL IPoA Access Service
This topic describes how to configure the ADSL IPoA access service based on the example network. After the configuration, the user can log in to the Internet through the ADSL line in the IPoA mode.

6.6 Configuration Example of the VDSL2 PPPoA Access Service
This topic describes how to configure the VDSL2 PPPoA access service in an example network. After the configuration, you can access the Internet in PPPoA mode over VDSL2 lines.

6.7 Configuration Example of the VDSL2 PPPoE Service

Based on the example network, this topic describes how to configure the VDSL2 PPPoE service and how to access the Internet in the PPPoE mode through the VDSL2 line after the configuration.

6.8 Querying Line Running Status of Lines on xDSL Ports
This topic describes how to learn about the running status of lines on activated xDSL ports by querying subcarrier information, including bit allocation, gain allocation, SNR, HLOG, and QLN.

6.9 Managing an SHDSL Regenerator
The single-pair high-speed digital subscriber line (SHDSL) can transmit signals for a maximum of 6 kilometers. In some sparsely populated areas, regenerators are needed between the central office (CO) and the customer premises equipment (CPE); such regenerators implement extremely long distance transmission by extending the transmission distance.

6.1 Introduction to the xDSL Access

Using the existing twisted pair and high frequency (higher than 4 kHz) data compress method, the xDSL technology is a modulation technology providing users with a high rate and high frequency Internet service. Because the xDSL have a higher frequency spectrum than common communication signal, the twisted pair can transmit the voice signal when providing the Internet service with the xDSL technology.

Context

- ADSL stands for asymmetric digital subscriber line. The ADSL technology uses the asymmetric transmission mode. It provides asymmetric upstream and downstream rates over the existing twisted pair. Users can access the Internet over the ADSL line. The ADSL technology has three standards, namely, ADSL standard, ADSL2 standard, and ADSL2+ standard.
  - The ADSL technology has the following features:
    - The asymmetric digital subscriber line uses the existing twisted pair to transmit data information with high bandwidth for enterprises and family users. Different from the current dialing telephone service, the service provided by the ADSL technology is continuous and always online.
    - The ADSL technology is asymmetric, that is, the ADSL technology uses most of the service channel in the downstream transmission and little service channel to receive information from the users.
    - The ADSL technology can store the analog (voice) and data signals on the same line at the same time.
  - The ADSL technology has the following specifications:
    - The ADSL technology supports the maximum downstream rate 8 Mbit/s, the maximum upstream rate 896 kbit/s, and the maximum transmission distance 5 km.
    - The ADSL2+ technology supports the maximum downstream rate 24 Mbit/s, the maximum upstream rate 2.5 Mbit/s, and the maximum transmission distance 6.5 km.
    - The ADSL2+ is the development of the ADSL technology and the device that supports the ADSL2+ access can support the ADSL and ADSL2 access.
- G.SHDSL stands for G.single-pair high-speed digital subscriber line. As a high-speed symmetric transmission technology, it uses the existing unused high frequency in the twisted pair to transmit the data at a high speed with different modulation methods.
  - The G.SHDSL technology has the following features:
    - The transmission rate of the G.SHDSL technology is related to the transmission distance and line quality. Generally, the longer the transmission distance, the poorer is the line quality and the lower is the transmission rate; the shorter the transmission distance, the better is the line quality and the higher is the transmission rate.
    - A G.SHDSL connection can automatically adjust its rate to a proper value according to the line status, such as distance and noise.
  - The G.SHDSL technology has the following specifications:
    - The G.SHDSL supports the transmission distance 3-6 km.
    - The G.SHDSL supports two-wire, four-wire, six-wire, and eight-wire G.SHDSL access. The rate of the two-wire G.SHDSL line ranges from 192 kbit/s to 5696 kbit/

s. The rate of the four-wire G.SHDSL line ranges from 384 kbit/s to 11392 kbit/s. The rate of the six-wire G.SHDSL line ranges from 576 kbit/s to 17088 kbit/s. The rate of the eight-wire G.SHDSL line ranges from 768 kbit/s to 22784 kbit/s.

- The very high speed digital subscriber line 2 (VDSL2) is the development of the VDSL. It uses the existing twisted pair to provide the asymmetric or symmetric high-speed access service for the users.
  - The VDSL2 technology has the following feature: The VDSL technology supports spectrum profiles of various types and in various encapsulation modes. Hence, the VDSL2 technology provides short-distance and high-rate solutions to the next generation FTTx access scenarios.
  - The VDSL2 technology has the following specifications:
    - The VDSL2 technology supports the maximum symmetric rates 100 Mbit/s, and the maximum transmission distance 3.5 km.
    - When ADSL or ADSL2+ terminal units are connected to VDSL2 lines, the VDSL2 lines can work in the ADSL or ADSL2+ mode.
    - The VDSL2 access service supports two encapsulation modes, that is, ATM and PTM.
      - ATM mode: Transmits the ATM cell on the channel
      - PTM mode: Transmits the IP packet on the channel

6.2 Configuring the xDSL-Related Profiles

Before you provision services for network elements, you can configure the xDSL-related profiles according to the global data plan. The xDSL-related profiles can improve the service quality by limiting the port rate and noise margin, and can monitor the performance of the port by configuring the related thresholds.

Context

- The asymmetric digital subscriber line (ADSL) adopts the asymmetric transmission mode. It provides asymmetric upstream and downstream rates over an existing POTS line. ADSL profiles include ADSL line profiles, ADSL alarm profiles, and ADSL extended profiles. The ADSL line profile provides parameters that are required for activating an ADSL port. After the ADSL line profile is configured successfully, when you configure the attributes of the ADSL port, you can directly reference the ADSL line profile to limit the port rate and noise margin to improve the service quality. The ADSL alarm profile is used to monitor the performance of the ADSL port. The ADSL extended profile is used to improve the reliability of the line, that is, the profile disables certain sub-channels that are affected by much interference.
- The very high speed digital subscriber line (VDSL2) is a transmission technology that is used to provide high-speed leased line access over the twisted pairs in the asymmetrical or symmetrical mode. VDSL2 is an extension of VDSL. The VDSL2 profiles include the VDSL2 line configuration profile and VDSL2 alarm configuration profile. The VDSL2 line profile limits the port rate and noise margin to improve the service quality by referencing the VDSL2 line configuration profile and VDSL2 channel configuration profile. The VDSL2 alarm profile monitors the performance of the VDSL2 port by referencing the VDSL2 line alarm configuration profile and VDSL2 channel alarm configuration profile.

- The G.SHDSL line profile provides parameters that are required for activating the ATM G.SHDSL port. After the G.SHDSL line profile is configured successfully, when you configure the attributes of the ATM G.SHDSL port, you can directly reference the G.SHDSL line profile to limit the port rate and noise margin to improve the service quality. The G.SHDSL alarm profile defines a series of alarm parameters for measuring the G.SHDSL port performance. You can monitor the performance of the G.SHDSL line by setting thresholds for these alarm parameters.

6.2.1 Configuring the IPoA Parameters

IP over ATM (IPoA) is a technology by which the payloads of the ATM packets are converted into the Ethernet frames which are transmitted to the upstream, and the IPoE packets are converted into the IPoA packets which are forwarded to the user. IPoA is used for the private line access. It meets the carriers' requirements for the transition from the ATM network to the IP network.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.

Step 3 On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the name of the system parameter profile. Select **Encapsulation Management** > **IPoA** from the **Parameters for Selection** navigation tree. Click > to add the parameters to the **Selected Parameters**, and then click **Next**.

Step 6 In the right pane, set **IPoA Enable state** to **Open**, and then set other related parameters according to the plan.

Step 7 Click **Finish**.

Step 8 Select the system parameter profile, right-click, and then choose **Download to NE**.

Step 9 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

6.2.2 Configuring the PPPoA Parameters

After the PPPoA conversion to PPPoE function is enabled, and the service is configured correctly, the service in ATM mode is transmitted upstream to the IP network through the uplink port.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.

Step 3 On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the name of the system parameter profile. Select **Encapsulation Management** > **PPPoA** from the **Parameters for Selection** navigation tree. Click > to add the parameters to the **Selected Parameters**, and then click **Next**.

Step 6 In the right pane, set **PPPoA to PPPoE switch** to **Open**, and then set other related parameters according to the plan.

Step 7 Click **Finish**.

Step 8 Select the system parameter profile, right-click, and then choose **Download to NE**.

Step 9 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

6.2.3 Configuring an ADSL Line Profile

An ADSL line profile provides parameters that are required for activating an ADSL port. After the ADSL line profile is configured successfully, you can directly refer to the ADSL line profile when configuring attributes of the ADSL port to limit the port rate and noise margin to improve the service quality.

Context

- A profile name identifies a profile. Therefore, the profile name must be specified and unique. Otherwise, the profile cannot be added.
- You can add profiles that have the same parameters but different names.
- A profile takes effect only after it is applied to NEs.

Procedure

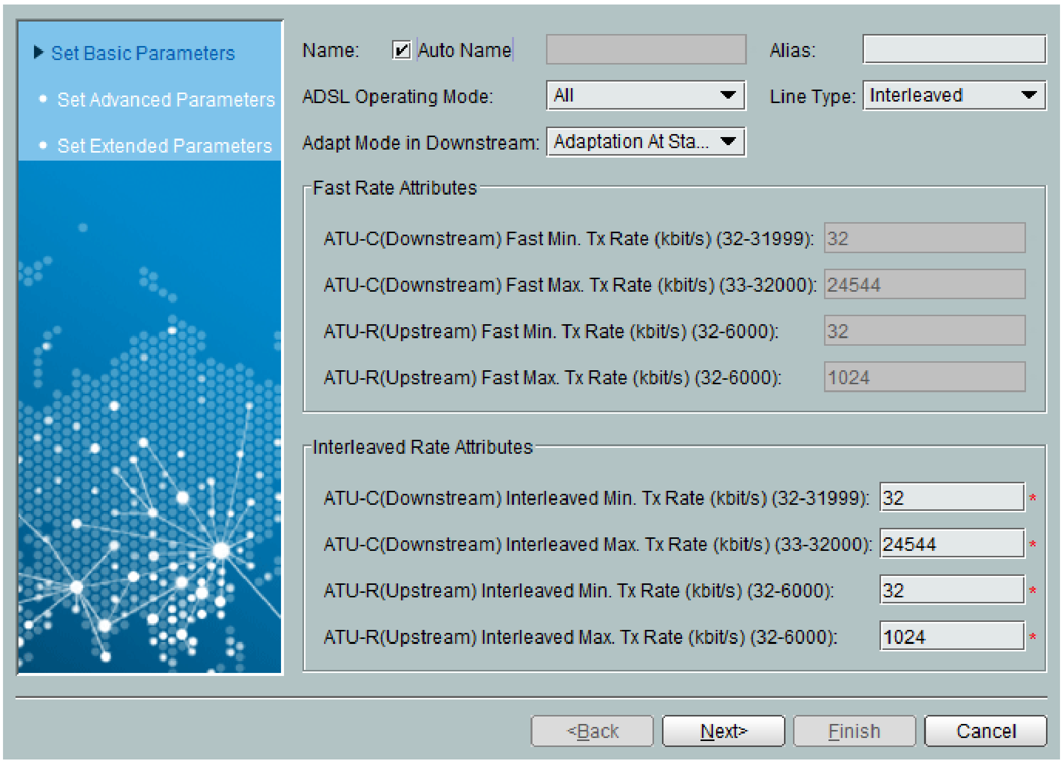
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **DSL Profile** > **ADSL Profile** from the navigation tree.

Step 3 Click the **ADSL Line Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: ☑ Auto Name
Alias:
ADSL Operating Mode: All
Line Type: Interleaved
Adapt Mode in Downstream: Adaptation At Sta...

Fast Rate Attributes

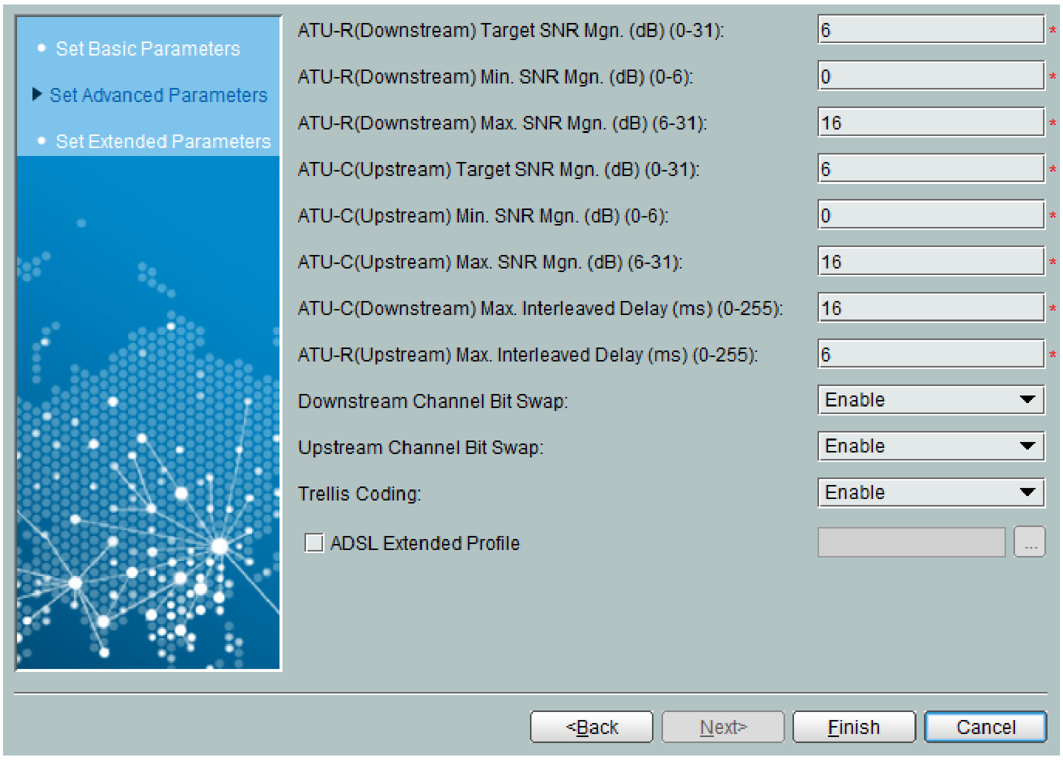
ATU-C(Downstream) Fast Min. Tx Rate (kbit/s) (32-31999): 32
ATU-C(Downstream) Fast Max. Tx Rate (kbit/s) (33-32000): 24544
ATU-R(Upstream) Fast Min. Tx Rate (kbit/s) (32-6000): 32
ATU-R(Upstream) Fast Max. Tx Rate (kbit/s) (32-6000): 1024

Interleaved Rate Attributes

ATU-C(Downstream) Interleaved Min. Tx Rate (kbit/s) (32-31999): 32 *
ATU-C(Downstream) Interleaved Max. Tx Rate (kbit/s) (33-32000): 24544 *
ATU-R(Upstream) Interleaved Min. Tx Rate (kbit/s) (32-6000): 32 *
ATU-R(Upstream) Interleaved Max. Tx Rate (kbit/s) (32-6000): 1024 *

Step 6 Click **Next**.

Step 7 In the dialog box that is displayed, set the parameters.



ATU-R(Downstream) Target SNR Mgn. (dB) (0-31): 6 *
ATU-R(Downstream) Min. SNR Mgn. (dB) (0-6): 0 *
ATU-R(Downstream) Max. SNR Mgn. (dB) (6-31): 16 *
ATU-C(Upstream) Target SNR Mgn. (dB) (0-31): 6 *
ATU-C(Upstream) Min. SNR Mgn. (dB) (0-6): 0 *
ATU-C(Upstream) Max. SNR Mgn. (dB) (6-31): 16 *
ATU-C(Downstream) Max. Interleaved Delay (ms) (0-255): 16 *
ATU-R(Upstream) Max. Interleaved Delay (ms) (0-255): 6 *
Downstream Channel Bit Swap: Enable
Upstream Channel Bit Swap: Enable
Trellis Coding: Enable
☐ ADSL Extended Profile

Step 8 Click **Finish**.

----End

6.2.4 Configuring an ADSL Alarm Profile

When the ADSL port is activated, it directly refer to the ADSL alarm profile to monitor the port performance. When the actual parameter value of the port exceeds the threshold, an alarm is generated.

Context

- A profile name identifies a profile. Therefore, the profile name must be specified and unique. Otherwise, the profile cannot be added.
- You can add profiles that have the same parameters but different names.
- A profile takes effect only after it is applied to NEs.

Procedure

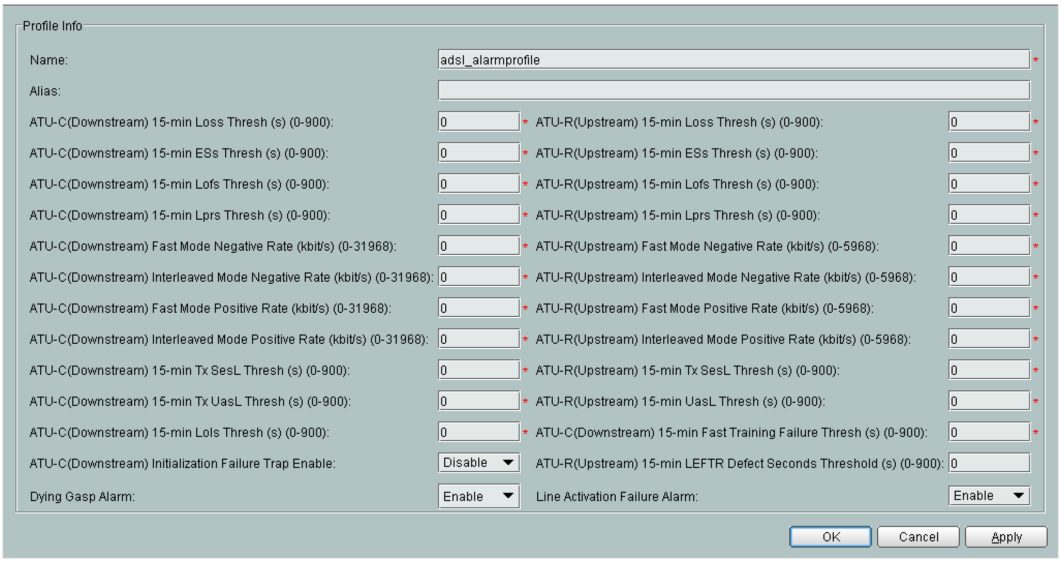
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **DSL Profile** > **ADSL Profile** from the navigation tree.

Step 3 Click the **ADSL Alarm Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Profile Info

Name: adsl_alarmprofile *
Alias:
ATU-C(Downstream) 15-min Loss Thresh (s) (0-900): 0 *
ATU-R(Upstream) 15-min Loss Thresh (s) (0-900): 0 *
ATU-C(Downstream) 15-min ESs Thresh (s) (0-900): 0 *
ATU-R(Upstream) 15-min ESs Thresh (s) (0-900): 0 *
ATU-C(Downstream) 15-min Lofs Thresh (s) (0-900): 0 *
ATU-R(Upstream) 15-min Lofs Thresh (s) (0-900): 0 *
ATU-C(Downstream) 15-min Lprs Thresh (s) (0-900): 0 *
ATU-R(Upstream) 15-min Lprs Thresh (s) (0-900): 0 *
ATU-C(Downstream) Fast Mode Negative Rate (kbit/s) (0-31968): 0 *
ATU-R(Upstream) Fast Mode Negative Rate (kbit/s) (0-5968): 0 *
ATU-C(Downstream) Interleaved Mode Negative Rate (kbit/s) (0-31968): 0 *
ATU-R(Upstream) Interleaved Mode Negative Rate (kbit/s) (0-5968): 0 *
ATU-C(Downstream) Fast Mode Positive Rate (kbit/s) (0-31968): 0 *
ATU-R(Upstream) Fast Mode Positive Rate (kbit/s) (0-5968): 0 *
ATU-C(Downstream) Interleaved Mode Positive Rate (kbit/s) (0-31968): 0 *
ATU-R(Upstream) Interleaved Mode Positive Rate (kbit/s) (0-5968): 0 *
ATU-C(Downstream) 15-min Tx SesL Thresh (s) (0-900): 0 *
ATU-R(Upstream) 15-min Tx SesL Thresh (s) (0-900): 0 *
ATU-C(Downstream) 15-min Tx UasL Thresh (s) (0-900): 0 *
ATU-R(Upstream) 15-min UasL Thresh (s) (0-900): 0 *
ATU-C(Downstream) 15-min Lols Thresh (s) (0-900): 0 *
ATU-C(Downstream) 15-min Fast Training Failure Thresh (s) (0-900): 0 *
ATU-C(Downstream) Initialization Failure Trap Enable: Disable
ATU-R(Upstream) 15-min LEFTR Defect Seconds Threshold (s) (0-900): 0
Dying Gasp Alarm: Enable
Line Activation Failure Alarm: Enable

Step 6 Click **OK**.

----End

6.2.5 Configuring a VDSL2 Line Profile

The VDSL2 line profile binds the specified VDSL2 line configuration profile to the VDSL2 channel configuration profile. After a VDSL2 line profile is bound to a VDSL2 port, the activated VDSL2 port directly references the VDSL2 line profile to limit the port rate and noise margin to improve the service quality.

Context

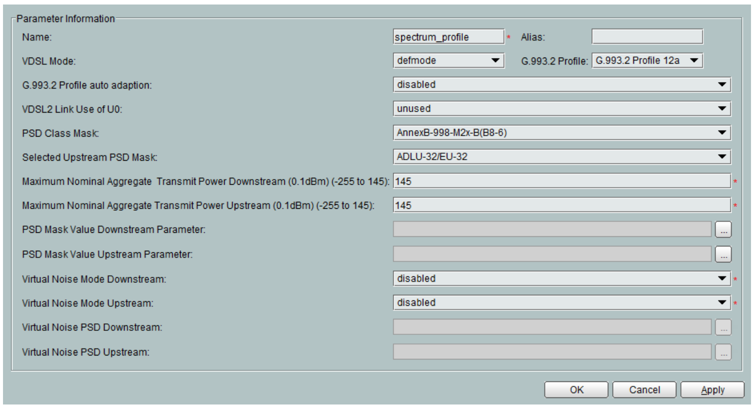
A profile takes effect only after it is applied to NEs.

Procedure

- Configure a VDSL2 line spectrum configuration profile.

  A VDSL2 line can be configured with multiple transmission modes. You can set frequency parameters related to a transmission mode in the line spectrum configuration profile. When the line is activated, the central office and the CPE negotiate to determine the transmission mode, and then the line spectrum configuration profile related to the transmission mode is used. As an NMS type profile, the VDSL2 line spectrum configuration profile, after being created, can be referenced by different line configuration profiles.

  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
  3. Click the **Line Spectrum Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
  4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
  5. In the dialog box that is displayed, set the parameters related to the line spectrum.



Parameter Information
Name: spectrum_profile *
Alias:
VDSL Mode: defmode
G.993.2 Profile: G.993.2 Profile 12a
G.993.2 Profile auto adaption: disabled
VDSL2 Link Use of U0: unused
PSD Class Mask: AnnexB-998-M2x-B(B8-6)
Selected Upstream PSD Mask: ADLU-32/EU-32
Maximum Nominal Aggregate Transmit Power Downstream (0.1dBm) (-255 to 145): 145 *
Maximum Nominal Aggregate Transmit Power Upstream (0.1dBm) (-255 to 145): 145 *
PSD Mask Value Downstream Parameter:
PSD Mask Value Upstream Parameter:
Virtual Noise Mode Downstream: disabled *
Virtual Noise Mode Upstream: disabled *
Virtual Noise PSD Downstream:
Virtual Noise PSD Upstream:

NOTE

Click ... next to **PSD Mask Value Downstream Parameter** and **PSD Mask Value Upstream Parameter**, and then add a VDSL2 PSD profile in the dialog box that is displayed.

  6. Click **OK**.

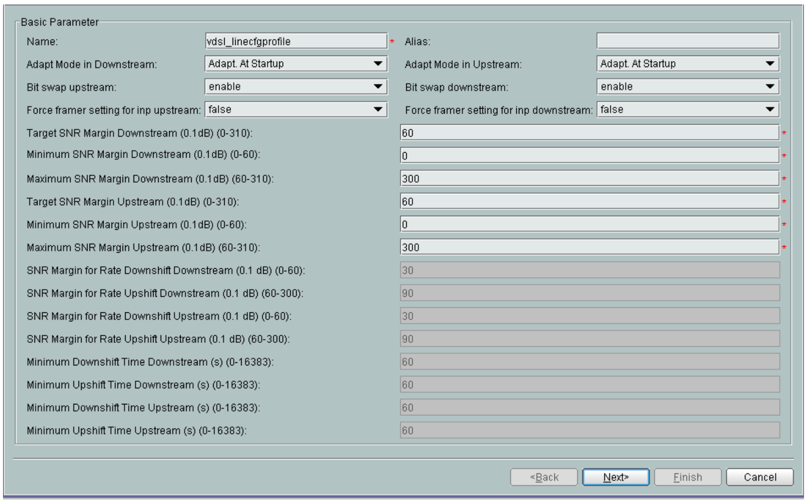
- Configure a VDSL2 line configuration profile.

- A VDSL2 line configuration profile is bound to a VDSL2 channel configuration profile to form a VDSL2 line profile. The line profile is directly referenced when the VDSL2 port is activated.
- When the VDSL2 port is activated, the central office and the CPE negotiate based on the specified line configuration profile to determine whether the line can work in normal state.
- When you set the SNR margin of the upstream and downstream channels, ensure that: minimum SNR margin ≤ target SNR margin ≤ maximum SNR margin.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
3. Click the **Line Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters of the line configuration profile.

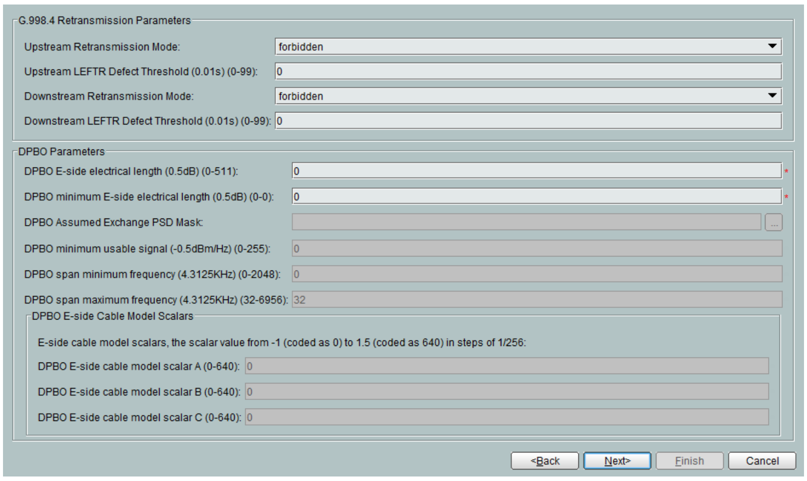
   The configuration procedure is as follows:

   a. In the dialog box, set the basic parameters of the line configuration profile.



Name: vdsl_linecfgprofile *
Alias:
Adapt Mode in Downstream: Adapt. At Startup
Adapt Mode in Upstream: Adapt. At Startup
Bit swap upstream: enable
Bit swap downstream: enable
Force framer setting for inp upstream: false
Force framer setting for inp downstream: false
Target SNR Margin Downstream (0.1dB) (0-310): 60 *
Minimum SNR Margin Downstream (0.1dB) (0-60): 0 *
Maximum SNR Margin Downstream (0.1dB) (60-310): 300 *
Target SNR Margin Upstream (0.1dB) (0-310): 60 *
Minimum SNR Margin Upstream (0.1dB) (0-60): 0 *
Maximum SNR Margin Upstream (0.1dB) (60-310): 300 *
SNR Margin for Rate Downshift Downstream (0.1 dB) (0-60): 30
SNR Margin for Rate Upshift Downstream (0.1 dB) (60-300): 90
SNR Margin for Rate Downshift Upstream (0.1 dB) (0-60): 30
SNR Margin for Rate Upshift Upstream (0.1 dB) (60-300): 90
Minimum Downshift Time Downstream (s) (0-16383): 60
Minimum Upshift Time Downstream (s) (0-16383): 60
Minimum Downshift Time Upstream (s) (0-16383): 60
Minimum Upshift Time Upstream (s) (0-16383): 60

   b. Click **Next**, and set the downstream power backoff parameters in the dialog box.



G.998.4 Retransmission Parameters

Upstream Retransmission Mode: forbidden
Upstream LEFTR Defect Threshold (0.01s) (0-99): 0
Downstream Retransmission Mode: forbidden
Downstream LEFTR Defect Threshold (0.01s) (0-99): 0

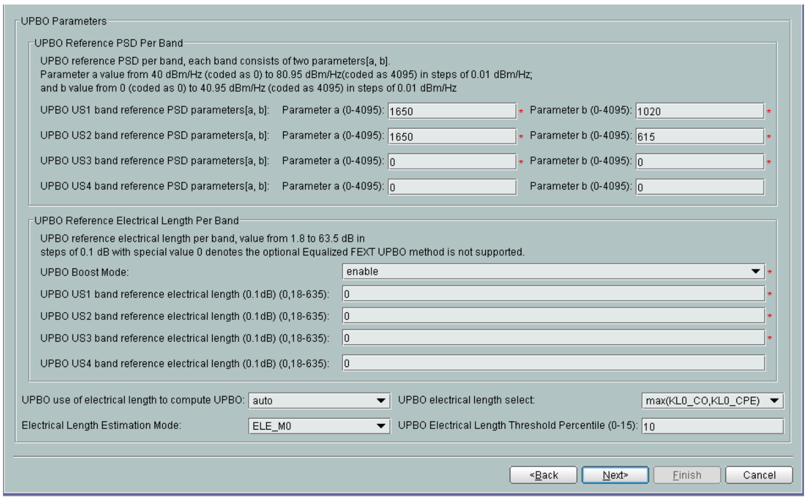
DPBO Parameters

DPBO E-side electrical length (0.5dB) (0-511): 0
DPBO minimum E-side electrical length (0.5dB) (0-0): 0
DPBO Assumed Exchange PSD Mask:
DPBO minimum usable signal (-0.5dBm/Hz) (0-255): 0
DPBO span minimum frequency (4.3125KHz) (0-2048): 0
DPBO span maximum frequency (4.3125KHz) (32-6956): 32

DPBO E-side Cable Model Scalars

E-side cable model scalars, the scalar value from -1 (coded as 0) to 1.5 (coded as 640) in steps of 1/256:
DPBO E-side cable model scalar A (0-640): 0
DPBO E-side cable model scalar B (0-640): 0
DPBO E-side cable model scalar C (0-640): 0

c. Click **Next**, and set the upstream power backoff parameters in the dialog box.



UPBO Parameters

UPBO Reference PSD Per Band

UPBO reference PSD per band, each band consists of two parameters[a, b].
Parameter a value from 40 dBm/Hz (coded as 0) to 80.95 dBm/Hz(coded as 4095) in steps of 0.01 dBm/Hz;
and b value from 0 (coded as 0) to 40.95 dBm/Hz (coded as 4095) in steps of 0.01 dBm/Hz

UPBO US1 band reference PSD parameters[a, b]: Parameter a (0-4095): 1650 Parameter b (0-4095): 1020
UPBO US2 band reference PSD parameters[a, b]: Parameter a (0-4095): 1650 Parameter b (0-4095): 615
UPBO US3 band reference PSD parameters[a, b]: Parameter a (0-4095): 0 Parameter b (0-4095): 0
UPBO US4 band reference PSD parameters[a, b]: Parameter a (0-4095): 0 Parameter b (0-4095): 0

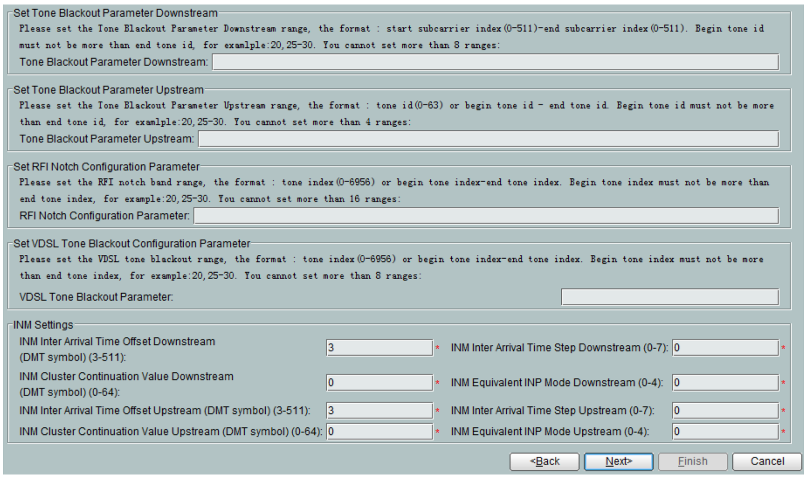
UPBO Reference Electrical Length Per Band

UPBO reference electrical length per band, value from 1.8 to 63.5 dB in
steps of 0.1 dB with special value 0 denotes the optional Equalized FEXT UPBO method is not supported.

UPBO Boost Mode: enable
UPBO US1 band reference electrical length (0.1dB) (0,18-635): 0
UPBO US2 band reference electrical length (0.1dB) (0,18-635): 0
UPBO US3 band reference electrical length (0.1dB) (0,18-635): 0
UPBO US4 band reference electrical length (0.1dB) (0,18-635): 0

UPBO use of electrical length to compute UPBO: auto
UPBO electrical length select: max(KL0_CO,KL0_CPE)
Electrical Length Estimation Mode: ELE_M0
UPBO Electrical Length Threshold Percentile (0-15): 10

d. Click **Next**, and set the advanced parameters in the dialog box.



Set Tone Blackout Parameter Downstream

Please set the Tone Blackout Parameter Downstream range, the format : start subcarrier index(0-511)-end subcarrier index(0-511). Begin tone id must not be more than end tone id, for examlple:20,25-30. You cannot set more than 8 ranges:
Tone Blackout Parameter Downstream:

Set Tone Blackout Parameter Upstream

Please set the Tone Blackout Parameter Upstream range, the format : tone id(0-63) or begin tone id - end tone id. Begin tone id must not be more than end tone id, for examlple:20,25-30. You cannot set more than 4 ranges:
Tone Blackout Parameter Upstream:

Set RFI Notch Configuration Parameter

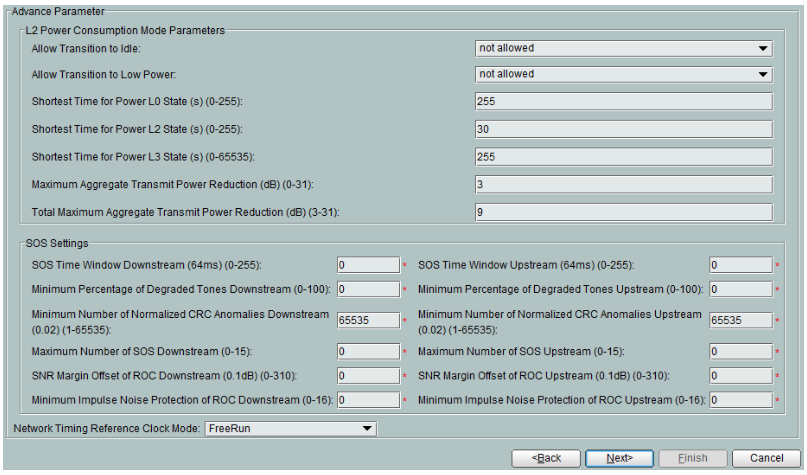
Please set the RFI notch band range, the format : tone index(0-6956) or begin tone index-end tone index. Begin tone index must not be more than end tone index, for example:20,25-30. You cannot set more than 16 ranges:
RFI Notch Configuration Parameter:

Set VDSL Tone Blackout Configuration Parameter

Please set the VDSL tone blackout range, the format : tone index(0-6956) or begin tone index-end tone index. Begin tone index must not be more than end tone index, for example:20,25-30. You cannot set more than 8 ranges:
VDSL Tone Blackout Parameter:

INM Settings

INM Inter Arrival Time Offset Downstream (DMT symbol) (3-511): 3
INM Inter Arrival Time Step Downstream (0-7): 0
INM Cluster Continuation Value Downstream (DMT symbol) (0-64): 0
INM Equivalent INP Mode Downstream (0-4): 0
INM Inter Arrival Time Offset Upstream (DMT symbol) (3-511): 3
INM Inter Arrival Time Step Upstream (0-7): 0
INM Cluster Continuation Value Upstream (DMT symbol) (0-64): 0
INM Equivalent INP Mode Upstream (0-4): 0



Advance Parameter

L2 Power Consumption Mode Parameters

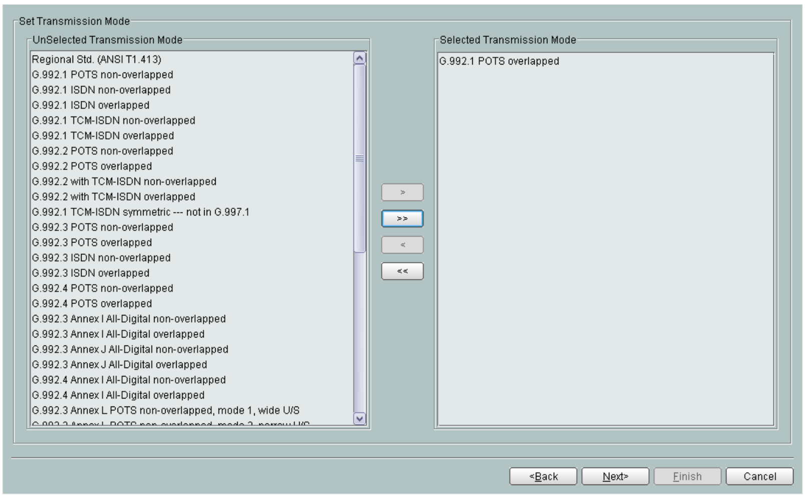
Allow Transition to Idle: not allowed
Allow Transition to Low Power: not allowed
Shortest Time for Power L0 State (s) (0-255): 255
Shortest Time for Power L2 State (s) (0-255): 30
Shortest Time for Power L3 State (s) (0-65535): 255
Maximum Aggregate Transmit Power Reduction (dB) (0-31): 3
Total Maximum Aggregate Transmit Power Reduction (dB) (3-31): 9

SOS Settings

SOS Time Window Downstream (64ms) (0-255): 0 *
SOS Time Window Upstream (64ms) (0-255): 0 *
Minimum Percentage of Degraded Tones Downstream (0-100): 0 *
Minimum Percentage of Degraded Tones Upstream (0-100): 0 *
Minimum Number of Normalized CRC Anomalies Downstream (0.02) (1-65535): 65535 *
Minimum Number of Normalized CRC Anomalies Upstream (0.02) (1-65535): 65535 *
Maximum Number of SOS Downstream (0-15): 0 *
Maximum Number of SOS Upstream (0-15): 0 *
SNR Margin Offset of ROC Downstream (0.1dB) (0-310): 0 *
SNR Margin Offset of ROC Upstream (0.1dB) (0-310): 0 *
Minimum Impulse Noise Protection of ROC Downstream (0-16): 0 *
Minimum Impulse Noise Protection of ROC Upstream (0-16): 0 *

Network Timing Reference Clock Mode: FreeRun

e. Click **Next**, and set the transmission mode in the dialog box.



Set Transmission Mode

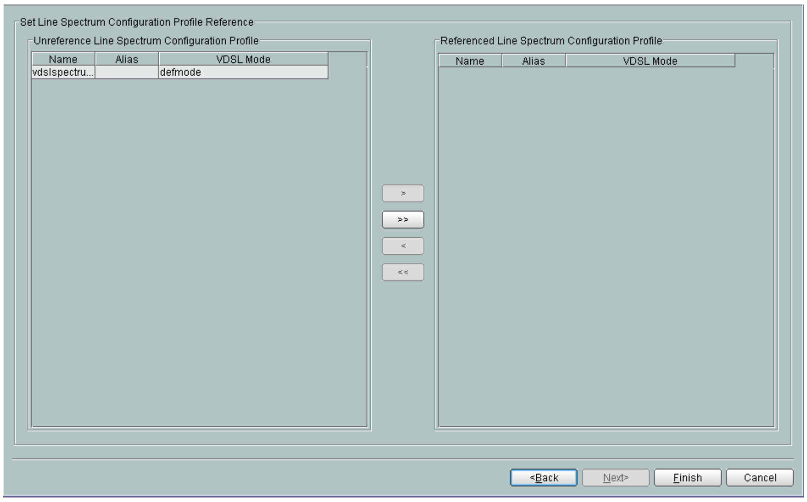
UnSelected Transmission Mode

- Regional Std. (ANSI T1.413)
- G.992.1 POTS non-overlapped
- G.992.1 ISDN non-overlapped
- G.992.1 ISDN overlapped
- G.992.1 TCM-ISDN non-overlapped
- G.992.1 TCM-ISDN overlapped
- G.992.2 POTS non-overlapped
- G.992.2 POTS overlapped
- G.992.2 with TCM-ISDN non-overlapped
- G.992.2 with TCM-ISDN overlapped
- G.992.1 TCM-ISDN symmetric --- not in G.997.1
- G.992.3 POTS non-overlapped
- G.992.3 POTS overlapped
- G.992.3 ISDN non-overlapped
- G.992.3 ISDN overlapped
- G.992.4 POTS non-overlapped
- G.992.4 POTS overlapped
- G.992.3 Annex I All-Digital non-overlapped
- G.992.3 Annex I All-Digital overlapped
- G.992.3 Annex J All-Digital non-overlapped
- G.992.3 Annex J All-Digital overlapped
- G.992.4 Annex I All-Digital non-overlapped
- G.992.4 Annex I All-Digital overlapped
- G.992.3 Annex L POTS non-overlapped, mode 1, wide U/S

Selected Transmission Mode

- G.992.1 POTS overlapped

f. Click **Next**, and set the line spectrum configuration profile that is bound to the line configuration profile in the dialog box.



Set Line Spectrum Configuration Profile Reference

Unreference Line Spectrum Configuration Profile

Name	Alias	VDSL Mode
vdslspectru...		defmode

Referenced Line Spectrum Configuration Profile

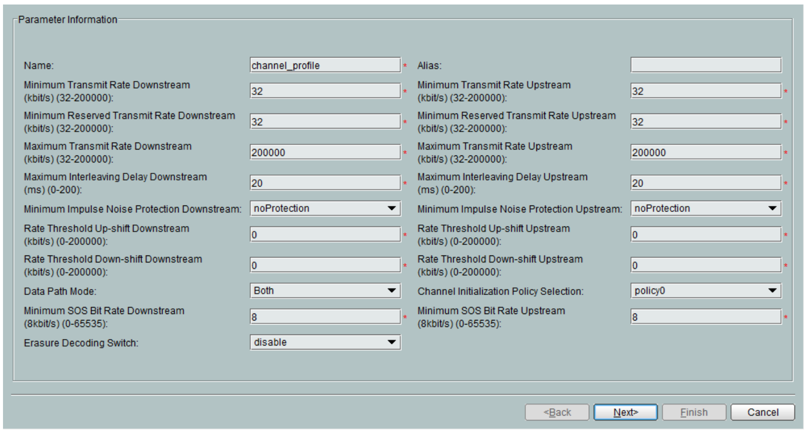
Name	Alias	VDSL Mode

6. Click **Finish**.

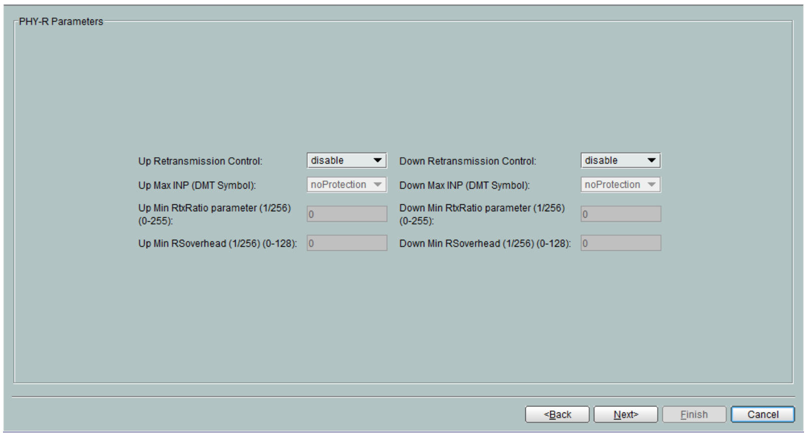
- Configure a VDSL2 channel configuration profile.
  - A VDSL2 channel configuration profile is a collection of most parameters for a VDSL2 channel, and the profile is referenced by a VDSL2 line profile.

- When the VDSL2 port is activated, the central office and the CPE negotiate based on the specified channel configuration profile to determine whether the line can work in normal state.

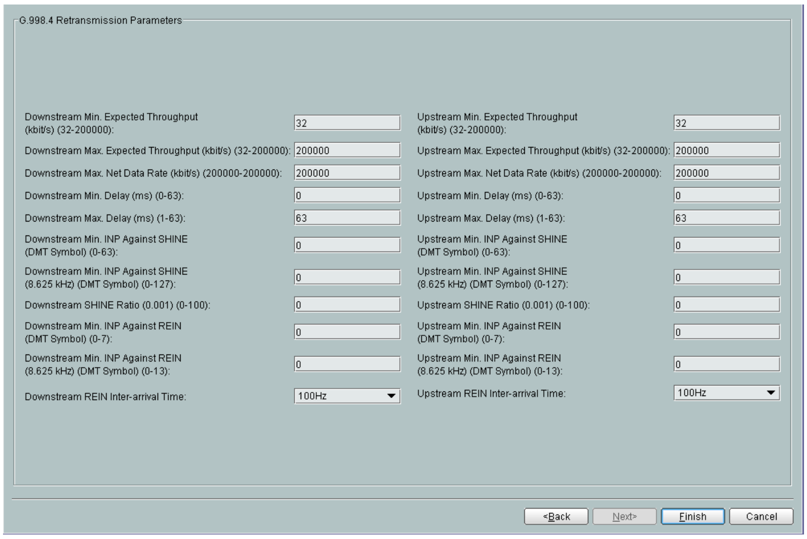
1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
3. Click the **Channel Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters related to the channel.


Parameter Information

Name: channel_profile *
Alias:
Minimum Transmit Rate Downstream (kbit/s) (32-200000): 32 *
Minimum Transmit Rate Upstream (kbit/s) (32-200000): 32 *
Minimum Reserved Transmit Rate Downstream (kbit/s) (32-200000): 32 *
Minimum Reserved Transmit Rate Upstream (kbit/s) (32-200000): 32 *
Maximum Transmit Rate Downstream (kbit/s) (32-200000): 200000 *
Maximum Transmit Rate Upstream (kbit/s) (32-200000): 200000 *
Maximum Interleaving Delay Downstream (ms) (0-200): 20 *
Maximum Interleaving Delay Upstream (ms) (0-200): 20 *
Minimum Impulse Noise Protection Downstream: noProtection
Minimum Impulse Noise Protection Upstream: noProtection
Rate Threshold Up-shift Downstream (kbit/s) (0-200000): 0 *
Rate Threshold Up-shift Upstream (kbit/s) (0-200000): 0 *
Rate Threshold Down-shift Downstream (kbit/s) (0-200000): 0 *
Rate Threshold Down-shift Upstream (kbit/s) (0-200000): 0 *
Data Path Mode: Both
Channel Initialization Policy Selection: policy0
Minimum SOS Bit Rate Downstream (8kbit/s) (0-65535): 8 *
Minimum SOS Bit Rate Upstream (8kbit/s) (0-65535): 8 *
Erasure Decoding Switch: disable


PHY-R Parameters

Up Retransmission Control: disable
Down Retransmission Control: disable
Up Max INP (DMT Symbol): noProtection
Down Max INP (DMT Symbol): noProtection
Up Min RtxRatio parameter (1/256) (0-255): 0
Down Min RtxRatio parameter (1/256) (0-255): 0
Up Min RSoverhead (1/256) (0-128): 0
Down Min RSoverhead (1/256) (0-128): 0

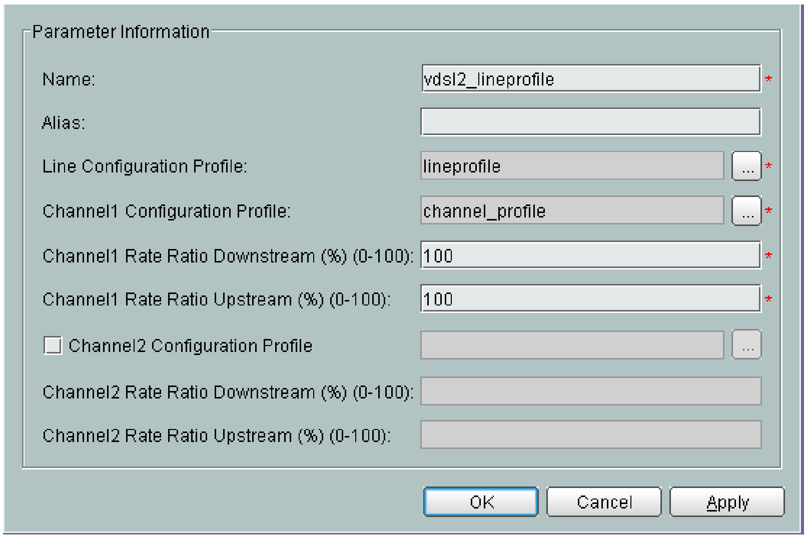

G.998.4 Retransmission Parameters

Downstream Min. Expected Throughput (kbit/s) (32-200000): 32
Downstream Max. Expected Throughput (kbit/s) (32-200000): 200000
Downstream Max. Net Data Rate (kbit/s) (200000-200000): 200000
Downstream Min. Delay (ms) (0-63): 0
Downstream Max. Delay (ms) (1-63): 63
Downstream Min. INP Against SHINE (DMT Symbol) (0-63): 0
Downstream Min. INP Against SHINE (8.625 kHz) (DMT Symbol) (0-127): 0
Downstream SHINE Ratio (0.001) (0-100): 0
Downstream Min. INP Against REIN (DMT Symbol) (0-7): 0
Downstream Min. INP Against REIN (8.625 kHz) (DMT Symbol) (0-13): 0
Downstream REIN Inter-arrival Time: 100Hz

Upstream Min. Expected Throughput (kbit/s) (32-200000): 32
Upstream Max. Expected Throughput (kbit/s) (32-200000): 200000
Upstream Max. Net Data Rate (kbit/s) (200000-200000): 200000
Upstream Min. Delay (ms) (0-63): 0
Upstream Max. Delay (ms) (1-63): 63
Upstream Min. INP Against SHINE (DMT Symbol) (0-63): 0
Upstream Min. INP Against SHINE (8.625 kHz) (DMT Symbol) (0-127): 0
Upstream SHINE Ratio (0.001) (0-100): 0
Upstream Min. INP Against REIN (DMT Symbol) (0-7): 0
Upstream Min. INP Against REIN (8.625 kHz) (DMT Symbol) (0-13): 0
Upstream REIN Inter-arrival Time: 100Hz

6. Click **Finish**.

- Configure a VDSL2 line profile.
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
  3. Click the **Line Template** tab, and select the required device type from the **Device Type** drop-down list.
  4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
  5. In the dialog box that is displayed, select or set related parameters for the VDSL2 channel configuration profile.


Parameter Information

Name: vdsl2_lineprofile *
Alias:
Line Configuration Profile: lineprofile ... *
Channel1 Configuration Profile: channel_profile ... *
Channel1 Rate Ratio Downstream (%) (0-100): 100 *
Channel1 Rate Ratio Upstream (%) (0-100): 100 *
☐ Channel2 Configuration Profile ...
Channel2 Rate Ratio Downstream (%) (0-100):
Channel2 Rate Ratio Upstream (%) (0-100):

  6. Click **OK**.

----End

6.2.6 Configuring a VDSL2 Alarm Profile

A VDSL2 alarm profile binds a specified line alarm configuration profile and a channel alarm configuration profile. After the binding is successful, an activated VDSL2 port directly references an alarm profile to monitor the performance of the VDSL2 port. When the parameter value of the port exceeds the preset threshold, an alarm is generated.

Context

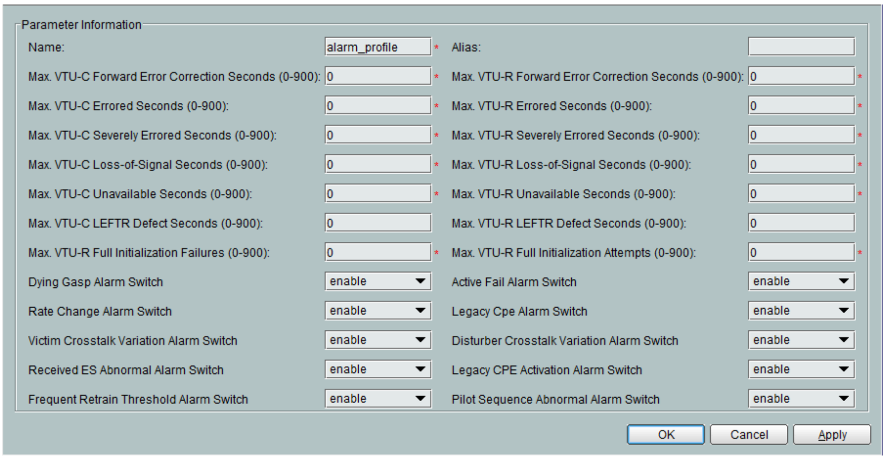
A profile takes effect only after it is applied to NEs.

Procedure

- VDSL2 line alarm configuration profile

  A VDSL2 line alarm configuration profile specifies a series of alarm thresholds that are used to monitor the performance of an activated VDSL2 line. When a certain measurement entry reaches the alarm threshold, the device is notified and an alarm is reported to the log host and the U2000. After being configured successfully, a VDSL2 line alarm configuration profile is bound to a VDSL2 channel alarm configuration profile to form a VDSL2 alarm profile, which can be bound to a VDSL2 port to take effect.

  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
  3. Click the **VDSL2 Alarm Profile** tab.
  4. Click the **Line Alarm Configuration Profile** tab.
  5. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
  6. In the dialog box that is displayed, set the alarm thresholds related to the line.



Name:	alarm_profile *	Alias:	
Max. VTU-C Forward Error Correction Seconds (0-900):	0 *	Max. VTU-R Forward Error Correction Seconds (0-900):	0 *
Max. VTU-C Errored Seconds (0-900):	0 *	Max. VTU-R Errored Seconds (0-900):	0 *
Max. VTU-C Severely Errored Seconds (0-900):	0 *	Max. VTU-R Severely Errored Seconds (0-900):	0 *
Max. VTU-C Loss-of-Signal Seconds (0-900):	0 *	Max. VTU-R Loss-of-Signal Seconds (0-900):	0 *
Max. VTU-C Unavailable Seconds (0-900):	0 *	Max. VTU-R Unavailable Seconds (0-900):	0 *
Max. VTU-C LEFTR Defect Seconds (0-900):	0	Max. VTU-R LEFTR Defect Seconds (0-900):	0
Max. VTU-R Full Initialization Failures (0-900):	0 *	Max. VTU-R Full Initialization Attempts (0-900):	0 *
Dying Gasp Alarm Switch	enable	Active Fail Alarm Switch	enable
Rate Change Alarm Switch	enable	Legacy Cpe Alarm Switch	enable
Victim Crosstalk Variation Alarm Switch	enable	Disturber Crosstalk Variation Alarm Switch	enable
Received ES Abnormal Alarm Switch	enable	Legacy CPE Activation Alarm Switch	enable
Frequent Retrain Threshold Alarm Switch	enable	Pilot Sequence Abnormal Alarm Switch	enable

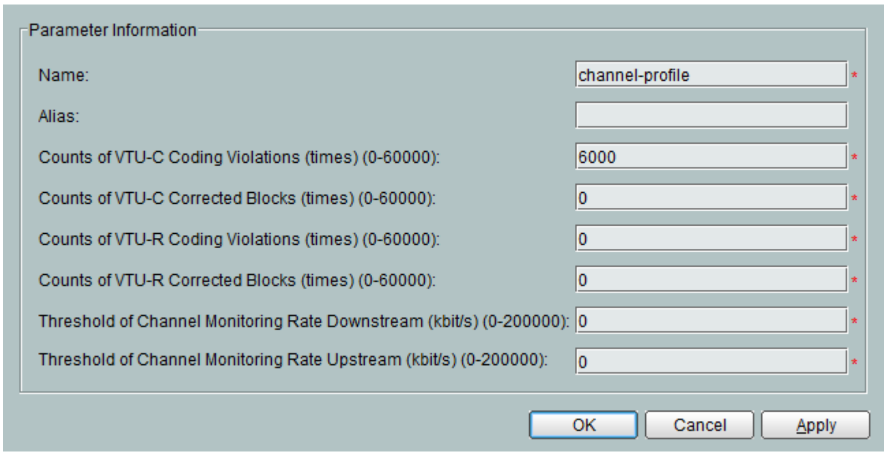
  7. Click **OK**.

- VDSL2 channel alarm configuration profile
  - A VDSL2 channel alarm configuration profile specifies a series of alarm thresholds that are used to monitor the performance of an activated VDSL2 channel. When a certain

measurement entry reaches the alarm threshold, the device is notified and an alarm is reported to the log host and the U2000. After being configured successfully, a VDSL2 channel alarm configuration profile is bound to a VDSL2 line alarm configuration profile to form a VDSL2 alarm profile, which can be bound to a VDSL2 port to take effect.

- A VDSL2 channel alarm configuration profile defines a 15-minute threshold. When the measurement entry within 15 minutes reaches the threshold that is defined in the profile, an alarm is generated.
- If the threshold is set to 0, it means that no measurement is performed and no alarm is generated.

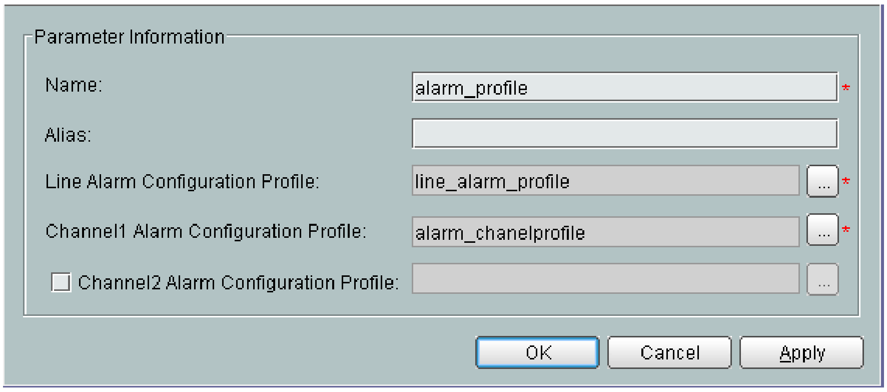
1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
3. Click the **Channel Alarm Configuration Profile** tab.
4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
5. In the dialog box that is displayed, set the alarm thresholds related to the channel.



Parameter Information
Name: channel-profile *
Alias:
Counts of VTU-C Coding Violations (times) (0-60000): 6000 *
Counts of VTU-C Corrected Blocks (times) (0-60000): 0 *
Counts of VTU-R Coding Violations (times) (0-60000): 0 *
Counts of VTU-R Corrected Blocks (times) (0-60000): 0 *
Threshold of Channel Monitoring Rate Downstream (kbit/s) (0-200000): 0 *
Threshold of Channel Monitoring Rate Upstream (kbit/s) (0-200000): 0 *

6. Click **OK**.

- Configure a VDSL2 alarm profile.
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
  3. Click the **Alarm Template** tab.
  4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
  5. In the dialog box that is displayed, set **Line Alarm Configuration Profile** and **Channel Alarm Configuration Profile** that are referenced by the alarm profile.


Parameter Information

Name: alarm_profile

Alias:

Line Alarm Configuration Profile: line_alarm_profile

Channel1 Alarm Configuration Profile: alarm_chanelprofile

☐ Channel2 Alarm Configuration Profile:

6. Click **OK**.

----End

6.2.7 Configuring a G.SHDSL Line Profile

A G.SHDSL line profile provides parameters that are required for activating an ATM G.SHDSL port. After the G.SHDSL line profile is configured successfully, you can directly refer to the G.SHDSL line profile when configuring ATM G.SHDSL port attributes to limit the port rate and noise margin to improve the service quality.

Context

- A profile name identifies a profile. Therefore, the profile name must be specified and unique. Otherwise, the profile cannot be added.
- You can add profiles that have the same parameters but different names.
- A profile takes effect only after it is applied to NEs.

Procedure

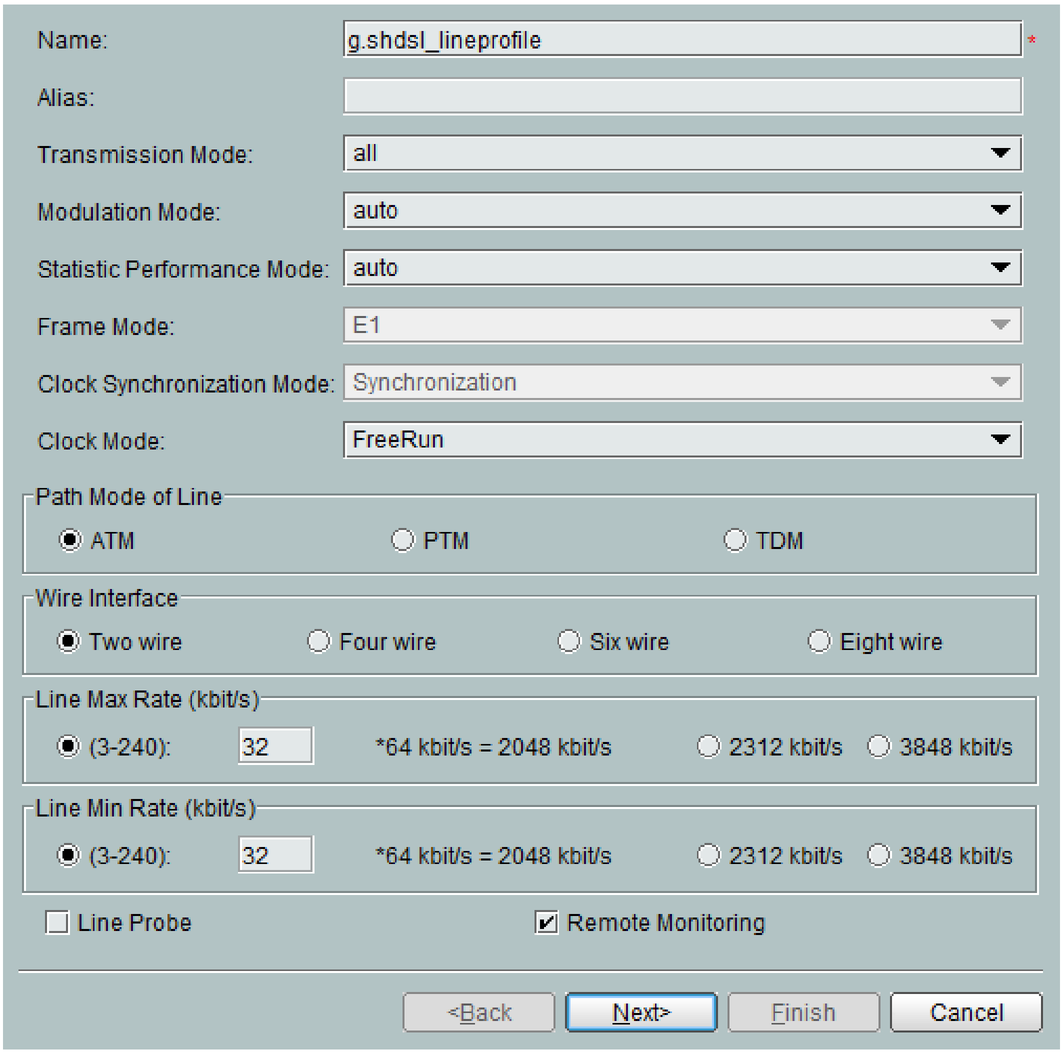
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **DSL Profile** > **G.SHDSL Profile** from the navigation tree.

Step 3 Click the **G.SHDSL Line Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: g.shdsl_lineprofile *

Alias:

Transmission Mode: all

Modulation Mode: auto

Statistic Performance Mode: auto

Frame Mode: E1

Clock Synchronization Mode: Synchronization

Clock Mode: FreeRun

Path Mode of Line: ● ATM ○ PTM ○ TDM

Wire Interface: ● Two wire ○ Four wire ○ Six wire ○ Eight wire

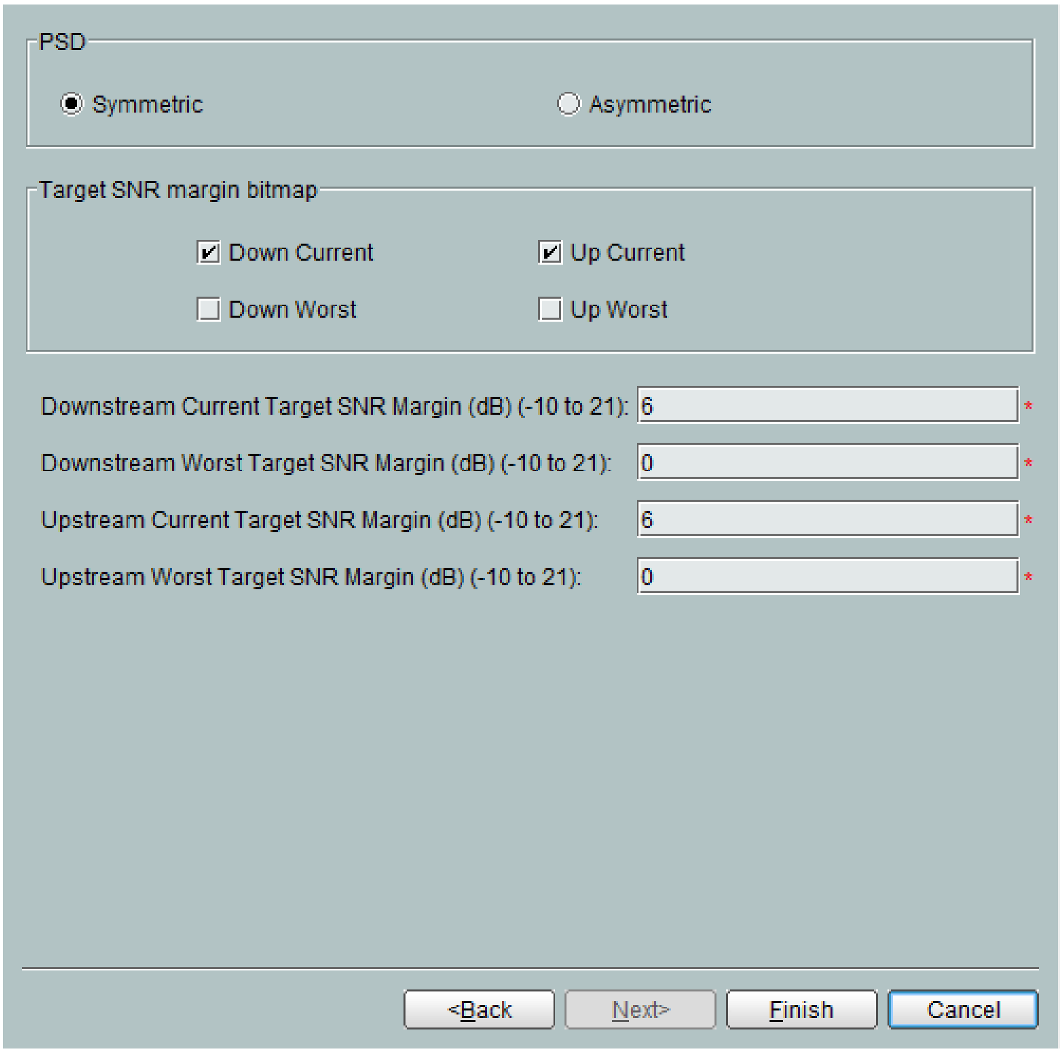
Line Max Rate (kbit/s): ● (3-240): 32 *64 kbit/s = 2048 kbit/s ○ 2312 kbit/s ○ 3848 kbit/s

Line Min Rate (kbit/s): ● (3-240): 32 *64 kbit/s = 2048 kbit/s ○ 2312 kbit/s ○ 3848 kbit/s

☐ Line Probe ☑ Remote Monitoring

Step 6 Click **Next**.

Step 7 In the dialog box that is displayed, set the parameters for the line profile.



PSD

● Symmetric ○ Asymmetric

Target SNR margin bitmap

☑ Down Current ☑ Up Current

☐ Down Worst ☐ Up Worst

Downstream Current Target SNR Margin (dB) (-10 to 21): 6 *

Downstream Worst Target SNR Margin (dB) (-10 to 21): 0 *

Upstream Current Target SNR Margin (dB) (-10 to 21): 6 *

Upstream Worst Target SNR Margin (dB) (-10 to 21): 0 *

Step 8 Click **Finish**.

----End

6.2.8 Configuring a G.SHDSL Alarm Profile

A G.SHDSL alarm profile defines a series of alarm parameters for measuring the performance of a G.SHDSL port. You can monitor the performance of the G.SHDSL circuit by setting thresholds for these alarm parameters. When the ATM G.SHDSL port is activated, it directly references the G.SHDSL alarm profile to monitor the port performance . When the parameter value of the port exceeds the preset threshold, an alarm is generated.

Context

- A profile name identifies a profile. Therefore, the profile name must be specified and unique. Otherwise, the profile cannot be added.
- You can add profiles that have the same parameters but different names.
- A profile takes effect only after it is applied to NEs.

Procedure

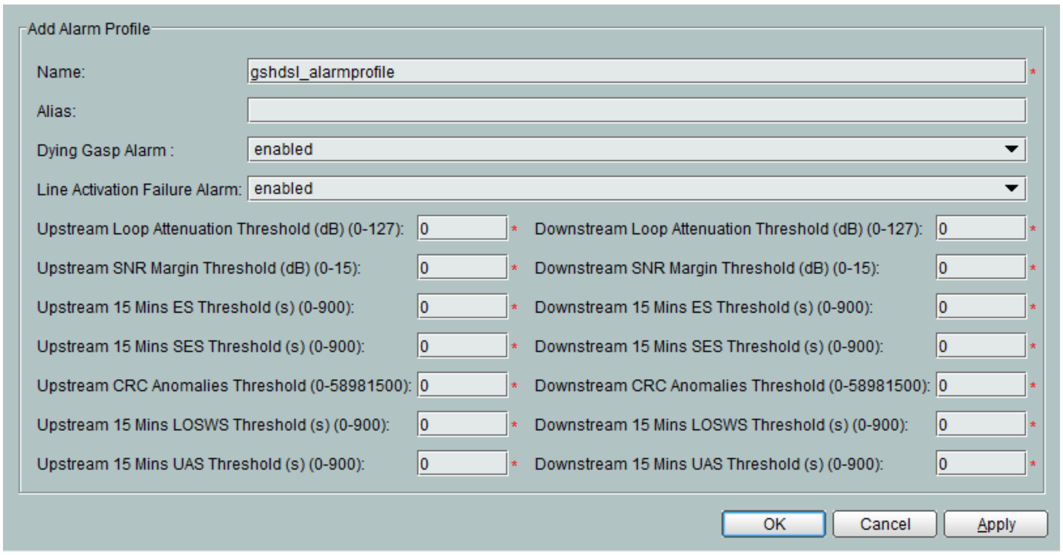
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **DSL Profile** > **G.SHDSL Profile** from the navigation tree.

Step 3 Click the **G.SHDSL Alarm Profile** tab, and select select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: gshdsl_alarmprofile *
Alias:
Dying Gasp Alarm : enabled
Line Activation Failure Alarm: enabled
Upstream Loop Attenuation Threshold (dB) (0-127): 0 *
Downstream Loop Attenuation Threshold (dB) (0-127): 0 *
Upstream SNR Margin Threshold (dB) (0-15): 0 *
Downstream SNR Margin Threshold (dB) (0-15): 0 *
Upstream 15 Mins ES Threshold (s) (0-900): 0 *
Downstream 15 Mins ES Threshold (s) (0-900): 0 *
Upstream 15 Mins SES Threshold (s) (0-900): 0 *
Downstream 15 Mins SES Threshold (s) (0-900): 0 *
Upstream CRC Anomalies Threshold (0-58981500): 0 *
Downstream CRC Anomalies Threshold (0-58981500): 0 *
Upstream 15 Mins LOSWS Threshold (s) (0-900): 0 *
Downstream 15 Mins LOSWS Threshold (s) (0-900): 0 *
Upstream 15 Mins UAS Threshold (s) (0-900): 0 *
Downstream 15 Mins UAS Threshold (s) (0-900): 0 *

Step 6 Click **OK**.

----End

6.2.9 Configuring an MEF IP Traffic Profile

The MEF IP traffic profile defines a series of traffic parameters. It is used to configure the parameters of the traffic streams by being bound to the service port so that the rate of the traffic stream can be limited. When configuring a service port, bind the service port to a MEF IP traffic profile.

Context

When an MEF IP traffic profile is added through the U2000, the MEF IP traffic profile is added to only the database of the U2000, but is not applied to the device. This MEF IP traffic profile is created on a device only when the device references the MEF IP traffic profile to create a service port or the MEF IP traffic profile is manually applied to the device.

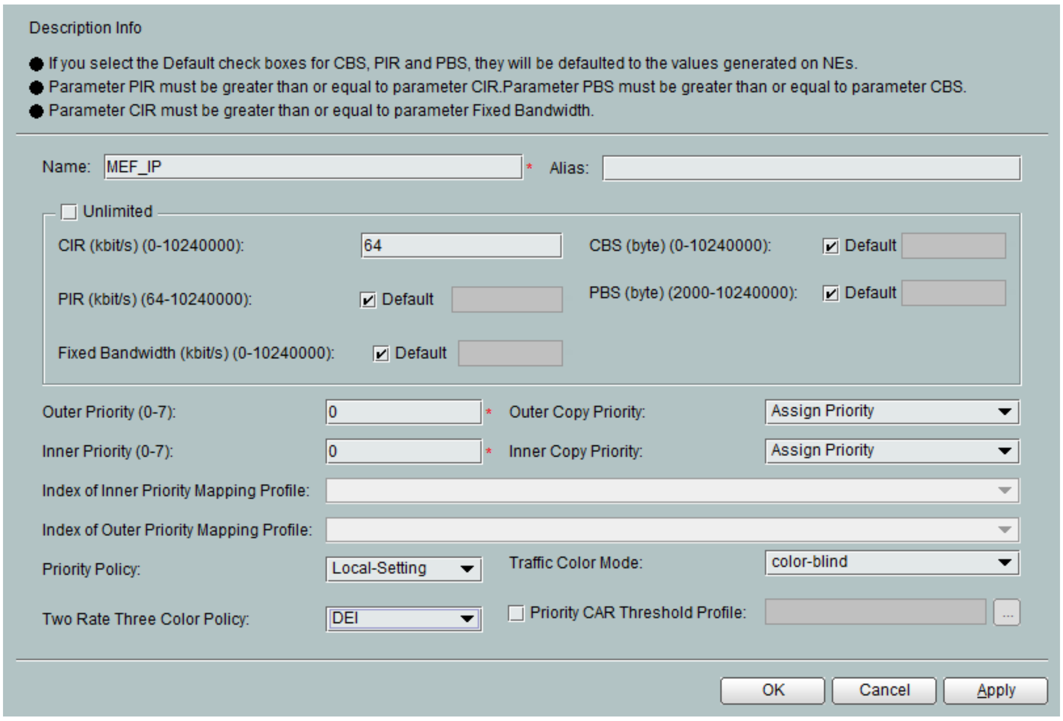
Procedure

Step 1 In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.

Step 2 Click the **MEF IP Traffic Profile** tab.

Step 3 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters.



Description Info

- If you select the Default check boxes for CBS, PIR and PBS, they will be defaulted to the values generated on NEs.
- Parameter PIR must be greater than or equal to parameter CIR.Parameter PBS must be greater than or equal to parameter CBS.
- Parameter CIR must be greater than or equal to parameter Fixed Bandwidth.

Name: MEF_IP *
Alias:
☐ Unlimited
CIR (kbit/s) (0-10240000): 64
CBS (byte) (0-10240000): ☑ Default
PIR (kbit/s) (64-10240000): ☑ Default
PBS (byte) (2000-10240000): ☑ Default
Fixed Bandwidth (kbit/s) (0-10240000): ☑ Default
Outer Priority (0-7): 0 *
Outer Copy Priority: Assign Priority
Inner Priority (0-7): 0 *
Inner Copy Priority: Assign Priority
Index of Inner Priority Mapping Profile:
Index of Outer Priority Mapping Profile:
Priority Policy: Local-Setting
Traffic Color Mode: color-blind
Two Rate Three Color Policy: DEI
☐ Priority CAR Threshold Profile:

Step 5 Click **OK**.

Step 6 Select the traffic profile, right-click, and then choose **Download to NE**.

Step 7 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

6.3 Configuring the xDSL Access Services

This topic describes how to configure the IPoA, PPPoA, and bridge access services based on the xDSL technology on the OLT.

6.3.1 Adding a VLAN

Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

Context

Table 6-1 describes VLAN types and their applications.

Table 6-1 VLAN types and their applications

VLAN Type	Description	Application
Standard VLAN	Ethernet ports in a standard VLAN are interconnected with each other. Ethernet ports in different standard VLANs are isolated from each other.	Only available for Ethernet ports. Applied to network management and subtending.
Smart VLAN	A smart VLAN contains multiple service virtual ports. In addition, traffic streams on these ports are isolated from each other and traffic streams on different VLANs are isolated from each other. A smart VLAN provides access for multiple users, saving the VLAN resources.	Applied to the access service, such as the residential community access.
MUX VLAN	A MUX VLAN contains only one service virtual port. In addition, traffic streams on different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. In this case, a MUX VLAN can uniquely identify an access user.	Applied to the access service, such as scenarios where users are distinguished based on VLANs.
Super VLAN	The super VLAN is a L3-based VLAN. It consists of multiple sub VLANs. Through ARP proxy, a super VLAN realizes L3 interconnection for these sub VLANs. A sub VLAN can be a standard VLAN, smart VLAN, or a MUX VLAN.	Applied to save IP address resources so that the utilization of the IP address is improved.

Table 6-2 describes the VLAN attributes.

Table 6-2 VLAN attributes

VLAN Attribute	Application
Common	A VLAN with the common attribute can be used as a L2 VLAN or to create a L3 interface.
QinQ	A QinQ VLAN packet contains two layers of VLAN tags: inner VLAN tag from the private network and outer VLAN tag from the OLT. Through the outer VLAN, a L2 VPN tunnel can be set up to transparently transmit the service between private networks.

VLAN Attribute	Application
Stacking	A stacking VLAN packet contains two layers of VLAN tags: inner VLAN tag and outer VLAN tag from the OLT. With this attribute, the upper layer BRAS device authenticates users based on the two VLAN tags, thus increasing the number of access users. In an upper network in the L2 working mode, you can forward packets according to the "VLAN + MAC", thus providing the wholesale service provisioning function for ISPs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

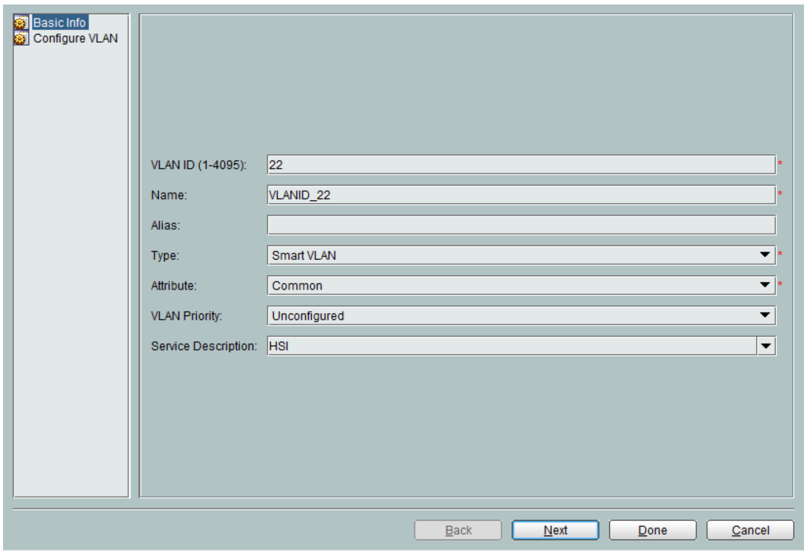
Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.

Step 4 Right-click the list, and then choose **Add** or **Batch Add**.

Step 5 In the dialog box that is displayed, set the parameters.

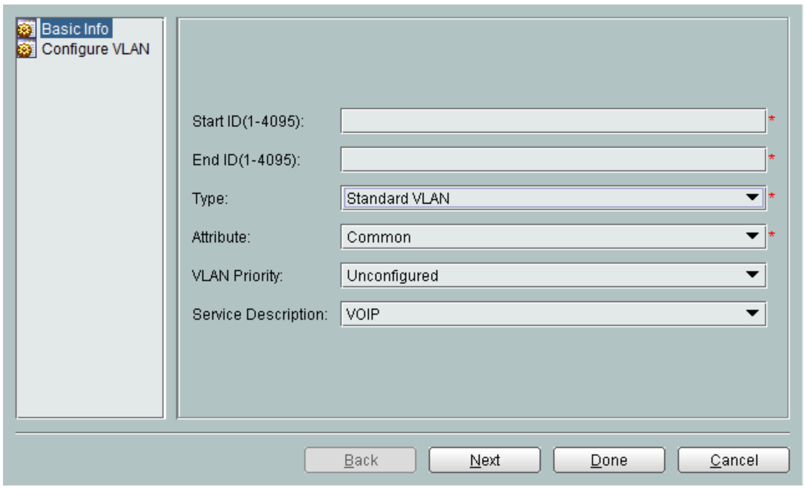
- When you add a VLAN, and then set the parameters as follows:
  - **VLAN ID**
  - **Name**
  - **Alias**
  - **Type**
  - **VLAN Priority**



VLAN ID (1-4095): 22 *
Name: VLANID_22 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI

- When you add VLANs in batches, and then set the parameters as follows:
  - **Start ID**

- **End ID**
- **Type**
- **VLAN Priority**



Start ID(1-4095):
End ID(1-4095):
Type: Standard VLAN
Attribute: Common
VLAN Priority: Unconfigured
Service Description: VOIP

Step 6 Click **Done**.

----End

6.3.2 Configuring the Upstream Port of a VLAN

To enable the user packets with a VLAN tag to be forwarded through an upstream port, perform this operation to add the upstream port to the VLAN. After the upstream port is successfully added, the user packets with this VLAN tag can be forwarded through the corresponding port.

Prerequisites

The corresponding VLAN must exist. For details about adding a VLAN, see **6.3.1 Adding a VLAN**.

Procedure

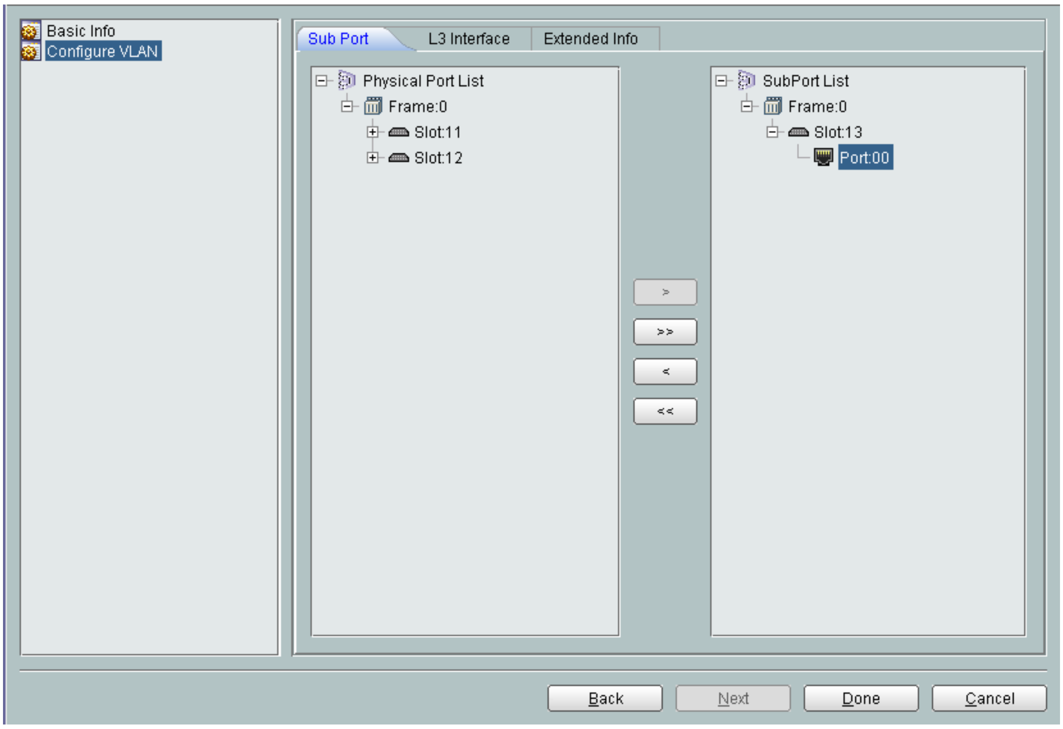
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⩔ to display the VLANs.

Step 4 Select the VLAN to be configured, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, choose **Configure VLAN** from the navigation tree. Click the **Sub Port** tab, and then set the upstream port of the VLAN.



Step 6 Click **Done**.

----End

6.3.3 Configuring a Service Port

After being configured successfully, the xDSL service port can carry service streams of various types. For MA5603U, you need configure a service port in VDSL2 port.

Procedure

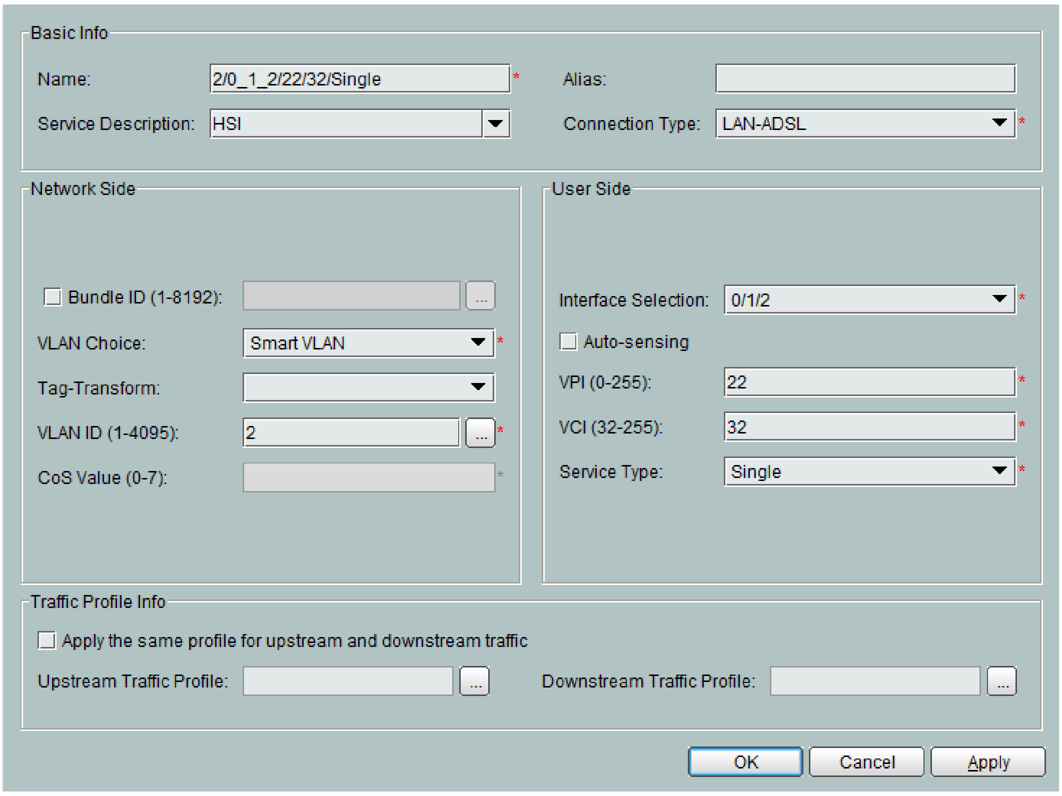
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ⌄ to display the ADSL ports.

Step 4 In the information list, select an ADSL port record. On the **Service Port** tab page in the lower pane, right-click, and then choose **Add**.

Step 5 In the dialog box that is displayed, set **Upstream Traffic Name**, **Downstream Traffic Name**, **VLAN Choice**, **Vlan ID**, **VPI**, **VCI**, and **Service Type**.



Name: 2/0_1_2/22/32/Single *
Alias:
Service Description: HSI
Connection Type: LAN-ADSL *
☐ Bundle ID (1-8192):
VLAN Choice: Smart VLAN *
Tag-Transform:
VLAN ID (1-4095): 2 *
CoS Value (0-7): *
Interface Selection: 0/1/2 *
☐ Auto-sensing
VPI (0-255): 22 *
VCI (32-255): 32 *
Service Type: Single *
☐ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile:
Downstream Traffic Profile:

NOTE

- The configuration of **VLAN ID** must be the same as that in **6.3.2 Configuring the Upstream Port of a VLAN**.
- Select only the traffic profile that exists on the device. Otherwise, the system reports an error.

Step 6 Click **OK**.

----End

6.3.4 Configuring the Attributes of an xDSL Port

This topic describes how to configure a line profile, an alarm profile, extended profile (optional) of an ADSL port. These attributes can be used after the ADSL port is activated.MA5603U, you need configure the attributes in VDSL2 port.

Context

You can modify the attributes of a port when the port is in the activated, activating, or deactivated state. After the profile bound to a port is modified, the profile parameters automatically take effect. If the port is in the deactivated state, modify the port attributes directly. If the port is in the activated or activating state, deactivate it before modifying the port attributes.

Procedure

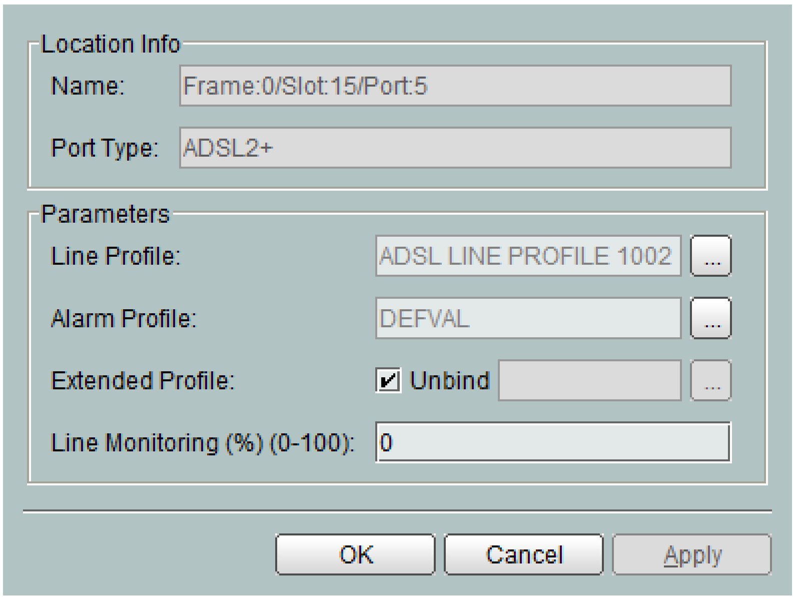
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ⌄ to display the ADSL ports.

Step 4 In the information list, select an ADSL port record, right-click, and then choose **Configure Attributes**.

Step 5 In the dialog box that is displayed, bind the ADSL port to the corresponding profile.



Location Info

Name: Frame:0/Slot:15/Port:5

Port Type: ADSL2+

Parameters

Line Profile: ADSL LINE PROFILE 1002

Alarm Profile: DEFVAL

Extended Profile: ☑ Unbind

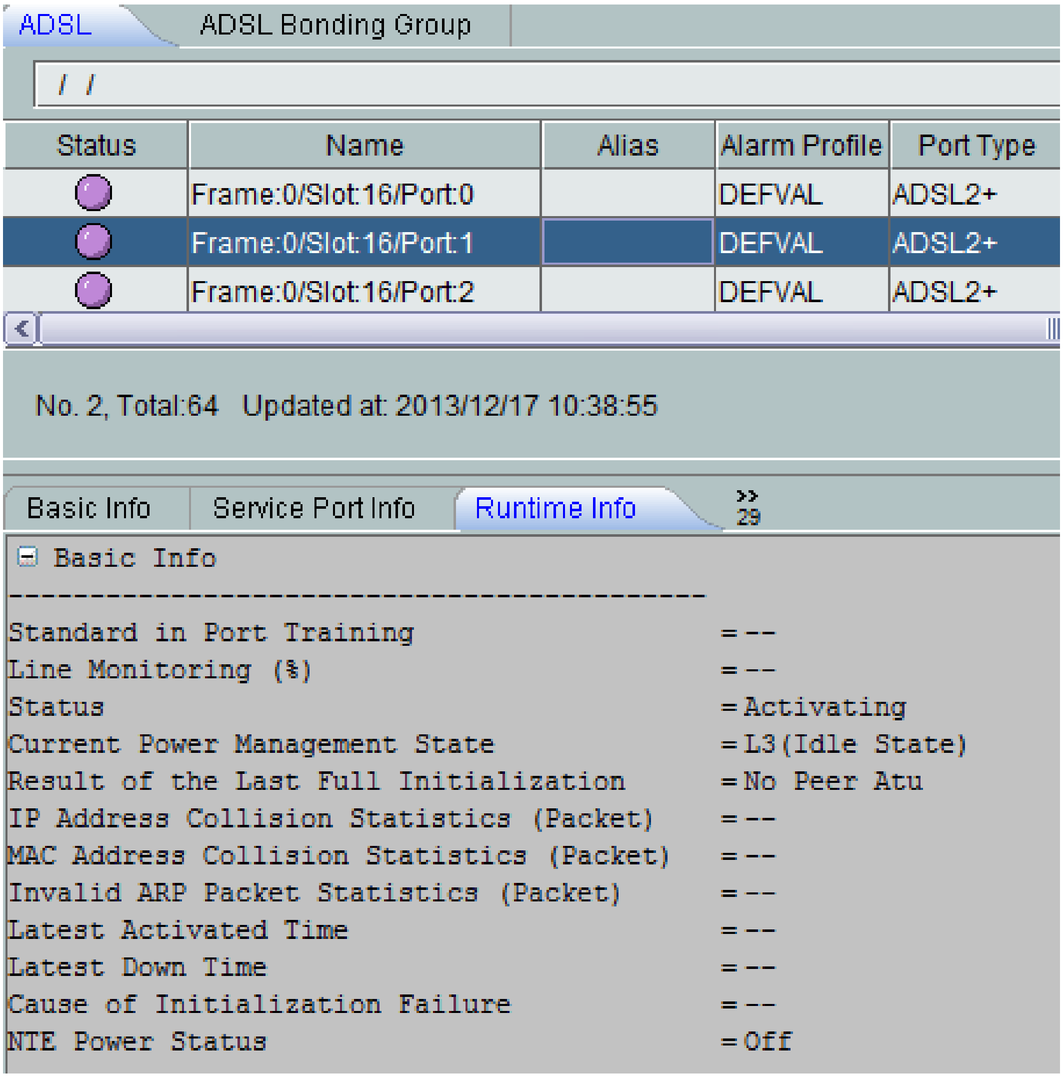
Line Monitoring (%) (0-100): 0

Step 6 Click **OK**.

----End

Result

Click the tab, you can check the line quality statistics informations etc.



Status	Name	Alias	Alarm Profile	Port Type
●	Frame:0/Slot:16/Port:0		DEFVAL	ADSL2+
●	Frame:0/Slot:16/Port:1		DEFVAL	ADSL2+
●	Frame:0/Slot:16/Port:2		DEFVAL	ADSL2+

No. 2, Total:64 Updated at: 2013/12/17 10:38:55

```
⊟ Basic Info
-------------------------------------------
Standard in Port Training                      =--
Line Monitoring (%)                            =--
Status                                         =Activating
Current Power Management State                 =L3(Idle State)
Result of the Last Full Initialization         =No Peer Atu
IP Address Collision Statistics (Packet)       =--
MAC Address Collision Statistics (Packet)      =--
Invalid ARP Packet Statistics (Packet)         =--
Latest Activated Time                          =--
Latest Down Time                               =--
Cause of Initialization Failure                =--
NTE Power Status                               =Off
```

6.3.5 Activating an xDSL Port

The xDSL port can transmit the service in the normal state only when it is activated successfully. For MA5603U, you need activate a VDSL2 port.

Context

- The xDSL port must be activated and then it can transmit the service.
- When you need to modify the line profile bound to an activated port, you should deactivated the port firstly, then you can bound a new profile to the deactivated port. Finally, activates the port again.
- When you activate a port:
  - If the ATU-R is online (powered on), the activating process is complete after the training is successful.
  - If the ATU-R is offline (powered off), the connection set up during the activating process is interrupted, and the ATU-C is in the detection state. When the ATU-R is powered on again, the training automatically initiates. If the training is successful, the port is activated.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ⇊ to display the ADSL ports.

Step 4 In the information list, select an deactivated ADSL port, right-click, and then choose **Activate**.

----End

6.3.6 Configuring a MAC Address Pool

In case of IPoA or PPPoA access, the OLT needs to convert the IPoA/PPPoA packets to the IPoE/PPPoE packets. In this case, the MAC address pool allocates a MAC address to the user and adds a MAC address (source MAC address) to the ATM cell, thus converting the ATM cell to the Ethernet packet.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Properties** > **MAC Address Pool** from the navigation tree on the tab page that is displayed.

Step 3 In the information list, right-click and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set **Start MAC Address**, **Address Range** and **Type**.

Step 5 Click **OK**.

----End

6.3.7 Configuring the IPoA Encapsulation Type of an xDSL Port

This topic describes how to configure the Internet Protocol over ATM (IPoA) encapsulation type for the IPoA access service on a specified service virtual port. After you configure the encapsulation type, packets of the specified permanent virtual channel (PVC) are transmitted downstream or upstream in the configured encapsulation type. The following uses ADSL ports as an example to describe how to configure the encapsulation type. You can use a similar method to configure an encapsulation format for G.SHDSL ports and VDSL2 ports.

Context

- This operation is applicable to the IPoA access service.
- The IPoA is used to transmit IP packets over ATM-LAN. The IPoA stipulates that connections must be set up between ATM terminals over the ATM network, especially IP data communication through the setup of switched virtual circuits (SVCs).
- With the development of IP networks, IP access modes become the mainstream for DSLAM devices. To adapt to the earlier subscriber modems in ATM access mode, the OLT converts

the IPoA packets to IPoE packets, and transmits the IPoE packets upstream to the upper-layer IP network.

- The IPoA is used for the private line access. It meets carrier requirements for the ATM-to-IP network transition.
- In IPoA access mode, packets can be configured with dynamic IP addresses (the source IP address is not specified) or static IP addresses (the source IP address is specified). To switch from a dynamic IP address to a static IP address in IPoA mode, encapsulate the packet in LLC-Bridge format and re-encapsulate it with a static IP address.
- The OLT limits the access rate of a subscriber by means of traffic profiles or ADSL line profiles. If the two rate limit modes work together, the user bandwidth adopts the minimum value in the two profiles.

Procedure

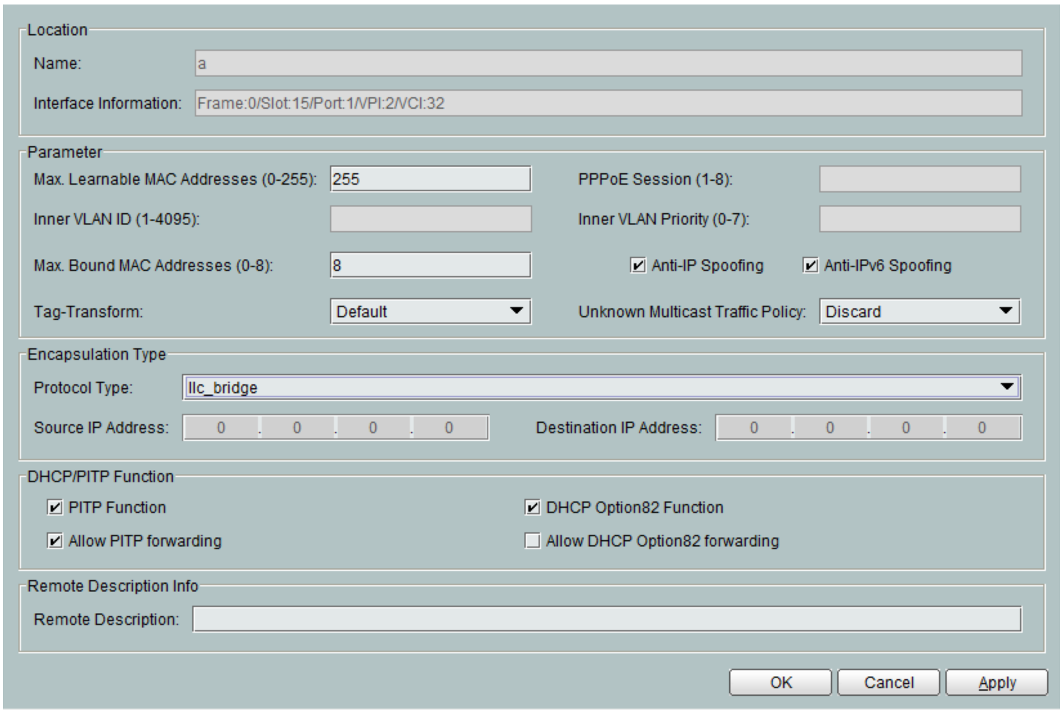
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ⏬ to display the ADSL ports.

Step 4 Click the **Service Port Info** tab in the lower pane. Select a record from the service port list, right-click, and then choose **Configure Extended Properties**.

Step 5 In the dialog box that is displayed, set the **Protocol Type** to **llc_ip** and then set the **Source IP Address** and **Destination IP Address** parameters.



Location
Name: a
Interface Information: Frame:0/Slot:15/Port:1/VPI:2/VCI:32

Parameter
Max. Learnable MAC Addresses (0-255): 255
PPPoE Session (1-8):
Inner VLAN ID (1-4095):
Inner VLAN Priority (0-7):
Max. Bound MAC Addresses (0-8): 8
☑ Anti-IP Spoofing
☑ Anti-IPv6 Spoofing
Tag-Transform: Default
Unknown Multicast Traffic Policy: Discard

Encapsulation Type
Protocol Type: llc_bridge
Source IP Address: 0 . 0 . 0 . 0
Destination IP Address: 0 . 0 . 0 . 0

DHCP/PITP Function
☑ PITP Function
☑ DHCP Option82 Function
☑ Allow PITP forwarding
☐ Allow DHCP Option82 forwarding

Remote Description Info
Remote Description:

Step 6 Click **OK**.

----End

6.3.8 Configuring the PPPoA Encapsulation Type of an xDSL Port

This topic describes how to configure the Point to Point Protocol over ATM (PPPoA) encapsulation type to llc_ppp for the PPPoA access service on an xDSL port. The following uses ADSL ports as an example to describe how to configure the encapsulation type. You can use a similar method to configure an encapsulation format for G.SHDSL ports and VDSL2 ports.

Context

- The PPPoA protocol is used to manage user authentication and serves as the PPP protocol for asynchronous transfer mode (ATM).
- With the development of IP networks, IP access modes become the mainstream for DSLAM devices. To adapt to the earlier subscriber modems in ATM access mode, the OLT converts the PPPoA packets to PPPoE packets, and transmits the PPPoE packets upstream to the upper-layer IP network.
- Currently, PPPoA subscribers mainly use the Internet access service.
- The OLT limits the access rate of a subscriber by means of traffic profiles or ADSL line profiles. If the two rate limit modes work together, the user bandwidth adopts the minimum value in the two profiles.

Procedure

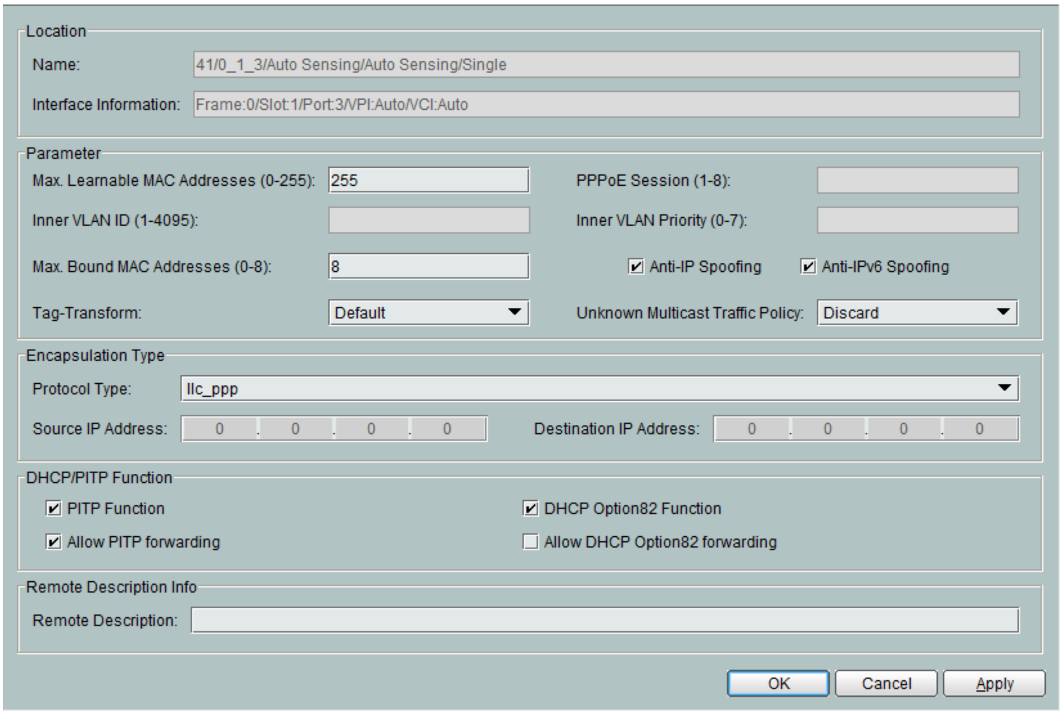
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ︾ to display the ADSL ports.

Step 4 Click the **Service Port Info** tab in the lower pane. Select a record from the service port list, right-click, and then choose **Configure Extended Properties**.

Step 5 In the dialog box that is displayed, set **Protocol Type** to **llc_ppp**.



Location

Name: 41/0_1_3/Auto Sensing/Auto Sensing/Single

Interface Information: Frame:0/Slot:1/Port:3/VPI:Auto/VCI:Auto

Parameter

Max. Learnable MAC Addresses (0-255): 255

PPPoE Session (1-8):

Inner VLAN ID (1-4095):

Inner VLAN Priority (0-7):

Max. Bound MAC Addresses (0-8): 8

☑ Anti-IP Spoofing ☑ Anti-IPv6 Spoofing

Tag-Transform: Default

Unknown Multicast Traffic Policy: Discard

Encapsulation Type

Protocol Type: llc_ppp

Source IP Address: 0 . 0 . 0 . 0

Destination IP Address: 0 . 0 . 0 . 0

DHCP/PITP Function

☑ PITP Function

☑ DHCP Option82 Function

☑ Allow PITP forwarding

☐ Allow DHCP Option82 forwarding

Remote Description Info

Remote Description:

Step 6 Click **OK**.

----End

6.4 Configuration Example of a VDSL2 Access Service in Bridging Mode

This topic describes how to configure a VDSL2 access service in bridging mode in an example network. Configure the access service by referring to this example when the service streams on the modem is activated in bridging mode. After the configuration, you can access the Internet in PPPoE mode over VDSL2 lines.

Prerequisites

- Network devices and lines function properly.
- The VDSL2 service cards function properly.

Data Plan

When the service streams are activated in bridge mode, packets can be encapsulated in ATM or PTM mode.

- In ATM mode, modems encapsulate received subscribers' Ethernet packets into ATM packets in bridging mode and then transmit the packets upstream to the OLT. Configure the service encapsulation type on the OLT as the bridging mode.
- In PTM mode, modems encapsulate received subscribers' Ethernet packets into PTM packets in bridging mode and then transmit the packets upstream to the OLT. You do not need to configure the service encapsulation type on the OLT.

NOTE

The OLT can restrict the access rate of a user through either a traffic profile or a preset VDSL2 line profile by different means. When both profiles are applied, the smaller value works as the user bandwidth. The following example uses the traffic profile as an example to restrict the access rate of the user.

Table 6-3 Data plan for the VDSL2 access service in bridging mode

Item	Data	Remarks
MEF IP traffic profile	● Name: ip_profile ● CIR: 2048 kbit/s ● Accept default values for other parameters	The Tx service port and the Rx service port use the parameters in the traffic profile for rate restriction.
Line spectrum configuration profile	Name: vdsl_linespectrumcfgprofile Accept the default value for this parameter	-
Channel configuration profile	Name: vdsl_channelcfgprofile Accept the default value for this parameter	-
Line configuration profile	● Name: vdsl_linecfgprofile ● RFI Notch Configuration Parameter: 20 ● VDSL Tone Blackout Parameter: 25 ● Accept default values for other parameters	-
VDSL2 line profile	● Name: vdsl_lineprofile ● Line Configuration Profile: vdsl_linecfgprofile ● Channel 1 Alarm Configuration Profile: vdsl_channelcfgprofile ● Accept default values for other parameters	-
Line alarm configuration profile	Name: vdsl_linealarmprofile Accept the default value for this parameter	-
Channel alarm configuration profile	Name: vdsl_channelalarmprofile Accept the default value for this parameter	-

Item	Data	Remarks
VDSL2 alarm profile	● Name: vdsl_alarmprofile ● Line Alarm Configuration Profile: vdsl_linealarmprofile ● Channel 1 Alarm Configuration Profile: vdsl_channelalarmprofile ● Accept default values for other parameters	-
Service card	VDSL2 Port: 0/16/0 VPI: 0 VCI: 35 Service Type: Single	-
	VLAN ID: 800 VLAN selection: Smart VLAN VLAN Attribute: Common	This VLAN must be the same as the VLAN configured on the upper layer device.
Upstream port	0/9/0	The upstream port is also the subport of VLANs 800.

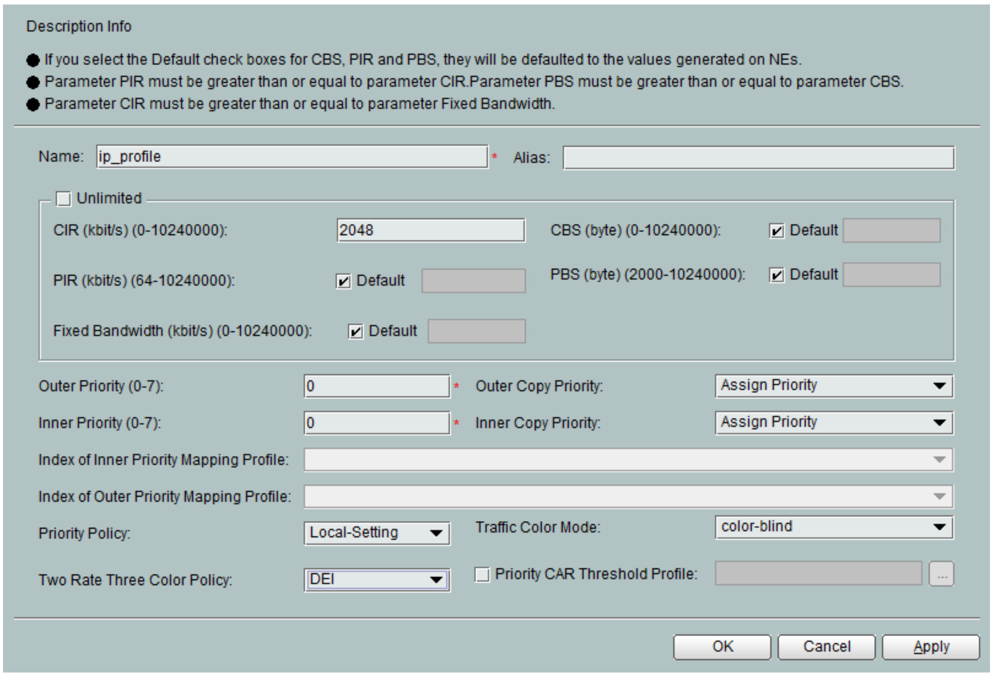
Procedure

Step 1 Configure an MEF IP traffic profile.

The MEF IP traffic profile defines a series of traffic parameters. It is used to configure the parameters of the traffic streams by being bound to the service port so that the rate of the traffic stream can be limited. When configuring a service port, bind the service port to a MEF IP traffic profile.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
3. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
4. In the dialog box that is displayed, set MEF IP traffic profile parameters.

Figure 6-1 Adding a traffic profile



Description Info

- ● If you select the Default check boxes for CBS, PIR and PBS, they will be defaulted to the values generated on NEs.
- ● Parameter PIR must be greater than or equal to parameter CIR.Parameter PBS must be greater than or equal to parameter CBS.
- ● Parameter CIR must be greater than or equal to parameter Fixed Bandwidth.

Name: ip_profile *
Alias:
☐ Unlimited
CIR (kbit/s) (0-10240000): 2048
CBS (byte) (0-10240000): ☑ Default
PIR (kbit/s) (64-10240000): ☑ Default
PBS (byte) (2000-10240000): ☑ Default
Fixed Bandwidth (kbit/s) (0-10240000): ☑ Default
Outer Priority (0-7): 0 *
Outer Copy Priority: Assign Priority
Inner Priority (0-7): 0 *
Inner Copy Priority: Assign Priority
Index of Inner Priority Mapping Profile:
Index of Outer Priority Mapping Profile:
Priority Policy: Local-Setting
Traffic Color Mode: color-blind
Two Rate Three Color Policy: DEI
☐ Priority CAR Threshold Profile:

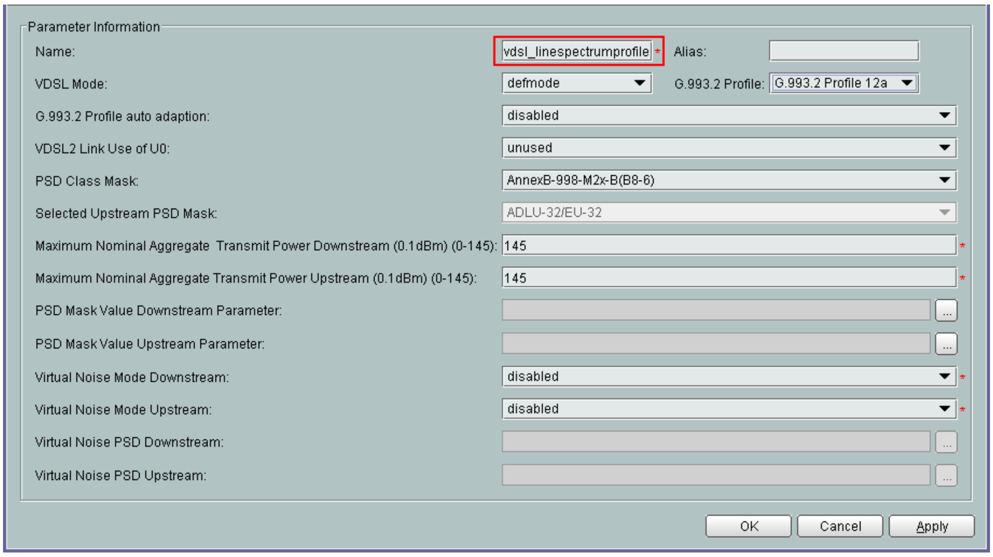
5. Click **OK**.
6. Select the MEF IP traffic profile, right-click, and then choose **Download to NE**.
7. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 2 Configure a VDSL2 line profile.

The VDSL2 line profile binds the specified VDSL2 line configuration profile to the VDSL2 channel configuration profile. After a VDSL2 line profile is bound to a VDSL2 port, the activated VDSL2 port directly references the VDSL2 line profile to limit the port rate and noise margin to improve the service quality.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
3. Click the **Line Spectrum Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters of the VDSL2 line spectrum configuration profile.

Figure 6-2 Adding a VDSL2 line spectrum configuration profile

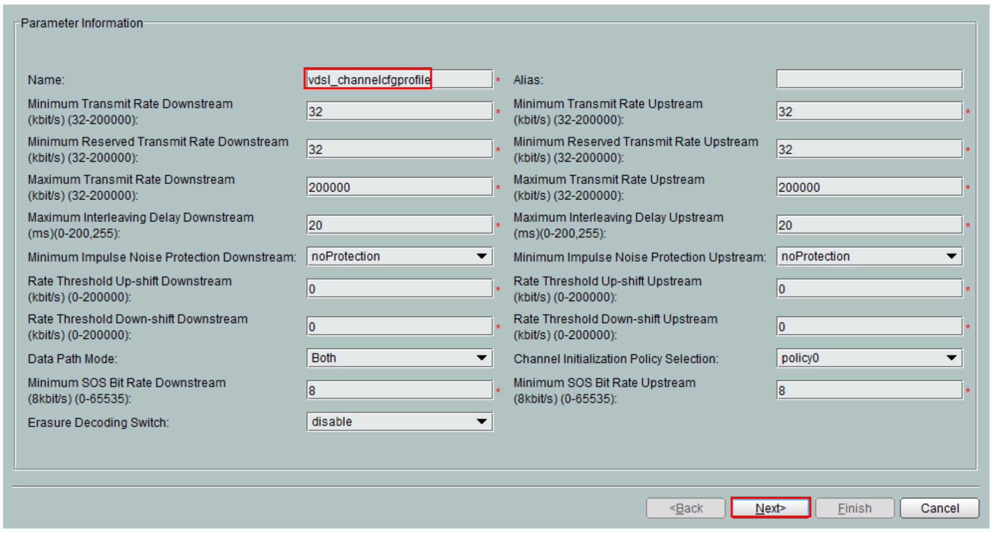


Parameter Information

Name: vdsl_linespectrumprofile *
Alias:
VDSL Mode: defmode
G.993.2 Profile: G.993.2 Profile 12a
G.993.2 Profile auto adaption: disabled
VDSL2 Link Use of U0: unused
PSD Class Mask: AnnexB-998-M2x-B(B8-6)
Selected Upstream PSD Mask: ADLU-32/EU-32
Maximum Nominal Aggregate Transmit Power Downstream (0.1dBm) (0-145): 145 *
Maximum Nominal Aggregate Transmit Power Upstream (0.1dBm) (0-145): 145 *
PSD Mask Value Downstream Parameter:
PSD Mask Value Upstream Parameter:
Virtual Noise Mode Downstream: disabled *
Virtual Noise Mode Upstream: disabled *
Virtual Noise PSD Downstream:
Virtual Noise PSD Upstream:

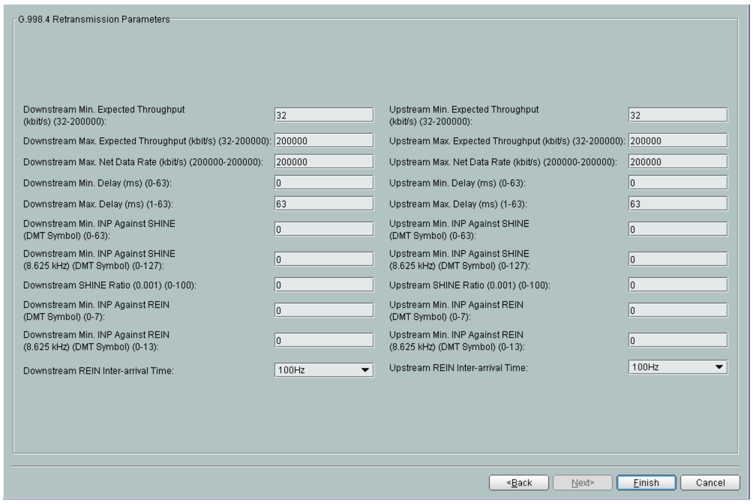
6. Click **OK**.
7. Click the **Channel Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
8. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
9. In the dialog box that is displayed, set the parameters of the VDSL2 channel configuration profile.

Figure 6-3 Adding a VDSL2 channel configuration profile



Parameter Information

Name: vdsl_channelcfgprofile *
Alias:
Minimum Transmit Rate Downstream (kbit/s) (32-200000): 32 *
Minimum Transmit Rate Upstream (kbit/s) (32-200000): 32 *
Minimum Reserved Transmit Rate Downstream (kbit/s) (32-200000): 32 *
Minimum Reserved Transmit Rate Upstream (kbit/s) (32-200000): 32 *
Maximum Transmit Rate Downstream (kbit/s) (32-200000): 200000 *
Maximum Transmit Rate Upstream (kbit/s) (32-200000): 200000 *
Maximum Interleaving Delay Downstream (ms)(0-200,255): 20 *
Maximum Interleaving Delay Upstream (ms)(0-200,255): 20 *
Minimum Impulse Noise Protection Downstream: noProtection
Minimum Impulse Noise Protection Upstream: noProtection
Rate Threshold Up-shift Downstream (kbit/s) (0-200000): 0 *
Rate Threshold Up-shift Upstream (kbit/s) (0-200000): 0 *
Rate Threshold Down-shift Downstream (kbit/s) (0-200000): 0 *
Rate Threshold Down-shift Upstream (kbit/s) (0-200000): 0 *
Data Path Mode: Both
Channel Initialization Policy Selection: policy0
Minimum SOS Bit Rate Downstream (8kbit/s) (0-65535): 8 *
Minimum SOS Bit Rate Upstream (8kbit/s) (0-65535): 8 *
Erasure Decoding Switch: disable

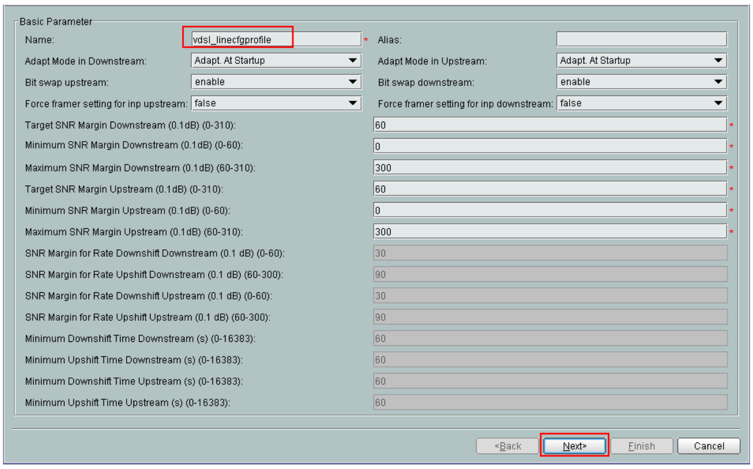


Downstream Min. Expected Throughput (kbit/s) (32-200000): 32
Downstream Max. Expected Throughput (kbit/s) (32-200000): 200000
Downstream Max. Net Data Rate (kbit/s) (200000-200000): 200000
Downstream Min. Delay (ms) (0-63): 0
Downstream Max. Delay (ms) (1-63): 63
Downstream Min. INP Against SHINE (DMT Symbol) (0-63): 0
Downstream Min. INP Against SHINE (8.625 kHz) (DMT Symbol) (0-127): 0
Downstream SHINE Ratio (0.001) (0-100): 0
Downstream Min. INP Against REIN (DMT Symbol) (0-7): 0
Downstream Min. INP Against REIN (8.625 kHz) (DMT Symbol) (0-13): 0
Downstream REIN Inter-arrival Time: 100Hz

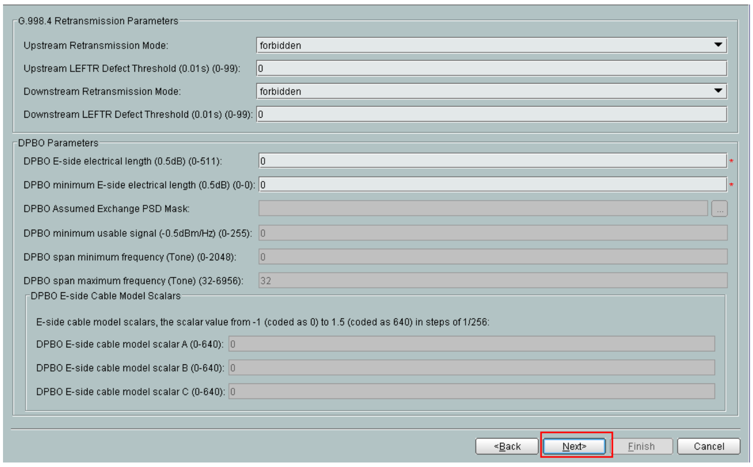
Upstream Min. Expected Throughput (kbit/s) (32-200000): 32
Upstream Max. Expected Throughput (kbit/s) (32-200000): 200000
Upstream Max. Net Data Rate (kbit/s) (200000-200000): 200000
Upstream Min. Delay (ms) (0-63): 0
Upstream Max. Delay (ms) (1-63): 63
Upstream Min. INP Against SHINE (DMT Symbol) (0-63): 0
Upstream Min. INP Against SHINE (8.625 kHz) (DMT Symbol) (0-127): 0
Upstream SHINE Ratio (0.001) (0-100): 0
Upstream Min. INP Against REIN (DMT Symbol) (0-7): 0
Upstream Min. INP Against REIN (8.625 kHz) (DMT Symbol) (0-13): 0
Upstream REIN Inter-arrival Time: 100Hz

10. Click **OK**.
11. Select the channel configuration profile, right-click, and then choose **Download to NE**.
12. In the dialog box that is displayed, select the required OLT, and then click **OK**.
13. Click the **Line Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
14. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
15. In the dialog box that is displayed, set the parameters of the VDSL2 line configuration profile.

Figure 6-4 Adding a VDSL2 line configuration profile



Name: vdsl_linecfgprofile *
Alias:
Adapt Mode in Downstream: Adapt. At Startup
Adapt Mode in Upstream: Adapt. At Startup
Bit swap upstream: enable
Bit swap downstream: enable
Force framer setting for inp upstream: false
Force framer setting for inp downstream: false
Target SNR Margin Downstream (0.1dB) (0-310): 60 *
Minimum SNR Margin Downstream (0.1dB) (0-60): 0 *
Maximum SNR Margin Downstream (0.1dB) (60-310): 300 *
Target SNR Margin Upstream (0.1dB) (0-310): 60 *
Minimum SNR Margin Upstream (0.1dB) (0-60): 0 *
Maximum SNR Margin Upstream (0.1dB) (60-310): 300 *
SNR Margin for Rate Downshift Downstream (0.1 dB) (0-60): 30
SNR Margin for Rate Upshift Downstream (0.1 dB) (60-300): 90
SNR Margin for Rate Downshift Upstream (0.1 dB) (0-60): 30
SNR Margin for Rate Upshift Upstream (0.1 dB) (60-300): 90
Minimum Downshift Time Downstream (s) (0-16383): 60
Minimum Upshift Time Downstream (s) (0-16383): 60
Minimum Downshift Time Upstream (s) (0-16383): 60
Minimum Upshift Time Upstream (s) (0-16383): 60



G.998.4 Retransmission Parameters

Upstream Retransmission Mode: forbidden

Upstream LEFTR Defect Threshold (0.01s) (0-99): 0

Downstream Retransmission Mode: forbidden

Downstream LEFTR Defect Threshold (0.01s) (0-99): 0

DPBO Parameters

DPBO E-side electrical length (0.5dB) (0-511): 0 *

DPBO minimum E-side electrical length (0.5dB) (0-0): 0 *

DPBO Assumed Exchange PSD Mask:

DPBO minimum usable signal (-0.5dBm/Hz) (0-255): 0

DPBO span minimum frequency (Tone) (0-2048): 0

DPBO span maximum frequency (Tone) (32-6956): 32

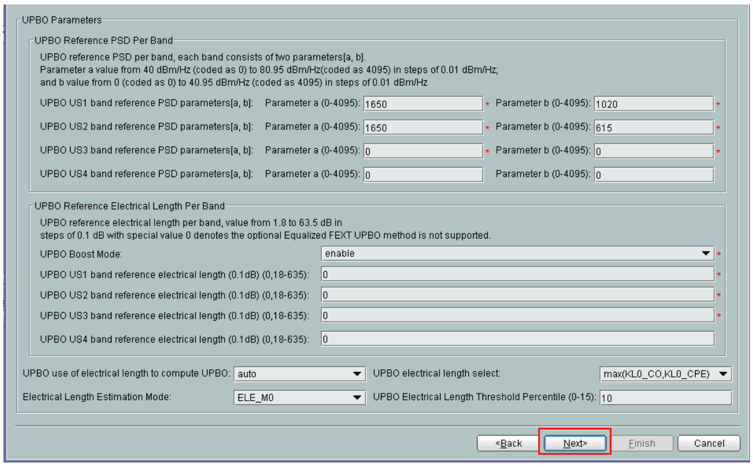
DPBO E-side Cable Model Scalars

E-side cable model scalars, the scalar value from -1 (coded as 0) to 1.5 (coded as 640) in steps of 1/256:

DPBO E-side cable model scalar A (0-640): 0

DPBO E-side cable model scalar B (0-640): 0

DPBO E-side cable model scalar C (0-640): 0



UPBO Parameters

UPBO Reference PSD Per Band

UPBO reference PSD per band, each band consists of two parameters[a, b].
Parameter a value from 40 dBm/Hz (coded as 0) to 80.95 dBm/Hz(coded as 4095) in steps of 0.01 dBm/Hz;
and b value from 0 (coded as 0) to 40.95 dBm/Hz (coded as 4095) in steps of 0.01 dBm/Hz

UPBO US1 band reference PSD parameters[a, b]: Parameter a (0-4095): 1650 * Parameter b (0-4095): 1020 *

UPBO US2 band reference PSD parameters[a, b]: Parameter a (0-4095): 1650 * Parameter b (0-4095): 615 *

UPBO US3 band reference PSD parameters[a, b]: Parameter a (0-4095): 0 * Parameter b (0-4095): 0 *

UPBO US4 band reference PSD parameters[a, b]: Parameter a (0-4095): 0 Parameter b (0-4095): 0

UPBO Reference Electrical Length Per Band

UPBO reference electrical length per band, value from 1.8 to 63.5 dB in
steps of 0.1 dB with special value 0 denotes the optional Equalized FEXT UPBO method is not supported.

UPBO Boost Mode: enable *

UPBO US1 band reference electrical length (0.1dB) (0,18-635): 0 *

UPBO US2 band reference electrical length (0.1dB) (0,18-635): 0 *

UPBO US3 band reference electrical length (0.1dB) (0,18-635): 0 *

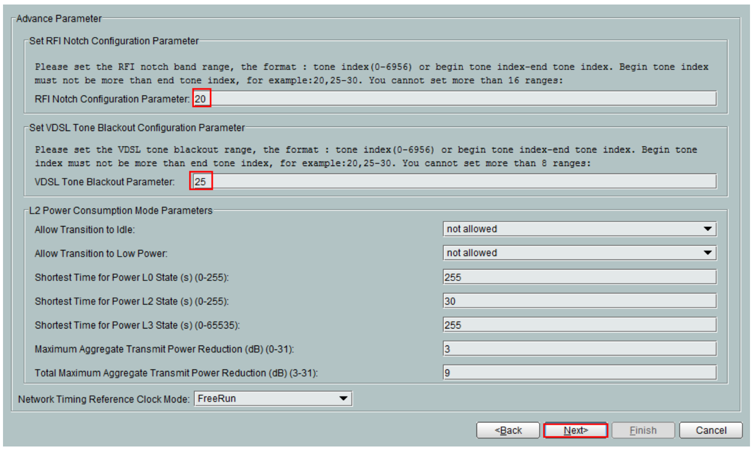
UPBO US4 band reference electrical length (0.1dB) (0,18-635): 0

UPBO use of electrical length to compute UPBO: auto

UPBO electrical length select: max(KL0_CO,KL0_CPE)

Electrical Length Estimation Mode: ELE_M0

UPBO Electrical Length Threshold Percentile (0-15): 10



Advance Parameter

Set RFI Notch Configuration Parameter

Please set the RFI notch band range, the format : tone index(0-6956) or begin tone index-end tone index. Begin tone index must not be more than end tone index, for example:20,25-30. You cannot set more than 16 ranges:

RFI Notch Configuration Parameter: 20

Set VDSL Tone Blackout Configuration Parameter

Please set the VDSL tone blackout range, the format : tone index(0-6956) or begin tone index-end tone index. Begin tone index must not be more than end tone index, for example:20,25-30. You cannot set more than 8 ranges:

VDSL Tone Blackout Parameter: 25

L2 Power Consumption Mode Parameters

Allow Transition to Idle: not allowed

Allow Transition to Low Power: not allowed

Shortest Time for Power L0 State (s) (0-255): 255

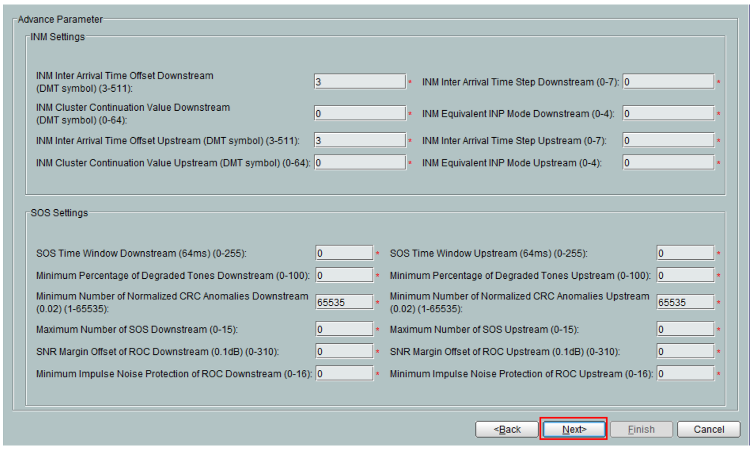
Shortest Time for Power L2 State (s) (0-255): 30

Shortest Time for Power L3 State (s) (0-65535): 255

Maximum Aggregate Transmit Power Reduction (dB) (0-31): 3

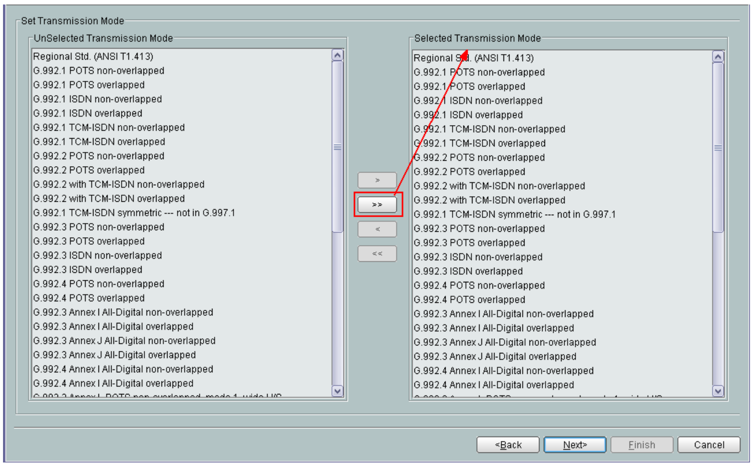
Total Maximum Aggregate Transmit Power Reduction (dB) (3-31): 9

Network Timing Reference Clock Mode: FreeRun



INM Inter Arrival Time Offset Downstream (DMT symbol) (3-511): 3 *
INM Inter Arrival Time Step Downstream (0-7): 0 *
INM Cluster Continuation Value Downstream (DMT symbol) (0-64): 0 *
INM Equivalent INP Mode Downstream (0-4): 0 *
INM Inter Arrival Time Offset Upstream (DMT symbol) (3-511): 3 *
INM Inter Arrival Time Step Upstream (0-7): 0 *
INM Cluster Continuation Value Upstream (DMT symbol) (0-64): 0 *
INM Equivalent INP Mode Upstream (0-4): 0 *

SOS Time Window Downstream (64ms) (0-255): 0 *
SOS Time Window Upstream (64ms) (0-255): 0 *
Minimum Percentage of Degraded Tones Downstream (0-100): 0 *
Minimum Percentage of Degraded Tones Upstream (0-100): 0 *
Minimum Number of Normalized CRC Anomalies Downstream (0.02) (1-65535): 65535 *
Minimum Number of Normalized CRC Anomalies Upstream (0.02) (1-65535): 65535 *
Maximum Number of SOS Downstream (0-15): 0 *
Maximum Number of SOS Upstream (0-15): 0 *
SNR Margin Offset of ROC Downstream (0.1dB) (0-310): 0 *
SNR Margin Offset of ROC Upstream (0.1dB) (0-310): 0 *
Minimum Impulse Noise Protection of ROC Downstream (0-16): 0 *
Minimum Impulse Noise Protection of ROC Upstream (0-16): 0 *

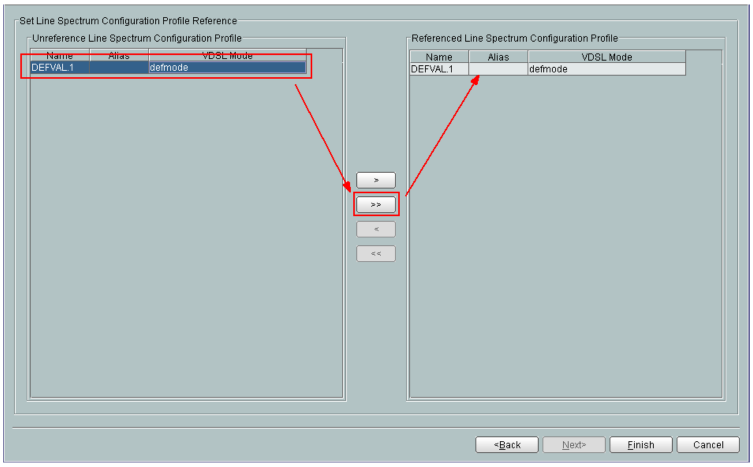


UnSelected Transmission Mode:

Regional Std. (ANSI T1.413)
G.992.1 POTS non-overlapped
G.992.1 POTS overlapped
G.992.1 ISDN non-overlapped
G.992.1 ISDN overlapped
G.992.1 TCM-ISDN non-overlapped
G.992.1 TCM-ISDN overlapped
G.992.2 POTS non-overlapped
G.992.2 POTS overlapped
G.992.2 with TCM-ISDN non-overlapped
G.992.2 with TCM-ISDN overlapped
G.992.1 TCM-ISDN symmetric --- not in G.997.1
G.992.3 POTS non-overlapped
G.992.3 POTS overlapped
G.992.3 ISDN non-overlapped
G.992.3 ISDN overlapped
G.992.4 POTS non-overlapped
G.992.4 POTS overlapped
G.992.3 Annex I All-Digital non-overlapped
G.992.3 Annex I All-Digital overlapped
G.992.3 Annex J All-Digital non-overlapped
G.992.3 Annex J All-Digital overlapped
G.992.4 Annex I All-Digital non-overlapped
G.992.4 Annex I All-Digital overlapped

Selected Transmission Mode:

Regional Std. (ANSI T1.413)
G.992.1 POTS non-overlapped
G.992.1 POTS overlapped
G.992.1 ISDN non-overlapped
G.992.1 ISDN overlapped
G.992.1 TCM-ISDN non-overlapped
G.992.1 TCM-ISDN overlapped
G.992.2 POTS non-overlapped
G.992.2 POTS overlapped
G.992.2 with TCM-ISDN non-overlapped
G.992.2 with TCM-ISDN overlapped
G.992.1 TCM-ISDN symmetric --- not in G.997.1
G.992.3 POTS non-overlapped
G.992.3 POTS overlapped
G.992.3 ISDN non-overlapped
G.992.3 ISDN overlapped
G.992.4 POTS non-overlapped
G.992.4 POTS overlapped
G.992.3 Annex I All-Digital non-overlapped
G.992.3 Annex I All-Digital overlapped
G.992.3 Annex J All-Digital non-overlapped
G.992.3 Annex J All-Digital overlapped
G.992.4 Annex I All-Digital non-overlapped
G.992.4 Annex I All-Digital overlapped


Set Line Spectrum Configuration Profile Reference
Unreference Line Spectrum Configuration Profile
Referenced Line Spectrum Configuration Profile
>
>>
<
<<
<Back
Next>
Finish
Cancel

Unreference Line Spectrum Configuration Profile:

Name	Alias	VDSL Mode
DEFVAL.1		defmode

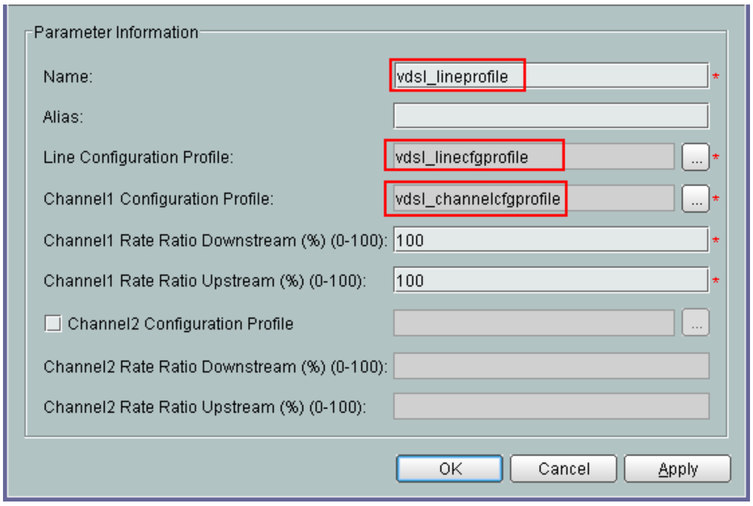
Referenced Line Spectrum Configuration Profile:

Name	Alias	VDSL Mode
DEFVAL.1		defmode

16. Click **Finish**.
17. Select the VDSL2 line configuration profile, right-click, and then choose **Download to NE**.
18. In the dialog box that is displayed, select the required OLT, and then click **OK**.
19. Click the **Line Template** tab, and select the required device type from the **Device Type** drop-down list.
20. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

21. In the dialog box that is displayed, set the parameters of the VDSL2 line profile.

Figure 6-5 Adding a VDSL2 line profile



Parameter Information

Name: vdsl_lineprofile *

Alias:

Line Configuration Profile: vdsl_linecfgprofile ... *

Channel1 Configuration Profile: vdsl_channelcfgprofile ... *

Channel1 Rate Ratio Downstream (%) (0-100): 100 *

Channel1 Rate Ratio Upstream (%) (0-100): 100 *

☐ Channel2 Configuration Profile ...

Channel2 Rate Ratio Downstream (%) (0-100):

Channel2 Rate Ratio Upstream (%) (0-100):

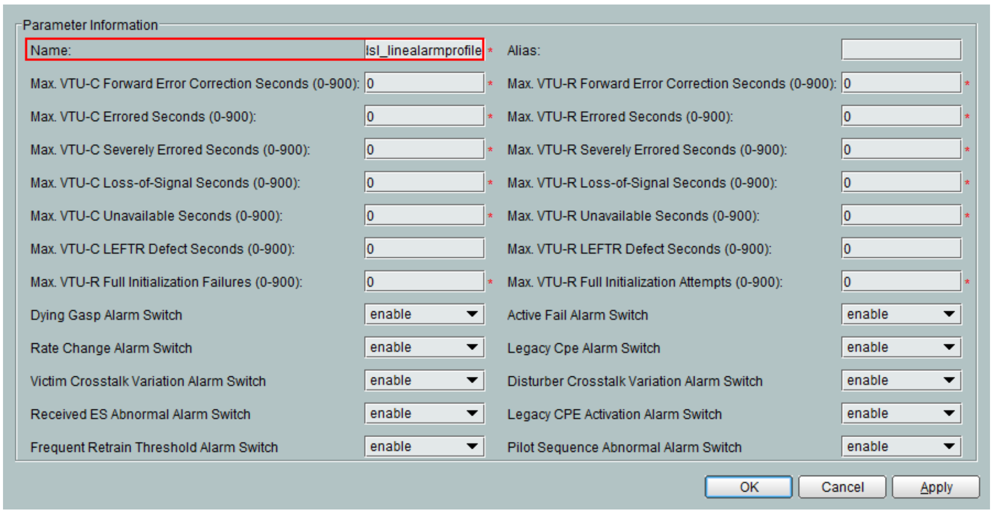
22. Click **OK**.
23. Select the line profile, right-click, and then choose **Download to NE**.
24. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 3 Configure a VDSL2 alarm profile.

A VDSL2 alarm profile binds a specified line alarm configuration profile and a channel alarm configuration profile. After the binding is successful, an activated VDSL2 port directly references an alarm profile to monitor the performance of the VDSL2 port. When the parameter value of the port exceeds the preset threshold, an alarm is generated.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
3. Click the **VDSL2 Alarm Profile**.
4. Click the **Line Alarm Configuration Profile** tab.
5. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
6. In the dialog box that is displayed, set the parameters of the VDSL2 line alarm configuration profile.

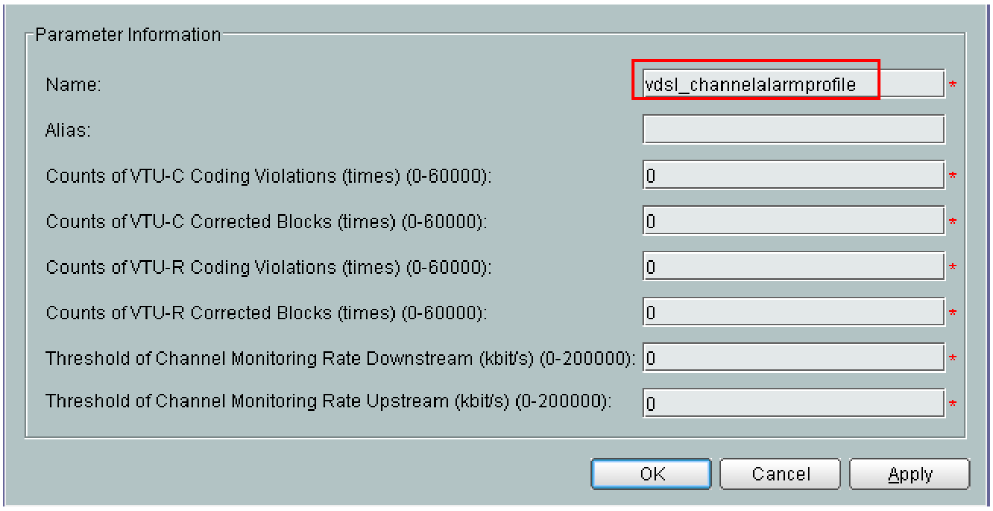
Figure 6-6 Adding a VDSL2 line alarm configuration profile


Parameter Information

Name: lsl_linealarmprofile *
Alias:
Max. VTU-C Forward Error Correction Seconds (0-900): 0 *
Max. VTU-R Forward Error Correction Seconds (0-900): 0 *
Max. VTU-C Errored Seconds (0-900): 0 *
Max. VTU-R Errored Seconds (0-900): 0 *
Max. VTU-C Severely Errored Seconds (0-900): 0 *
Max. VTU-R Severely Errored Seconds (0-900): 0 *
Max. VTU-C Loss-of-Signal Seconds (0-900): 0 *
Max. VTU-R Loss-of-Signal Seconds (0-900): 0 *
Max. VTU-C Unavailable Seconds (0-900): 0 *
Max. VTU-R Unavailable Seconds (0-900): 0 *
Max. VTU-C LEFTR Defect Seconds (0-900): 0
Max. VTU-R LEFTR Defect Seconds (0-900): 0
Max. VTU-R Full Initialization Failures (0-900): 0 *
Max. VTU-R Full Initialization Attempts (0-900): 0 *
Dying Gasp Alarm Switch: enable
Active Fail Alarm Switch: enable
Rate Change Alarm Switch: enable
Legacy Cpe Alarm Switch: enable
Victim Crosstalk Variation Alarm Switch: enable
Disturber Crosstalk Variation Alarm Switch: enable
Received ES Abnormal Alarm Switch: enable
Legacy CPE Activation Alarm Switch: enable
Frequent Retrain Threshold Alarm Switch: enable
Pilot Sequence Abnormal Alarm Switch: enable

7. Click **OK**.
8. Select the VDSL2 line alarm configuration profile, right-click, and then choose **Download to NE**.
9. In the dialog box that is displayed, select the required OLT, and then click **OK**.
10. Click the **Channel Alarm Configuration Profile** tab.
11. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
12. In the dialog box that is displayed, set the parameters of the VDSL2 channel alarm configuration profile.

Figure 6-7 Adding a VDSL2 channel alarm configuration profile

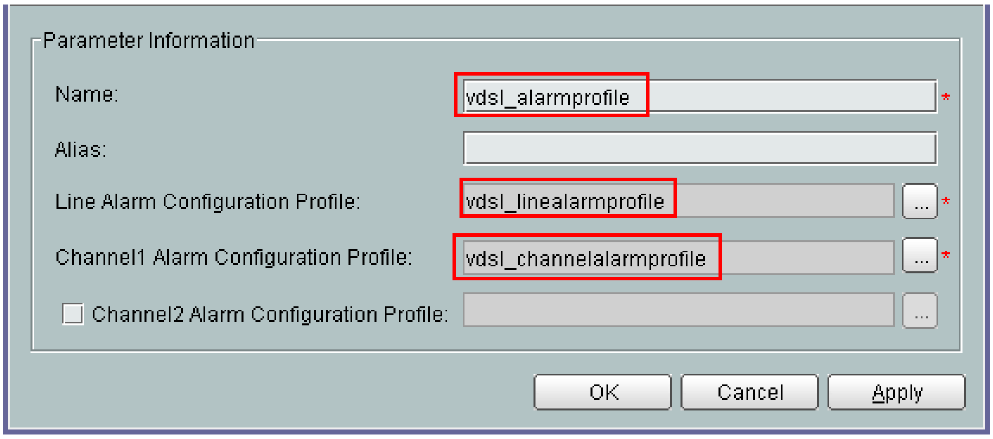

Parameter Information

Name: vdsl_channelalarmprofile *
Alias:
Counts of VTU-C Coding Violations (times) (0-60000): 0 *
Counts of VTU-C Corrected Blocks (times) (0-60000): 0 *
Counts of VTU-R Coding Violations (times) (0-60000): 0 *
Counts of VTU-R Corrected Blocks (times) (0-60000): 0 *
Threshold of Channel Monitoring Rate Downstream (kbit/s) (0-200000): 0 *
Threshold of Channel Monitoring Rate Upstream (kbit/s) (0-200000): 0 *

13. Click **OK**.
14. Select the VDSL2 channel alarm configuration profile, right-click, and then choose **Download to NE**.

15. In the dialog box that is displayed, select the required OLT, and then click **OK**.
16. Click the **Alarm Template** tab.
17. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
18. In the dialog box that is displayed, set the parameters of the VDSL2 alarm profile.

Figure 6-8 Adding a VDSL2 alarm profile



Parameter Information

Name: vdsl_alarmprofile *

Alias:

Line Alarm Configuration Profile: vdsl_linealarmprofile *

Channel1 Alarm Configuration Profile: vdsl_channelalarmprofile *

☐ Channel2 Alarm Configuration Profile:

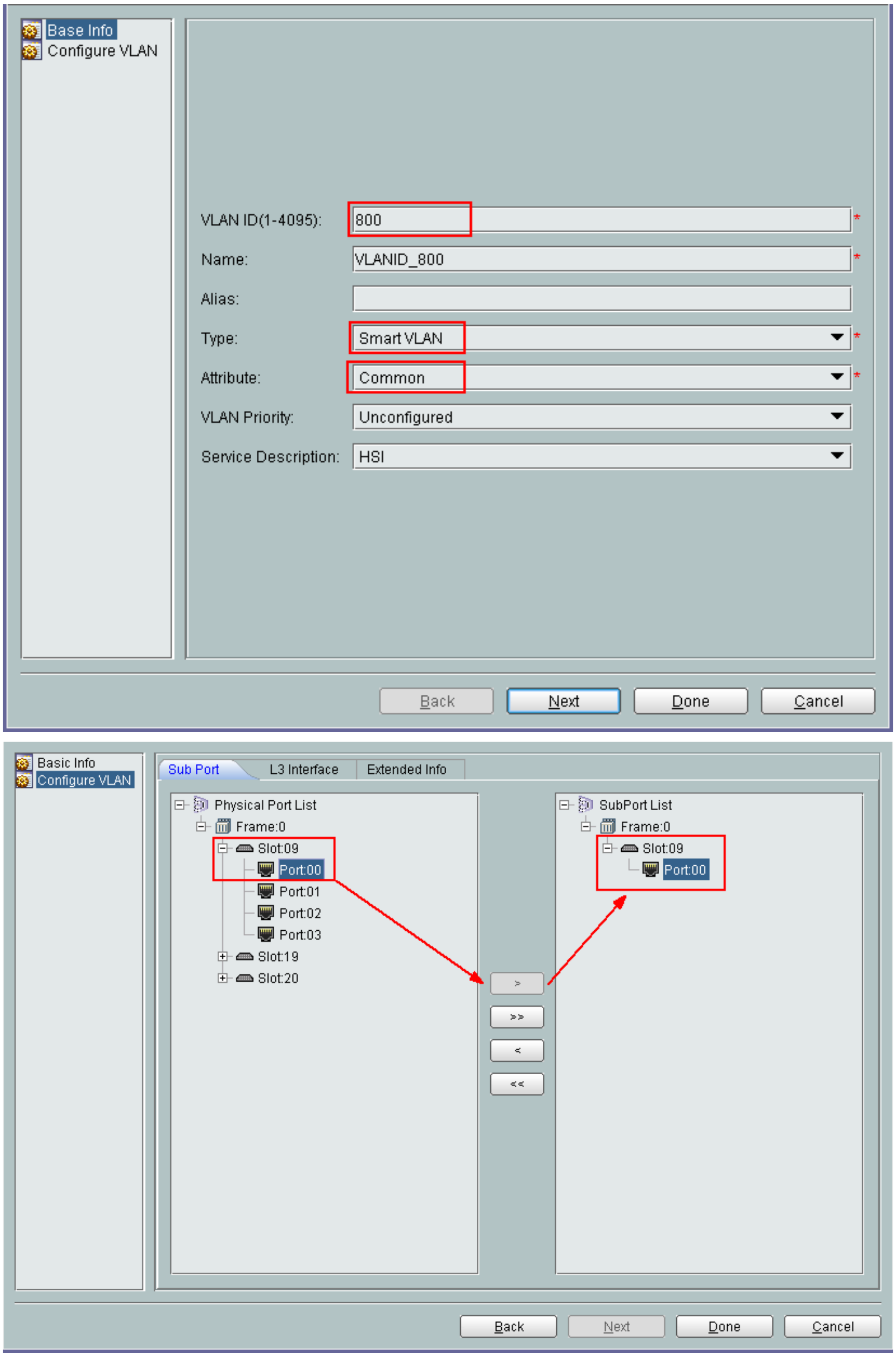
19. Click **OK**.
20. Select the VDSL2 alarm profile, right-click, and then choose **Download to NE**.
21. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 4 Add a VLAN and configure an upstream port to the VLAN.

Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree. On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.
3. Right-click the list, and then choose **Add**.
4. In the dialog box that is displayed, set VLAN parameters.

Figure 6-9 Adding a VLAN and configuring an upstream port to the VLAN



VLAN ID(1-4095): 800 *
Name: VLANID_800 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI

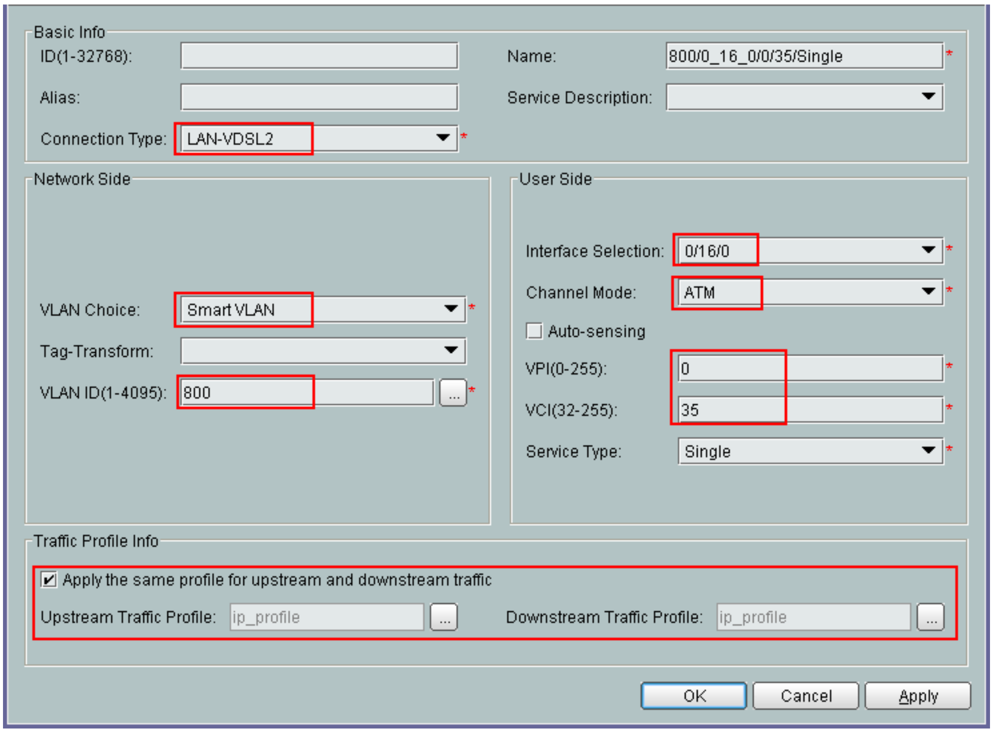
5. Click **OK**.

Step 5 Configure the service port.

After being configured successfully, the VDSL2 service port can carry service streams of various types.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ⌄ to display the VDSL2 ports.
4. In the information list, select a VDSL2 port record. On the **Service Port Info** tab page in the lower pane, right-click, and then choose **Add**.
5. In the dialog box that is displayed, set the service-port parameters.

Figure 6-10 Adding a service virtual port



Basic Info
ID(1-32768):
Name: 800/0_16_0/0/35/Single *
Alias:
Service Description:
Connection Type: LAN-VDSL2 *

Network Side
VLAN Choice: Smart VLAN *
Tag-Transform:
VLAN ID(1-4095): 800 *

User Side
Interface Selection: 0/16/0 *
Channel Mode: ATM *
☐ Auto-sensing
VPI(0-255): 0 *
VCI(32-255): 35 *
Service Type: Single *

Traffic Profile Info
☑ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile: ip_profile
Downstream Traffic Profile: ip_profile

6. Click **OK**.

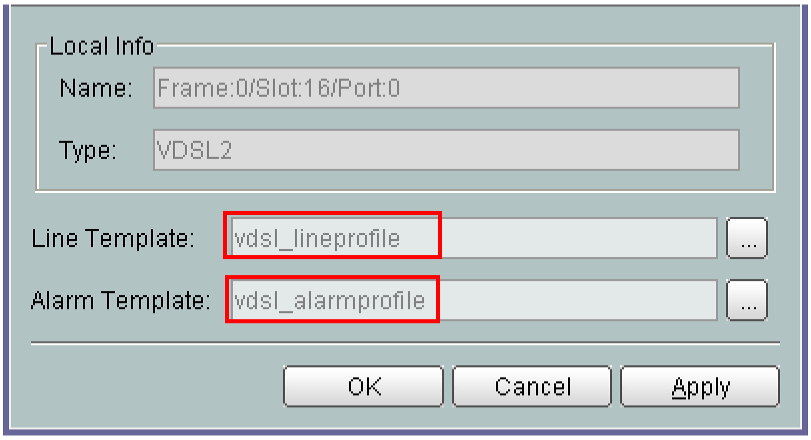
Step 6 Configure the attributes of the VDSL2 port.

Configures a line profile, an alarm profile, extended profile (optional) of a VDSL2 port. These attributes can be used after the VDSL2 port is activated.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ⌄ to display the VDSL2 ports.
4. In information list, right-click port **0/16/0** and choose **Configure Attributes** from the shortcut menu.

5. In the dialog box that is displayed, set the VDSL2 port parameters.

Figure 6-11 Configuring VDSL2 port attributes



Local Info
Name: Frame:0/Slot:16/Port:0
Type: VDSL2
Line Template: vdsl_lineprofile
Alarm Template: vdsl_alarmprofile

6. Click **OK**.

Step 7 Activate the VDSL2 port.

The VDSL2 port can transmit the service in the normal state only when it is activated successfully.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ⮟ to display the VDSL2 ports.
4. In the list, choose ports **0/16/0** to be activated. Right-click, and then choose **Activate**.

Step 8 Save the data.

Backup the data from the OLT to the U2000.

1. In the **Main Topology**, select **OLT** in the **Physical Root** navigation tree, right-click, and then choose **Save Data Immediately**.
2. Click **OK**.

----End

Result

After the configuration is complete, the PC of the user can pass the authentication and can access the Internet.

6.5 Configuration Example of the ADSL IPoA Access Service

This topic describes how to configure the ADSL IPoA access service based on the example network. After the configuration, the user can log in to the Internet through the ADSL line in the IPoA mode.

Prerequisites

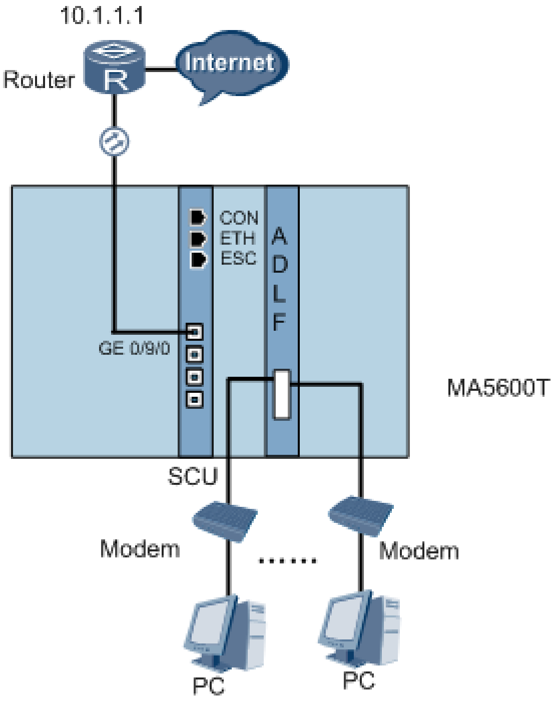
- The example network as shown in **Figure 6-12** must be complete.
- The network devices and lines must be in the normal state.
- The ADSL service cards are in the normal state.

Example Network

Figure 6-12 shows an example network of the ADSL IPoA service.

The PC is connected to the ADSL service port of the OLT through the ADSL modem. After transmitted through the modem, the user packets are transmitted to the OLT in the IPoA mode and then transmitted upstream to the upper layer network.

Figure 6-12 Example network of the ADSL IPoA access service



Data Plan

Table 6-4 Data plan for the ADSL service in IPoA mode

Item	Data	Remarks
Service card	ADSL Port: 0/11/0-0/11/31 VPI: 0 VCI: 35 Service Type: Single	-
	VLAN ID: 20-51 VLAN Type: MUX VLAN VLAN Attribute: Common	The VLAN must be consistent with the VLAN configured on the upper layer device.
Upstream port	0/19/0	The upstream port is also the subport of VLANs 20-51.
MEF IP Traffic Profile	● Name: ip_profile ● CIR: 2048 kbit/s ● Accept the default values for the other parameters.	The Tx service port and the Rx service port use the parameters in the traffic profile for rate restriction.
Line Profile	Name: adsl_lineprofile ADSL Operating Mode: g.dmt Line Type: Interleaved Adapt Mode in Downstream: Adaptation at Runtime Rate parameters: ● ATU-C(Downstream) Interleaved Min.Tx Rate: 32 kbit/s ● ATU-R(Upstream) Interleaved Min.Tx Rate: 32 kbit/s ● ATU-C(Downstream) Interleaved Max.Tx Rate: 2048 kbit/s ● ATU-R(Upstream) Interleaved Max.Tx Rate: 512 kbit/s Accept the default values for the other parameters.	The OLT restricts the access rate of a user through either a traffic profile or an ADSL line profile. When both are applied, the smaller value works.

Item	Data	Remarks
Alarm Profile	Name: adsl_alarmprofile ● ATU-C(Downstream) 15-min Loss Thresh: 60s ● ATU-C(Upstream) 15-min Loss Thresh: 60s ● ATU-C(Downstream) 15-min ESs Thresh: 60s ● ATU-C(Upstream) 15-min ESs Thresh: 60s Accept the default values for the other parameters.	-
MAC Address Pool	Start MAC Address: 00-00-00-00-00-10 Address Range: 256 Type: xpoa	-
IPoA encapsulation type	llc_ip	Before configuring the encapsulation type of the service port as IPoA, you must enable the IPoA function.
IPoA default gateway	IP Address: 10.1.1.1	It indicates the IP address of the upper layer router. The destination IP address (Dst IP) in the extended attribute of the service port must be the same as this IP address.
Modem	Working mode: IPoA IP Address: 10.1.1.10-10.1.1.41	The source IP address (Src IP) in the extended attribute of the service port must be the same as this IP address.

Procedure

Step 1 Add a VLAN and configure an upstream port to the VLAN.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree. On the **VLAN** tab page, set the filter criteria or click ⏬ to display the VLANs.
3. Right-click the list, and then choose **Batch Add**.
4. In the dialog box that is displayed, click the **Base Info** tab, and then set the parameters as follows:
   - **Start ID** and **End ID**: **20** and **51** respectively
   - **Type**: **MUX VLAN**
   - **Attribute**: **Common**
5. Click **Next**.
6. Click the **Sub Port** tab, configure the upstream port in the VLAN, and then set **Sub Port** to **0/19/0**.
7. Click **Done**.

Step 2 Configure the MEF IP traffic profile.

1. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
2. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
3. In the dialog box that is displayed, set the MEF IP traffic profile parameters **Name** to **ip_profile** and **CIR** to **2048kbit/s**.
4. Click **OK**.
5. Select the MEF IP traffic profile, right-click, and then choose **Download to NE**.
6. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 3 Configure the ADSL line profile.

1. In the dialog box that is displayed, choose **DSL Profile** > **ADSL Profile** from the navigation tree.
2. Click the **ADSL Line Profile** tab, and select the required device type from the **Device Type** drop-down list.
3. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
4. In the dialog box that is displayed, set the ADSL line profile parameters as follows:
   - **Name**: **adsl_lineprofile**
   - **ADSL Operating Mode**: **G.dmt**
   - **Line Type**: **Interleaved**
   - **Adapt Mode in Downstream**: **Adaptation at Runtime**
   - **ATU-C(Downstream)/ATU-R(Upstream) Interleaved Min.Tx Rate**: **32kbit/s**
   - **ATU-C(Downstream) Interleaved Max.Tx Rate**: **2048kbit/s**
   - **ATU-R(Upstream) Interleaved Max.Tx Rate**: **512kbit/s**
5. Click **Next** to set the ADSL line profile advanced parameters and extended parameters, click **Finish**.
6. Select the line profile, right-click, and then choose **Download to NE**.

7. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 4 Configure the ADSL alarm profile.

1. In the dialog box that is displayed, choose **DSL Profile** > **ADSL Profile** from the navigation tree.
2. Click the **ADSL Alarm Profile** tab, and select the required device type from the **Device Type** drop-down list.
3. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters of the ADSL alarm profile as follows:
   - **Name**: **adsl_alarmprofile**
   - **ATU-C(Downstream) 15-min Loss Thresh**: **60s**
   - **ATU-C(Upstream) 15-min Loss Thresh**: **60s**
   - **ATU-C(Downstream) 15-min ESs Thresh**: **60s**
   - **ATU-C(Upstream) 15-min ESs Thresh**: **60s**
5. Click **OK**.
6. Select the alarm profile, right-click, and then choose **Download to NE**.
7. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 5 Enable the protocol conversion function and configure the IPoA default gateway.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. On the tab page that is displayed, choose **NE Properties** > **Encapsulation Management** > **IPoA** from the navigation tree.
3. In the right pane of the interface, set **IPoA Enable state** as **Open** and set **IP address of the default gateway** to **10.1.1.1**.
4. Click **Apply**.

Step 6 Configure a service port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **ADSL Port** from the navigation tree.
3. On the **ADSL** tab page, set the filter criteria or click ︾ to display the ADSL ports.
4. In the information list, select an ADSL port record. On the **Service Port Info** tab page in the lower pane, right-click, and then choose **Add**.
5. In the dialog box that is displayed, set the parameters of the ADSL service port as follows:
   - In the **Traffic Profile Info** area, select **Apply the same profile for upstream and downstream traffic**, and then set the **Upstream Traffic Name** and **Downstream Traffic Name** both to **ip_profile**.
   - In the **User Side** area, set the **Interface Selection** to **0/11/0-0/11/31**.
   - In the **Network Side** area, set the VLAN parameter as follows and make them consistent with the parameters when you add the VLAN.
     - **VLAN Choice**: **MUX VLAN**
     - **Start ID** and **End ID**: **20** and **51** respectively

- In the **User Side** area, set the VPI/VCI parameters as follows:
  - **VPI**: **0**
  - **VCI**: **35**
- In the **Attributes** area, set the **Service Type** parameter to **Single**.

6. Click **OK**.

Step 7 Configure the attributes of an ADSL port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **ADSL Port** from the navigation tree.
3. On the **ADSL** tab page, set the filter criteria or click ︾ to display the ADSL ports.
4. In information list, right-click port **0/11/0-0/11/31** and choose **Configure Attributes** from the shortcut menu.
5. In the dialog box that is displayed, bind the ADSL port with the corresponding profile, and then set the **Line Profile** parameter to **adsl_lineprofile** and the **Alarm Profile** parameter to **adsl_alarmprofile**.
6. Click **OK**.

Step 8 Activate an ADSL port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **ADSL Port** from the navigation tree.
3. On the **ADSL** tab page, set the filter criteria or click ︾ to display the ADSL ports.
4. Select a record from the port list 0/11/0-0/11/31 to be configured, right-click, and then choose **Activate**.

Step 9 Configure the MAC address pool.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **NE Properties** > **MAC Address Pool** from the navigation tree on the tab page that is displayed.
3. In the information list, right-click and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the **Start MAC Address** parameter to **00-00-00-00-00-10**, the **Address Range** parameter to **256** and the **Type** parameter to **xpoa**.
5. Click **OK**.

Step 10 Configure the IPoA encapsulation type of the ADSL port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **Connection** > **Service Port** from the navigation tree.
3. On the **Service Port** tab page, set the filter criteria to display the required service virtual ports.

4. Select a record that you need from the service port list, right-click, and then choose **Configure Extended Properties**.
5. In the dialog box that is displayed, set the **Protocol Type** parameter to **llc_ip** and the **Source IP Address** parameter to **10.1.1.10** and the **Destination IP Address** parameter to **10.1.1.1**.
6. Click **Apply**, and then configure the IPoA encapsulation type of port 0/11/1-0/11/31 according to the preceding operation: The **Source IP Address** parameter is **10.1.1.11-10.1.1.41** and the **Destination IP Address** parameter is **10.1.1.1**.
7. Click **OK**.

Step 11 Save the data.

1. In the **Main Topology**, select **OLT** in the **Physical Root** navigation tree, right-click, and then choose **Save Data Immediately**.
2. Click **OK**.

----End

Result

After the configuration is complete, the user PC can pass the authentication and log in to the Internet in the IPoA mode.

6.6 Configuration Example of the VDSL2 PPPoA Access Service

This topic describes how to configure the VDSL2 PPPoA access service in an example network. After the configuration, you can access the Internet in PPPoA mode over VDSL2 lines.

Prerequisites

- The network devices and lines function properly.
- The VDSL2 service cards function properly.

Data Plan

The computer is connected to the VDSL2 service port of the OLT through the VDSL2 modem. After transmitted through the modem, the user packets are transmitted to the OLT in PPPoA mode and then transmitted upstream to the upper layer network.

NOTE

The OLT restricts the access rate of a user through either a traffic profile or a VDSL2 line profile. When both are applied, the smaller value works.

Table 6-5 Data plan for the VDSL2 PPPoA access service

Item	Data	Remarks
MEF IP traffic profile	● Name: ip_profile ● CIR: 2048 kbit/s	Receive and transmit service virtual ports are rate limited by parameters in the traffic profile.
VDSL2 line spectrum configuration profile	● Name: vdsl_linespectrumprofile ● Accept default values for other parameters	-
VDSL2 channel configuration profile	● Name: vdsl_channelcfgprofile ● Accept default values for other parameters	-
VDSL2 line configuration profile	● Name: vdsl_linecfgprofile ● RFI Notch Configuration Parameter: 20 ● VDSL Tone Blackout Parameter: 25 ● Accept default values for other parameters	-
VDSL2 line profile	● Name: vdsl_lineprofile ● Line Configuration Profile: vdsl_linecfgprofile ● Channel 1 Configuration Profile: vdsl_channelcfgprofile ● Accept default values for other parameters	-
VDSL2 line alarm configuration profile	● Name: vdsl_linealarmprofile ● Accept default values for other parameters	-
VDSL2 channel alarm configuration profile	● Name: vdsl_channelalarmprofile ● Accept default values for other parameters	-
VDSL2 alarm profile	● Name: vdsl_alarmprofile ● Line Alarm Configuration Profile: vdsl_linealarmprofile ● Channel1 Alarm Configuration Profile: vdsl_channelalarmprofile ● Accept default values for other parameters	-

Item	Data	Remarks
Service card	VDSL2 Port: 0/16/0 VPI: 0 VCI: 35 Service Type: Single	-
	VLAN ID: 800 Type: Smart VLAN Attribute: Common	The VLAN must be consistent with the VLAN configured on the upper layer device.
Upstream port	0/9/0	The upstream port is also the subport of VLANs 800.
PPPoA parameters	● PPPoA to PPPoE switch: Open ● Accept default values for other parameters	-
MAC address pool	● Start MAC Address: 00-00-00-00-00-10 ● Address Range: 256 ● Type: xpoa	-

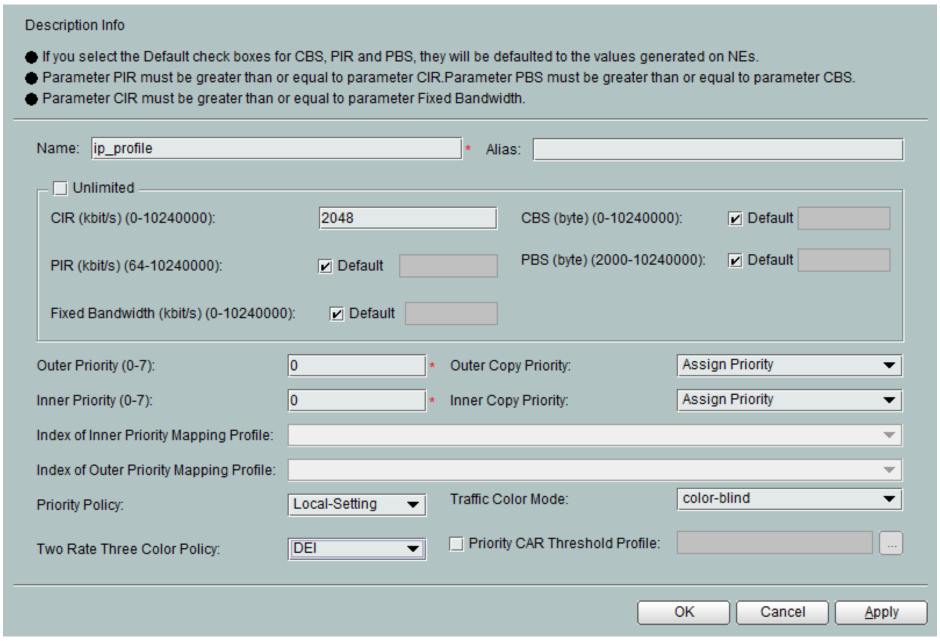
Procedure

Step 1 Configure an MEF IP traffic profile.

The MEF IP traffic profile defines a series of traffic parameters. It is used to configure the parameters of the traffic streams by being bound to the service port so that the rate of the traffic stream can be limited. When configuring a service port, bind the service port to a MEF IP traffic profile.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
3. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
4. In the dialog box that is displayed, set MEF IP traffic profile parameters.

Figure 6-13 Adding an MEF IP traffic profile



Description Info

- If you select the Default check boxes for CBS, PIR and PBS, they will be defaulted to the values generated on NEs.
- Parameter PIR must be greater than or equal to parameter CIR.Parameter PBS must be greater than or equal to parameter CBS.
- Parameter CIR must be greater than or equal to parameter Fixed Bandwidth.

Name: ip_profile * Alias:

☐ Unlimited

CIR (kbit/s) (0-10240000): 2048

CBS (byte) (0-10240000): ☑ Default

PIR (kbit/s) (64-10240000): ☑ Default

PBS (byte) (2000-10240000): ☑ Default

Fixed Bandwidth (kbit/s) (0-10240000): ☑ Default

Outer Priority (0-7): 0 *

Outer Copy Priority: Assign Priority

Inner Priority (0-7): 0 *

Inner Copy Priority: Assign Priority

Index of Inner Priority Mapping Profile:

Index of Outer Priority Mapping Profile:

Priority Policy: Local-Setting

Traffic Color Mode: color-blind

Two Rate Three Color Policy: DEI

☐ Priority CAR Threshold Profile:

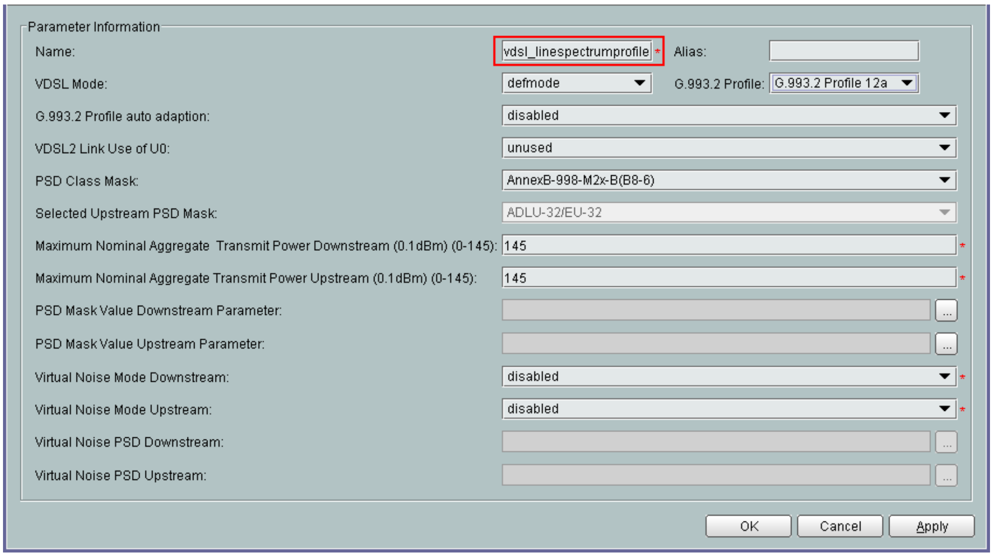
5. Click **OK**.
6. Select the MEF IP traffic profile, right-click, and then choose **Download to NE**.
7. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 2 Configure a VDSL2 line profile.

The VDSL2 line profile binds the specified VDSL2 line configuration profile to the VDSL2 channel configuration profile. After a VDSL2 line profile is bound to a VDSL2 port, the activated VDSL2 port directly references the VDSL2 line profile to limit the port rate and noise margin to improve the service quality.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
3. Click the **Line Spectrum Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters of the VDSL2 line spectrum configuration profile.

Figure 6-14 Adding a VDSL2 line spectrum configuration profile

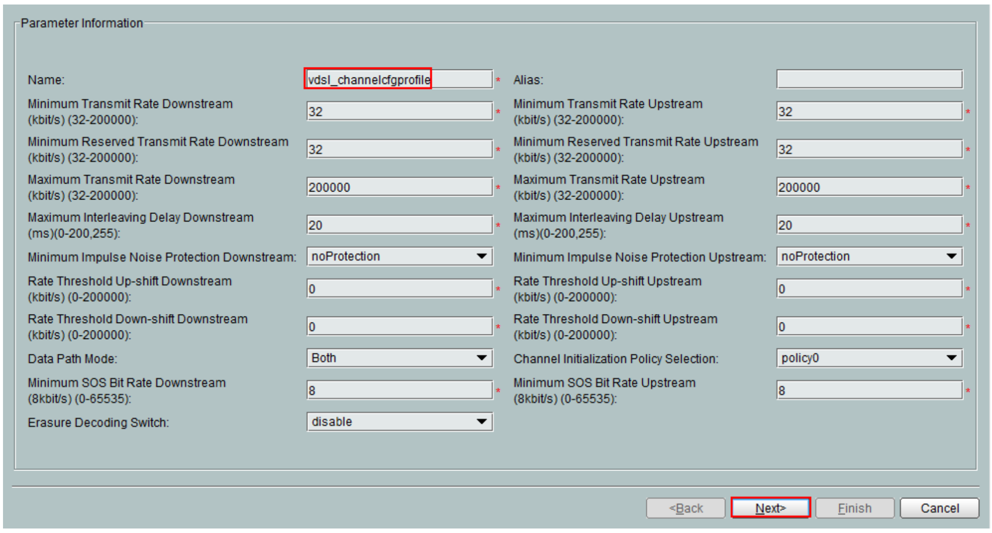


Parameter Information

Name: vdsl_linespectrumprofile
Alias:
VDSL Mode: defmode
G.993.2 Profile: G.993.2 Profile 12a
G.993.2 Profile auto adaption: disabled
VDSL2 Link Use of U0: unused
PSD Class Mask: AnnexB-998-M2x-B(B8-6)
Selected Upstream PSD Mask: ADLU-32/EU-32
Maximum Nominal Aggregate Transmit Power Downstream (0.1dBm) (0-145): 145
Maximum Nominal Aggregate Transmit Power Upstream (0.1dBm) (0-145): 145
PSD Mask Value Downstream Parameter:
PSD Mask Value Upstream Parameter:
Virtual Noise Mode Downstream: disabled
Virtual Noise Mode Upstream: disabled
Virtual Noise PSD Downstream:
Virtual Noise PSD Upstream:

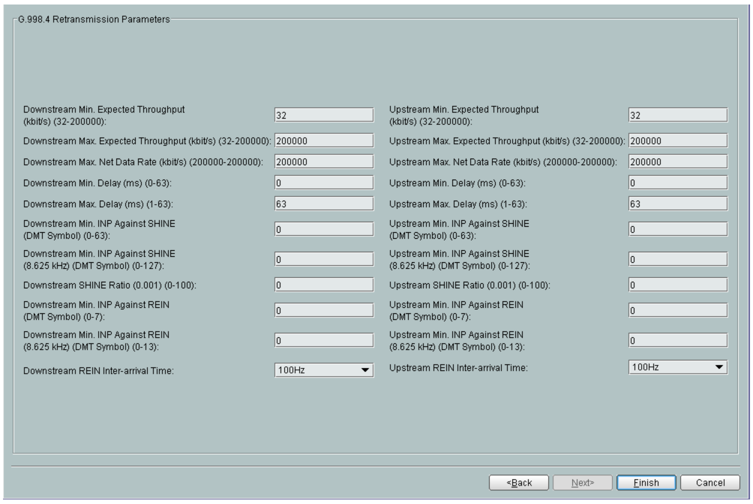
6. Click **OK**.
7. Click the **Channel Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
8. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
9. In the dialog box that is displayed, set the parameters of the VDSL2 channel configuration profile.

Figure 6-15 Adding a VDSL2 channel configuration profile



Parameter Information

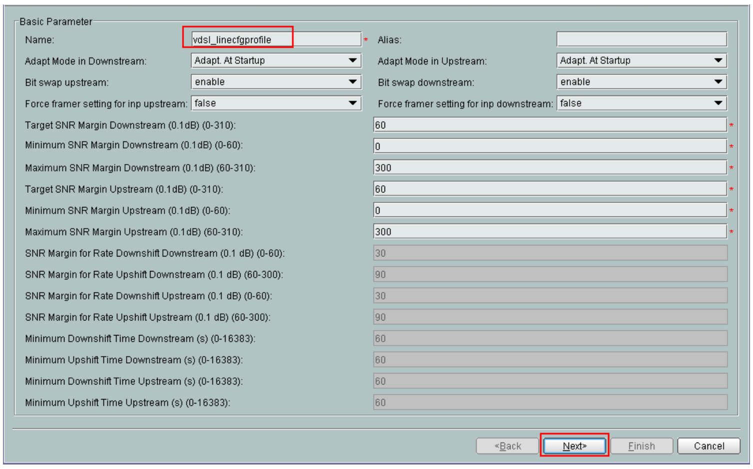
Name: vdsl_channelcfgprofile
Alias:
Minimum Transmit Rate Downstream (kbit/s) (32-200000): 32
Minimum Transmit Rate Upstream (kbit/s) (32-200000): 32
Minimum Reserved Transmit Rate Downstream (kbit/s) (32-200000): 32
Minimum Reserved Transmit Rate Upstream (kbit/s) (32-200000): 32
Maximum Transmit Rate Downstream (kbit/s) (32-200000): 200000
Maximum Transmit Rate Upstream (kbit/s) (32-200000): 200000
Maximum Interleaving Delay Downstream (ms)(0-200,255): 20
Maximum Interleaving Delay Upstream (ms)(0-200,255): 20
Minimum Impulse Noise Protection Downstream: noProtection
Minimum Impulse Noise Protection Upstream: noProtection
Rate Threshold Up-shift Downstream (kbit/s) (0-200000): 0
Rate Threshold Up-shift Upstream (kbit/s) (0-200000): 0
Rate Threshold Down-shift Downstream (kbit/s) (0-200000): 0
Rate Threshold Down-shift Upstream (kbit/s) (0-200000): 0
Data Path Mode: Both
Channel Initialization Policy Selection: policy0
Minimum SOS Bit Rate Downstream (8kbit/s) (0-65535): 8
Minimum SOS Bit Rate Upstream (8kbit/s) (0-65535): 8
Erasure Decoding Switch: disable


G.998.4 Retransmission Parameters

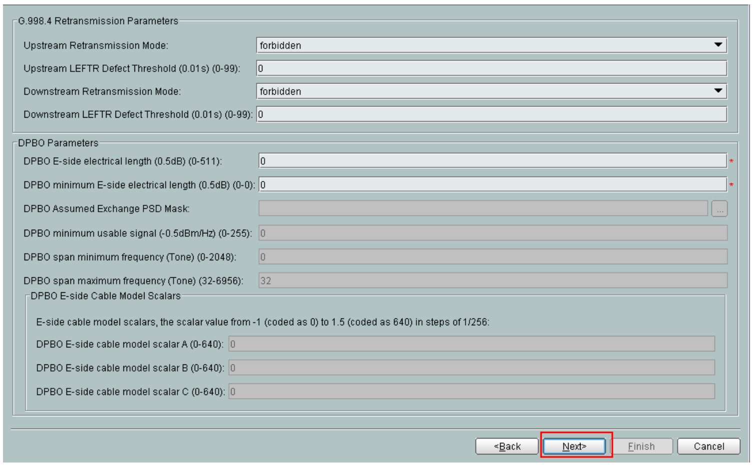
Downstream Min. Expected Throughput (kbit/s) (32-200000): 32
Upstream Min. Expected Throughput (kbit/s) (32-200000): 32
Downstream Max. Expected Throughput (kbit/s) (32-200000): 200000
Upstream Max. Expected Throughput (kbit/s) (32-200000): 200000
Downstream Max. Net Data Rate (kbit/s) (200000-200000): 200000
Upstream Max. Net Data Rate (kbit/s) (200000-200000): 200000
Downstream Min. Delay (ms) (0-63): 0
Upstream Min. Delay (ms) (0-63): 0
Downstream Max. Delay (ms) (1-63): 63
Upstream Max. Delay (ms) (1-63): 63
Downstream Min. INP Against SHINE (DMT Symbol) (0-63): 0
Upstream Min. INP Against SHINE (DMT Symbol) (0-63): 0
Downstream Min. INP Against SHINE (8.625 kHz) (DMT Symbol) (0-127): 0
Upstream Min. INP Against SHINE (8.625 kHz) (DMT Symbol) (0-127): 0
Downstream SHINE Ratio (0.001) (0-100): 0
Upstream SHINE Ratio (0.001) (0-100): 0
Downstream Min. INP Against REIN (DMT Symbol) (0-7): 0
Upstream Min. INP Against REIN (DMT Symbol) (0-7): 0
Downstream Min. INP Against REIN (8.625 kHz) (DMT Symbol) (0-13): 0
Upstream Min. INP Against REIN (8.625 kHz) (DMT Symbol) (0-13): 0
Downstream REIN Inter-arrival Time: 100Hz
Upstream REIN Inter-arrival Time: 100Hz

10. Click **OK**.
11. Select the VDSL2 channel configuration profile, right-click, and then choose **Download to NE**.
12. In the dialog box that is displayed, select the required OLT, and then click **OK**.
13. Click the **Line Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
14. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
15. In the dialog box that is displayed, set the parameters of the VDSL2 line configuration profile. The parameters not highlighted in the red box use default values.

Figure 6-16 Adding a VDSL2 line configuration profile


Basic Parameter

Name: vdsl_linecfgprofile *
Alias:
Adapt Mode in Downstream: Adapt. At Startup
Adapt Mode in Upstream: Adapt. At Startup
Bit swap upstream: enable
Bit swap downstream: enable
Force framer setting for inp upstream: false
Force framer setting for inp downstream: false
Target SNR Margin Downstream (0.1dB) (0-310): 60 *
Minimum SNR Margin Downstream (0.1dB) (0-60): 0 *
Maximum SNR Margin Downstream (0.1dB) (60-310): 300 *
Target SNR Margin Upstream (0.1dB) (0-310): 60 *
Minimum SNR Margin Upstream (0.1dB) (0-60): 0 *
Maximum SNR Margin Upstream (0.1dB) (60-310): 300 *
SNR Margin for Rate Downshift Downstream (0.1 dB) (0-60): 30
SNR Margin for Rate Upshift Downstream (0.1 dB) (60-300): 90
SNR Margin for Rate Downshift Upstream (0.1 dB) (0-60): 30
SNR Margin for Rate Upshift Upstream (0.1 dB) (60-300): 90
Minimum Downshift Time Downstream (s) (0-16383): 60
Minimum Upshift Time Downstream (s) (0-16383): 60
Minimum Downshift Time Upstream (s) (0-16383): 60
Minimum Upshift Time Upstream (s) (0-16383): 60



G.998.4 Retransmission Parameters

Upstream Retransmission Mode: forbidden
Upstream LEFTR Defect Threshold (0.01s) (0-99): 0
Downstream Retransmission Mode: forbidden
Downstream LEFTR Defect Threshold (0.01s) (0-99): 0

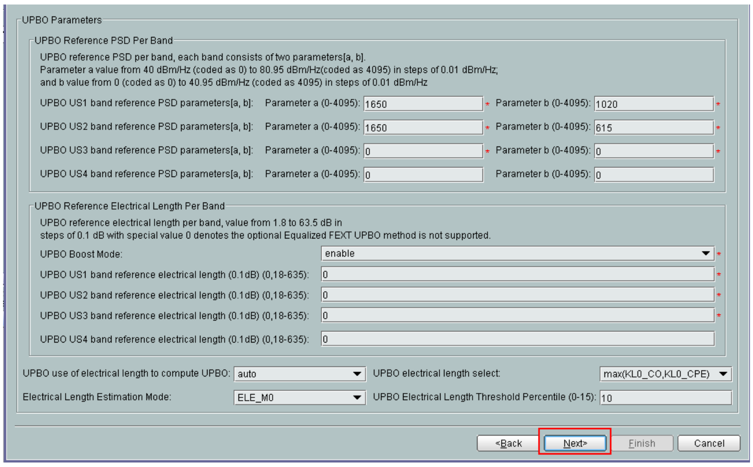
DPBO Parameters

DPBO E-side electrical length (0.5dB) (0-511): 0 *
DPBO minimum E-side electrical length (0.5dB) (0-0): 0 *
DPBO Assumed Exchange PSD Mask:
DPBO minimum usable signal (-0.5dBm/Hz) (0-255): 0
DPBO span minimum frequency (Tone) (0-2048): 0
DPBO span maximum frequency (Tone) (32-6956): 32

DPBO E-side Cable Model Scalars

E-side cable model scalars, the scalar value from -1 (coded as 0) to 1.5 (coded as 640) in steps of 1/256:

DPBO E-side cable model scalar A (0-640): 0
DPBO E-side cable model scalar B (0-640): 0
DPBO E-side cable model scalar C (0-640): 0



UPBO Parameters

UPBO Reference PSD Per Band

UPBO reference PSD per band, each band consists of two parameters[a, b].
Parameter a value from 40 dBm/Hz (coded as 0) to 80.95 dBm/Hz(coded as 4095) in steps of 0.01 dBm/Hz;
and b value from 0 (coded as 0) to 40.95 dBm/Hz (coded as 4095) in steps of 0.01 dBm/Hz

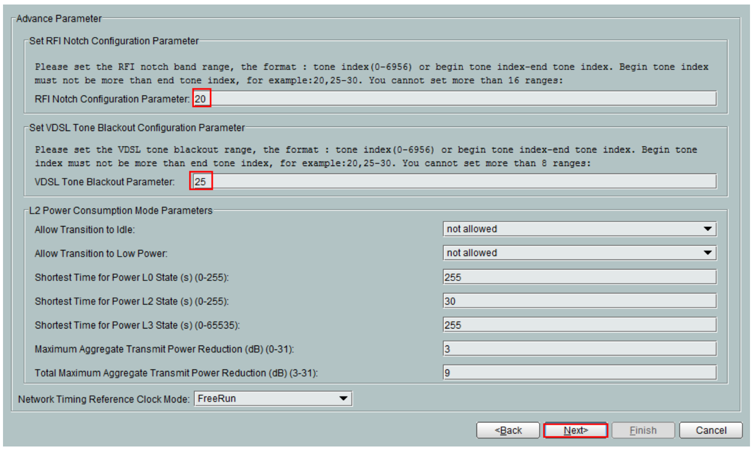
UPBO US1 band reference PSD parameters[a, b]: Parameter a (0-4095): 1650 * Parameter b (0-4095): 1020 *
UPBO US2 band reference PSD parameters[a, b]: Parameter a (0-4095): 1650 * Parameter b (0-4095): 615 *
UPBO US3 band reference PSD parameters[a, b]: Parameter a (0-4095): 0 * Parameter b (0-4095): 0 *
UPBO US4 band reference PSD parameters[a, b]: Parameter a (0-4095): 0 Parameter b (0-4095): 0

UPBO Reference Electrical Length Per Band

UPBO reference electrical length per band, value from 1.8 to 63.5 dB in
steps of 0.1 dB with special value 0 denotes the optional Equalized FEXT UPBO method is not supported.

UPBO Boost Mode: enable *
UPBO US1 band reference electrical length (0.1dB) (0,18-635): 0 *
UPBO US2 band reference electrical length (0.1dB) (0,18-635): 0 *
UPBO US3 band reference electrical length (0.1dB) (0,18-635): 0 *
UPBO US4 band reference electrical length (0.1dB) (0,18-635): 0

UPBO use of electrical length to compute UPBO: auto
UPBO electrical length select: max(KL0_CO,KL0_CPE)
Electrical Length Estimation Mode: ELE_M0
UPBO Electrical Length Threshold Percentile (0-15): 10



Advance Parameter

Set RFI Notch Configuration Parameter

Please set the RFI notch band range, the format : tone index(0-6956) or begin tone index-end tone index. Begin tone index must not be more than end tone index, for example:20,25-30. You cannot set more than 16 ranges:

RFI Notch Configuration Parameter: 20

Set VDSL Tone Blackout Configuration Parameter

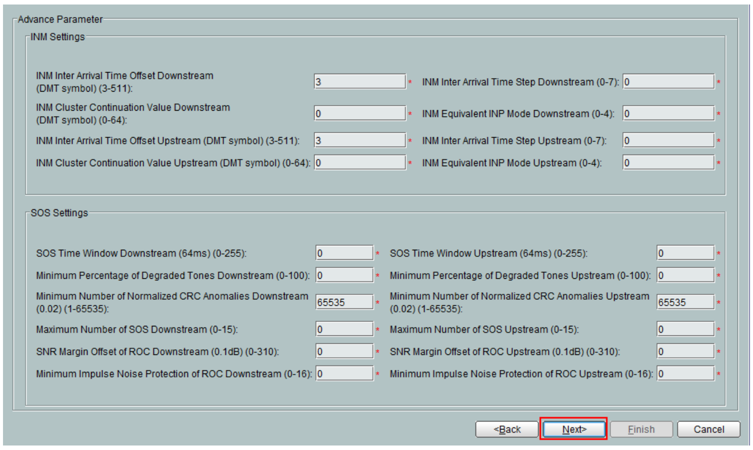
Please set the VDSL tone blackout range, the format : tone index(0-6956) or begin tone index-end tone index. Begin tone index must not be more than end tone index, for example:20,25-30. You cannot set more than 8 ranges:

VDSL Tone Blackout Parameter: 25

L2 Power Consumption Mode Parameters

Allow Transition to Idle: not allowed
Allow Transition to Low Power: not allowed
Shortest Time for Power L0 State (s) (0-255): 255
Shortest Time for Power L2 State (s) (0-255): 30
Shortest Time for Power L3 State (s) (0-65535): 255
Maximum Aggregate Transmit Power Reduction (dB) (0-31): 3
Total Maximum Aggregate Transmit Power Reduction (dB) (3-31): 9

Network Timing Reference Clock Mode: FreeRun



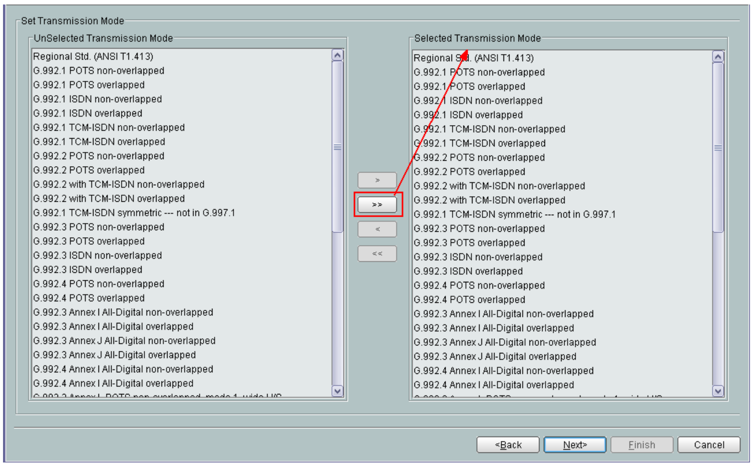
Advance Parameter

INM Settings

INM Inter Arrival Time Offset Downstream (DMT symbol) (3-511): 3 *
INM Inter Arrival Time Step Downstream (0-7): 0 *
INM Cluster Continuation Value Downstream (DMT symbol) (0-64): 0 *
INM Equivalent INP Mode Downstream (0-4): 0 *
INM Inter Arrival Time Offset Upstream (DMT symbol) (3-511): 3 *
INM Inter Arrival Time Step Upstream (0-7): 0 *
INM Cluster Continuation Value Upstream (DMT symbol) (0-64): 0 *
INM Equivalent INP Mode Upstream (0-4): 0 *

SOS Settings

SOS Time Window Downstream (64ms) (0-255): 0 *
SOS Time Window Upstream (64ms) (0-255): 0 *
Minimum Percentage of Degraded Tones Downstream (0-100): 0 *
Minimum Percentage of Degraded Tones Upstream (0-100): 0 *
Minimum Number of Normalized CRC Anomalies Downstream (0.02) (1-65535): 65535 *
Minimum Number of Normalized CRC Anomalies Upstream (0.02) (1-65535): 65535 *
Maximum Number of SOS Downstream (0-15): 0 *
Maximum Number of SOS Upstream (0-15): 0 *
SNR Margin Offset of ROC Downstream (0.1dB) (0-310): 0 *
SNR Margin Offset of ROC Upstream (0.1dB) (0-310): 0 *
Minimum Impulse Noise Protection of ROC Downstream (0-16): 0 *
Minimum Impulse Noise Protection of ROC Upstream (0-16): 0 *



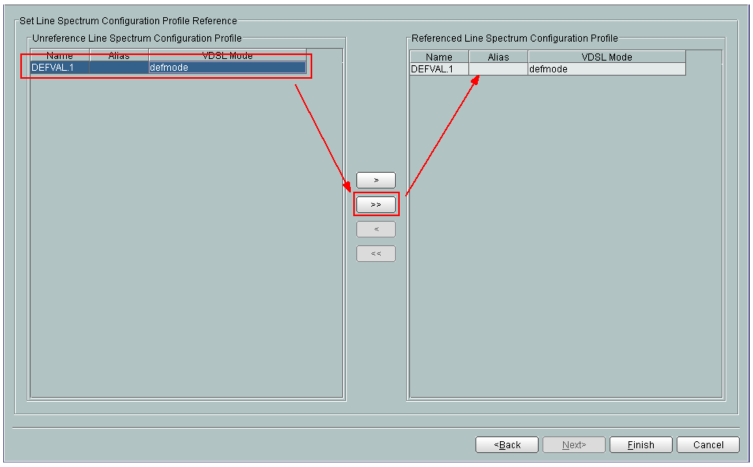
Set Transmission Mode

UnSelected Transmission Mode

Regional Std. (ANSI T1.413)
G.992.1 POTS non-overlapped
G.992.1 POTS overlapped
G.992.1 ISDN non-overlapped
G.992.1 ISDN overlapped
G.992.1 TCM-ISDN non-overlapped
G.992.1 TCM-ISDN overlapped
G.992.2 POTS non-overlapped
G.992.2 POTS overlapped
G.992.2 with TCM-ISDN non-overlapped
G.992.2 with TCM-ISDN overlapped
G.992.1 TCM-ISDN symmetric --- not in G.997.1
G.992.3 POTS non-overlapped
G.992.3 POTS overlapped
G.992.3 ISDN non-overlapped
G.992.3 ISDN overlapped
G.992.4 POTS non-overlapped
G.992.4 POTS overlapped
G.992.3 Annex I All-Digital non-overlapped
G.992.3 Annex I All-Digital overlapped
G.992.3 Annex J All-Digital non-overlapped
G.992.3 Annex J All-Digital overlapped
G.992.4 Annex I All-Digital non-overlapped
G.992.4 Annex I All-Digital overlapped

Selected Transmission Mode

Regional Std. (ANSI T1.413)
G.992.1 POTS non-overlapped
G.992.1 POTS overlapped
G.992.1 ISDN non-overlapped
G.992.1 ISDN overlapped
G.992.1 TCM-ISDN non-overlapped
G.992.1 TCM-ISDN overlapped
G.992.2 POTS non-overlapped
G.992.2 POTS overlapped
G.992.2 with TCM-ISDN non-overlapped
G.992.2 with TCM-ISDN overlapped
G.992.1 TCM-ISDN symmetric --- not in G.997.1
G.992.3 POTS non-overlapped
G.992.3 POTS overlapped
G.992.3 ISDN non-overlapped
G.992.3 ISDN overlapped
G.992.4 POTS non-overlapped
G.992.4 POTS overlapped
G.992.3 Annex I All-Digital non-overlapped
G.992.3 Annex I All-Digital overlapped
G.992.3 Annex J All-Digital non-overlapped
G.992.3 Annex J All-Digital overlapped
G.992.4 Annex I All-Digital non-overlapped
G.992.4 Annex I All-Digital overlapped



Set Line Spectrum Configuration Profile Reference

Unreference Line Spectrum Configuration Profile

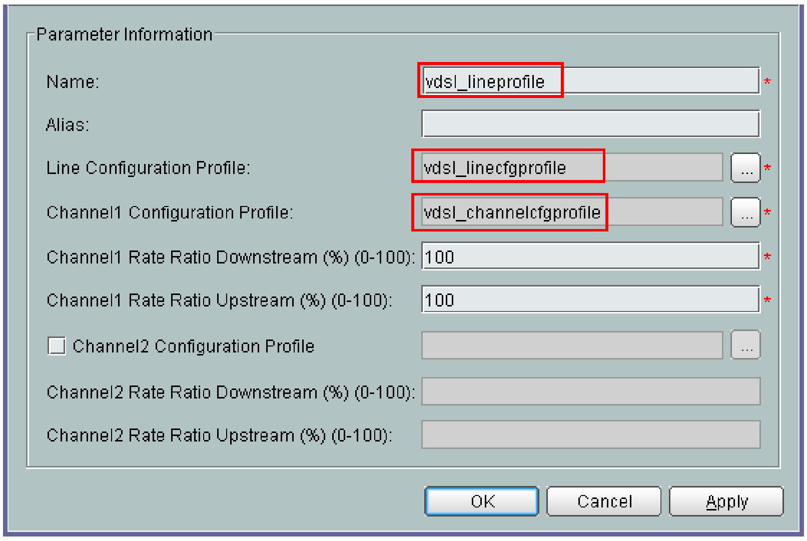
Name	Alias	VDSL Mode
DEFVAL.1		defmode

Referenced Line Spectrum Configuration Profile

Name	Alias	VDSL Mode
DEFVAL.1		defmode

16. Click **OK**.
17. Select the VDSL2 line configuration profile, right-click, and then choose **Download to NE**.
18. In the dialog box that is displayed, select the required OLT, and then click **OK**.
19. Click the **Line Template** tab.
20. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
21. In the dialog box that is displayed, set the parameters of the VDSL2 line profile.

Figure 6-17 Adding a VDSL2 line profile


Parameter Information
Name: vdsl_lineprofile *
Alias:
Line Configuration Profile: vdsl_linecfgprofile ... *
Channel1 Configuration Profile: vdsl_channelcfgprofile ... *
Channel1 Rate Ratio Downstream (%) (0-100): 100 *
Channel1 Rate Ratio Upstream (%) (0-100): 100 *
☐ Channel2 Configuration Profile ...
Channel2 Rate Ratio Downstream (%) (0-100):
Channel2 Rate Ratio Upstream (%) (0-100):
OK
Cancel
Apply

- **Name**: **vdsl_lineprofile**
- **Line Configuration Profile**: **vdsl_linecfgprofile**
- **Channel1 Configuration Profile**: **vdsl_channelcfgprofile**
- Accept default values for other parameters

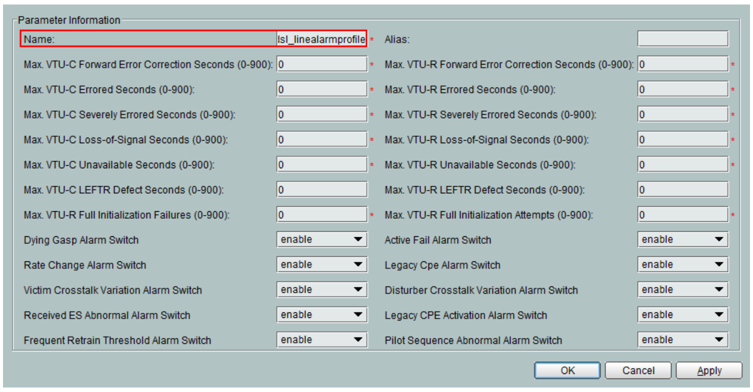
22. Click **OK**.
23. Select the line profile, right-click, and then choose **Download to NE**.
24. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 3 Configure a VDSL2 alarm profile.

A VDSL2 alarm profile binds a specified line alarm configuration profile and a channel alarm configuration profile. After the binding is successful, an activated VDSL2 port directly references an alarm profile to monitor the performance of the VDSL2 port. When the parameter value of the port exceeds the preset threshold, an alarm is generated.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
3. Click the **VDSL2 Alarm Profile**.
4. Click the **Line Alarm Configuration Profile** tab.
5. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
6. In the dialog box that is displayed, set the parameters of the VDSL2 line alarm configuration profile.

Figure 6-18 Adding a VDSL2 line alarm configuration profile



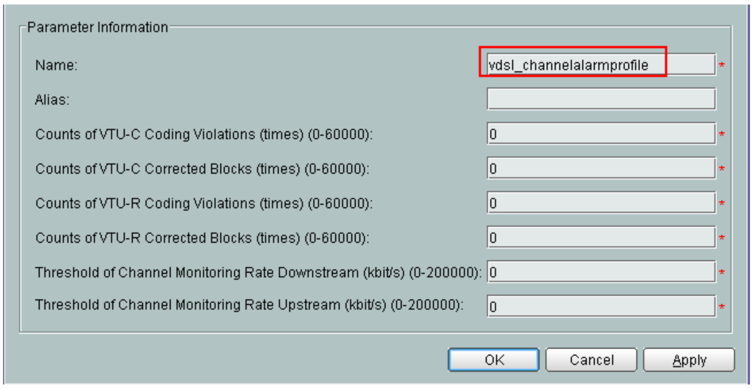
Parameter Information

Name: lsl_linealarmprofile *
Max. VTU-C Forward Error Correction Seconds (0-900): 0 *
Max. VTU-C Errored Seconds (0-900): 0 *
Max. VTU-C Severely Errored Seconds (0-900): 0 *
Max. VTU-C Loss-of-Signal Seconds (0-900): 0 *
Max. VTU-C Unavailable Seconds (0-900): 0 *
Max. VTU-C LEFTR Defect Seconds (0-900): 0
Max. VTU-R Full Initialization Failures (0-900): 0 *
Dying Gasp Alarm Switch: enable
Rate Change Alarm Switch: enable
Victim Crosstalk Variation Alarm Switch: enable
Received ES Abnormal Alarm Switch: enable
Frequent Retrain Threshold Alarm Switch: enable

Alias:
Max. VTU-R Forward Error Correction Seconds (0-900): 0 *
Max. VTU-R Errored Seconds (0-900): 0 *
Max. VTU-R Severely Errored Seconds (0-900): 0 *
Max. VTU-R Loss-of-Signal Seconds (0-900): 0 *
Max. VTU-R Unavailable Seconds (0-900): 0 *
Max. VTU-R LEFTR Defect Seconds (0-900): 0
Max. VTU-R Full Initialization Attempts (0-900): 0 *
Active Fail Alarm Switch: enable
Legacy Cpe Alarm Switch: enable
Disturber Crosstalk Variation Alarm Switch: enable
Legacy CPE Activation Alarm Switch: enable
Pilot Sequence Abnormal Alarm Switch: enable

7. Click **OK**.
8. Select the VDSL2 line alarm configuration profile, right-click, and then choose **Download to NE**.
9. In the dialog box that is displayed, select the required OLT, and then click **OK**.
10. Click the **Channel Alarm Configuration Profile** tab.
11. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
12. In the dialog box that is displayed, set the parameters of the VDSL2 channel alarm configuration profile.

Figure 6-19 Adding a VDSL2 channel alarm configuration profile

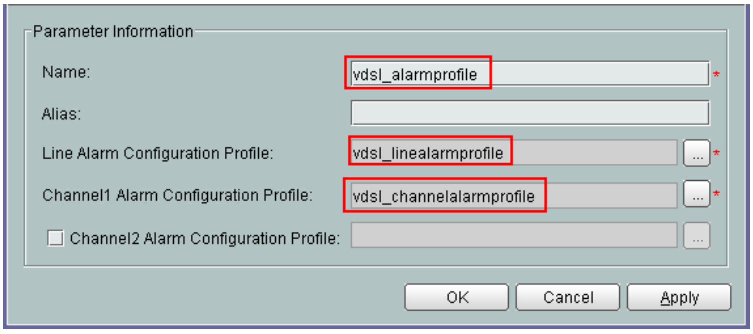


Parameter Information

Name: vdsl_channelalarmprofile *
Alias:
Counts of VTU-C Coding Violations (times) (0-60000): 0 *
Counts of VTU-C Corrected Blocks (times) (0-60000): 0 *
Counts of VTU-R Coding Violations (times) (0-60000): 0 *
Counts of VTU-R Corrected Blocks (times) (0-60000): 0 *
Threshold of Channel Monitoring Rate Downstream (kbit/s) (0-200000): 0 *
Threshold of Channel Monitoring Rate Upstream (kbit/s) (0-200000): 0 *

13. Click **OK**.
14. Select the VDSL2 channel alarm configuration profile, right-click, and then choose **Download to NE**.
15. In the dialog box that is displayed, select the required OLT, and then click **OK**.
16. Click the **Alarm Template** tab.
17. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
18. In the dialog box that is displayed, set the parameters of the VDSL2 alarm profile.

Figure 6-20 Adding a VDSL2 alarm profile



Name: vdsl_alarmprofile *
Alias:
Line Alarm Configuration Profile: vdsl_linealarmprofile ... *
Channel1 Alarm Configuration Profile: vdsl_channelalarmprofile ... *
☐ Channel2 Alarm Configuration Profile: ...

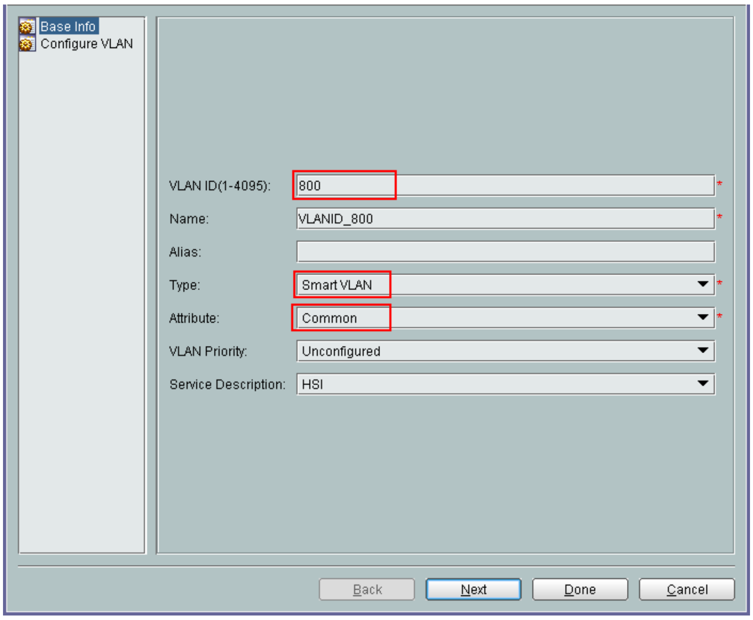
19. Click **OK**.
20. Select the VDSL2 alarm profile, right-click, and then choose **Download to NE**.
21. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 4 Add a VLAN and configure an upstream port to the VLAN.

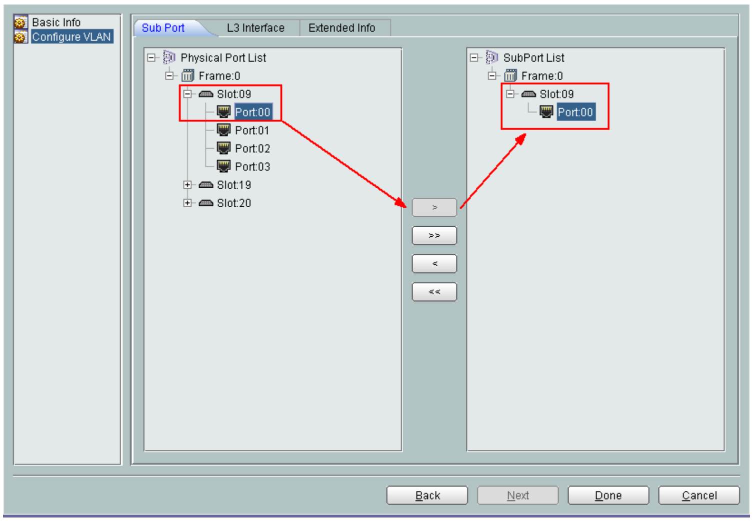
Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree. On the **VLAN** tab page, set the filter criteria or click ⩔ to display the VLANs.
3. Right-click the list, and then choose **Add**.
4. In the dialog box that is displayed, set the values of the parameters.

Figure 6-21 Adding a VLAN and configuring an upstream port to the VLAN



VLAN ID(1-4095): 800 *
Name: VLANID_800 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI



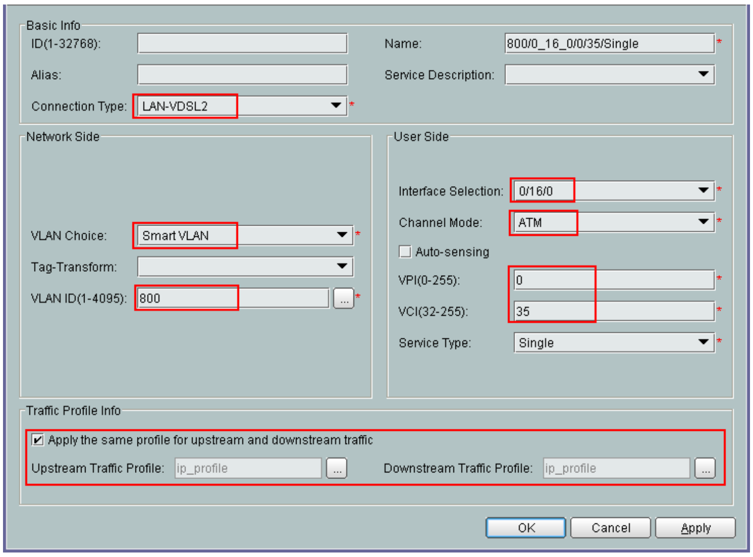
5. Click **OK**.

Step 5 Configure the service virtual port.

After being configured successfully, the VDSL2 service port can carry service streams of various types.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ⌄ to display the VDSL2 ports.
4. In the information list, select a VDSL2 port record. On the **Service Port Info** tab page in the lower pane, right-click, and then choose **Add**.
5. Set the parameters of the VDSL2 port in the dialog box that is displayed. Set the values of the parameters.

Figure 6-22 Adding a service virtual port



Basic Info
ID(1-32768):
Name: 800/0_16_0/0/35/Single
Alias:
Service Description:
Connection Type: LAN-VDSL2

Network Side
VLAN Choice: Smart VLAN
Tag-Transform:
VLAN ID(1-4095): 800

User Side
Interface Selection: 0/16/0
Channel Mode: ATM
☐ Auto-sensing
VPI(0-255): 0
VCI(32-255): 35
Service Type: Single

Traffic Profile Info
☑ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile: ip_profile
Downstream Traffic Profile: ip_profile

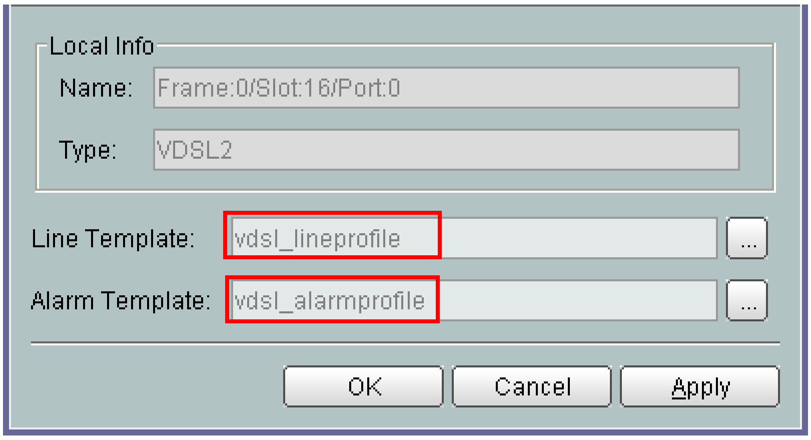
6. Click **OK**.

Step 6 Configure the attributes of the VDSL2 port.

Configures a line profile, an alarm profile, extended profile (optional) of a VDSL2 port. These attributes can be used after the VDSL2 port is activated.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ︾ to display the VDSL2 ports.
4. In information list, right-click port **0/16/0** and choose **Configure Attributes** from the shortcut menu.
5. In the dialog box that is displayed, set the values of the parameters.

Figure 6-23 Configuring VDSL2 port attributes



Name: Frame:0/Slot:16/Port:0

Type: VDSL2

Line Template: vdsl_lineprofile

Alarm Template: vdsl_alarmprofile

6. Click **OK**.

Step 7 Activate the VDSL2 port.

The VDSL2 port can transmit the service in the normal state only when it is activated successfully.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ︾ to display the VDSL2 ports.
4. In the list, choose ports **0/16/0** to be activated. Right-click, and then choose **Activate**.

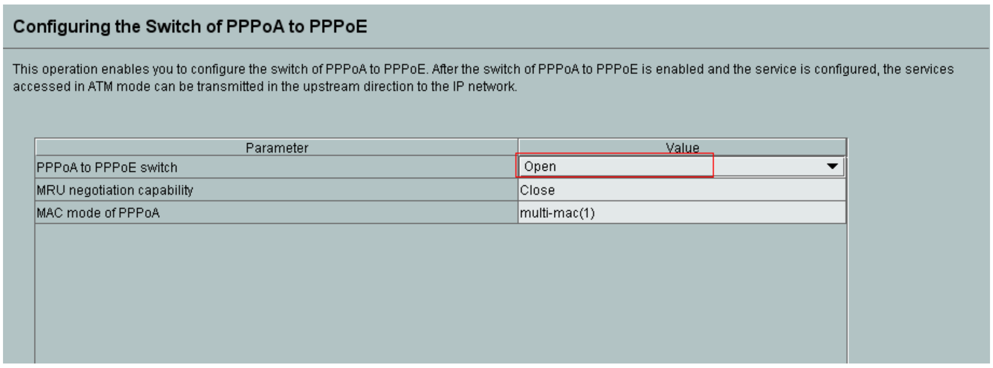
Step 8 Set PPPoA parameters.

Enable the PPPoA gateway to enable the PPPoA access service.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

2. On the tab that is displayed, choose **NE Properties** > **Encapsulation Management** > **PPPoA** from the navigation tree.
3. In the right pane of the interface, set the parameters.

Figure 6-24 Setting PPPoA parameters



Configuring the Switch of PPPoA to PPPoE

This operation enables you to configure the switch of PPPoA to PPPoE. After the switch of PPPoA to PPPoE is enabled and the service is configured, the services accessed in ATM mode can be transmitted in the upstream direction to the IP network.

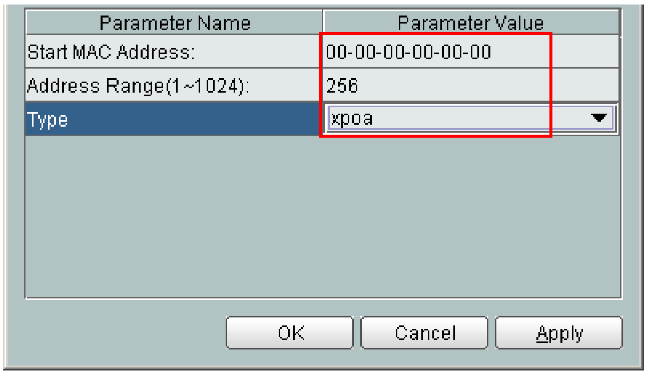
Parameter	Value
PPPoA to PPPoE switch	Open
MRU negotiation capability	Close
MAC mode of PPPoA	multi-mac(1)

Step 9 Configure the MAC address pool.

In case of PPPoA access, the OLT needs to convert the PPPoA packets to the IPoE packets. In this case, the MAC address pool allocates a MAC address to the user and adds a MAC address (source MAC address) to the ATM cell, thus converting the ATM cell to the Ethernet packet.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **NE Properties** > **MAC Address Pool** from the navigation tree on the tab page that is displayed.
3. In the information list, right-click and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters.

Figure 6-25 Configuring the MAC address pool



Parameter Name	Parameter Value
Start MAC Address:	00-00-00-00-00-00
Address Range(1~1024):	256
Type	xpoa

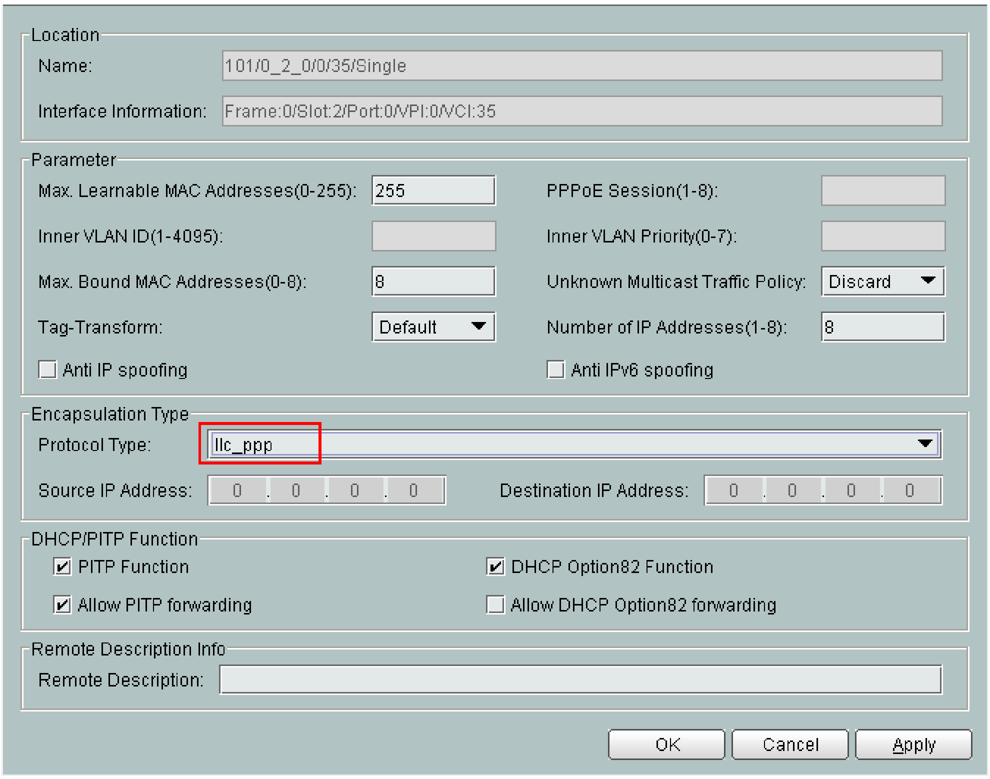
5. Click **OK**.

Step 10 Configure the PPPoA encapsulation type of the VDSL2 port.

Configures the Internet Protocol over ATM (PPPoA) encapsulation type for the PPPoA access service on a specified service virtual port. After you configure the encapsulation type, packets of the specified permanent virtual channel (PVC) are transmitted downstream or upstream in the configured encapsulation type.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **Connection** > **Service Port** from the navigation tree.
3. On the **Service Port** tab page, set the filter criteria to display the required service virtual ports.
4. Select a record that you need from the service port list, right-click, and then choose **Configure Extended Properties**.
5. In the dialog box that is displayed, set the parameters.

Figure 6-26 Configuring the encapsulation type for the PPPoA service of a VDSL2 port



Location
Name: 101/0_2_0/0/35/Single
Interface Information: Frame:0/Slot:2/Port:0/VPI:0/VCI:35

Parameter
Max. Learnable MAC Addresses(0-255): 255
PPPoE Session(1-8):
Inner VLAN ID(1-4095):
Inner VLAN Priority(0-7):
Max. Bound MAC Addresses(0-8): 8
Unknown Multicast Traffic Policy: Discard
Tag-Transform: Default
Number of IP Addresses(1-8): 8
☐ Anti IP spoofing
☐ Anti IPv6 spoofing

Encapsulation Type
Protocol Type: llc_ppp
Source IP Address: 0 . 0 . 0 . 0
Destination IP Address: 0 . 0 . 0 . 0

DHCP/PITP Function
☑ PITP Function
☑ DHCP Option82 Function
☑ Allow PITP forwarding
☐ Allow DHCP Option82 forwarding

Remote Description Info
Remote Description:

6. Click **OK**.

Step 11 Save data.

Backup the data from the OLT to the U2000.

1. In the **Main Topology**, select **OLT** in the **Physical Root** navigation tree, right-click, and then choose **Save Data Immediately**.
2. Click **OK**.

----End

Result

After the configuration is complete, the user computer can pass the authentication and log in to the Internet.

6.7 Configuration Example of the VDSL2 PPPoE Service

Based on the example network, this topic describes how to configure the VDSL2 PPPoE service and how to access the Internet in the PPPoE mode through the VDSL2 line after the configuration.

Prerequisites

- Network devices and lines must be in the normal state.
- The VDSL2 service card must be in the normal state.

Example Network

The PC is connected to the VDSL2 service port of the OLT through the VDSL2 modem. After being sent to the modem, the user packets are sent to the OLT in the PPPoE mode, and then sent upstream to the upper layer network through the upstream port of the control card.

Data Plan

Table 6-6 Data plan for the VDSL2 PPPoE service

Item	Data	Remarks
Service card	VDSL2 port: 0/11/0-0/11/23 VPI: 0 VCI: 35 Service type: Single	-
	VLAN ID: 20-43 VLAN selection: MUX VLAN VLAN attribute: Common	This VLAN must be the same as the VLAN configured on the upper layer device.
Upstream port	0/19/0	The upstream port is also the subport of VLANs 20-43.
MEF IP Traffic Profile IP Traffic Profile	● Name: ip_profile ● CIR: 2048 kbit/s ● Use the default values for other parameters.	The Tx service port and the Rx service port use the parameters in the traffic profile for rate limitation.

Item	Data	Remarks
Line Spectrum Configuration Profile	Name: vdsl_linespectrumcfgprofile Accept the default values for the parameters.	-
Line Configuration Profile	Name: vdsl_linecfgprofile Accept the default values for the parameters.	-
Channel1 Configuration Profile	Name: vdsl_channelcfgprofile Accept the default values for the parameters.	-
VDSL2 Line Profile	Name: vdsl_lineprofile Accept the default values for the parameters.	The OLT can restrict the access rate of a user through either a traffic profile or a preset VDSL2 line profile by different means. When both profiles are applied, the smaller value works as the user bandwidth. The following example uses the traffic profile as an example to restrict the access rate of the user.
Line Alarm Configuration Profile	Name: vdsl_linealarmprofile Accept the default values for the parameters.	-
Channel1 Alarm Configuration Profile	Name: vdsl_channelalarmprofile Accept the default values for the parameters.	-
VDSL2 Alarm Profile	Name: vdsl_alarmprofile Accept the default values for the parameters.	-
Modem	Working mode: PPPoE Obtain the IP address automatically.	-

Procedure

Step 1 Add a VLAN and configure the upstream port of the VLAN.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

2. Choose **VLAN** from the navigation tree. On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.
3. Right-click the list, and then choose **Batch Add**.
4. In the dialog box that is displayed, click the **Base Info** tab to configure the VLAN parameters. Set the values of the parameters as follows:
   - Set **Start ID** and **End ID** to **20** and **43** respectively.
   - Set **Type** to **MUX VLAN**.
   - Set **Attribute** to **Common**.
5. Click **Next**.
6. Click the **Sub Port** tab to configure the upstream port of the VLAN. Set **Subport** to 0/19/0.
7. Click **OK**.

Step 2 Configure the MEF IP traffic profile.

1. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
2. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
3. In the dialog box that is displayed, set the MEF IP traffic profile parameters **Name** to **ip_profile** and **CIR** to **2048kbit/s**.
4. Click **OK**.
5. Select the MEF IP traffic profile, right-click, and then choose **Download to NE**.
6. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 3 Configure the VDSL2 line profile.

1. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
2. Click the **Line Spectrum Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
3. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters of the VDSL2 line spectrum configuration profile as follows:
   - **Name**: **vdsl_linespectrumcfgprofile**
   - Accept the default values for the other parameters.
5. Click **OK**.
6. Click the **Channel Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
7. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
8. In the dialog box that is displayed, set the parameters of the VDSL2 channel configuration profile as follows:
   - **Name**: **vdsl_channelcfgprofile**
   - Accept the default values for the other parameters.
9. Click **OK**.

10. Select the VDSL2 channel configuration profile, right-click, and then choose **Download to NE**.
11. In the dialog box that is displayed, select the required OLT, and then click **OK**.
12. Click the **Line Configuration Profile** tab, and select the required device type from the **Device Type** drop-down list.
13. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
14. In the dialog box that is displayed, set the parameters of the VDSL2 line configuration profile as follows:
    - **Name**: **vdsl_linecfgprofile**
    - Accept the default values for the other parameters.
    - Select the VDSL2 line spectrum configuration template whose **Name** is **vdsl_linespectrumprofile**.
15. Click **OK**.
16. Select the VDSL2 line configuration profile, right-click, and then choose **Download to NE**.
17. In the dialog box that is displayed, select the required OLT, and then click **OK**.
18. Click the **Line Template** tab.
19. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
20. In the dialog box that is displayed, set the parameters of the VDSL2 line profile as follows:
    - **Name**: **vdsl_lineprofile**
    - **Line Configuration Profile**: **vdsl_linecfgprofile**
    - **Channel1 Configuration Profile**: **vdsl_channelcfgprofile**
    - Accept the default values for the other parameters.
21. Click **OK**.
22. Select the line profile, right-click, and then choose **Download to NE**.
23. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 4 Configure the VDSL2 alarm profile.

1. In the dialog box that is displayed, choose **DSL Profile** > **VDSL2 Profile** from the navigation tree.
2. Click the **VDSL2 Alarm Profile**.
3. Click the **Line Alarm Configuration Profile** tab.
4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters of the VDSL2 line alarm configuration profile as follows:
    - **Name**: **vdsl_linealarmprofile**
    - Accept the default values for the other parameters.
6. Click **OK**.
7. Select the VDSL2 line alarm configuration profile, right-click, and then choose **Download to NE**.
8. In the dialog box that is displayed, select the required OLT, and then click **OK**.
9. Click the **Channel Alarm Configuration Profile** tab.

10. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
11. In the dialog box that is displayed, set the parameters of the VDSL2 channel alarm configuration profile as follows:
    - **Name**: **vdsl_channelalarmprofile**
    - Accept the default values for the other parameters.
12. Click **OK**.
13. Select the VDSL2 channel alarm configuration profile, right-click, and then choose **Download to NE**.
14. In the dialog box that is displayed, select the required OLT, and then click **OK**.
15. Click the **Alarm Template** tab.
16. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
17. In the dialog box that is displayed, set the parameters of the VDSL2 alarm profile as follows:
    - **Name**: **vdsl_alarmprofile**
    - **Line Alarm Configuration Profile**: **vdsl_linealarmprofile**
    - **Channel1 Alarm Configuration Profile**: **vdsl_channelalarmprofile**
    - Accept the default values for the other parameters.
18. Click **OK**.
19. Select the VDSL2 alarm profile, right-click, and then choose **Download to NE**.
20. In the dialog box that is displayed, select the required OLT, and then click **OK**.

Step 5 Configure the service port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ⌄ to display the VDSL2 ports.
4. In the information list, select a VDSL2 port record. On the **Service Port Info** tab page in the lower pane, right-click, and then choose **Add**.
5. Set the parameters of the VDSL2 port in the dialog box that is displayed. Set the values of the parameters as follows:
    - In **Attributes**, set **Connection Type** to **LAN-VDSL2**.
    - In the **Traffic Profile Info** area, select **Keep the upstream and downstream settings the same**, and then set the **Upstream Traffic Name** and **Downstream Traffic Name** both to **ip_profile**.
    - In **User Side**, set **Interface Selection** to **0/11/0-0/11/23**.
    - In **Network Side**, set the VLAN parameters. The parameters must be the same as the parameters that are set in step 1.
        - Set **VLAN Choice** to **MUX VLAN**.
        - Set **Start ID** and **End ID** to **20** and **43** respectively.
    - In **User Side**, set the parameters of the VPI/VCI. Set the values of the parameters as follows:
        - Set **VPI** to **0**.
        - Set **VCI** to **35**.

- In **Attributes**, set **Service Type** to **Single**.

6. Click **OK**.

Step 6 Configure the attributes of the VDSL2 port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ⌄ to display the VDSL2 ports.
4. In information list, right-click port **0/11/0-0/11/23** and choose **Configure Attributes** from the shortcut menu.
5. In the dialog box that is displayed, bind the VDSL2 port to the corresponding profile, and set **Line Template** to **vdsl2_lineprofile** and **Alarm Template** to **vdsl_alarmprofile**.
6. Click **OK**.

Step 7 Activate the VDSL2 port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **VDSL2 Port** from the navigation tree.
3. On the **VDSL2** tab page, set the filter criteria or click ⌄ to display the VDSL2 ports.
4. In the list, choose ports **0/11/0-0/11/23** to be activated. Right-click, and then choose **Activate**.

Step 8 Save the data.

1. In the **Main Topology**, select **OLT** in the **Physical Root** navigation tree, right-click, and then choose **Save Data Immediately**.
2. Click **OK**.

----End

Result

After the configuration is complete, the PC of the user can pass the authentication and can access the Internet in the PPPoE mode.

6.8 Querying Line Running Status of Lines on xDSL Ports

This topic describes how to learn about the running status of lines on activated xDSL ports by querying subcarrier information, including bit allocation, gain allocation, SNR, HLOG, and QLN.

Prerequisites

Ports have been activated.

Context

NOTE

This operation applies to ADSL and VDSL2 ports. This topic uses VDSL2 ports as an example.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **VDSL2 Port** from the navigation tree.

Step 3 On the **VDSL2** tab page, set the filter criteria or click ︾ to display the VDSL2 ports.

Step 4 Select a desired port and click tabs in the lower pane to view relevant information.

- **Bit Allocation Info** tab: displays the line bearer rates allocated to subcarriers.
- **Gain Allocation Info** tab: displays the gains allocated to subcarriers.
- **SNR Info** tab: displays the SNR margins of subcarriers.
- **HLOG Info** tab: displays HLOG information about channels.
- **QLN Info** tab: displays QLN information about subcarriers.

NOTE

For VDSL2 ports, you can query the background noise of lines after the vectoring function is enabled.

Step 5 Double-click in the diagram of the tab. In the dialog box that is displayed, enter the desired subcarrier and click **Locate**. Information about the specific subcarrier is displayed. You can print or save the query results by clicking **Print** or **Save**.

----End

6.9 Managing an SHDSL Regenerator

The single-pair high-speed digital subscriber line (SHDSL) can transmit signals for a maximum of 6 kilometers. In some sparsely populated areas, regenerators are needed between the central office (CO) and the customer premises equipment (CPE); such regenerators implement extremely long distance transmission by extending the transmission distance.

Prerequisites

- A regenerator connects to an SHDSL port.
- SHDSL ports support Elcon regenerators only.
- SHDSL trunk management functions apply only to the H802SHLB board and the H80ASHLM board.
- Only the Ethernet in the first mile (EFM) SHDSL trunk can be managed.
- A maximum of 8 regenerators can be connected to an SHDSL port.

Context

The OLT supports trunk management. Line profiles of the SHDSL and parameters of alarm profiles are applied to trunks and ports. Therefore, separately configuring the trunk is not required. This chapter describes how to maintain a regenerator.

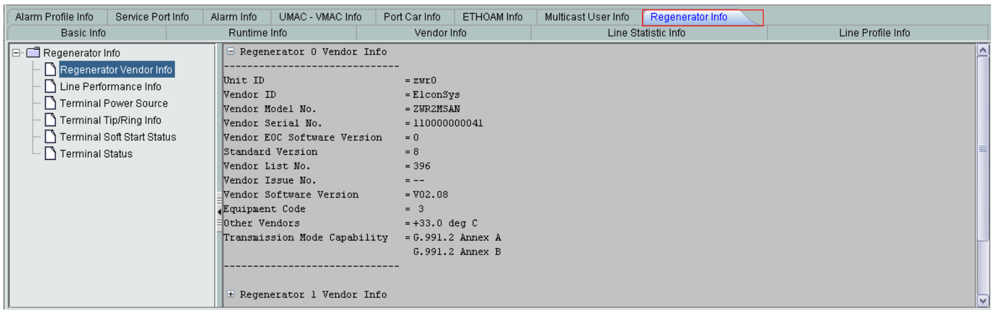
Procedure

Step 1 Choose **DSL** > **(ATM) G.SHDSL Port** from the navigation tree.

Step 2 On the **(ATM) G.SHDSL Port** tab page, set the filter criteria or click to display the G.SHDSL ports.

Step 3 To query information about a regenerator , select a port connected to a regenerator and click the following tabs under the port list:

- **Query the number of regenerator**: Click the **Runtime info** tab to query the number of regenerator in the **Line info**.
- **Query regenerator info**: Click the **Regenerator Info** tab. On the tab, choose **Regenerator Vendor Info**, **Line Performance Info**, **Terminal Power Source**, **Terminal Tip/Ring Info**, **Terminal Soft Start Status**, or **Terminal Status** from the navigation tree to query related information.



```
⊟ Regenerator 0 Vendor Info
-----------------------------
Unit ID                      = zwr0
Vendor ID                    = ElconSys
Vendor Model No.             = ZWR2MSAN
Vendor Serial No.            = 110000000041
Vendor EOC Software Version  = 0
Standard Version             = 8
Vendor List No.              = 396
Vendor Issue No.             = --
Vendor Software Version      = V02.08
Equipment Code               =  3
Other Vendors                = +33.0 deg C
Transmission Mode Capability = G.991.2 Annex A
                               G.991.2 Annex B
-----------------------------

⊞ Regenerator 1 Vendor Info
```

Step 4 Right-click a port connected to a regenerator and choose **Performance** > **Query Historical Data** from the main menu. In the **Query Historical Data** window, you can query the 15-minute and 24-hour historical performance data for upstream and downstream lines.

----End

7 Configuring the GPON Access

About This Chapter

Gigabit-capable Passive Optical Network (GPON) is defined by ITU-T Recommendations G. 984.x family. It supports the upstream rate of 1.25 Gbit/s and downstream rate of 2.5 Gbit/s. The OLT supports GPON access and GPON upstream transmission.

Context

The characteristics of GPON access are as follows:

- The GPON access supports high-bandwidth transmission. It effectively removes the bandwidth bottleneck in the access through twisted pairs and meets the subscribers' requirements for high-bandwidth services, such as the high definition TV (HDTV) and live programs.
- The GPON access meets the requirements for long-distance access. It avoids the disadvantages of twisted pairs in respect of coverage area, and reduces the network nodes.
- The GPON access supports a maximum of 20 km in physical distance, and a maximum of 60 km in logical distance.

The Gigabit-capable passive optical network (GPON) technology provides flexible access for broadband and narrowband services, and supports ultra high bandwidth, multi-rate mode, and single optical fiber for providing users with voice, data, video, leased line, and distributed services over the IP network.

The characteristics of GPON upstream transmission are as follows:

- The upstream port is a GPON NNI port. One GPON NNI upstream port is supported, with the upstream rate of 2.488 Gbit/s and the downstream rate of 1.244 Gbit/s.
- When working with the upper layer OLT, the OLT provides more users with high-bandwidth access.
- The OLT can configure and manage the services of the ONT through the OMCI protocol.

The GPON access service has various scenarios, which are mainly fiber to the home (FTTH), fiber to the building (FTTB), and fiber to the curb (FTTC). For different scenarios, the basic configuration procedures are the same except for some configuration data. **Table 7-1** describes the differences of the configurations in different scenarios.

Table 7-1 Configuration description of the GPON access service in different scenarios

Application Scenario	General Networking	Description
FTTH	The ONU is installed at the user's home to provide the user with multiple services through the Ethernet port and the telephone port.	● When configuring the triple play service, you need to configure different T-CONTs and GEM ports for the three types of services to separate the traffic. In addition, you need to configure different VLANs on the user side to distinguish the services. ● When configuring the home Internet access service, if multiple PCs connected to the same ONU need to interconnect with each other, you need to configure the services of all the ports provided by the ONU with the same T-CONT and GEM port. In addition, the VLAN configuration of the ports must be the same. ● If the ONU is connected to service terminals such as PC and STB that do not support the packets with a VLAN tag, you need to configure the native VLAN for the ONU port. Then, a VLAN tag is added to the packet when the packet reaches the ONU port and removed from the packet when the packet is transmitted from the ONU port.

Application Scenario	General Networking	Description
FTTB	The ONU is installed in a building corridor and is connected to a layer-2 switch which provides multiple Ethernet ports for providing users with access services.	● When configuring the home Internet access service, if multiple users connected to the ONU need not interconnect with each other and each user needs to be authenticated individually, you need to configure the users on each ONU port with different T-CONTs, GEM ports, and VLANs. ● When this scenario is applied in the small office and home office (SOHO) network, the ONU is connected to a layer-2 switch. In this case, you need to configure the services on each ONU port with different T-CONTs and GEM ports. ● When the ONU is connected to a layer-2 switch, the packets that reach the ONU carry VLAN tags. In this case, you need not configure the native VLAN for the ONU port, but you need to make sure that the user-side VLANs are consistent with the VLAN tags of the packets.
FTTC	The ONU is installed in the cabinet at the curb and is connected to a Mini DSLAM or a Mini DSLAM with the GPON upstream function to provide users with access services.	You only need to configure the service port for the OLT according to the upstream VLAN of the Mini DSLAM. Since each service port may carry heavy traffic, it is recommended that you configure different T-CONTs and GEM ports for different service ports.

For the current version, the GPON profiles are classified into two types of profiles, that is, the GPON profiles in the distributed mode and the GPON profiles in the profile mode. The GPON profiles that are in the distributed mode are used to support the device versions earlier than V800R006C02, and the GPON profiles that are in the profile mode are used to optimize the configuration of the optical network unit (ONU) for configuring the ONUs in batches.

This topic describes how to configure the GPON access service. The GPON access supports high-bandwidth transmission, which effectively removes the bandwidth bottleneck in the access through twisted pairs and meets the users' requirements on high-bandwidth services, such as high definition TV (HDTV) and live programs.

This topic describes how to configure the GPON access service. The GPON access supports high-bandwidth transmission, which effectively removes the bandwidth bottleneck in the access through twisted pairs and meets the users' requirements on high-bandwidth services, such as high definition TV (HDTV) and live programs.

7.4 Provisioning a GPON FTTH Service (OLT in Profile Mode)
This topic uses gigabit-capable passive optical network (GPON) as an example to describe how to quickly provision an xPON fiber to the home (FTTH) service in profile mode. In this scenario, users can configure service channels for an OLT PON port in a window, including channels for Internet access, voice over IP (VoIP), and multicast services.

7.5 Provisioning a GPON FTTB Service (OLT in Profile Mode)
This topic uses gigabit-capable passive optical network (GPON) as an example to describe how to quickly provision an xPON FTTB service in profile mode. In an xPON FTTB network, the OLT, functioning as an OLT, connects MDUs or ONUs over the ODN network. The ONUs or MDUs then provide services for users. Depending on the access modes of MDUs, users can access an MDU in LAN mode or xDSL mode to access composite services, including voice, Internet access, and multicast services.

7.6 Configuring the GPON Upstream Service
This topic describes how to configure the GPON upstream service. As a multi-dwelling unit (MDU), the MA5600T, MA5603T or MA5606T features wide coverage, flexible networking, and low maintenance cost of the GPON network. The MA5600T, MA5603T or MA5606T works with the OLT to form a GPON network, which provides high-bandwidth broadband access for users. In addition, the MA5600T, MA5603T or MA5606T supports a higher user density at the OLT end.

7.7 Configuring the ONT Auto-online Function
This topic describes how to configure the ONT auto-online function. If the ONT auto-find function is enabled on the OLT, the OLT obtains the registration information of the ONT when an ONT goes online. By default, the ONT auto-find function of a GPON port is disabled.

7.1 Configuring the GPON Profile

For the current version, the GPON profiles are classified into two types of profiles, that is, the GPON profiles in the distributed mode and the GPON profiles in the profile mode. The GPON profiles that are in the distributed mode are used to support the device versions earlier than V800R006C02, and the GPON profiles that are in the profile mode are used to optimize the configuration of the optical network unit (ONU) for configuring the ONUs in batches.

Context

In the distributed mode, the GPON profiles of the OLT include the dynamic bandwidth allocation (DBA) profiles, GPON alarm profiles, MDU SNMP Profile and GPON ONT capability profiles.

In the profile mode, the GPON profiles of the OLT include the dynamic bandwidth allocation (DBA) profiles, GPON line profiles, GPON service profiles, MDU SNMP Profile and GPON alarm profiles.

7.1.1 Configuring an MDU SNMP Profile

The MDU Simple Network Management Protocol (SNMP) profile is a collection of SNMP parameters. You can configure the information about an MDU management channel to OLT to implement the remote deployment and maintenance for the MDU.

Context

You can configure the SNMP parameter profile of the MDU on the U2000, and configure the information about an MDU management channel to the OLT. Then, the OLT manages the MDU through the SNMP mode so that the remote deployment and maintenance for the MDU can be implemented.

Procedure

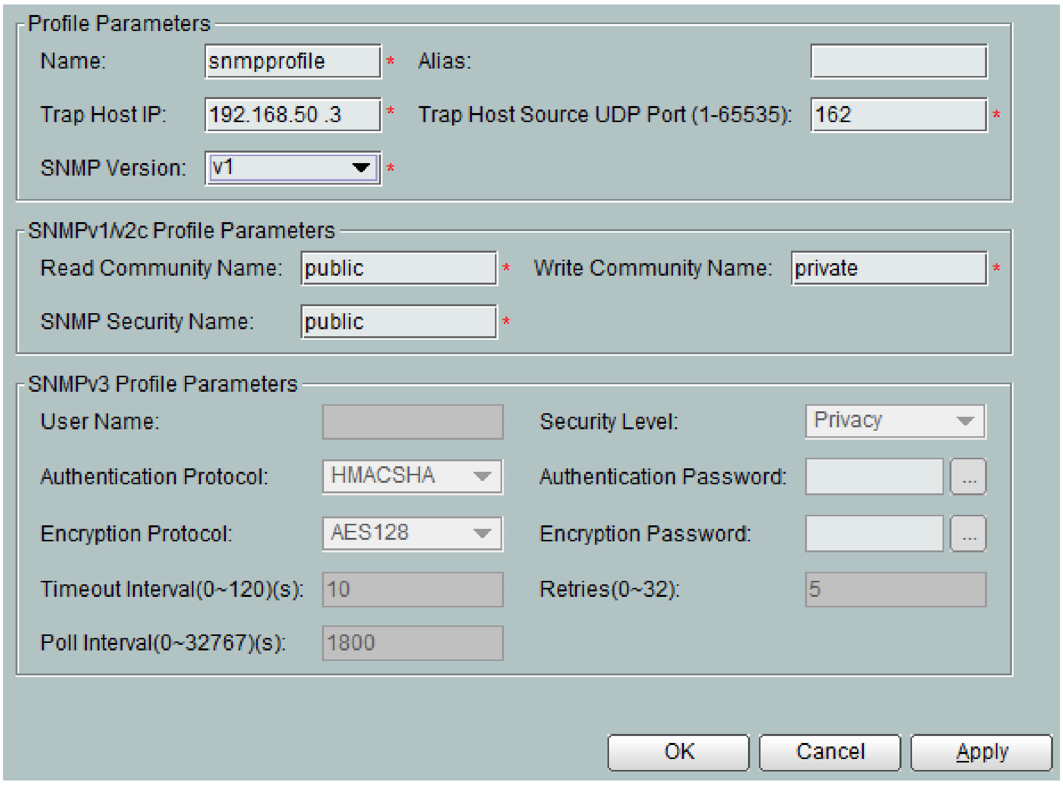
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

Step 3 Click the **MDU SNMP Profile** tab.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Profile Parameters
Name: snmpprofile *
Alias:
Trap Host IP: 192.168.50 .3 *
Trap Host Source UDP Port (1-65535): 162 *
SNMP Version: v1 *

SNMPv1/v2c Profile Parameters
Read Community Name: public *
Write Community Name: private *
SNMP Security Name: public *

SNMPv3 Profile Parameters
User Name:
Security Level: Privacy
Authentication Protocol: HMACSHA
Authentication Password:
Encryption Protocol: AES128
Encryption Password:
Timeout Interval(0~120)(s): 10
Retries(0~32): 5
Poll Interval(0~32767)(s): 1800

Step 6 Click **OK**.

Step 7 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 8 In the dialog box that is displayed, select the required NE(s), and click **OK**.

NOTE

The MDU SNMP profile that is generated by the U2000 can be referenced by the OLT only after the profile is applied to the corresponding OLT.

----End

7.1.2 Configuring a DBA Profile

A DBA profile contains the traffic parameters of a T-CONT. After a DBA profile is configured successfully and bound to a T-CONT, the system controls the traffic of the T-CONT based on the traffic parameters specified in the DBA profile. In this case, the DBA profile provides the flexible dynamic bandwidth allocation.

Context

- A DBA profile can be used to control the rate of upstream traffic of an ONU.
- The traffic specified in the DBA profile is the traffic of the GPON encapsulation mode (GEM) frames that encapsulate data. Hence, the actual traffic of packets is slightly smaller than the traffic specified in the DBA profile.
- The DBA profile added through the U2000 exists only in the database of the U2000, but is not applied to the device. The DBA profile can be created on the device only when the DBA profile is bound to the T-CONT.

Procedure

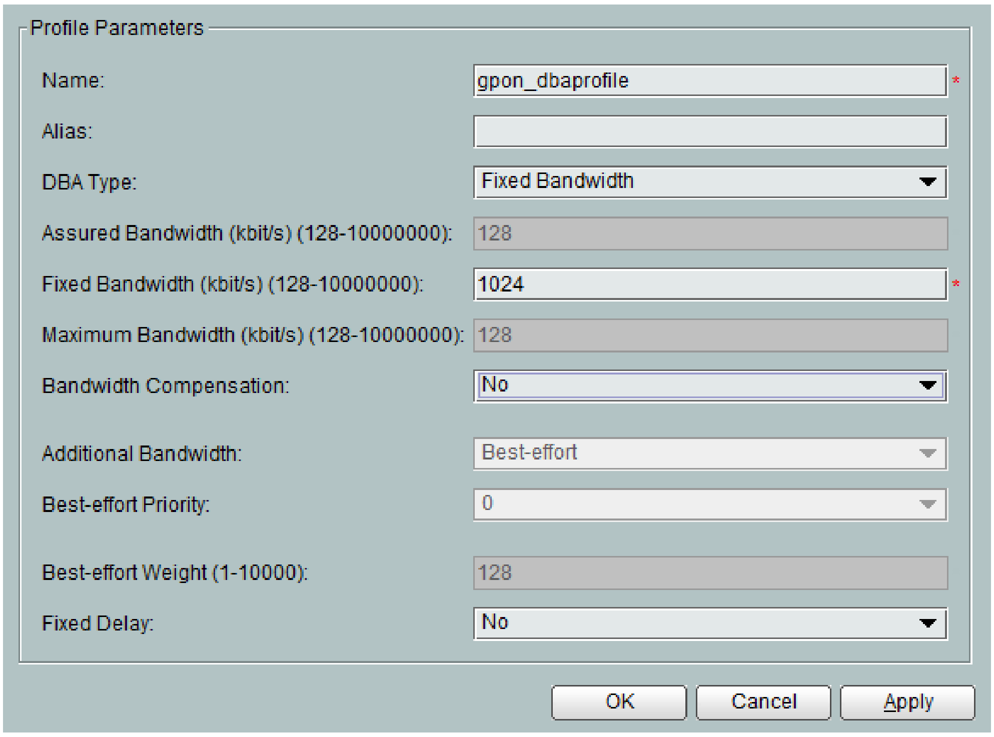
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

Step 3 Click the **DBA Profile** tab.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: gpon_dbaprofile *
Alias:
DBA Type: Fixed Bandwidth
Assured Bandwidth (kbit/s) (128-10000000): 128
Fixed Bandwidth (kbit/s) (128-10000000): 1024 *
Maximum Bandwidth (kbit/s) (128-10000000): 128
Bandwidth Compensation: No
Additional Bandwidth: Best-effort
Best-effort Priority: 0
Best-effort Weight (1-10000): 128
Fixed Delay: No

Step 6 Click **OK**.

----End

7.1.3 Configuring a GPON Line Profile

The GPON line profiles contain the parameters required for setting up the channels for the GPON lines.

Procedure

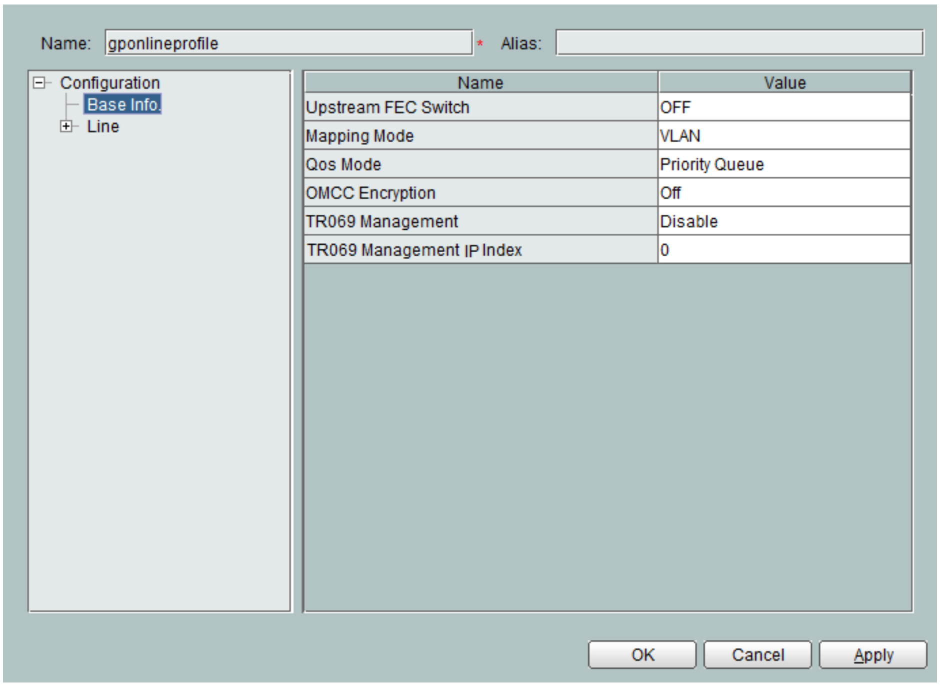
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

Step 3 Click the **GPON Line Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 4 In the dialog box that is displayed, set **Name** and the parameters related to the line profile.

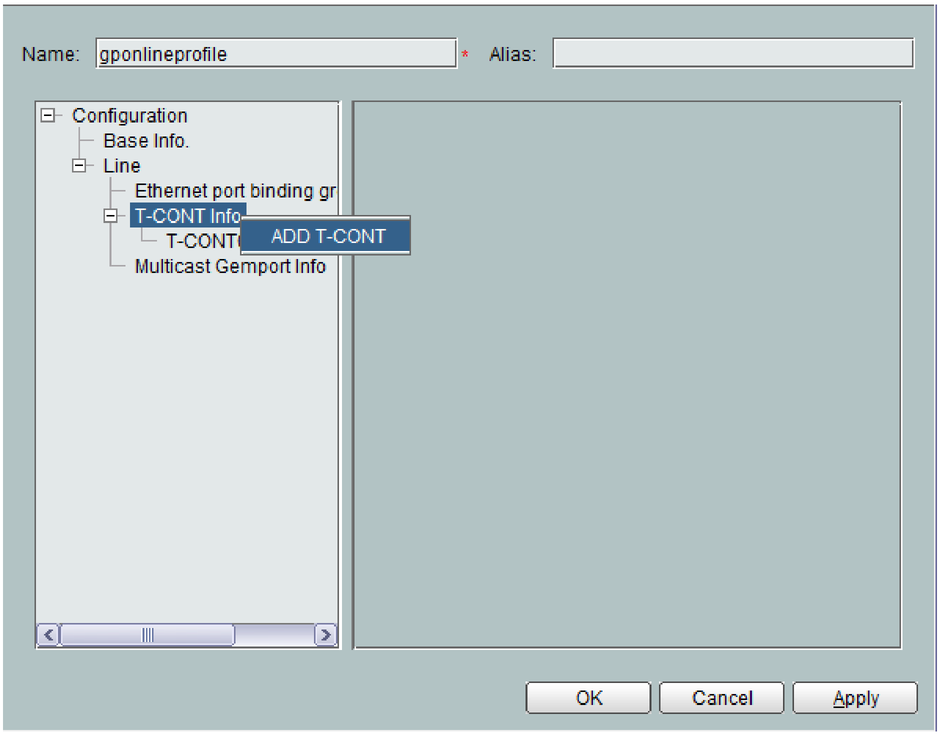
1. Choose **Basic Info** from the navigation tree, and then set the basic parameters of the profile.



Name: gponlineprofile * Alias:

Name	Value
Upstream FEC Switch	OFF
Mapping Mode	VLAN
Qos Mode	Priority Queue
OMCC Encryption	Off
TR069 Management	Disable
TR069 Management IP Index	0

2. Right-click **T-CONT Info.** in the navigation tree and choose **ADD T-CONT** from the shortcut menu. In the dialog box that is displayed, set **T-CONT Index** and **DBA Profile**.

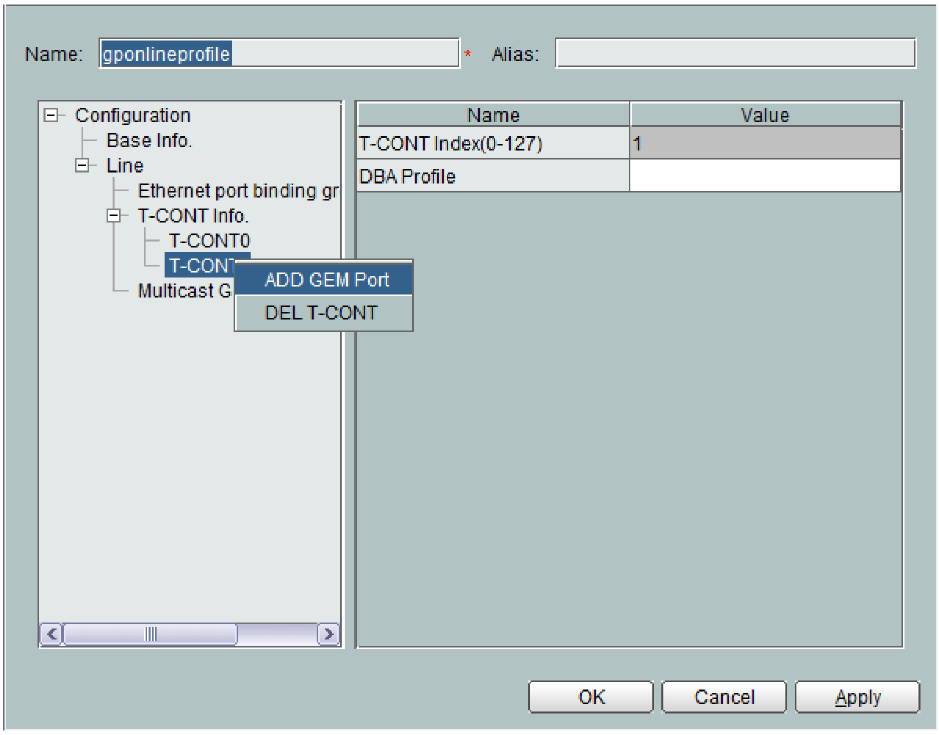


Name: gponlineprofile * Alias:

3. Right-click **T-CONTx** in the navigation tree and choose **ADD GEM Port** from the shortcut menu. In the dialog box that is displayed, set **GEM Port Index**.

NOTE

x indicates the T-CONT index.



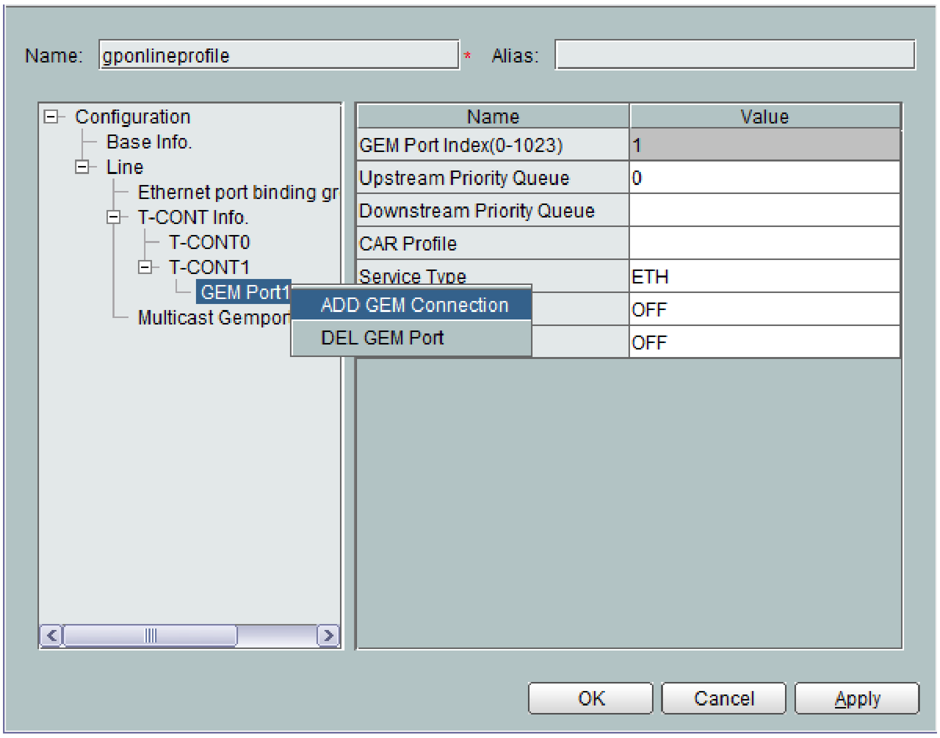
Name: gponlineprofile * Alias:

Name	Value
T-CONT Index(0-127)	1
DBA Profile	

4. Right-click **GEM Portx** in the navigation tree and choose **ADD GEM Connection** from the shortcut menu. In the dialog box that is displayed, set the basic parameters of the GEM Connection.

NOTE

x indicates the GEM port index.



Name: gponlineprofile * Alias:

Name	Value
GEM Port Index(0-1023)	1
Upstream Priority Queue	0
Downstream Priority Queue	
CAR Profile	
Service Type	ETH
	OFF
	OFF

Step 5 Click **OK**.

Step 6 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 7 In the dialog box that is displayed, select the required NE(s), and click **OK**.

NOTE

The GPON Line Profile that is generated by the U2000 can be referenced by the OLT only after the profile is applied to the corresponding OLT.

----End

7.1.4 Configuring a GPON Service Profile

The GPON service profile consolidates the parameters related to the ONU service into a profile.

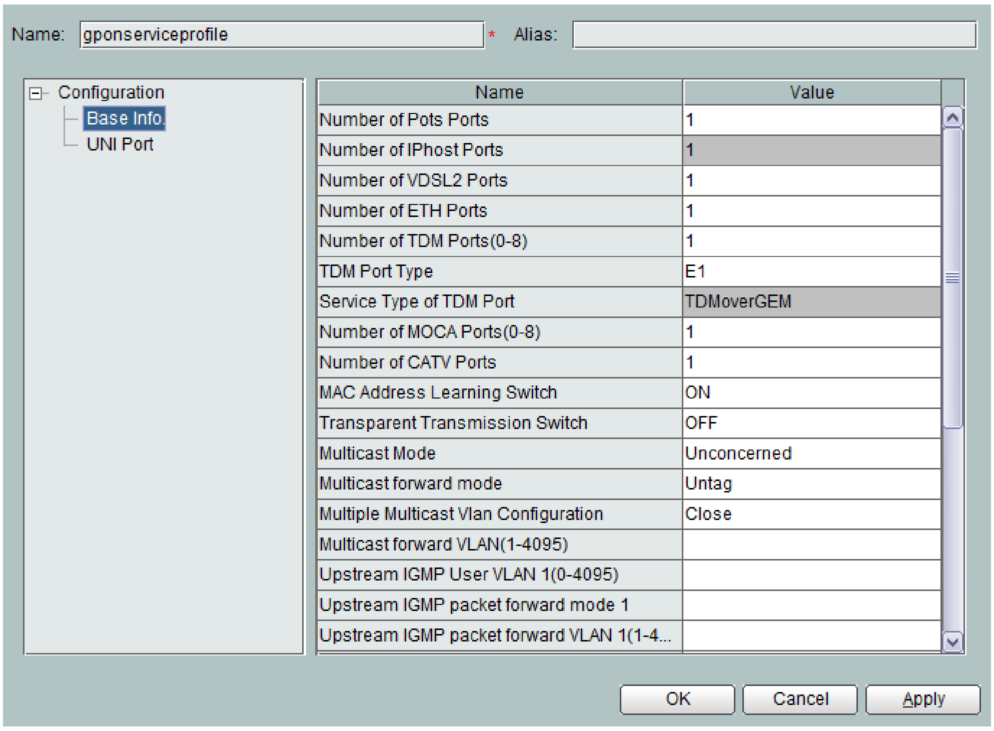
Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

Step 3 Click the **GPON Service Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 4 In the dialog box that is displayed, set **Name** and the parameters related to the service profile.



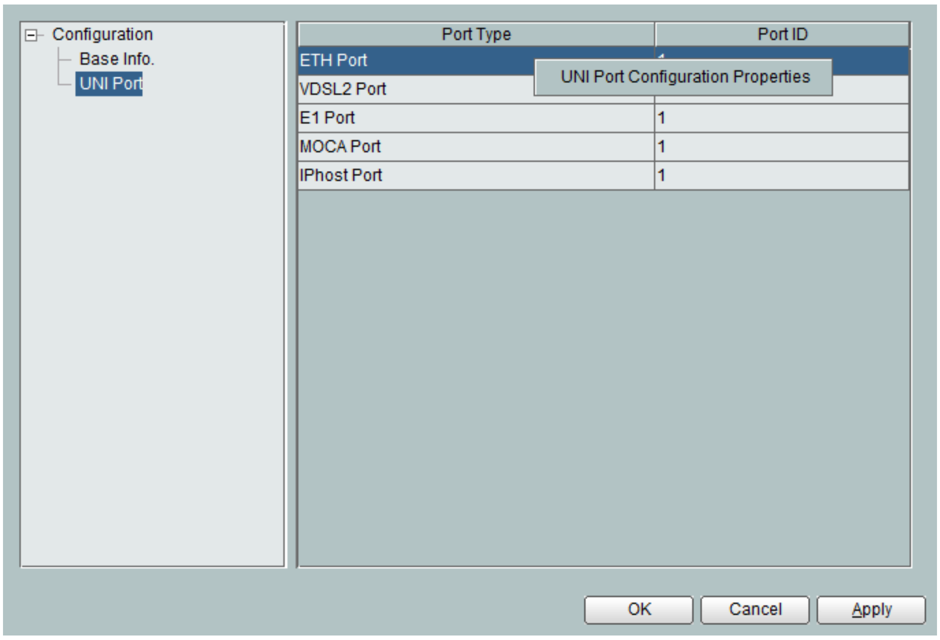
Name: gponserviceprofile * Alias:

Name	Value
Number of Pots Ports	1
Number of IPhost Ports	1
Number of VDSL2 Ports	1
Number of ETH Ports	1
Number of TDM Ports(0-8)	1
TDM Port Type	E1
Service Type of TDM Port	TDMoverGEM
Number of MOCA Ports(0-8)	1
Number of CATV Ports	1
MAC Address Learning Switch	ON
Transparent Transmission Switch	OFF
Multicast Mode	Unconcerned
Multicast forward mode	Untag
Multiple Multicast Vlan Configuration	Close
Multicast forward VLAN(1-4095)	
Upstream IGMP User VLAN 1(0-4095)	
Upstream IGMP packet forward mode 1	
Upstream IGMP packet forward VLAN 1(1-4...	

1. Choose **Basic Info** from the navigation tree, and then set the basic parameters of the profile.
2. Choose **UNI Port** from the navigation tree.

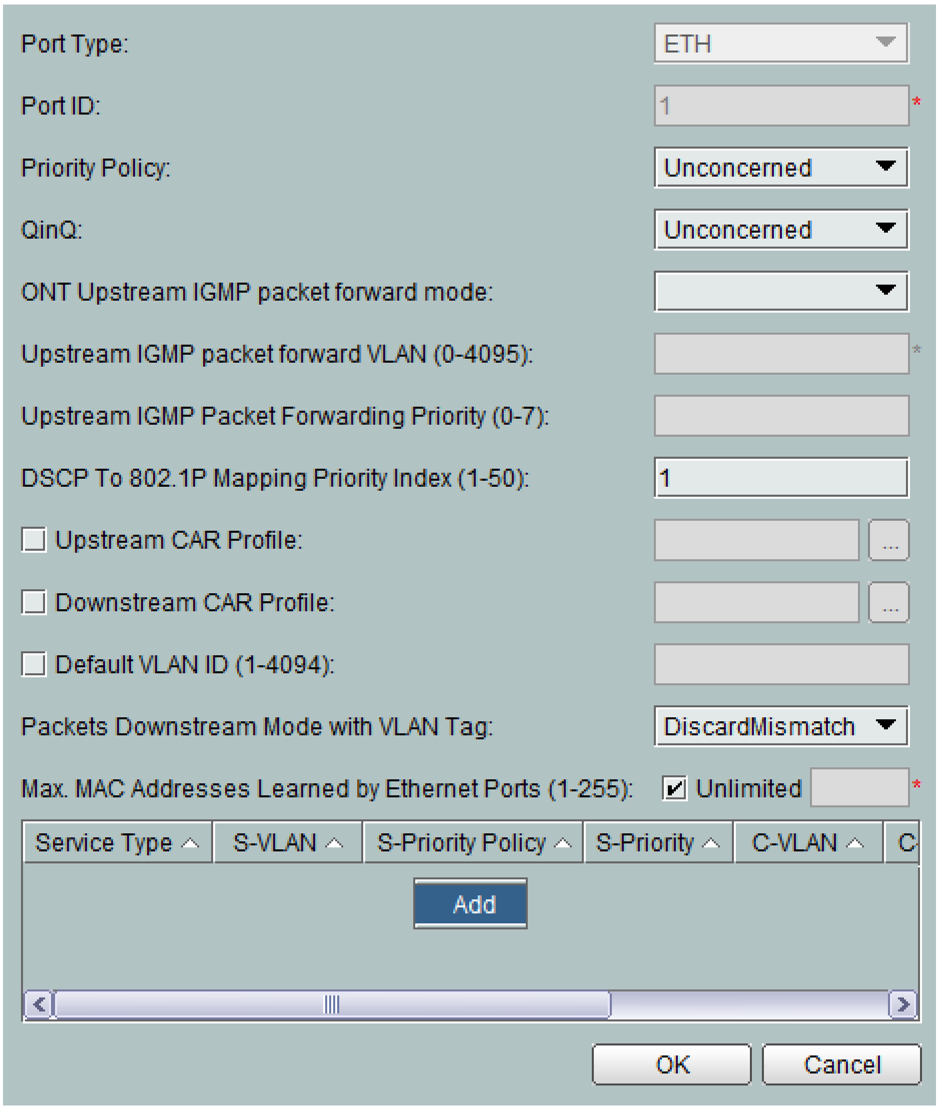
Copyright © Huawei Technologies Co., Ltd.

- When **Port Type** is set to **Eth Port**, In the right pane, select the record from the port list, right-click, and then choose **UNI Port Configuration Properties**.



Port Type	Port ID
ETH Port	1
VDSL2 Port	
E1 Port	1
MOCA Port	1
IPhost Port	1

In the dialog box that is displayed, right-click, and then choose **Add** to select the required VLAN ID.



Port Type: ETH

Port ID: 1 *

Priority Policy: Unconcerned

QinQ: Unconcerned

ONT Upstream IGMP packet forward mode:

Upstream IGMP packet forward VLAN (0-4095): *

Upstream IGMP Packet Forwarding Priority (0-7):

DSCP To 802.1P Mapping Priority Index (1-50): 1

☐ Upstream CAR Profile:

☐ Downstream CAR Profile:

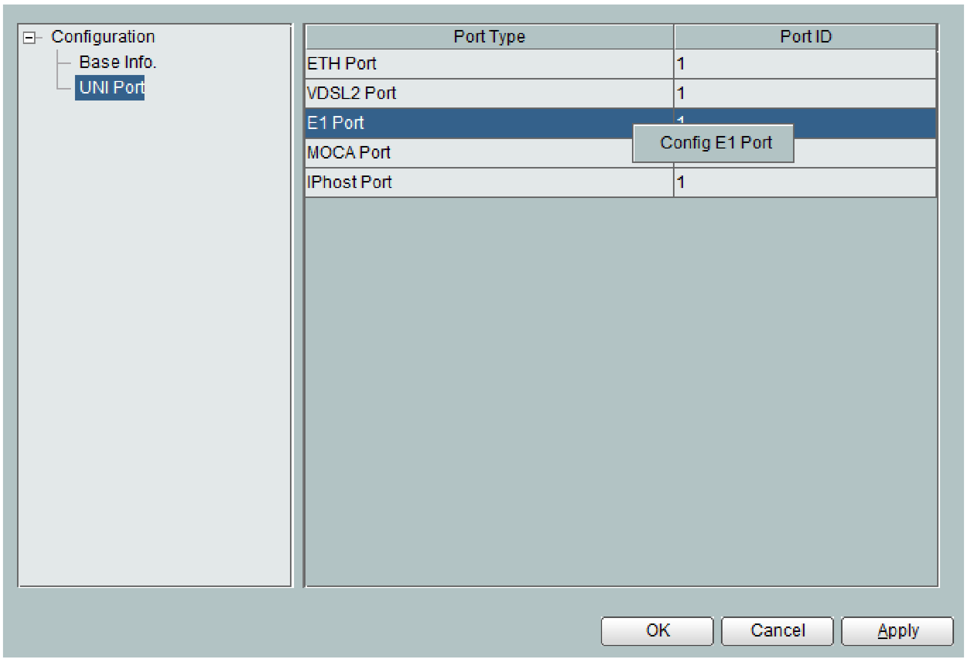
☐ Default VLAN ID (1-4094):

Packets Downstream Mode with VLAN Tag: DiscardMismatch

Max. MAC Addresses Learned by Ethernet Ports (1-255): ☑ Unlimited *

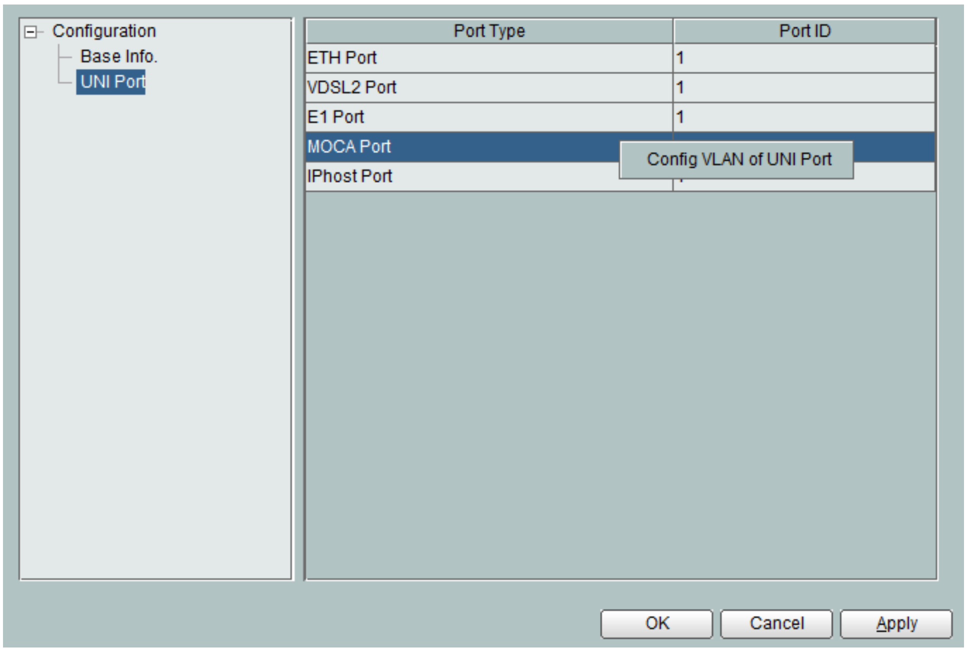
Service Type	S-VLAN	S-Priority Policy	S-Priority	C-VLAN	C

- When **Port Type** is set to **E1 Port**, In the right pane, select the record from the port list, right-click, and then choose **Config E1 Port** to configure the coding mode.



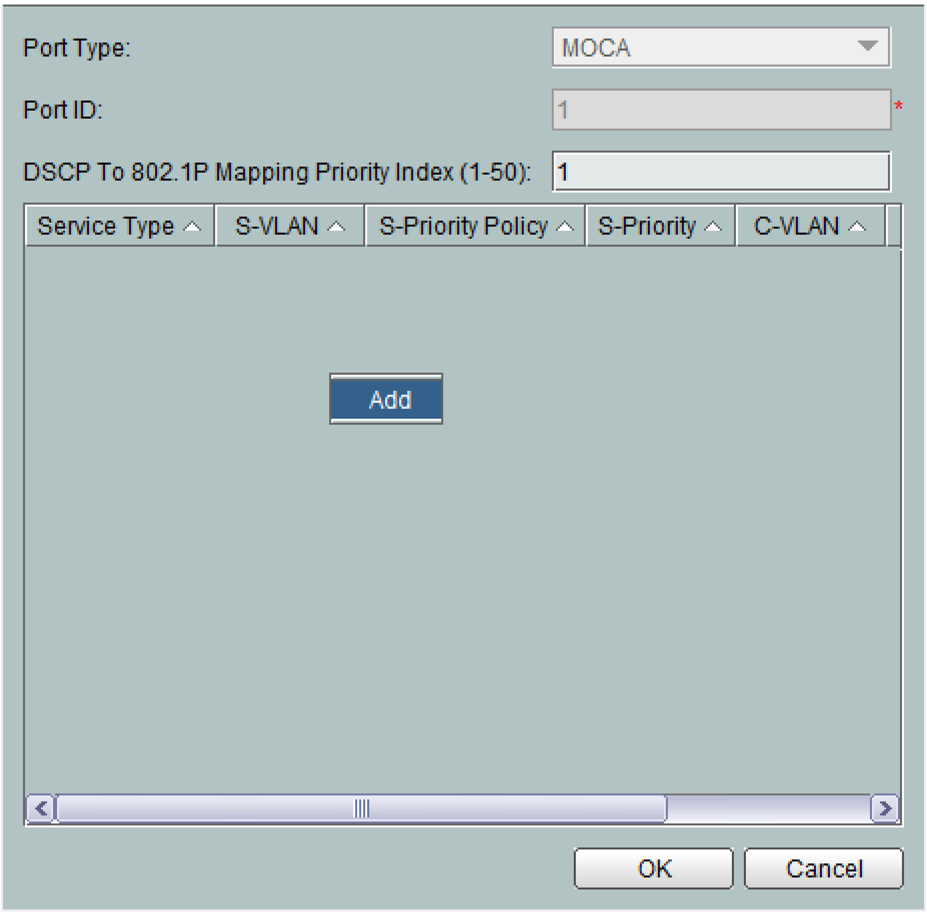
Port Type	Port ID
ETH Port	1
VDSL2 Port	1
E1 Port	
MOCA Port	
IPhost Port	1

- When **Port Type** is set to **Moca Port**, In the right pane, select the record from the port list, right-click, and then choose **Config VLAN of UNI Port**.



Port Type	Port ID
ETH Port	1
VDSL2 Port	1
E1 Port	1
MOCA Port	
IPhost Port	

In the dialog box that is displayed, right-click, and then choose **Add** to select the required VLAN ID.

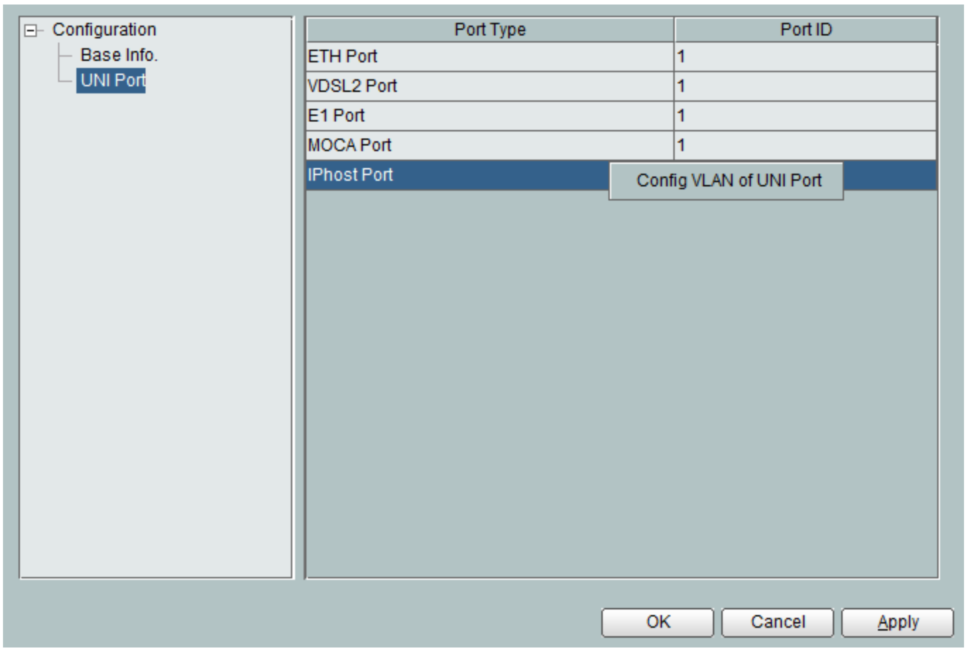

Port Type: MOCA

Port ID: 1

DSCP To 802.1P Mapping Priority Index (1-50): 1

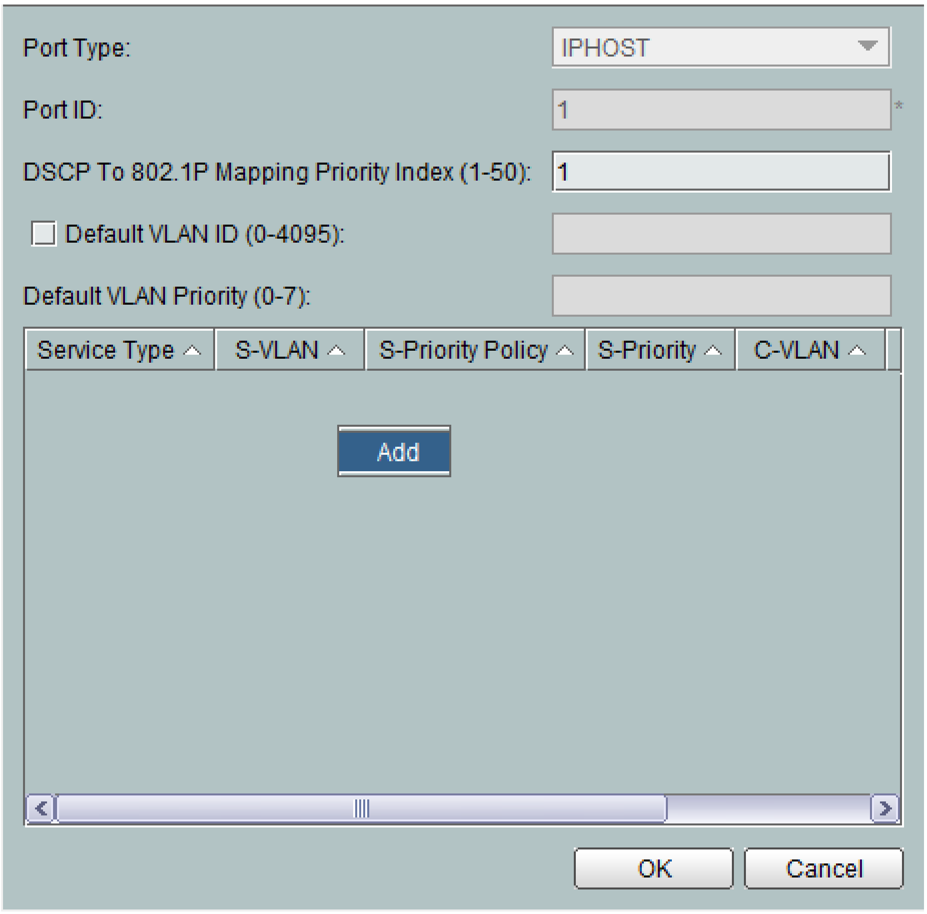
Service Type	S-VLAN	S-Priority Policy	S-Priority	C-VLAN

- When **Port Type** is set to **IPhost Port**, In the right pane, select the record from the port list, right-click, and then choose **Config VLAN of UNI Port**.



Port Type	Port ID
ETH Port	1
VDSL2 Port	1
E1 Port	1
MOCA Port	1
IPhost Port	

In the dialog box that is displayed, right-click, and then choose **Add** to select the required VLAN ID.


Port Type: IPHOST

Port ID: 1 *

DSCP To 802.1P Mapping Priority Index (1-50): 1

☐ Default VLAN ID (0-4095):

Default VLAN Priority (0-7):

Step 5 Click **OK**.

Step 6 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 7 In the dialog box that is displayed, select the required NE(s), and click **OK**.

NOTE

The GPON Service Profile that is generated by the U2000 can be referenced by the OLT only after the profile is applied to the corresponding OLT.

----End

7.1.5 Configuring a GPON ONT Capability Profile (OLT in Distributed Mode)

The GPON ONT capability profile identifies the actual capability of the GPON ONT. The GPON ONT capability profile aims at pre-configuring ONTs. Before ONTs are installed at user homes, the ONTs do not exist. In this case, the actual capabilities of the ONTs are not determined, and services cannot be configured. Through the U2000, offline ONTs can be added, and GPON ONT capability profiles can be bound to the offline ONTs. Then, the service data can be configured. After the ONTs are installed at user homes, service data can be automatically applied to the ONTs.

Context

- The ONT capability profile must match the hardware capability of the ONT that is bound to the profile. Otherwise, applying certain configurations fails.
- The GPON ONT capability profile added through the U2000 exists only in the database of the U2000, but is not applied to the device. The GPON ONT capability profile can be created on the device only when the GPON ONT capability profile is bound to the ONT.

Procedure

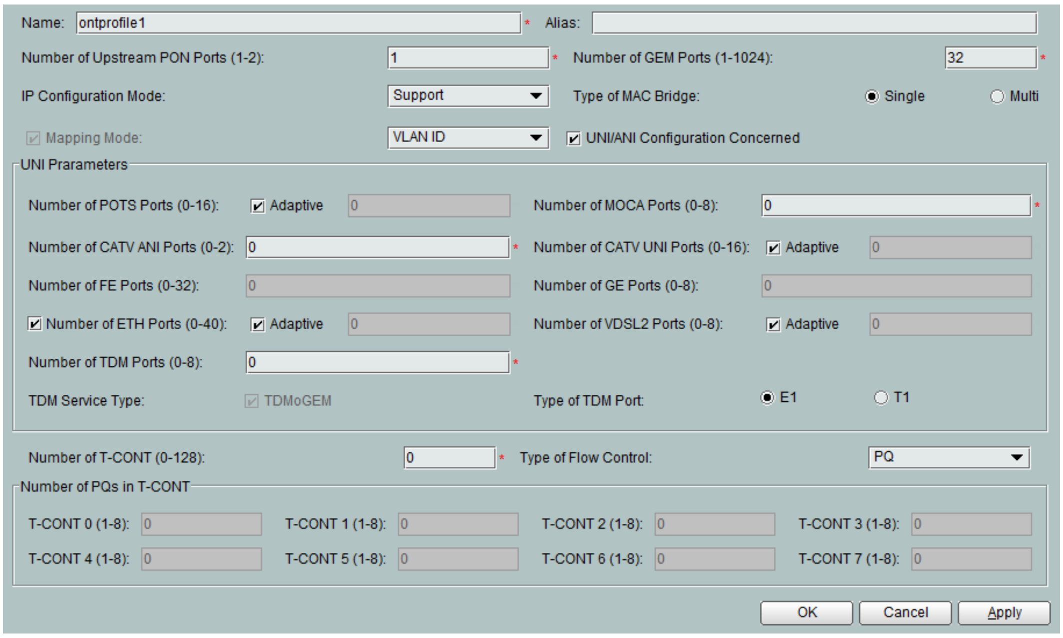
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

Step 3 Click the **GPON ONT Capacity Profile** tab.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: ontprofile1 * Alias:
Number of Upstream PON Ports (1-2): 1 *
Number of GEM Ports (1-1024): 32 *
IP Configuration Mode: Support
Type of MAC Bridge: ● Single ○ Multi
☑ Mapping Mode: VLAN ID
☑ UNI/ANI Configuration Concerned

UNI Prarameters
Number of POTS Ports (0-16): ☑ Adaptive 0
Number of MOCA Ports (0-8): 0 *
Number of CATV ANI Ports (0-2): 0 *
Number of CATV UNI Ports (0-16): ☑ Adaptive 0
Number of FE Ports (0-32): 0
Number of GE Ports (0-8): 0
☑ Number of ETH Ports (0-40): ☑ Adaptive 0
Number of VDSL2 Ports (0-8): ☑ Adaptive 0
Number of TDM Ports (0-8): 0 *
TDM Service Type: ☑ TDMoGEM
Type of TDM Port: ● E1 ○ T1

Number of T-CONT (0-128): 0 *
Type of Flow Control: PQ

Number of PQs in T-CONT
T-CONT 0 (1-8): 0
T-CONT 1 (1-8): 0
T-CONT 2 (1-8): 0
T-CONT 3 (1-8): 0
T-CONT 4 (1-8): 0
T-CONT 5 (1-8): 0
T-CONT 6 (1-8): 0
T-CONT 7 (1-8): 0

Step 6 Click **OK**.

Step 7 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 8 In the dialog box that is displayed, select the required NE(s), and click **OK**.

NOTE

The GPON ONT Capability Profile that is generated by the U2000 can be referenced by the OLT only after the profile is applied to the corresponding OLT.

----End

7.1.6 Configuring a GPON Alarm Profile

A GPON alarm profile contains a series of alarm threshold parameters that are used for performance measurement and monitoring of the active ONU lines. After a GPON alarm profile is bound to an ONU, if the performance statistics of the line exceeds the threshold that is specified in the profile, the ONU sends alarms to the log host and the U2000.

Procedure

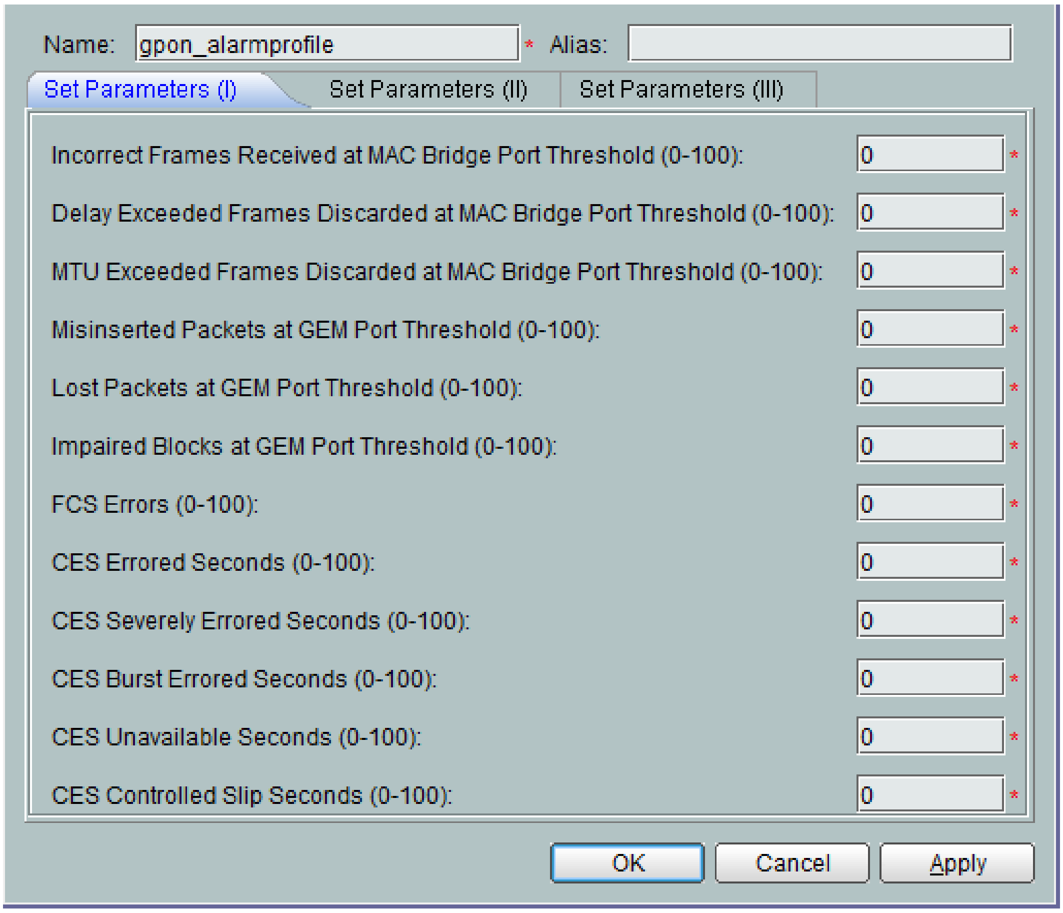
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

Step 3 Click the **GPON Alarm Profile** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters as follows.



Name: gpon_alarmprofile *
Alias:

Incorrect Frames Received at MAC Bridge Port Threshold (0-100): 0 *
Delay Exceeded Frames Discarded at MAC Bridge Port Threshold (0-100): 0 *
MTU Exceeded Frames Discarded at MAC Bridge Port Threshold (0-100): 0 *
Misinserted Packets at GEM Port Threshold (0-100): 0 *
Lost Packets at GEM Port Threshold (0-100): 0 *
Impaired Blocks at GEM Port Threshold (0-100): 0 *
FCS Errors (0-100): 0 *
CES Errored Seconds (0-100): 0 *
CES Severely Errored Seconds (0-100): 0 *
CES Burst Errored Seconds (0-100): 0 *
CES Unavailable Seconds (0-100): 0 *
CES Controlled Slip Seconds (0-100): 0 *

Step 6 Click **OK**.

Step 7 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 8 In the dialog box that is displayed, select the required NE(s), and click **OK**.

NOTE

The GPON Alarm Profile that is generated by the U2000 can be referenced by the OLT only after the profile is applied to the corresponding OLT.

----End

7.1.7 Configuring the ONT Value-Added Service Configuration Profile

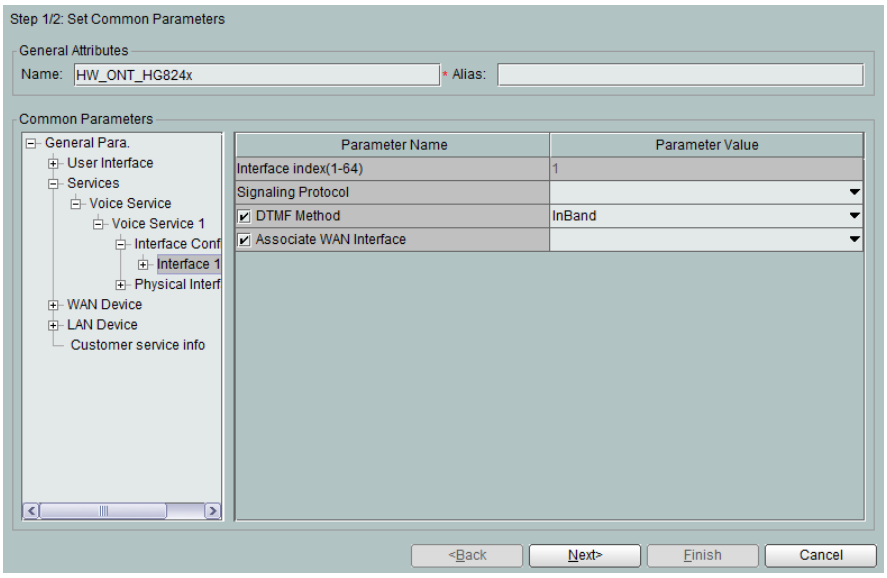
After configuring a general ONT value-added service profile or an ONT value-added service profile and binding it to an ONT successfully, you can activate the ONT and directly provision the value-added service defined by the profile to the subscribers of the ONT. Each ONT can be bound to only one general ONT value-added service profile or ONT value-added service profile.

Context

A general value-added service (VAS) profile is a collection of ONT common parameters and integrates the VAS profiles of different ONTs. The general VAS profile is used to implement the cross-model and cross-version service provisioning and replacement, and cross-version upgrades. The value-added service configuration profiles vary with the types of the ONTs and the software versions.

Procedure

- **Configure an ONT general VAS profile.**
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **PON Profile** > **ONT VAS Profile** from the navigation tree.
  3. Click the **General ONT VAS Profile** tab.
  4. In the information list, right-click and choose **Add (Service Configuration Type)** from the shortcut menu.
  5. In the dialog box that is displayed, set the required parameters.

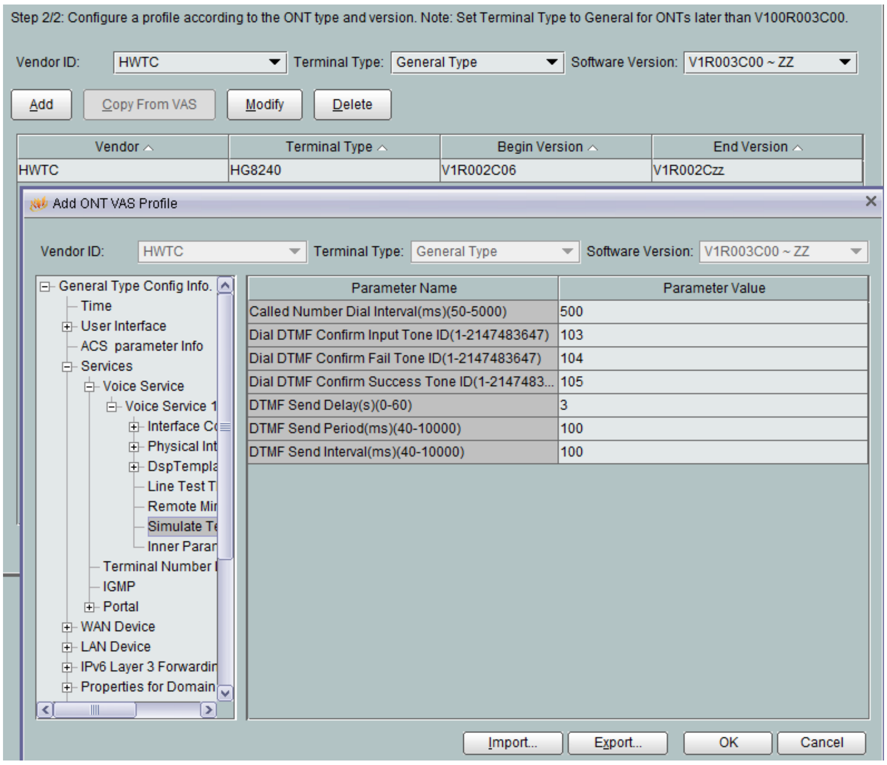


Step 1/2: Set Common Parameters

Name: HW_ONT_HG824x * Alias:

Parameter Name	Parameter Value
Interface index(1-64)	1
Signaling Protocol	
☑ DTMF Method	InBand
☑ Associate WAN Interface	

6. Click **Next**.
7. In the dialog box that is displayed, set user-defined parameters for the ONTs of different software versions.



Step 2/2: Configure a profile according to the ONT type and version. Note: Set Terminal Type to General for ONTs later than V100R003C00.

Vendor ID: HWTC Terminal Type: General Type Software Version: V1R003C00 ~ ZZ

Vendor	Terminal Type	Begin Version	End Version
HWTC	HG8240	V1R002C06	V1R002Czz

Add ONT VAS Profile

Vendor ID: HWTC Terminal Type: General Type Software Version: V1R003C00 ~ ZZ

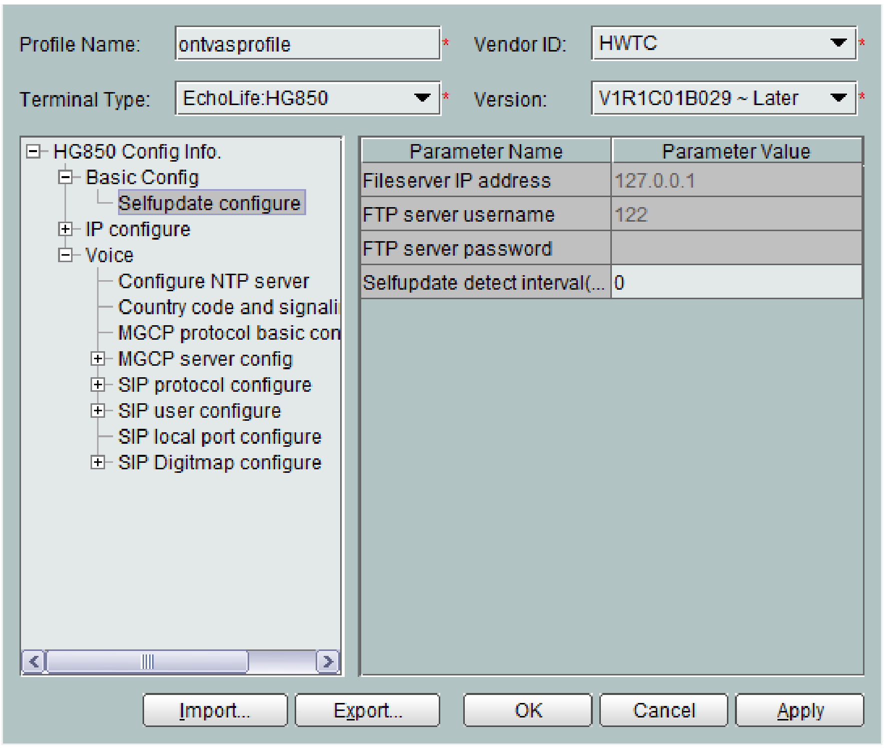
Parameter Name	Parameter Value
Called Number Dial Interval(ms)(50-5000)	500
Dial DTMF Confirm Input Tone ID(1-2147483647)	103
Dial DTMF Confirm Fail Tone ID(1-2147483647)	104
Dial DTMF Confirm Success Tone ID(1-2147483...	105
DTMF Send Delay(s)(0-60)	3
DTMF Send Period(ms)(40-10000)	100
DTMF Send Interval(ms)(40-10000)	100

8. Click **Finish**.
9. In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
10. In the dialog box that is displayed, select the required NE(s), and click **OK**.

- **Configure an ONT VAS profile.**
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in

Application Center and choose **Access Service** > **Access Profile Management** from the main menu (application style).

2. In the dialog box that is displayed, choose **PON Profile** > **ONT VAS Profile** from the navigation tree.
3. Click the **ONT VAS Profile** tab.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set **Profile Name**, **Vendor ID**, **Terminal Type**, and **Version**.



Profile Name: ontvasprofile *
Vendor ID: HWTC *
Terminal Type: EchoLife:HG850 *
Version: V1R1C01B029 ~ Later *

Parameter Name	Parameter Value
Fileserver IP address	127.0.0.1
FTP server username	122
FTP server password	
Selfupdate detect interval(...	0

6. Click **OK**.
7. In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
8. In the dialog box that is displayed, select the required NE(s), and click **OK**.

----End

7.1.8 Configuring an ONT Automatic Discovery Interval

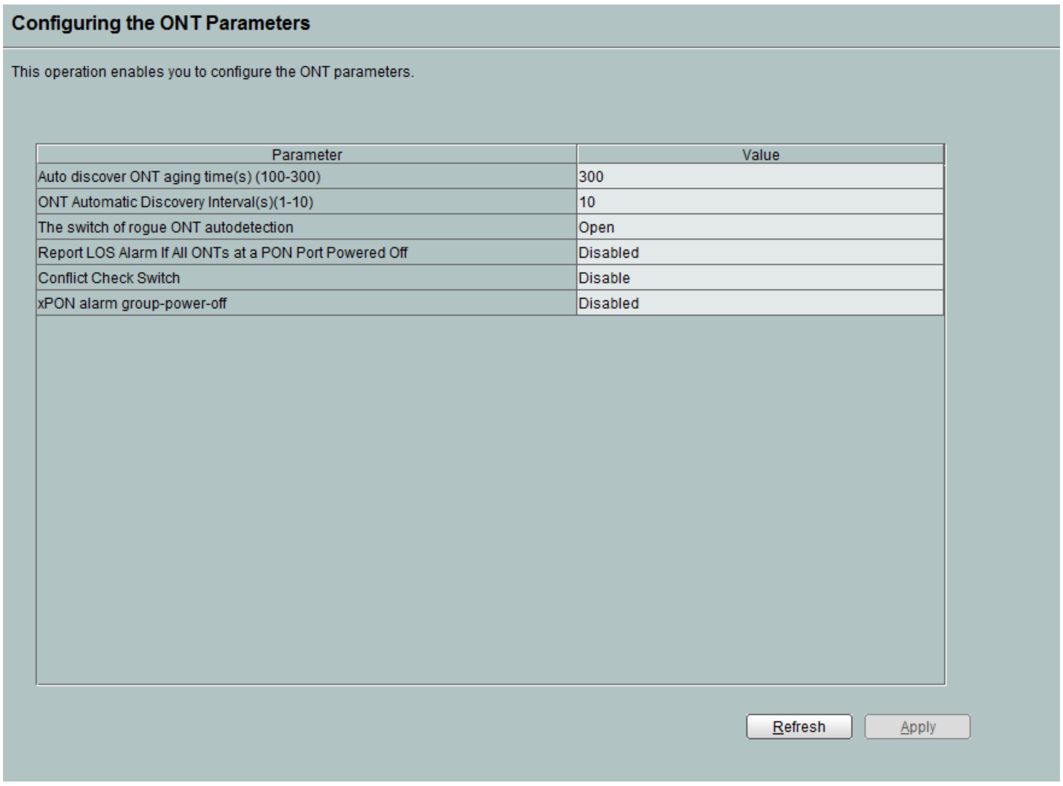
This topic describes how to configure the parameters relevant to the function of ONT automatic discovery.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Properties** > **xPON** > **ONT**.

Step 3 In the right pane, set **Auto discover ONT aging time** and **ONT Automatic Discovery Interval**.



Configuring the ONT Parameters

This operation enables you to configure the ONT parameters.

Parameter	Value
Auto discover ONT aging time(s) (100-300)	300
ONT Automatic Discovery Interval(s)(1-10)	10
The switch of rogue ONT autodetection	Open
Report LOS Alarm If All ONTs at a PON Port Powered Off	Disabled
Conflict Check Switch	Disable
xPON alarm group-power-off	Disabled

Step 4 Click **Apply**.

----End

7.2 Configuring the GPON Access Service - Distributed Mode

This topic describes how to configure the GPON access service. The GPON access supports high-bandwidth transmission, which effectively removes the bandwidth bottleneck in the access through twisted pairs and meets the users' requirements on high-bandwidth services, such as high definition TV (HDTV) and live programs.

Prerequisites

- The corresponding VLAN must be already created in the system. For details on adding a VLAN, see **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN must be already configured. For details on configuring the upstream port of a VLAN, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MEF IP traffic profile must be already configured in the system. For details on configuring the MEF IP traffic profile, see **5.2 Configuring an MEF IP Traffic Profile**. For details on configuring the IP traffic profile, see Configuring an IP Traffic Profile.

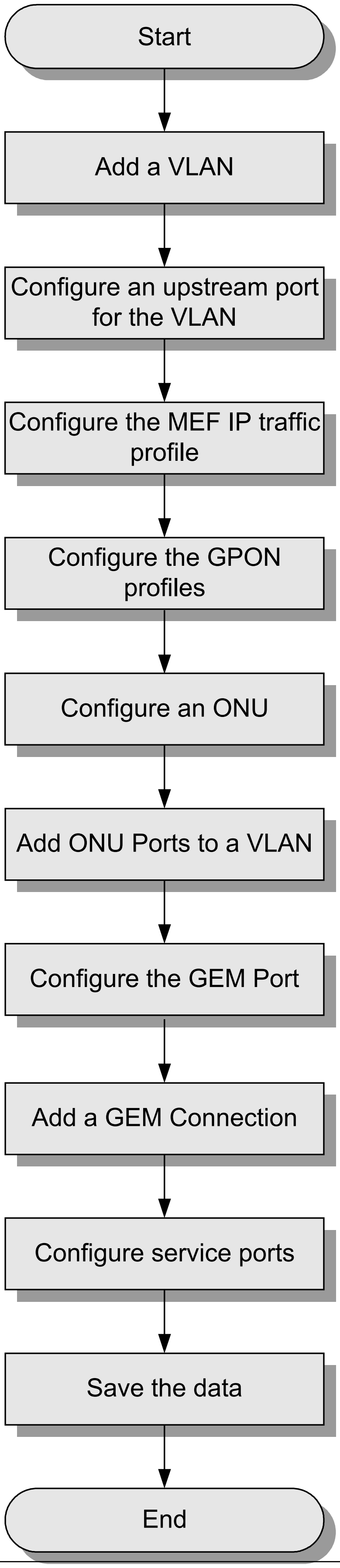
In the distributed mode, you are required to configure the GPON ONU capability profiles and DBA profiles and download to the NEs so that they can be applied to the GPON access services.

- The GPON ONU capability profile must be already configured in the system. For details on configuring the GPON ONU capability profile, see **7.1.5 Configuring a GPON ONT Capability Profile (OLT in Distributed Mode)**.
- The DBA profile must be already configured in the system. For details on configuring the DBA profile, see **7.1.2 Configuring a DBA Profile**.

Context

Figure 7-1 shows the flowchart for configuring the GPON access service.

Figure 7-1 Flowchart for configuring the GPON access service



7.2.1 Configuring the ONU

This topic describes how to add an ONU and configure the basic attribute parameters of the ONU. To add an ONU offline and configure the service of the ONU offline, perform this operation. After the ONU goes online, the configuration data is applied to the ONU, and then the configuration of the ONU is completed.

Context

- T-CONT is short for transmission container. The T-CONT can be used for carrying services only after it is bound to the dynamic bandwidth allocation (DBA) profile.
- After a T-CONT is bound to a DBA profile, the T-CONT uses the parameters defined in the DBA profile. The T-CONT can flexibly provide DBA solutions based on different configurations of the DBA profiles.
- You can bind a T-CONT to a DBA profile only after adding an ONU.
- By default, T-CONT 0 of an ONU is used by OMCI and is bound to dba-profile_1.

Procedure

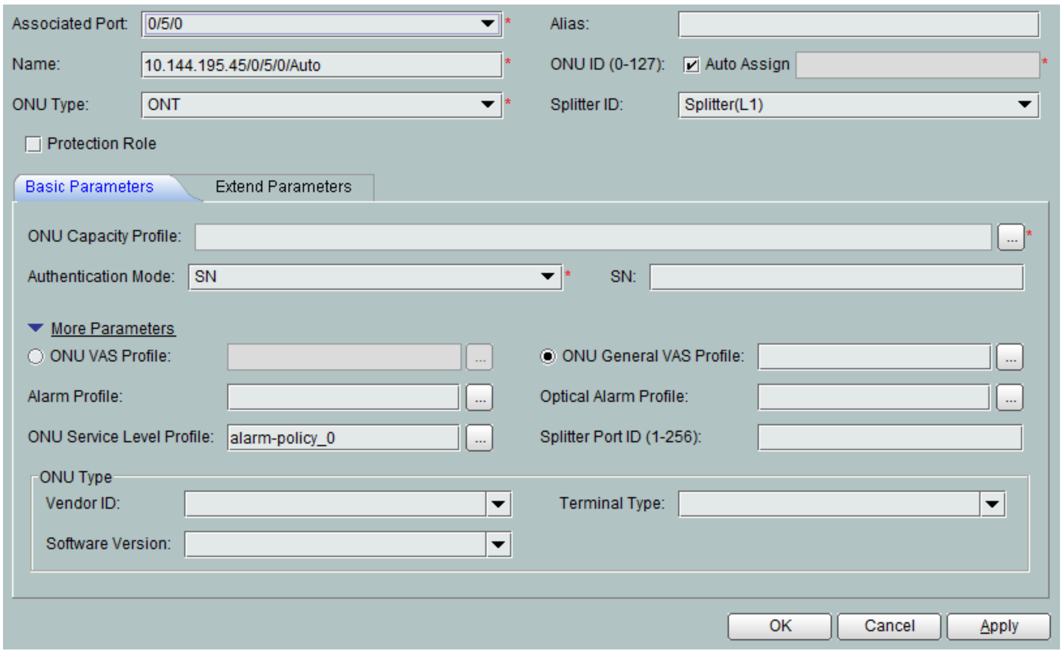
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

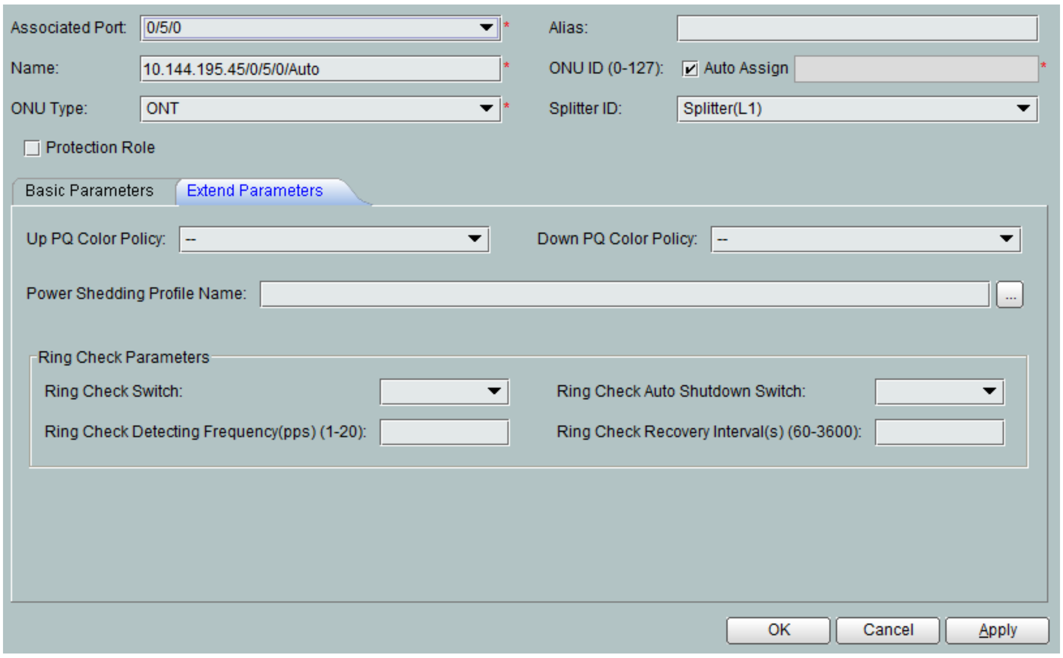
Step 3 Click the **GPON ONU** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Associated Port: 0/5/0 *
Alias:
Name: 10.144.195.45/0/5/0/Auto *
ONU ID (0-127): ☑ Auto Assign *
ONU Type: ONT *
Splitter ID: Splitter(L1)
☐ Protection Role
ONU Capacity Profile: *
Authentication Mode: SN *
SN:
○ ONU VAS Profile:
● ONU General VAS Profile:
Alarm Profile:
Optical Alarm Profile:
ONU Service Level Profile: alarm-policy_0
Splitter Port ID (1-256):
Vendor ID:
Terminal Type:
Software Version:


Associated Port: 0/5/0
Name: 10.144.195.45/0/5/0/Auto
ONU Type: ONT
ONU ID (0-127): ☑ Auto Assign
Splitter ID: Splitter(L1)
☐ Protection Role
Up PQ Color Policy: --
Down PQ Color Policy: --
Alias:
Basic Parameters
Extend Parameters
Power Shedding Profile Name:
...
Ring Check Parameters
Ring Check Switch:
Ring Check Auto Shutdown Switch:
Ring Check Detecting Frequency(pps) (1-20):
Ring Check Recovery Interval(s) (60-3600):
OK
Cancel
Apply

NOTE

- **Terminal Type** and **Software Version** that you set must be the same as the version information of the actual ONU.
- When **ONU Type** is set to **MDU**, click the **Network Management Channel Parameters** tab and set **IP Address** in the **Network Parameters** area to the IP address of the Layer 3 interface of the VLAN. For details, see **14.1.1.3 Configuring a VLAN L3 Interface**.

Step 6 Click **OK**.

Step 7 Choose the ONU from the list, and click the **T-CONT** tab in the lower pane.

Step 8 Right-click the list in the **T-CONT** tab page, and then choose **Bind**.

Step 9 Choose an available **T-CONT ID** from the **Bind DBA** dialog box that is displayed, and click … next to **DBA Profile Name**.

Step 10 Choose the DBA profile from the **DBA Profile** dialog box that is displayed, and click **OK**.

Step 11 In the **Bind DBA** dialog box, click **OK**.

----End

7.2.2 Adding ONU Ports to a VLAN

This topic describes how to add ONU ports to a VLAN.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

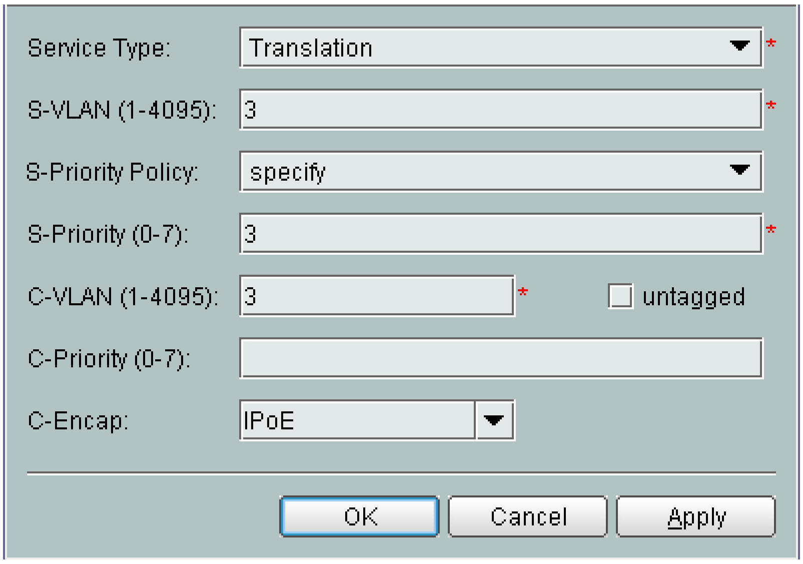
Step 3 On the **GPON ONU** tab page, set the filter criteria or click ⌄ to display the required GPON ONUs.

Step 4 Select an ONU record, and then click the **Current ONU: UNI Port Info** tab in the lower pane.

Step 5 On the **Current ONU: UNI Port Info** tab page, select a record from the list, right-click, and then choose **Configure VLAN Switch**.

Step 6 On the displayed dialog box, right-click, and then choose **Add**.

Step 7 Configure the parameters in the dialog box that is displayed, as shown in the following figure.



Service Type: Translation *
S-VLAN (1-4095): 3 *
S-Priority Policy: specify
S-Priority (0-7): 3 *
C-VLAN (1-4095): 3 * ☐ untagged
C-Priority (0-7):
C-Encap: IPoE

Step 8 Click **OK**.

----End

7.2.3 Configuring the GEM Port

This topic describes how to add the GEM port for transmitting traffic streams.

Context

Other method to configuring the GEM Port: In the NE Explorer, choose **GPON** > **GEM Port**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

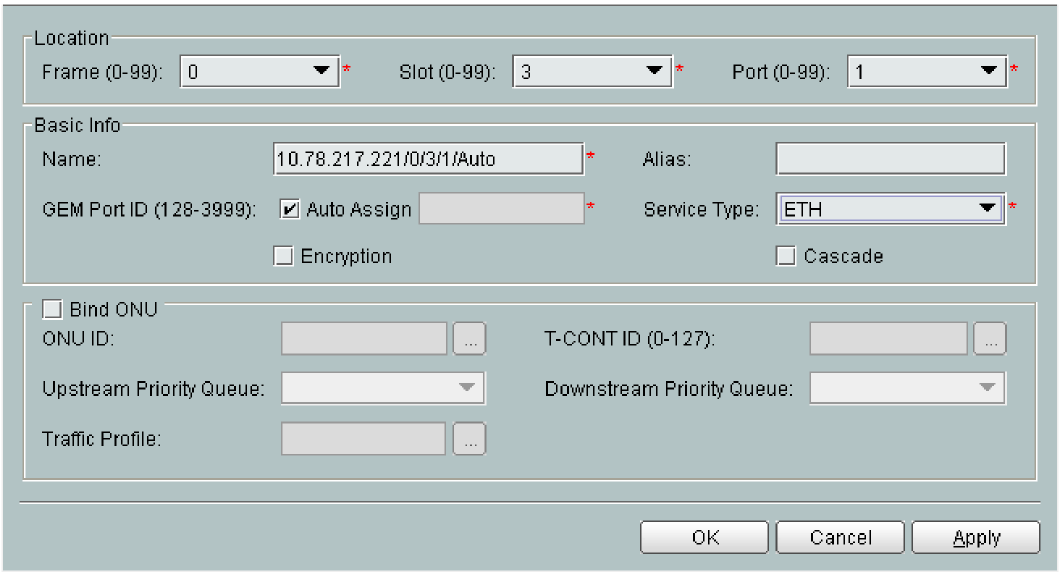
Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 On the **GPON ONU** tab page, set the filter criteria or click ⌄ to display the required GPON ONUs.

Step 4 In the GPON ONU list, select a record and click the **GEM Port** tab in the lower pane.

Step 5 In the information list, right-click and choose **Add** from the shortcut menu.

Step 6 In the dialog box that is displayed, set the parameters.



Location

Frame (0-99): 0 *

Slot (0-99): 3 *

Port (0-99): 1 *

Basic Info

Name: 10.78.217.221/0/3/1/Auto *

Alias:

GEM Port ID (128-3999): ☑ Auto Assign *

Service Type: ETH *

☐ Encryption

☐ Cascade

☐ Bind ONU

ONU ID:

T-CONT ID (0-127):

Upstream Priority Queue:

Downstream Priority Queue:

Traffic Profile:

Step 7 Click **OK**.

----End

7.2.4 Adding a GEM Connection

This topic describes how to establish a connection between the ONU-side service and the GEM port, that is, to create a mapping between the GEM port and the upstream traffic stream of the ONU user port. The GEM port can be used for carrying services only after the corresponding GEM connection is established.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

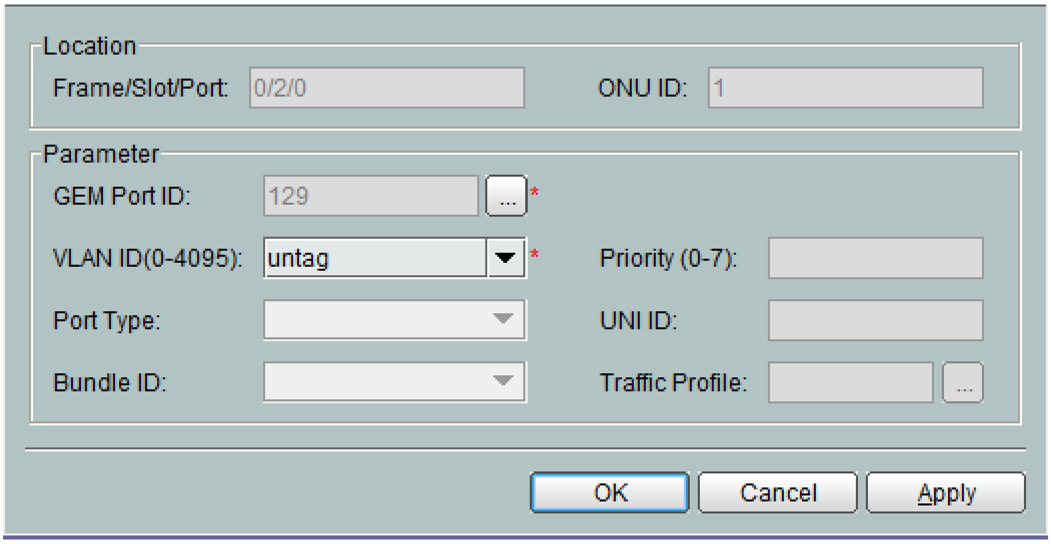
Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 On the **GPON ONU** tab page, set the filter criteria or click ⌄ to display the required GPON ONUs.

Step 4 Select an ONU from the ONU list for adding the GEM connection, and click the **GEM Connection** tab in the lower pane.

Step 5 Right-click the list in the **GEM Connection** tab page, and then choose **Add**.

Step 6 In the dialog box that is displayed, set the parameters.



Frame/Slot/Port: 0/2/0

ONU ID: 1

GEM Port ID: 129

VLAN ID(0-4095): untag

Priority (0-7):

Port Type:

UNI ID:

Bundle ID:

Traffic Profile:

Step 7 Click **OK**.

----End

7.2.5 Configuring the Service Port

This topic describes how to configure the service port for the GPON access service.

Prerequisites

- The VLAN to which the service port belongs must have been configured. For details, see **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN must have been configured. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- A suitable MEF IP traffic profile must have been configured. For details, see **5.2 Configuring an MEF IP Traffic Profile**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

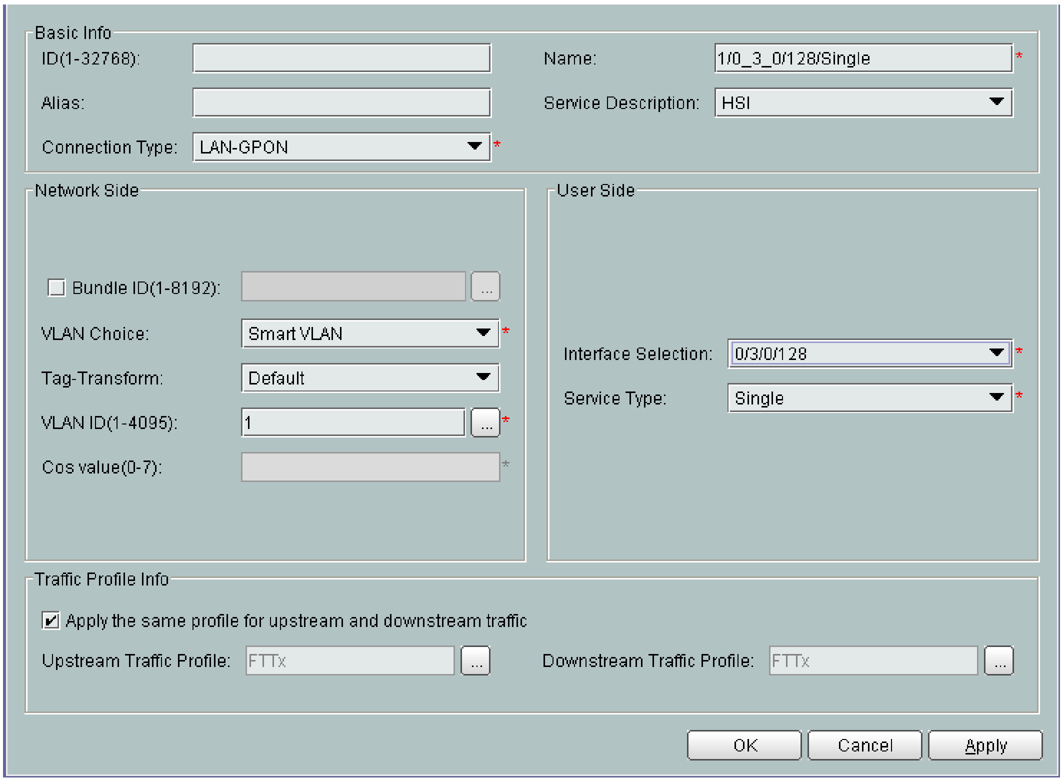
Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 On the **GPON ONU** tab page, set the filter criteria or click to display the required GPON ONUs.

Step 4 Select a record from the list, and click the **Service Port Info** tab in the lower pane.

Step 5 Right-click the service port list in the lower part of the page, and then choose **Add**.

Step 6 In the dialog box that is displayed, set the parameters.

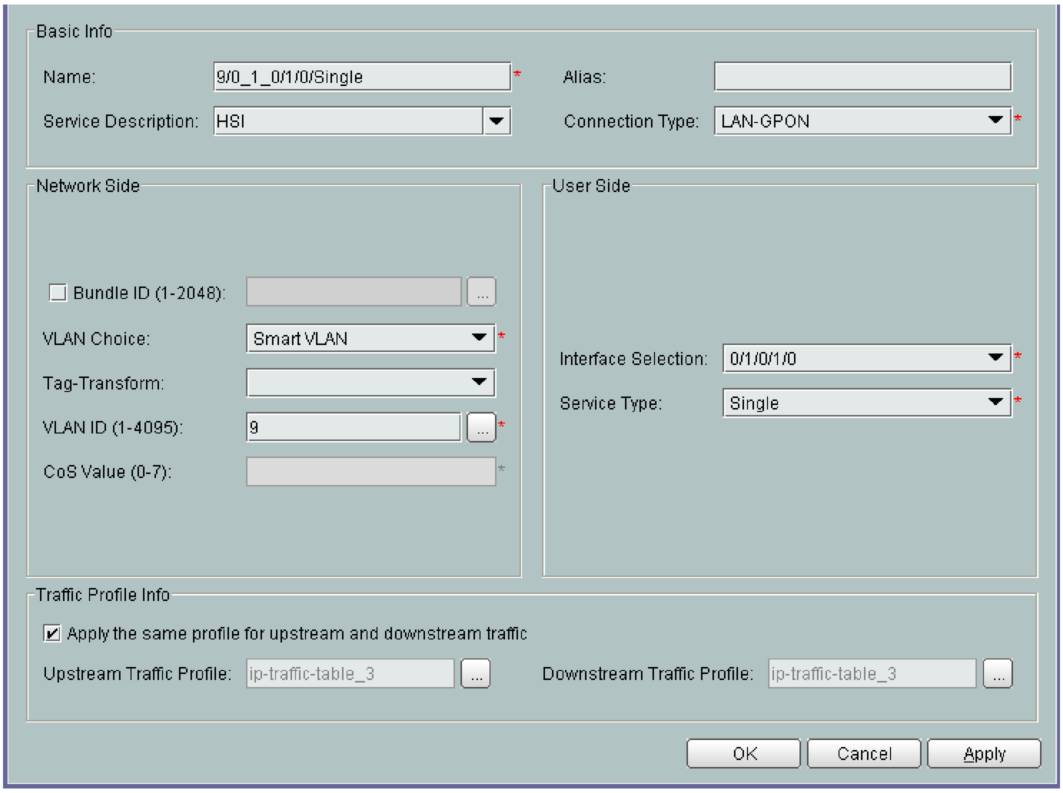


Basic Info
ID(1-32768):
Name: 1/0_3_0/128/Single *
Alias:
Service Description: HSI
Connection Type: LAN-GPON *

Network Side
☐ Bundle ID(1-8192):
VLAN Choice: Smart VLAN *
Tag-Transform: Default
VLAN ID(1-4095): 1 *
Cos value(0-7): *

User Side
Interface Selection: 0/3/0/128 *
Service Type: Single *

Traffic Profile Info
☑ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile: FTTx
Downstream Traffic Profile: FTTx



Basic Info
Name: 9/0_1_0/1/0/Single *
Alias:
Service Description: HSI
Connection Type: LAN-GPON *

Network Side
☐ Bundle ID (1-2048):
VLAN Choice: Smart VLAN *
Tag-Transform:
VLAN ID (1-4095): 9 *
CoS Value (0-7): *

User Side
Interface Selection: 0/1/0/1/0 *
Service Type: Single *

Traffic Profile Info
☑ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile: ip-traffic-table_3
Downstream Traffic Profile: ip-traffic-table_3

Step 7 Click **OK**.

----End

7.3 Configuring the GPON Access Service - Profile Mode

This topic describes how to configure the GPON access service. The GPON access supports high-bandwidth transmission, which effectively removes the bandwidth bottleneck in the access through twisted pairs and meets the users' requirements on high-bandwidth services, such as high definition TV (HDTV) and live programs.

Prerequisites

- The profile mode can be enabled only when the version is later than V800R006.
- The corresponding VLAN must be already created in the system. For details on adding a VLAN, see **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN must be already configured. For details on configuring the upstream port of a VLAN, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MEF IP traffic profile or IP profile must be already configured in the system. For details on configuring the MEF IP traffic profile, see **5.2 Configuring an MEF IP Traffic Profile**. For details on configuring the IP traffic profile, see Configuring an IP Traffic Profile.

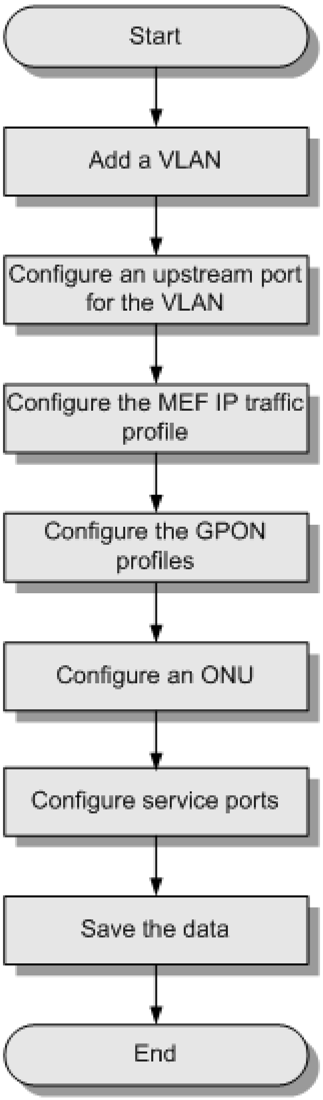
In the profile mode, you are required to configure the line profiles and service profiles and download to the NEs so that they can be applied to the GPON access services.

- The line profile must be already configured in the system. For details on configuring the line profile, see **7.1.3 Configuring a GPON Line Profile**.
- The service profile must be already configured in the system. For details on configuring the service profile, see **7.1.4 Configuring a GPON Service Profile**.

Context

Figure 7-2 shows the flowchart for configuring the GPON access service.

Figure 7-2 Flowchart for configuring the GPON access service


Start
Add a VLAN
Configure an upstream port for the VLAN
Configure the MEF IP traffic profile
Configure the GPON profiles
Configure an ONU
Configure service ports
Save the data
End

7.3.1 Configuring the ONU

This topic describes how to add an ONU and configure the basic attribute parameters of the ONU. To add an ONU offline and configure the service of the ONU offline, perform this operation. After the ONU goes online, the configuration data is applied to the ONU through the ONU management protocol, and then the configuration of the ONU is complete.

Procedure

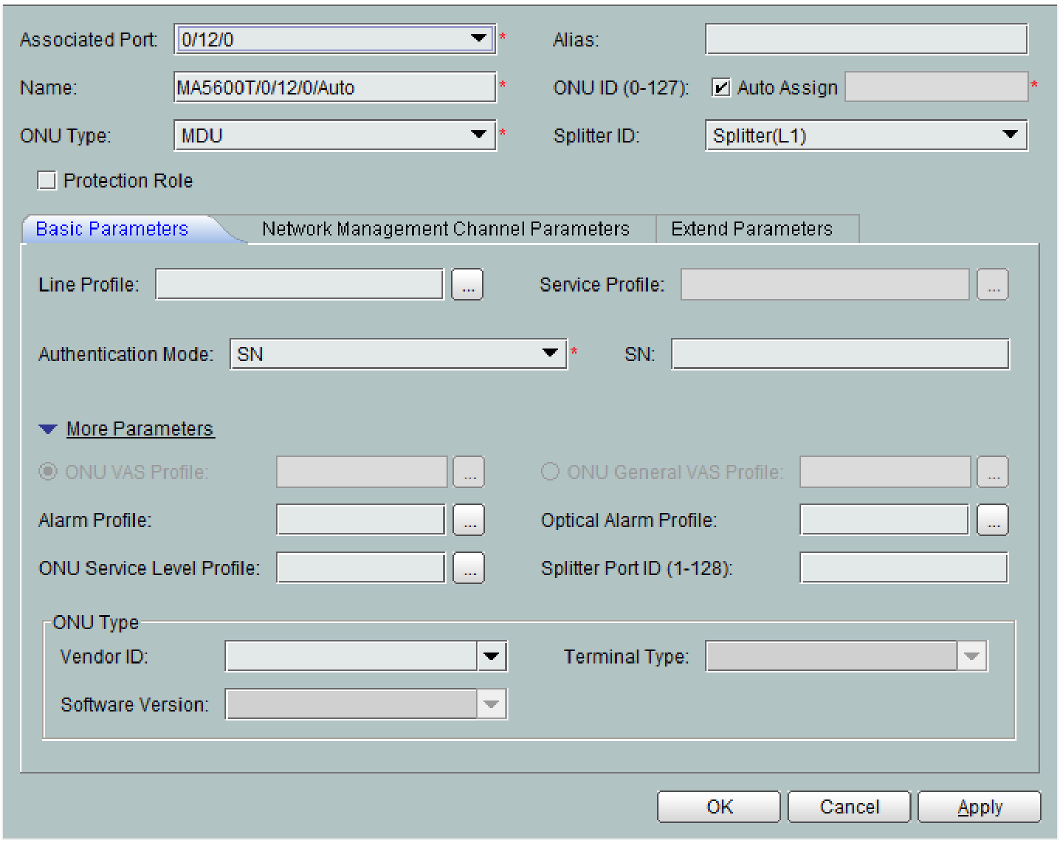
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

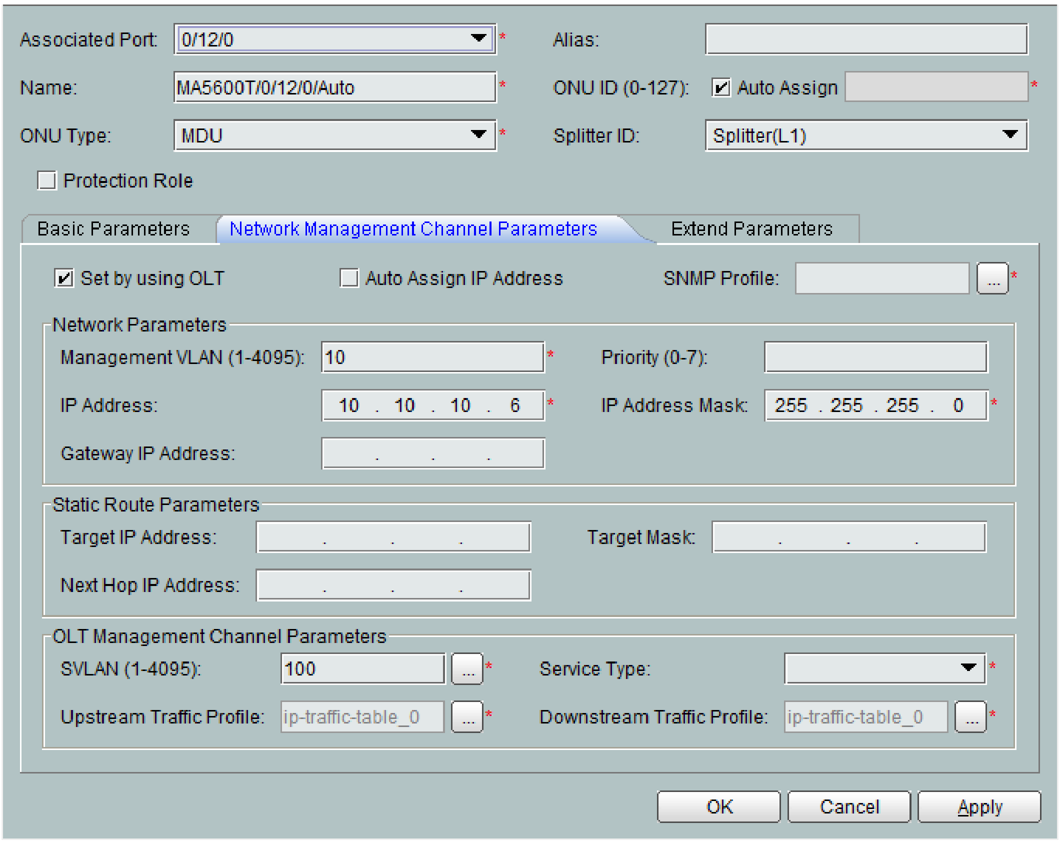
Step 3 Click the **GPON ONU** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Associated Port: 0/12/0
Name: MA5600T/0/12/0/Auto
ONU Type: MDU
ONU ID (0-127): ☑ Auto Assign
Splitter ID: Splitter(L1)
☐ Protection Role
Authentication Mode: SN
● ONU VAS Profile:
○ ONU General VAS Profile:



Associated Port: 0/12/0
Name: MA5600T/0/12/0/Auto
ONU Type: MDU
ONU ID (0-127): ☑ Auto Assign
Splitter ID: Splitter(L1)
☐ Protection Role
☑ Set by using OLT
☐ Auto Assign IP Address
Management VLAN (1-4095): 10
IP Address: 10 . 10 . 10 . 6
IP Address Mask: 255 . 255 . 255 . 0
SVLAN (1-4095): 100
Upstream Traffic Profile: ip-traffic-table_0
Downstream Traffic Profile: ip-traffic-table_0

NOTE

- **Terminal Type** and **Software Version** that you set must be the same as the version information of the actual ONU.
- When the **Set By using OLT** check box is cleared, ONUs are configured and managed remotely on the OLT through the OMCI protocol.
- When the **Set By using OLT** check box is selected, ONUs are configured and managed remotely on the OLT through the SNMP protocol.
- Do not add the SNMP parameters on the ONU through the serial port, but issue the SNMP profile from the OLT to the ONU only.
- If **ONU Type** is **MDU** and the **OLT sets network management channel parameters** check box is selected, OLT management channel parameters must be set.

Step 6 Click **OK**.

----End

7.3.2 Configuring the Service Port

This topic describes how to configure the service port for the GPON access service.

Prerequisites

- The VLAN to which the service port belongs must have been configured: **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN must have been configured: **5.3 Configuring the Upstream Port of a VLAN**.
- A suitable MEF IP traffic profile must have been configured: **5.2 Configuring an MEF IP Traffic Profile**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

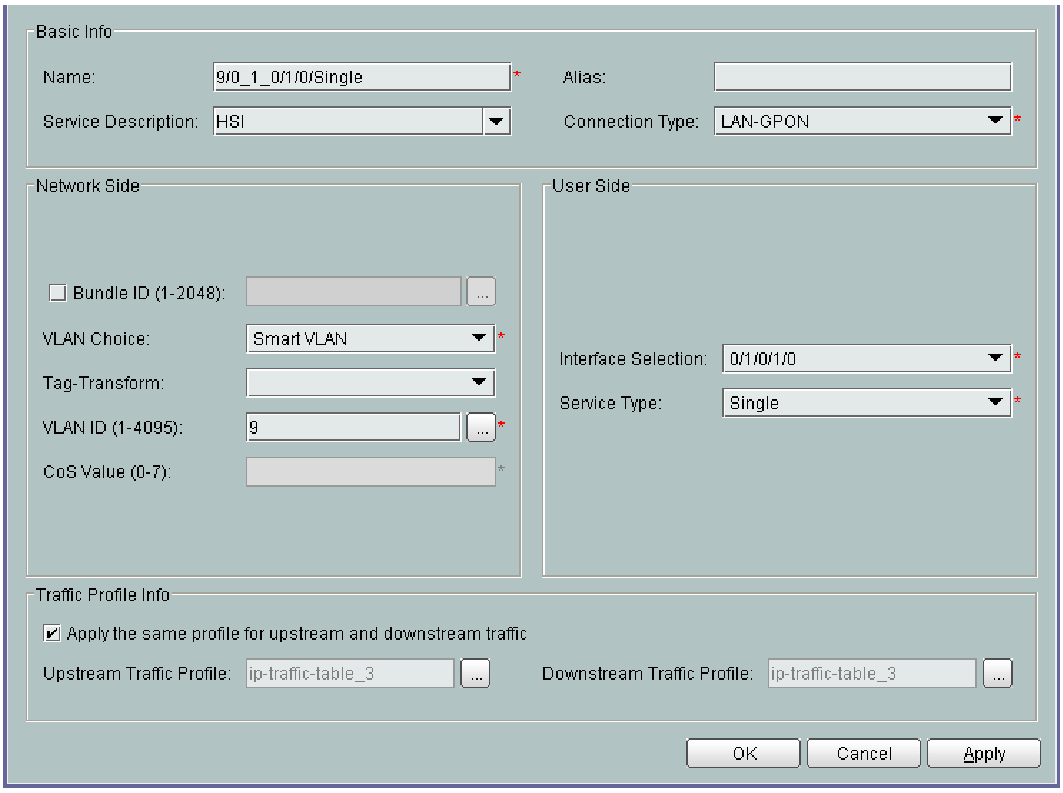
Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 On the **GPON ONU** tab page, set the filter criteria or click ︾ to display the required GPON ONUs.

Step 4 Select a record from the list, and click the **Service Port Info** tab in the lower pane.

Step 5 Right-click the service port list in the lower part of the page, and then choose **Add**.

Step 6 In the dialog box that is displayed, set the parameters.



Basic Info

Name: 9/0_1_0/1/0/Single *

Alias:

Service Description: HSI

Connection Type: LAN-GPON *

Network Side

☐ Bundle ID (1-2048):

VLAN Choice: Smart VLAN *

Tag-Transform:

VLAN ID (1-4095): 9 *

CoS Value (0-7):

User Side

Interface Selection: 0/1/0/1/0 *

Service Type: Single *

Traffic Profile Info

☑ Apply the same profile for upstream and downstream traffic

Upstream Traffic Profile: ip-traffic-table_3

Downstream Traffic Profile: ip-traffic-table_3

Step 7 Click **OK**.

----End

7.4 Provisioning a GPON FTTH Service (OLT in Profile Mode)

This topic uses gigabit-capable passive optical network (GPON) as an example to describe how to quickly provision an xPON fiber to the home (FTTH) service in profile mode. In this scenario, users can configure service channels for an OLT PON port in a window, including channels for Internet access, voice over IP (VoIP), and multicast services.

Prerequisites

- The OLT has been added to the U2000 and ONTs have been connected to the OLT by fibers. In addition, the ONT communicates with the OLT successfully.
- The corresponding virtual local area network (VLAN) has been added to the system. For details on how to add a VLAN, see **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN has been configured. For details on how to configure the upstream port of a VLAN, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MEF IP traffic profile has been already configured on the system. For details on how to configure the MEF IP traffic profile, see **5.2 Configuring an MEF IP Traffic Profile**.

Configuring ONT value-added services by clicking **Configure Value-Added Service** or switching to the **Add Service** mode by clicking **Switch** on the upper right corner, In **Add Service** mode, you are required to configure the line profiles, service profiles and ONT VAS Profile so that they can be applied to the GPON access services.

- The line profile has been configured on the system. For details on how to configure a line profile, see **7.1.3 Configuring a GPON Line Profile**.
- The service profile has been configured on the system. For details on how to configure a service profile, see **7.1.4 Configuring a GPON Service Profile**.
- The ONT VAS Profile has been configured on the system. For details on how to configure a ONT VAS Profile, see **7.1.7 Configuring the ONT Value-Added Service Configuration Profile**.

Procedure

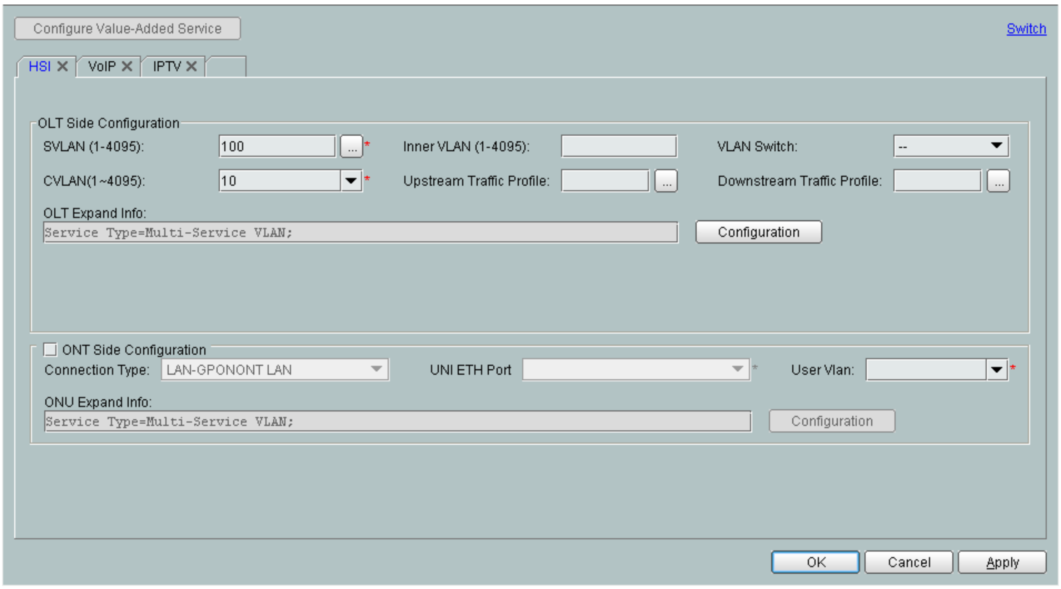
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 Click the **ONU Details** tab.

Step 4 Click … next to **Name**. In the dialog box that is displayed, select the required ONT and click **OK**.

Step 5 In the lower part of **ONU Details** tab page, click **Provisioning Service**. In the dialog box that is displayed, configure the GPON FTTH service.



SVLAN (1-4095): 100

CVLAN(1~4095): 10

VLAN Switch: --

OLT Expand Info: Service Type=Multi-Service VLAN;

☐ ONT Side Configuration

Connection Type: LAN-GPONONT LAN

ONU Expand Info: Service Type=Multi-Service VLAN;

NOTE

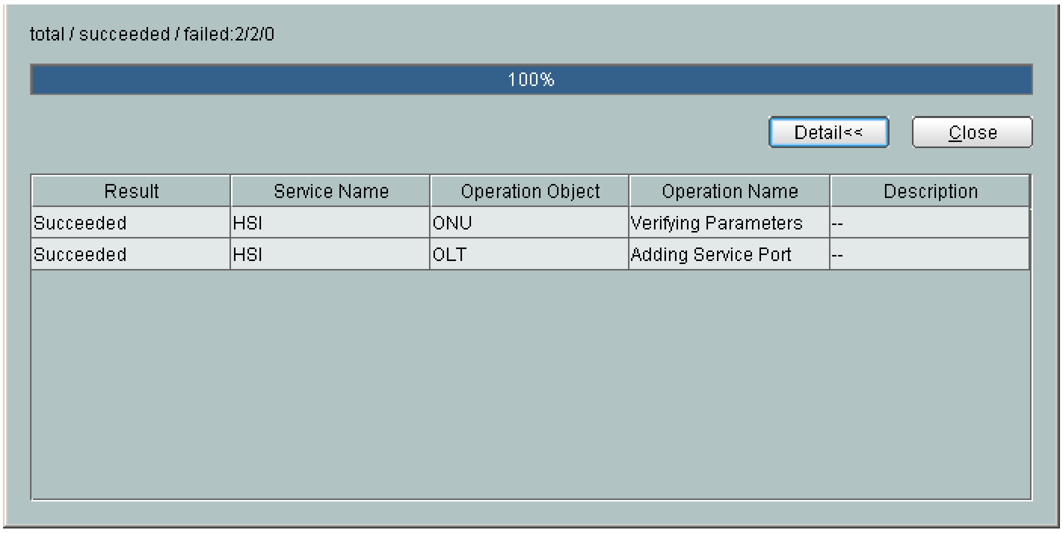
- **SVLAN** refers to the upstream VLAN on the OLT side.
- **CVLAN** refers to the downstream VLAN on the OLT side. It can also be called a customer VLAN. The value of this parameter must be the same as the **VLAN ID(1-4094)** value of the GEM connection in the line profile to which the ONT is bound.

The following functions are provided to optimize certain operations:

- Provisioning other FTTH services by adding tab pages, including but are not limited to Internet access, voice, and multicast services. On a new tab page, you can set **Service Type**, **Service Name** to provision a service. **Service Name** is a character string consisting of a maximum of four bytes.
- Storing certain information. When you click **OK** to complete the configuration, certain parameter settings are stored. The stored settings are displayed for reference when you set the same parameters next time.
- Configuring ONT value-added services by clicking **Configure Value-Added Service** or switching to the **Add Service** mode by clicking **Switch** on the upper right corner.
- Displaying important parameter settings in the blank area. You can click certain buttons to display a dialog box. After you set the parameters in the dialog box, the dialog box is closed and the parameter settings are displayed in the blank area of the preceding window.

Step 6 Click **OK**.

Step 7 In the **Progress** dialog box, check the operation result.



total / succeeded / failed:2/2/0

Result	Service Name	Operation Object	Operation Name	Description
Succeeded	HSI	ONU	Verifying Parameters	--
Succeeded	HSI	OLT	Adding Service Port	--

----End

Result

The GPON FTTH service is provisioned successfully.

7.5 Provisioning a GPON FTTB Service (OLT in Profile Mode)

This topic uses gigabit-capable passive optical network (GPON) as an example to describe how to quickly provision an xPON FTTB service in profile mode. In an xPON FTTB network, the OLT, functioning as an OLT, connects MDUs or ONUs over the ODN network. The ONUs or MDUs then provide services for users. Depending on the access modes of MDUs, users can access an MDU in LAN mode or xDSL mode to access composite services, including voice, Internet access, and multicast services.

Prerequisites

- The OLT communicates successfully with MDUs.
- The corresponding VLAN has been added to the system. For details on how to add a VLAN, see **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN has been configured. For details on how to configure the upstream port of a VLAN, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MEF IP traffic profile has been configured on the system. For details on how to configure the MEF IP traffic profile, see **5.2 Configuring an MEF IP Traffic Profile**.

Configuring ONT value-added services by clicking **Configure Value-Added Service** or switching to the **Add Service** mode by clicking **Switch** on the upper right corner. In **Add Service** mode, you need to configure a line profile rather than a service profile. For information on how to configure a line profile, see **7.1.3 Configuring a GPON Line Profile**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

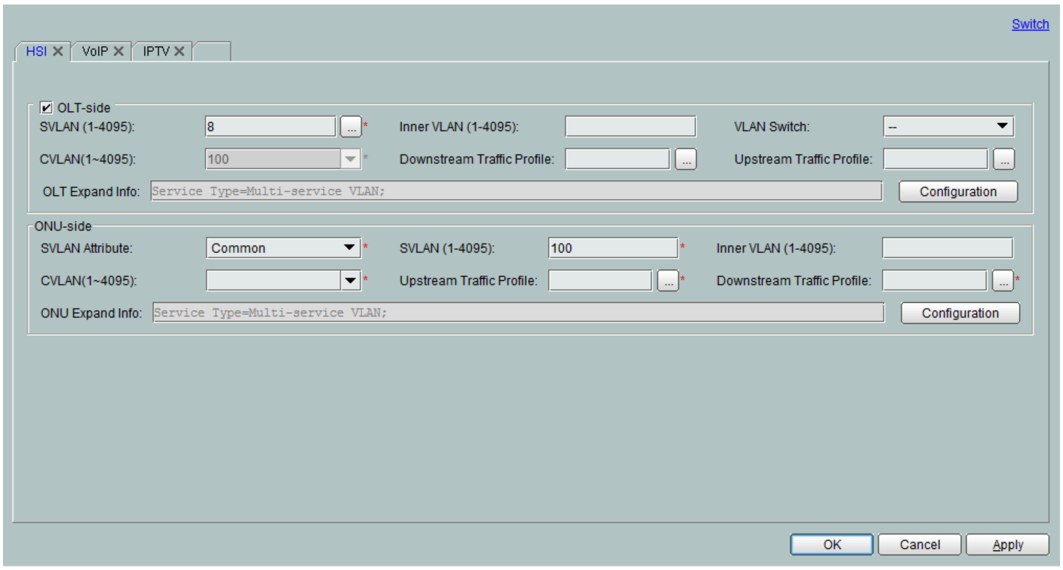
Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 Click the **ONU Details** tab.

Step 4 Click ... next to **Name**. In the dialog box that is displayed, select the required MDU and click **OK**.

Step 5 In the lower pane, click the **Ethernet Port**, **ADSL** or **VDSL2** tab, and specify the filter criteria or click ⩔ to display the ports.

Step 6 In the Ethernet port list, select a record and click **Provisioning Service**. In the dialog box that is displayed, configure the GPON FTTB service.



☑ OLT-side
SVLAN (1-4095): 8
CVLAN(1~4095): 100
Inner VLAN (1-4095):
Downstream Traffic Profile:
VLAN Switch: --
Upstream Traffic Profile:
OLT Expand Info: Service Type=Multi-service VLAN;

ONU-side
SVLAN Attribute: Common
CVLAN(1~4095):
SVLAN (1-4095): 100
Upstream Traffic Profile:
Inner VLAN (1-4095):
Downstream Traffic Profile:
ONU Expand Info: Service Type=Multi-service VLAN;

NOTE

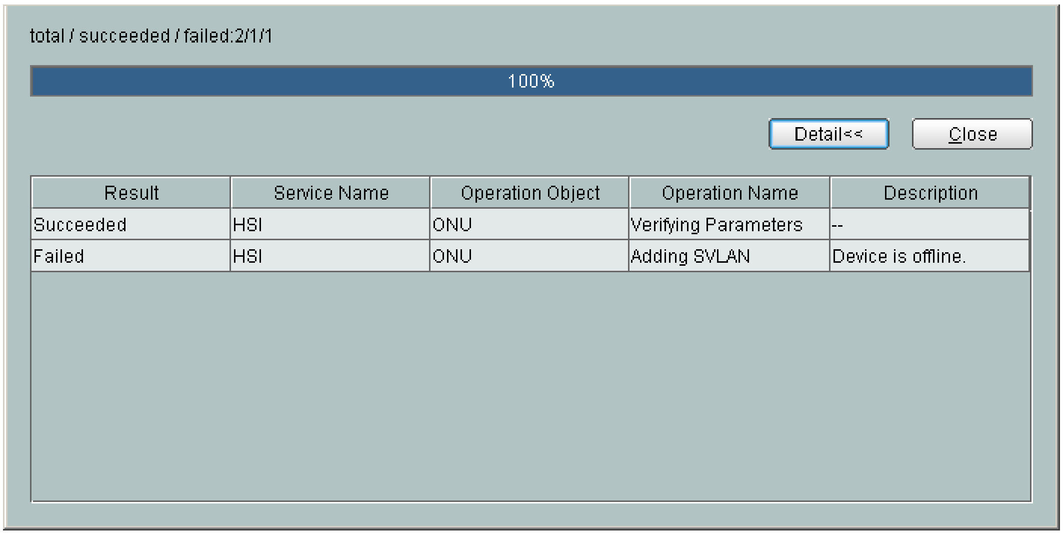
- In the **OLT Side Configuration** area:
  - **SVLAN** refers to the upstream VLAN of the OLT.
  - **CVLAN** is associated with **SVLAN** in the **ONU Side Configuration** area.
- In the **ONU Side Configuration** area:
  - **SVLAN** refers to the downstream VLAN of the OLT. It can also be called a customer VLAN. The value of this parameter must be the same as the value of the **VLAN ID(1-4094)** parameter for GEM connection in the bound line profile.
  - **CVLAN** refers to the downstream VLAN of the ONU. It is used to identify users.

The following functions are provided to optimize certain operations:

- Provisioning other FTTB services such as Internet access, voice, and multicast services by adding tab pages. On a new tab page, you can set **Service Type**, **Service Name** to provision a service. **Service Name** is a character string consisting of a maximum of 4 bytes.
- Storing certain information. When you click **OK** to complete the configuration, certain parameter settings are stored. The stored settings are displayed for reference the next time you set the same parameters.
- Switching to the **Add Service** mode by clicking **Switch** on the upper right corner.
- Displaying important parameter settings in the blank area. You can click certain buttons to display a dialog box. After you set the parameters in the dialog box, the dialog box is closed and the parameter settings are displayed in the blank area of the preceding window.

Step 7 Click **OK**.

Step 8 In the **Progress** dialog box, check the operation result.



total / succeeded / failed:2/1/1

100%

Result	Service Name	Operation Object	Operation Name	Description
Succeeded	HSI	ONU	Verifying Parameters	--
Failed	HSI	ONU	Adding SVLAN	Device is offline.

----End

Result

The GPON FTTB service is provisioned successfully.

7.6 Configuring the GPON Upstream Service

This topic describes how to configure the GPON upstream service. As a multi-dwelling unit (MDU), the MA5600T, MA5603T or MA5606T features wide coverage, flexible networking, and low maintenance cost of the GPON network. The MA5600T, MA5603T or MA5606T works with the OLT to form a GPON network, which provides high-bandwidth broadband access for users. In addition, the MA5600T, MA5603T or MA5606T supports a higher user density at the OLT end.

Prerequisites

- A corresponding VLAN must have been added to the system. For details on adding the VLAN, see **4.1.2.2 Adding a VLAN**.
- The Ethernet access service must have been configured in the system. For details on configuring the Ethernet access, see **5.4 (Optional) Configuring the Attributes of an Ethernet Port**.

Context

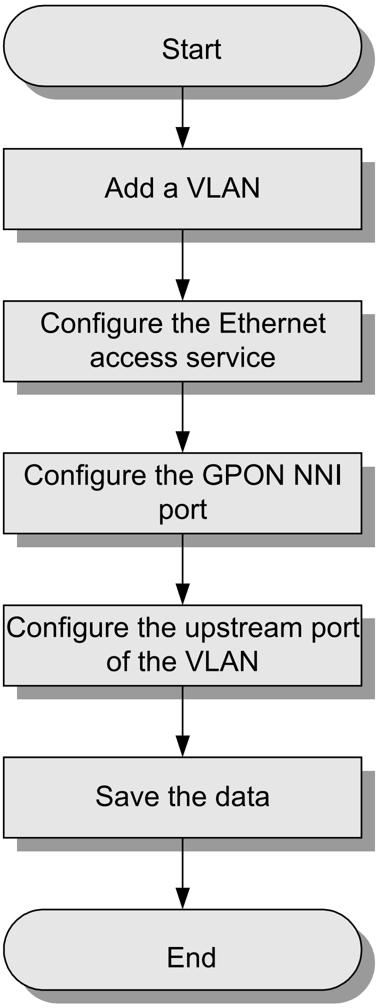
This topic describes only the configuration on the ONU side when the MA5600T, MA5603T or MA5606T works as a MDU. For details on the configuration on the OLT side, see **7.2 Configuring the GPON Access Service - Distributed Mode** or **7.3 Configuring the GPON Access Service - Profile Mode**.

The MA5600T, MA5603T or MA5606T provides GPON upstream ports for working with the OLT to form a GPON network. The principles of the GPON upstream service are as follows:

1. Through the Physical Layer OAM (PLOAM), the GPON upstream port of the MA5600T, MA5603T or MA5606T reports the port serial number to the OLT for registration. The OLT determines whether to register the GPON upstream port according to the internal serial number database.
2. After the GPON upstream port of the MA5600T, MA5603T or MA5606T registers with the OLT successfully, the OLT allocates the T-CONT to the port. The index of the T-CONT is Alloc ID which ranges from 0 to 4095.
3. The upstream packets of the MA5600T, MA5603T or MA5606T are mapped to a specified GEM port and then to the T-CONT.
4. You can configure the mapping actions of various traffic streams through the U2000.

Figure 7-3 shows the flowchart for configuring the GPON upstream service.

Figure 7-3 Flowchart for configuring the GPON upstream service


Start
Add a VLAN
Configure the Ethernet access service
Configure the GPON NNI port
Configure the upstream port of the VLAN
Save the data
End

7.6.1 Configuring the GPON NNI Port

This topic describes how to configure the parameters of the GPON upstream port so that the GPON upstream port can be interconnected with the upper layer OLT.

Procedure

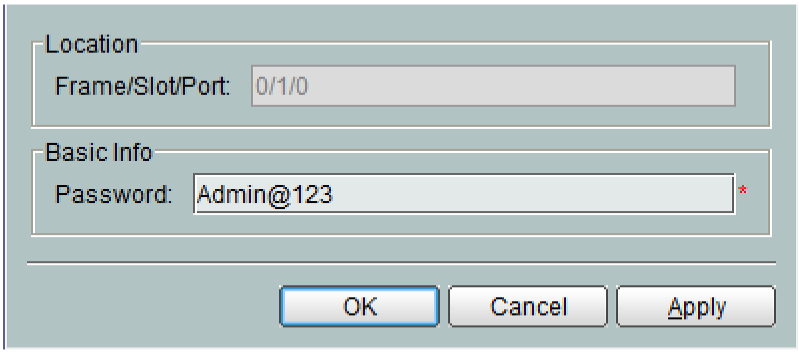
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **GPON** > **GPON NNI Port** from the navigation tree.

Step 3 On the **GPON NNI Port** tab page, set the filter criteria to display the required GPON NNI ports.

Step 4 Select the port to be configured, right-click, and then choose **GPON** > **Configure**.

Step 5 In the dialog box that is displayed, set **Password** of the port.



Location

Frame/Slot/Port: 0/1/0

Basic Info

Password: Admin@123 *

NOTE

To ensure system security, password must be complex enough. For example, a password must contain six or more characters of two types. The allowed characters are digits, letters, and special characters. Remember to change passwords regularly.

Step 6 Click **OK**.

----End

7.6.2 Configuring the Upstream Port of a VLAN

This topic describes how to add a GPON upstream port to a VLAN so that the port can communicate with the other ports of the VLAN. To forward the packets with a certain VLAN tag through the upstream port, you need to add the upstream port to the VLAN. After the upstream port is added to the VLAN successfully, the packets carrying the corresponding VLAN tag can be forwarded through this port.

Prerequisites

A corresponding VLAN must have been added to the system. For details on adding the VLAN, see **4.1.2.2 Adding a VLAN**.

Procedure

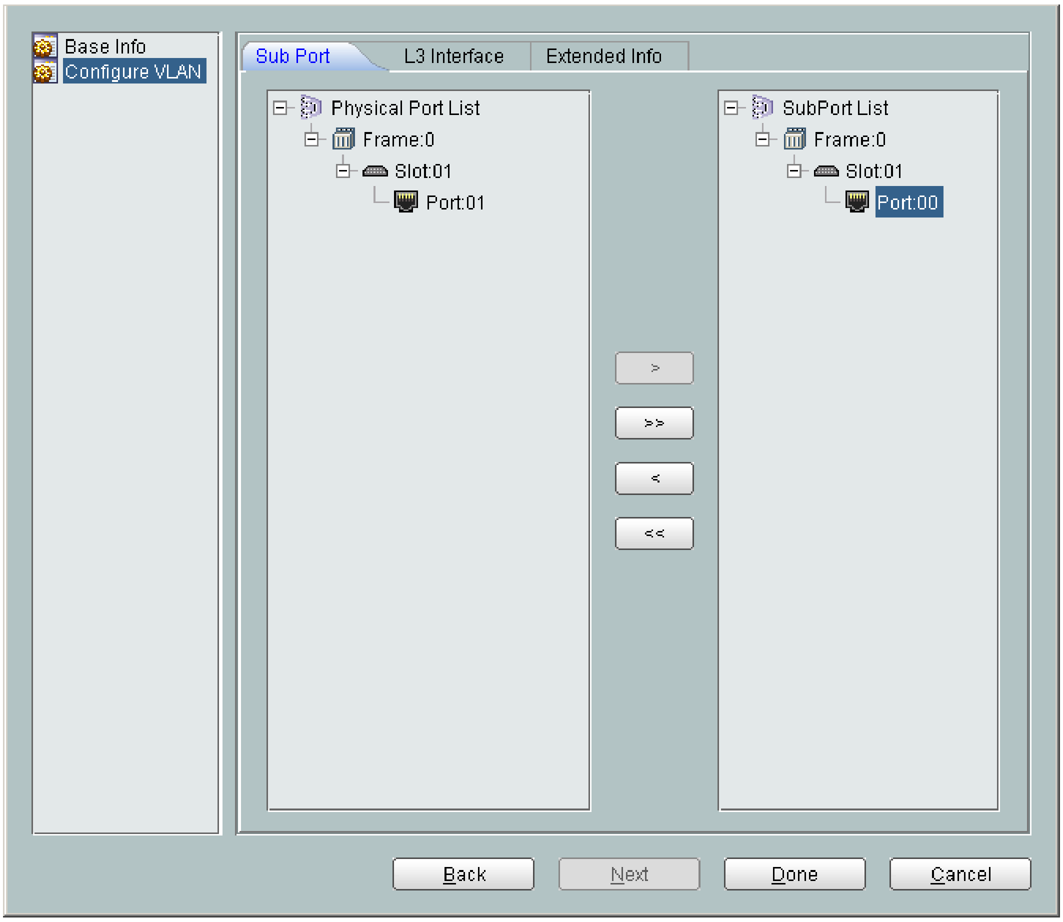
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.

Step 4 Select a VLAN, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, click the **Sub Port** tab, and add the upstream port to the subport list.



Step 6 Click **OK**.

----End

7.7 Configuring the ONT Auto-online Function

This topic describes how to configure the ONT auto-online function. If the ONT auto-find function is enabled on the OLT, the OLT obtains the registration information of the ONT when an ONT goes online. By default, the ONT auto-find function of a GPON port is disabled.

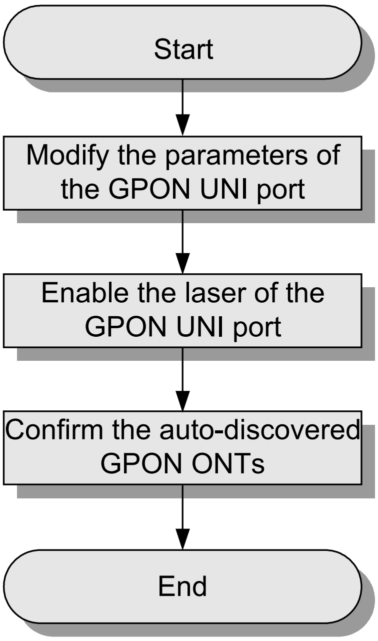
Prerequisites

The automatic discovery interval of the ONT must be already configured. For details on configuring an ONT automatic discovery interval, see **7.1.8 Configuring an ONT Automatic Discovery Interval**.

Context

Figure 7-4 shows the flowchart for configuring the ONT auto-online function.

Figure 7-4 Flowchart for configuring the ONT auto-online function


Start
Modify the parameters of the GPON UNI port
Enable the laser of the GPON UNI port
Confirm the auto-discovered GPON ONTs
End

7.7.1 Configuring the GPON UNI Port

This topic describes how to configure the parameters of the GPON UNI port. By configuring the GPON UNI port, you can enable the **ONT auto discovery**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 On the **GPON UNI Port** tab page, set the filter criteria to display the required GPON UNI ports.

Step 4 Select a port from the list for modifying, right-click, and then choose **Modify**. In the dialog box that is displayed, set **ONT Auto Discovery** to **Enable**.

NOTE

Or you can select a port from the list for modifying, right-click, and then choose **Enable ONU Auto Discovery**.

Step 5 Click **OK**.

----End

7.7.2 Configuring the Optical Port of the GPON UNI Port

This topic describes how to enable the laser of the GPON port.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **GPON** > **GPON Management** from the navigation tree.

Step 3 On the **GPON UNI Port** tab page, set the filter criteria to display the required GPON UNI ports.

Step 4 Select a GPON UNI port from the list, right-click, and then choose **Enable GPON UNI Port**.

Step 5 In the dialog box that is displayed, and click **Yes**.

----End

7.7.3 Confirming the Auto-Find ONU

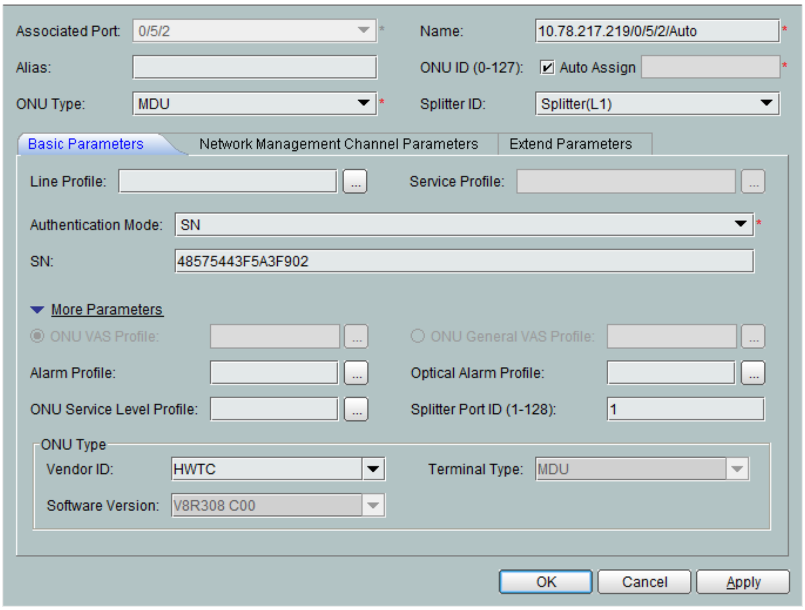
This topic describes how to confirm the auto-find ONU connected to a port. An auto-find ONU is in the auto-find state before it is confirmed. The auto-find ONU can start to work only after it is confirmed.

Procedure

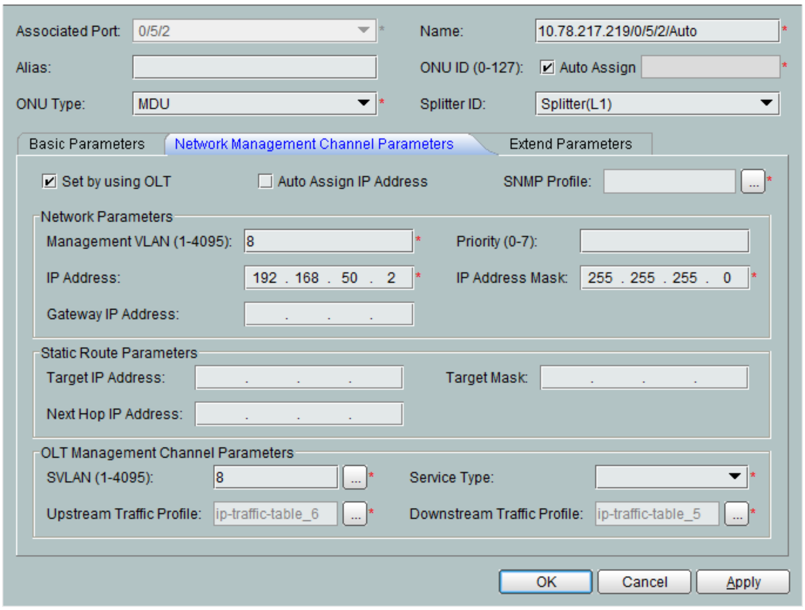
- **Path one:**
  1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
  2. Choose **GPON** > **GPON Management** from the navigation tree.
  3. On the **GPON UNI Port** tab page, set the filter criteria to display the required GPON UNI ports.
  4. Select a GPON UNI port from the list, and click the **ONU Info** tab in the lower part of the page.
  5. On the **ONU Info** tab page, click the **Auto Discover ONUs**.
  6. In the dialog box that is displayed, select an ONU that needs to be confirmed, and then click **Confirm**.

     NOTE

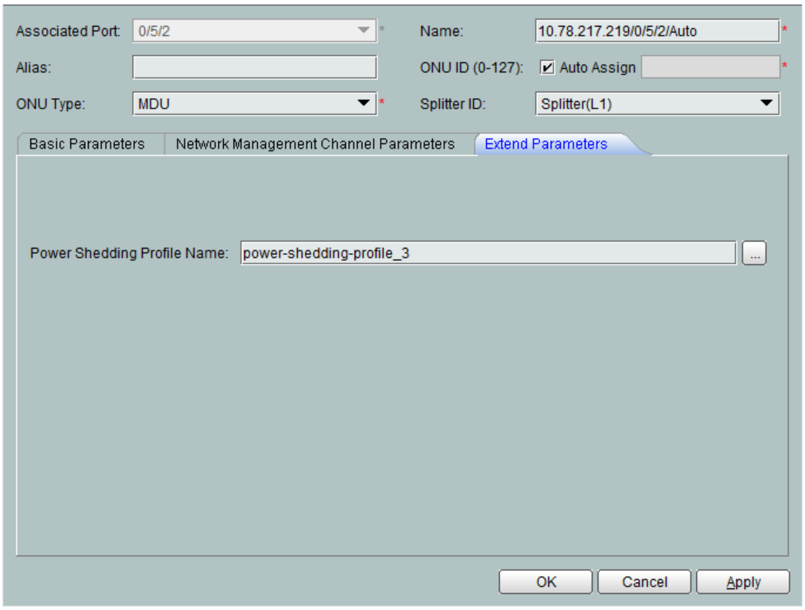
     Click the **Refresh** to obtain the ONUs in real time.
  7. In the dialog box that is displayed, set the parameters on the **Basic Parameters** , **Network Management Channel Parameters** and **Extend Parameters** tab pages.



Associated Port: 0/5/2 *
Name: 10.78.217.219/0/5/2/Auto *
Alias:
ONU ID (0-127): ☑ Auto Assign *
ONU Type: MDU *
Splitter ID: Splitter(L1)
Line Profile:
Service Profile:
Authentication Mode: SN *
SN: 48575443F5A3F902
● ONU VAS Profile:
○ ONU General VAS Profile:
Alarm Profile:
Optical Alarm Profile:
ONU Service Level Profile:
Splitter Port ID (1-128): 1
ONU Type
Vendor ID: HWTC
Terminal Type: MDU
Software Version: V8R308 C00



Associated Port: 0/5/2 *
Name: 10.78.217.219/0/5/2/Auto *
Alias:
ONU ID (0-127): ☑ Auto Assign *
ONU Type: MDU *
Splitter ID: Splitter(L1)
☑ Set by using OLT
☐ Auto Assign IP Address
SNMP Profile: *
Network Parameters
Management VLAN (1-4095): 8 *
Priority (0-7):
IP Address: 192 . 168 . 50 . 2 *
IP Address Mask: 255 . 255 . 255 . 0 *
Gateway IP Address: . . .
Static Route Parameters
Target IP Address: . . .
Target Mask: . . .
Next Hop IP Address: . . .
OLT Management Channel Parameters
SVLAN (1-4095): 8 *
Service Type: *
Upstream Traffic Profile: ip-traffic-table_6 *
Downstream Traffic Profile: ip-traffic-table_5 *



Associated Port: 0/5/2

Name: 10.78.217.219/0/5/2/Auto

Alias:

ONU ID (0-127): ☑ Auto Assign

ONU Type: MDU

Splitter ID: Splitter(L1)

Power Shedding Profile Name: power-shedding-profile_3

NOTE

- When **ONU Type** is set to **MDU** and the **Set by using OLT** check box is selected, ONUs are configured and managed remotely on the OLT through the SNMP protocol.
- Do not add the SNMP parameters on the ONU through the serial port, but issue the SNMP profile from the OLT to the ONU only.

8. Click **OK**.

- **Path two:**
  1. Choose **Configuration** > **Access Service Management** > **GPON ONU** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Service Management** > **GPON ONU** from the main menu (application style).
  2. Choose the **GPON ONU Auto Discovery** tab, and click **Filter**. Set the filter criteria to display the required ONUs.
  3. Right-click on an ONU that needs to be confirmed, and choose **Confirm ONU**. In the dialog box that is displayed, set the parameters on the **Basic Parameters** , **Network Management Channel Parameters** and **Extend Parameters** tab pages.
  4. Click **OK**.

----End

8 Configuring the EPON Access

About This Chapter

The Ethernet passive optical network (EPON) protocol is based on the Ethernet basic MAC protocol. Therefore, the EPON can be easily integrated with or interconnected to other Ethernet ports or devices, which helps reduce the cost of the access system and network. The EPON technology is used to implement the EPON access and the EPON upstream services. The EPON optical line terminal (OLT) configures and manages the service of the EPON optical network unit (ONT) through the extended OAM protocol.

Context

As one of the PON technologies, the EPON technology features the following common advantages of the PON technologies: high bandwidth, long transmission distance, flexible networking, and passive intermediate network nodes. The EPON technology, which is applicable to the broadband access network, can increase the bandwidth, optimize the performance, and reduce the maintenance cost of the network. Therefore, as a next-generation optical access technology, the EPON technology is preferred by the mainstream carriers. The EPON uses the wavelength division multiplexing (WDM) technology to process the signals in the dual directions at a time. The EPON provides the voice, data, and video services over a single optical fiber for users.

It uses the point-to-multipoint and passive optical transmission mode. Currently, EPON supports the following three transmission modes: 1 Gbit/s upstream/downstream symmetric mode, 10 Gbit/s upstream/downstream symmetric mode, and 10 Gbit/s downstream and 1 Gbit/s upstream asymmetrical mode, and a maximum transmission distance of 60 km. In the downstream direction, the EPON encrypts the broadcast transmission for different subscribers. In the upstream direction, the EPON uses the time division multiplexing (TDM) to support the broadband for different subscribers.

The EPON is composed of the OLT, the ODN and the ONU. The physical topology of the EPON is a point-to-multipoint tree structure, and the logic topology of the EPON is a structure of point-to-point links between the OLT and ONUs.

8.1 Configuring the EPON Profiles
The Ethernet passive optical network (EPON) profiles are a collection of profiles that contain the parameters required for configuring the EPON access services.

8.2 Configuring the EPON Access Service

This topic describes how to configure the EPON access service. The EPON access supports high-bandwidth transmission, which effectively removes the bandwidth bottleneck in the access through twisted pairs and meets the subscribers' requirements for high-bandwidth services, such as high definition TV (HDTV) and live programs.

8.3 Provisioning a EPON FTTH Service

This topic uses gigabit-capable passive optical network (EPON) as an example to describe how to quickly provision an EPON fiber to the home (FTTH) service . In this scenario, users can configure service channels for an OLT PON port in a window, including channels for Internet access, voice over IP (VoIP), and multicast services.

8.4 Provisioning a EPON FTTB Service

This topic describes how to quickly provision an EPON FTTB service. In an EPON FTTB network, the OLT, functioning as an OLT, connects MDUs or ONUs over the ODN network. The ONUs or MDUs then provide services for users. Depending on the access modes of MDUs, users can access an MDU in LAN mode or xDSL mode to access composite services, including VOIP, Internet access, and multicast services.

8.5 Configuring the EPON Upstream Service

This topic describes how to configure the EPON upstream service. As a multi-dwelling unit (MDU), the MA5600T, MA5603T or MA5606T takes advantage of the wide coverage, flexible networking, and low maintenance cost of the GPON network. The MA5600T, MA5603T or MA5606T, with the OLT, provides high-bandwidth broadband access for subscribers. In addition, the MA5600T, MA5603T or MA5606T improves the user density of the OLT.

8.6 Configuring the ONU Auto Discovery Function

This topic describes how to configure the ONU auto discovery function. If the ONU auto discovery function is enabled on the OLT, the OLT obtains the registration information about the ONU when an ONU goes online and then the ONU is in the auto discovered state. By default, the ONU auto discovery function of an EPON port is disabled.

8.1 Configuring the EPON Profiles

The Ethernet passive optical network (EPON) profiles are a collection of profiles that contain the parameters required for configuring the EPON access services.

Context

The EPON profiles of the OLT include the DBA profiles, EPON line profiles, MDU SNMP Profile and EPON service profiles.

8.1.1 Configuring an MDU SNMP Profile

The MDU Simple Network Management Protocol (SNMP) profile is a collection of SNMP parameters. You can configure the SNMP parameter profile of the MDU on the U2000, and configure the information about an MDU management channel to the OLT. Then, the OLT manages the MDU through the SNMP mode so that the remote deployment and maintenance for the MDU can be implemented.

Procedure

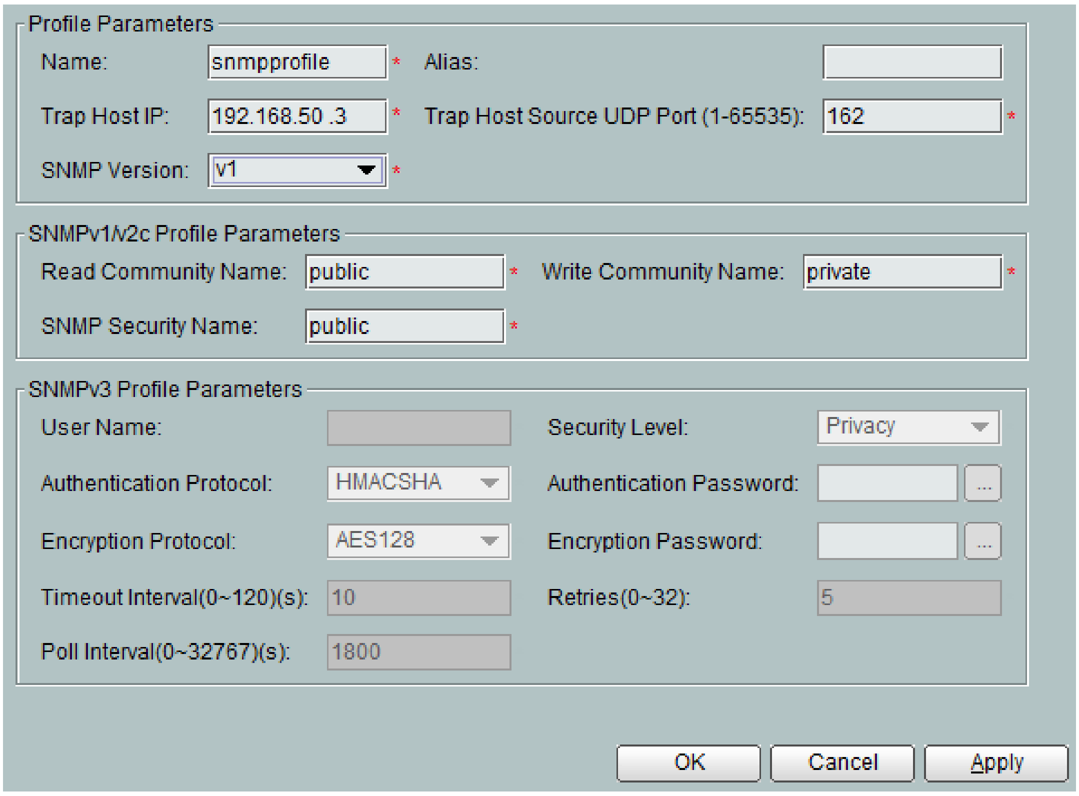
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.

Step 3 Click the **MDU SNMP Profile** tab.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: snmpprofile *
Alias:
Trap Host IP: 192.168.50 .3 *
Trap Host Source UDP Port (1-65535): 162 *
SNMP Version: v1 *
Read Community Name: public *
Write Community Name: private *
SNMP Security Name: public *
User Name:
Security Level: Privacy
Authentication Protocol: HMACSHA
Authentication Password:
Encryption Protocol: AES128
Encryption Password:
Timeout Interval(0~120)(s): 10
Retries(0~32): 5
Poll Interval(0~32767)(s): 1800

Step 6 Click **OK**.

Step 7 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 8 In the dialog box that is displayed, select the required NE(s), and click **OK**.

NOTE

The MDU SNMP profile that is generated by the U2000 can be referenced by the OLT only after the profile is applied to the corresponding OLT.

----End

8.1.2 Configuring a DBA Profile

A DBA profile contains the traffic parameters of an ONT. After a DBA profile is configured successfully and bound to an ONT, the system controls the traffic of the ONT based on the traffic parameters specified in the DBA profile.

Context

- A DBA profile can be used to control the rate of upstream traffic of an ONU.
- The OLT supports up to 512 DBA profiles.
- The profiles with the **Name** set to **dba-profile_1-dba-profile_9** are the default DBA profiles of the system. A default DBA profile provides typical values for traffic parameters. You can query the default DBA profiles but cannot add or delete them.

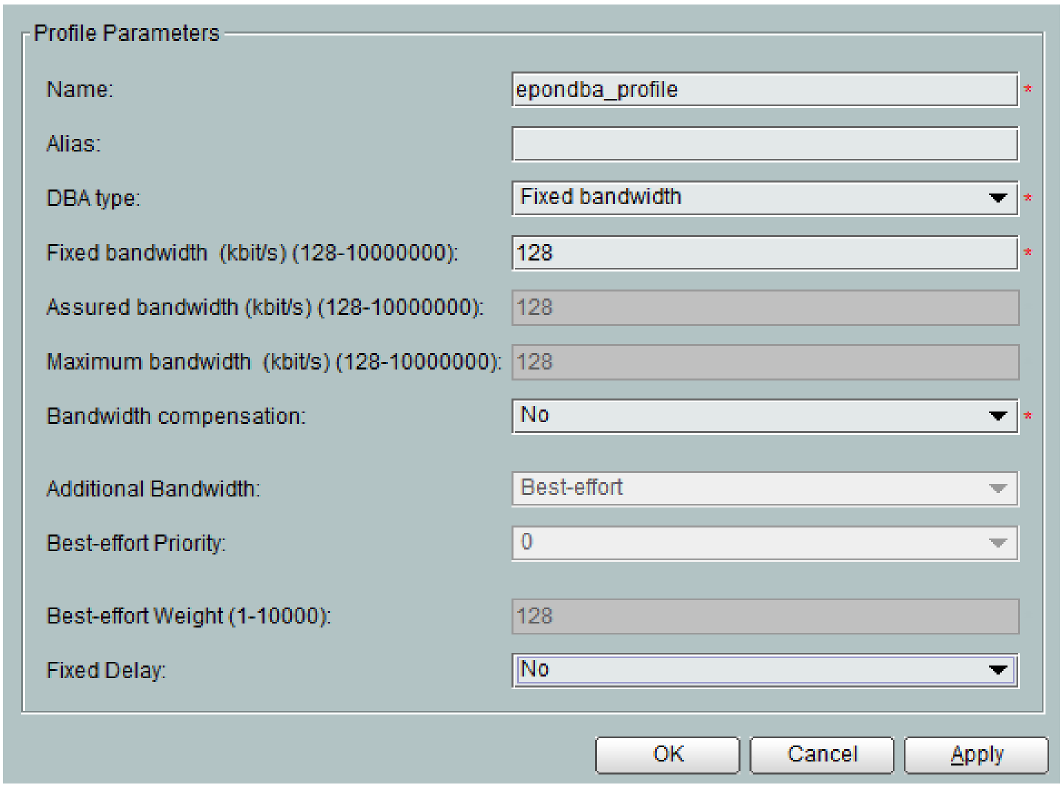
Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.

Step 3 Click the **DBA Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters.



Profile Parameters

Name: epondba_profile *
Alias:
DBA type: Fixed bandwidth *
Fixed bandwidth (kbit/s) (128-10000000): 128 *
Assured bandwidth (kbit/s) (128-10000000): 128
Maximum bandwidth (kbit/s) (128-10000000): 128
Bandwidth compensation: No *
Additional Bandwidth: Best-effort
Best-effort Priority: 0
Best-effort Weight (1-10000): 128
Fixed Delay: No

Step 5 Click **OK**.

Step 6 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 7 In the dialog box that is displayed, select the required NE(s), and click **OK**.

----End

8.1.3 Configuring an EPON Line Profile

The EPON line profile consolidates the parameters related to the ONT line into a profile.

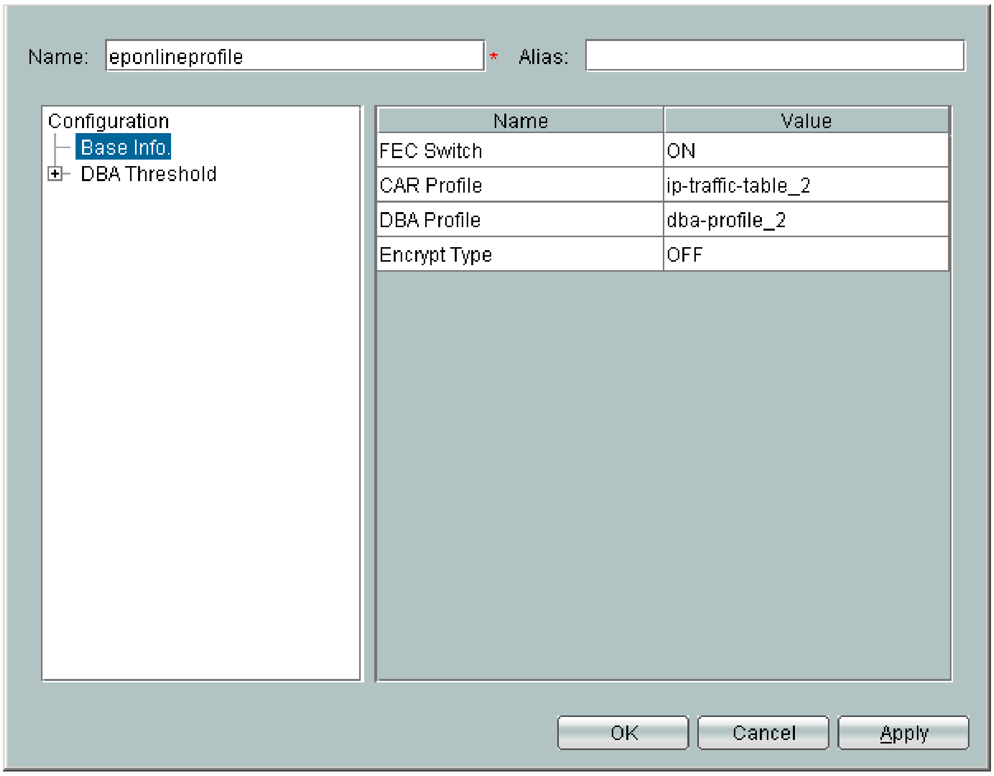
Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.

Step 3 Click the **EPON Line Profile** tab.In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 4 In the dialog box that is displayed, set **Name** and the parameters related to the line profile.



Name: eponlineprofile
Alias:

Name	Value
FEC Switch	ON
CAR Profile	ip-traffic-table_2
DBA Profile	dba-profile_2
Encrypt Type	OFF

Step 5 Click **OK**.

Step 6 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 7 In the dialog box that is displayed, select the required NE(s), and click **OK**.

----End

8.1.4 Configuring an EPON Service Profile

The EPON service profile consolidates the parameters related to the ONT service into a profile.

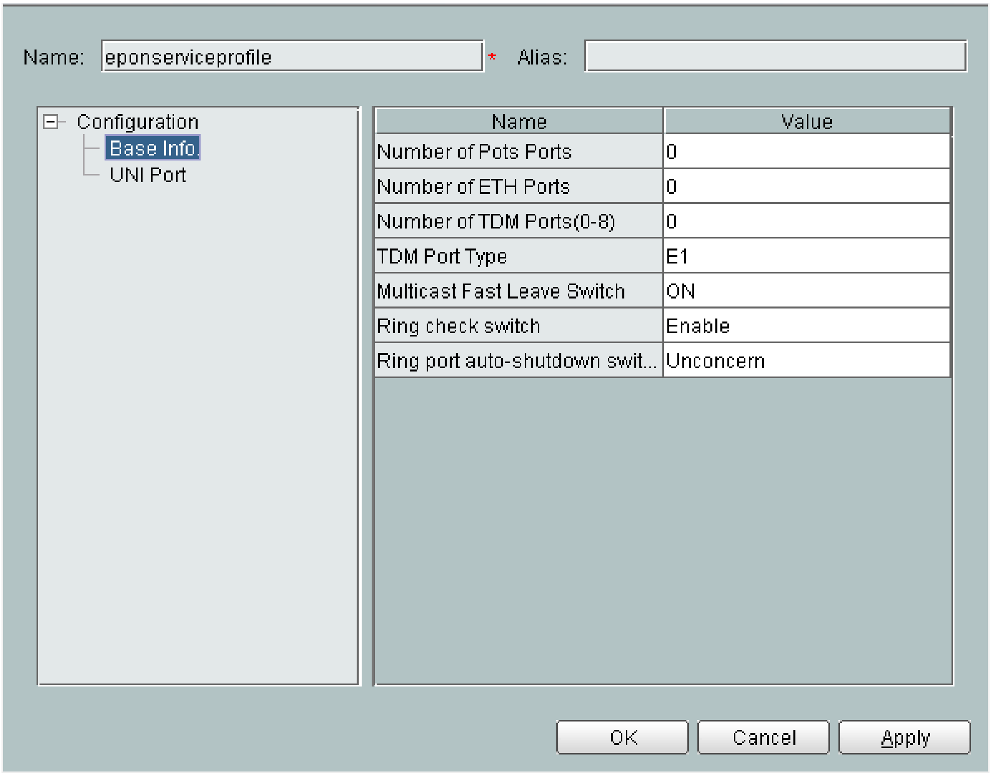
Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.

Step 3 Click the **EPON Service Profile** tab.In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

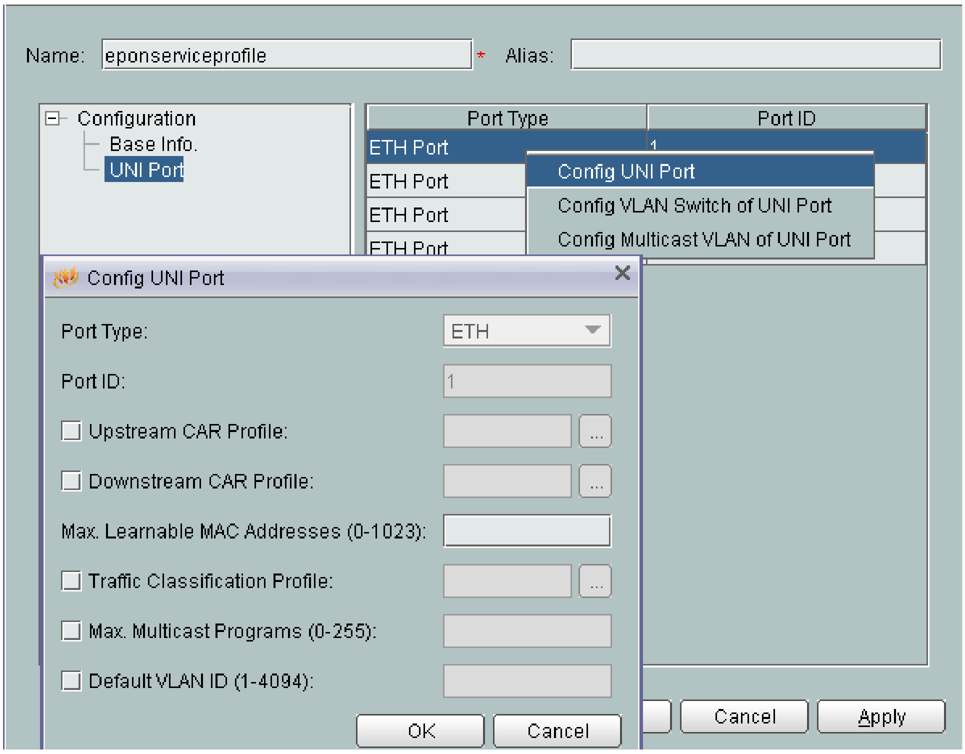
Step 4 In the dialog box that is displayed, set **Name** and the parameters related to the EPON service profile.



Name: eponserviceprofile * Alias:

Name	Value
Number of Pots Ports	0
Number of ETH Ports	0
Number of TDM Ports(0-8)	0
TDM Port Type	E1
Multicast Fast Leave Switch	ON
Ring check switch	Enable
Ring port auto-shutdown swit...	Unconcern

1. Choose **Basic Info** from the navigation tree, and then set the basic parameters of the profile.
2. Choose **UNI Port** from the navigation tree.
    a. In the right pane, right-click a record in the port list and choose **Config UNI Port** from the shortcut menu to set the parameters of the UNI port.



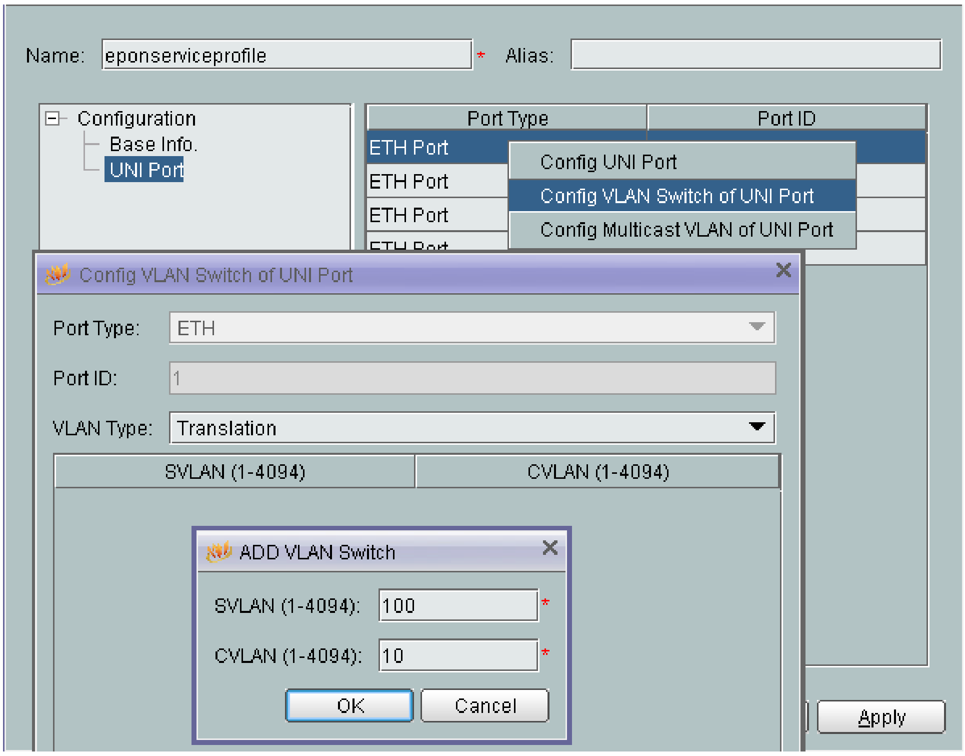
Name: eponserviceprofile

Port Type: ETH

Port ID: 1

Alias:
Configuration
Base Info.
UNI Port
Port Type
Port ID
ETH Port
ETH Port
ETH Port
ETH Port
Config UNI Port
Config VLAN Switch of UNI Port
Config Multicast VLAN of UNI Port
Config UNI Port
☐ Upstream CAR Profile:
☐ Downstream CAR Profile:
Max. Learnable MAC Addresses (0-1023):
☐ Traffic Classification Profile:
☐ Max. Multicast Programs (0-255):
☐ Default VLAN ID (1-4094):
OK
Cancel
Cancel
Apply

b. In the right pane, right-click a record in the port list and choose **Config VLAN Switch of UNI Port** from the shortcut menu to set the VLAN IDs on the user side and network side for the UNI port.



Name: eponserviceprofile

Port Type: ETH

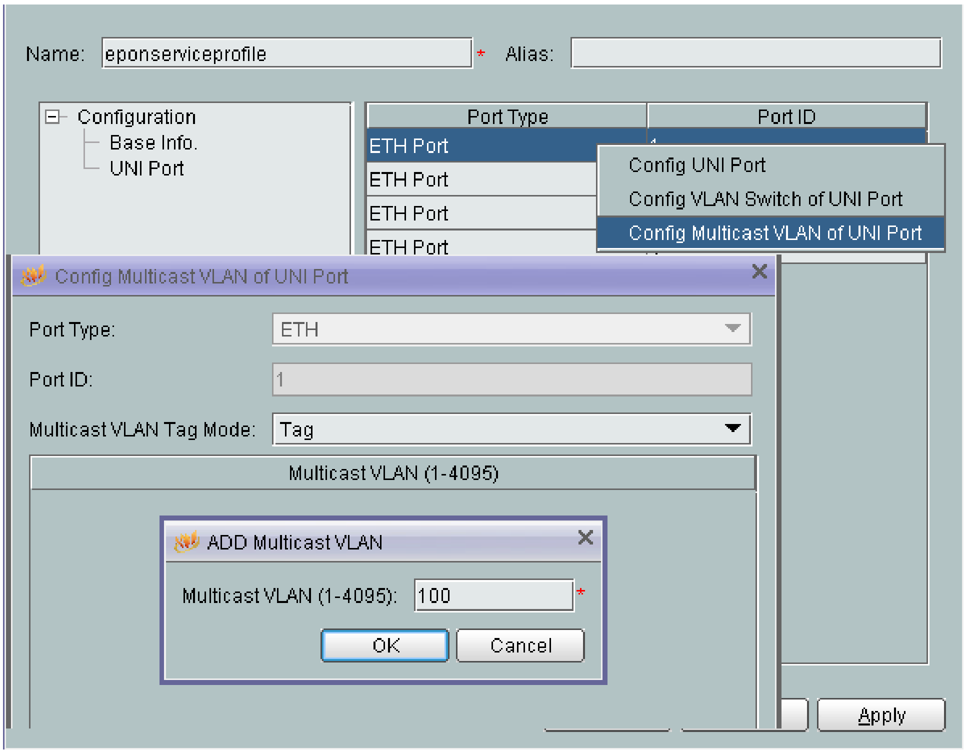
Port ID: 1

VLAN Type: Translation

SVLAN (1-4094): 100

CVLAN (1-4094): 10

c. In the right pane, right-click a record in the port list and choose **Config Multicast VLAN of UNI Port** from the shortcut menu to set the multicast VLAN ID for the UNI port.



Name: eponserviceprofile

Port Type: ETH

Port ID: 1

Multicast VLAN Tag Mode: Tag

Multicast VLAN (1-4095): 100

Step 5 Click **OK**.

Step 6 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 7 In the dialog box that is displayed, select the required NE(s), and click **OK**.

----End

8.1.5 Configuring an EPON ONT Capability Profile

The EPON ONT capability profile identifies the actual capability of the EPON ONT. The EPON ONT capability profile aims at pre-configuring ONTs. Before ONTs are installed at user homes, the ONTs do not exist. In this case, the actual capabilities of the ONTs are not determined, and services cannot be configured. Through the U2000, offline ONTs can be added, and EPON ONT capability profiles can be bound to the offline ONTs. Then, the service data can be configured. After the ONTs are installed at user homes, service data can be automatically applied to the ONTs.

Context

- The system supports up to 128 EPON ONT capability profiles.
- The profiles named **ont-profile_8** to **ont-profile_12** are the default EPON ONT capability profiles of the system. You can query the default EPON ONT capability profiles but cannot add or delete them.
- An EPON ONT capability profile must be bound to an ONT. The EPON ONT capability profile must match the hardware capability of the ONT.
- OLTs in distributed mode support EPON ONT capability profiles.

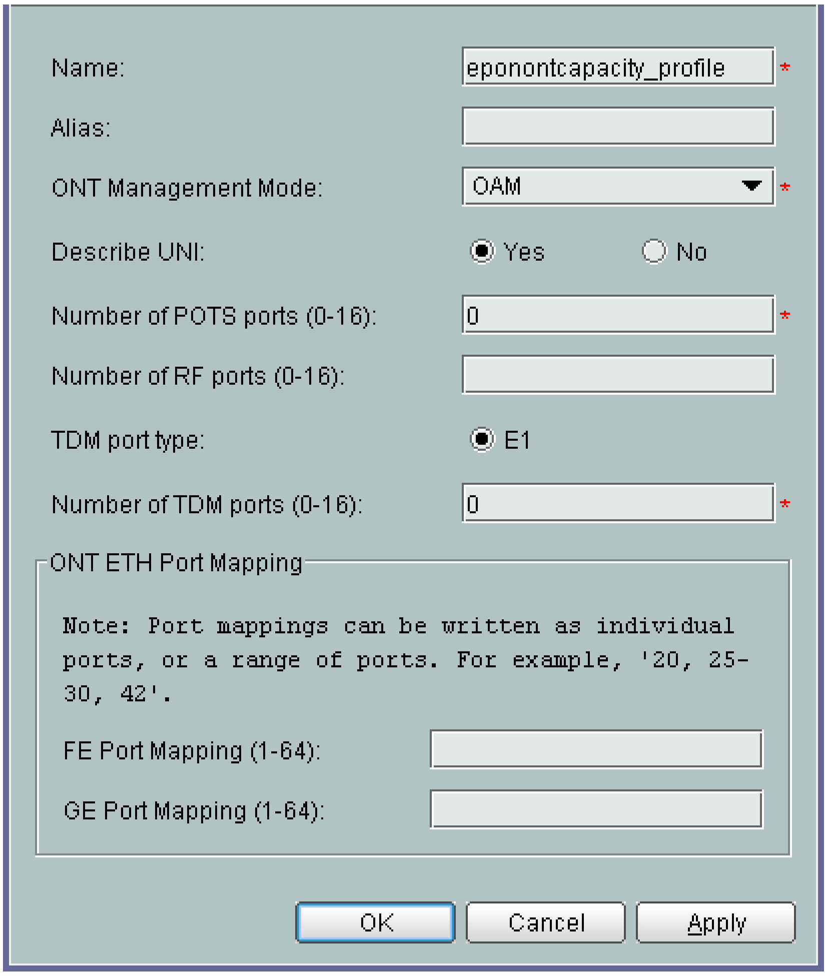
Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.

Step 3 Click the **EPON ONT Capacity Profile** tab. In the information list, right-click and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters.



Name: eponontcapacity_profile *
Alias:
ONT Management Mode: OAM *
Describe UNI: ● Yes ○ No
Number of POTS ports (0-16): 0 *
Number of RF ports (0-16):
TDM port type: ● E1
Number of TDM ports (0-16): 0 *

ONT ETH Port Mapping

Note: Port mappings can be written as individual ports, or a range of ports. For example, '20, 25-30, 42'.

FE Port Mapping (1-64):
GE Port Mapping (1-64):

Step 5 Click **OK**.

Step 6 In the information list, right-click the record and choose **Download to NE** from the shortcut menu.

Step 7 In the dialog box that is displayed, select the required NE(s), and click **OK**.

----End

8.1.6 Configuring the ONT Value-Added Service Configuration Profile

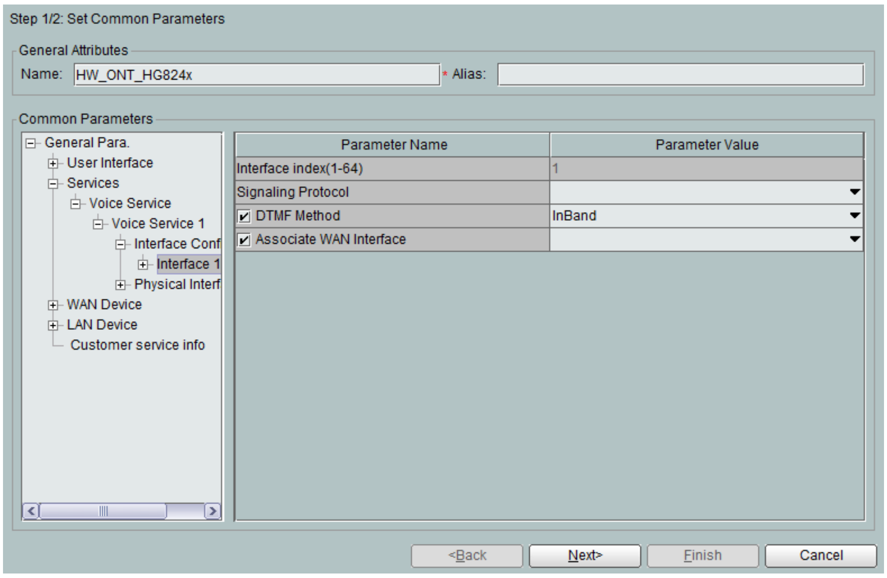
After configuring a general ONT value-added service profile or an ONT value-added service profile and binding it to an ONT successfully, you can activate the ONT and directly provision the value-added service defined by the profile to the subscribers of the ONT. Each ONT can be bound to only one general ONT value-added service profile or ONT value-added service profile.

Context

A general value-added service (VAS) profile is a collection of ONT common parameters and integrates the VAS profiles of different ONTs. The general VAS profile is used to implement the cross-model and cross-version service provisioning and replacement, and cross-version upgrades. The value-added service configuration profiles vary with the types of the ONTs and the software versions.

Procedure

- **Configure an ONT general VAS profile.**
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **PON Profile** > **ONT VAS Profile** from the navigation tree.
  3. Click the **General ONT VAS Profile** tab.
  4. In the information list, right-click and choose **Add (Service Configuration Type)** from the shortcut menu.
  5. In the dialog box that is displayed, set the required parameters.



Step 1/2: Set Common Parameters

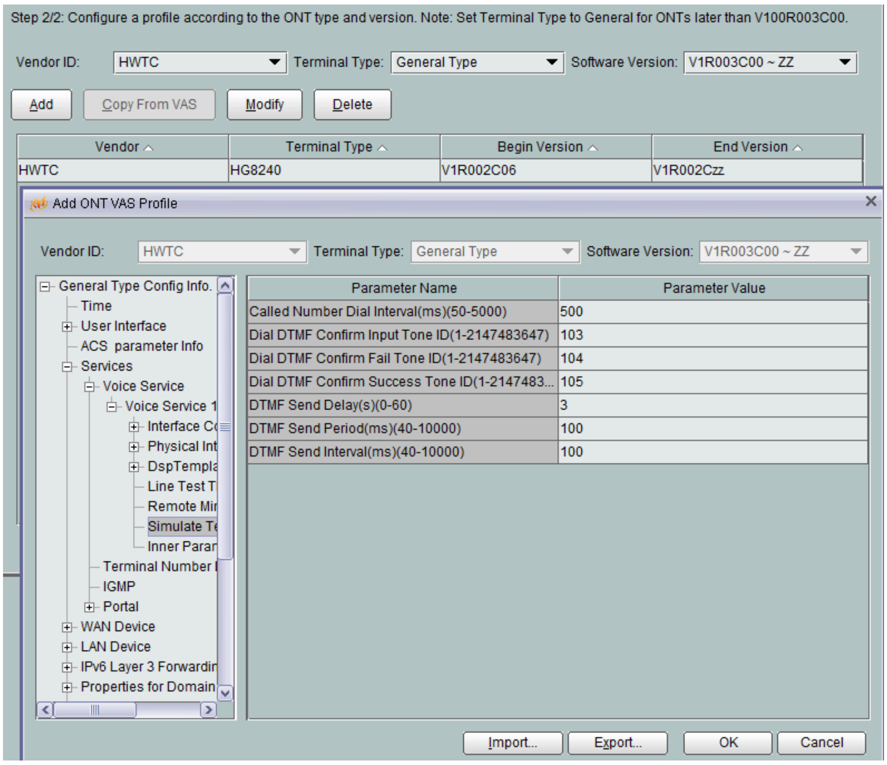
General Attributes

Name: HW_ONT_HG824x * Alias:

Common Parameters

Parameter Name	Parameter Value
Interface index(1-64)	1
Signaling Protocol	
☑ DTMF Method	InBand
☑ Associate WAN Interface	

  6. Click **Next**.
  7. In the dialog box that is displayed, set user-defined parameters for the ONTs of different software versions.


Step 2/2: Configure a profile according to the ONT type and version. Note: Set Terminal Type to General for ONTs later than V100R003C00.

Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ

Vendor	Terminal Type	Begin Version	End Version
HWTC	HG8240	V1R002C06	V1R002Czz

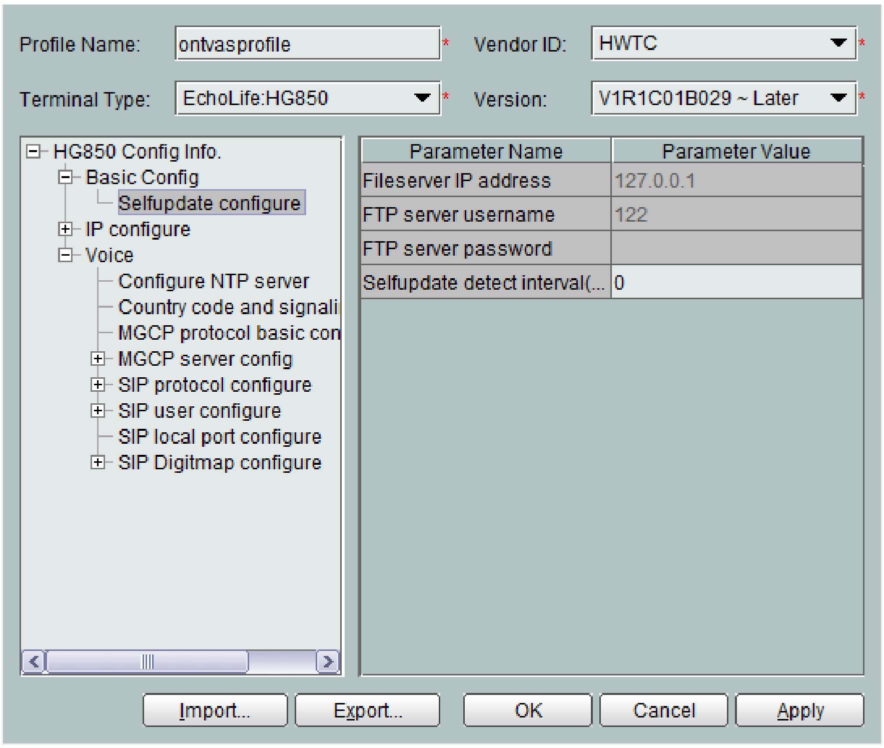
Add ONT VAS Profile

Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ

Parameter Name	Parameter Value
Called Number Dial Interval(ms)(50-5000)	500
Dial DTMF Confirm Input Tone ID(1-2147483647)	103
Dial DTMF Confirm Fail Tone ID(1-2147483647)	104
Dial DTMF Confirm Success Tone ID(1-2147483...	105
DTMF Send Delay(s)(0-60)	3
DTMF Send Period(ms)(40-10000)	100
DTMF Send Interval(ms)(40-10000)	100

8. Click **Finish**.
9. In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
10. In the dialog box that is displayed, select the required NE(s), and click **OK**.

- **Configure an ONT VAS profile.**
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **PON Profile** > **ONT VAS Profile** from the navigation tree.
  3. Click the **ONT VAS Profile** tab.
  4. In the information list, right-click and choose **Add** from the shortcut menu.
  5. In the dialog box that is displayed, set **Profile Name**, **Vendor ID**, **Terminal Type**, and **Version**.



Profile Name: ontvasprofile *
Vendor ID: HWTC *
Terminal Type: EchoLife:HG850 *
Version: V1R1C01B029 ~ Later *

Parameter Name	Parameter Value
Fileserver IP address	127.0.0.1
FTP server username	122
FTP server password	
Selfupdate detect interval(...	0

6. Click **OK**.
7. In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
8. In the dialog box that is displayed, select the required NE(s), and click **OK**.

----End

8.2 Configuring the EPON Access Service

This topic describes how to configure the EPON access service. The EPON access supports high-bandwidth transmission, which effectively removes the bandwidth bottleneck in the access through twisted pairs and meets the subscribers' requirements for high-bandwidth services, such as high definition TV (HDTV) and live programs.

Prerequisites

- The corresponding VLAN must have been created in the system. For details on adding a VLAN, see **4.1.2.2 Adding a VLAN**.
- The VLAN must have been configured with an upstream port. For details on configuring the upstream port of a VLAN, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MEF IP traffic profile or IP profile must have been configured in the system. For details on configuring the MEF IP traffic profile, see **5.2 Configuring an MEF IP Traffic Profile**. For details on configuring an IP traffic profile, see Configuring an IP Traffic Profile.

The line profiles and service profiles have been created and downloaded to the NEs so that they can be applied to the EPON access services.

- For details on configuring the line profiles, see **8.1.3 Configuring an EPON Line Profile**.
- For details on configuring the service profiles, see **8.1.4 Configuring an EPON Service Profile**.

Context

The EPON access service has multiple application scenarios, such as fiber to the home (FTTH), fiber to the building (FTTB), and fiber to the curb (FTTC). For different EPON application scenarios, the basic procedure for configuring the EPON access service is the same, but the detailed configuration data may be different. For the detailed configuration data, see **Table 8-1**.

Table 8-1 Configuration of the EPON access service in different scenarios

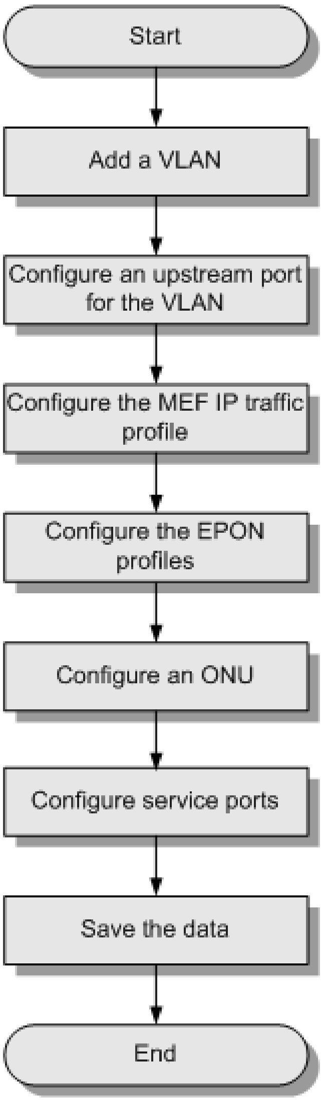
Application Scenario	General Networking	Description
FTTH	An ONU is installed at the subscriber's home to provide the subscriber with multiple services through the Ethernet port and the telephone port.	When the ONU is connected to a PC or STB, and does not support the data packets carrying a VLAN tag: ● You need not configure the native VLAN of the ONU port when only one service is required. ● You need to configure the native VLAN of the ONU port when multiple services are required so that a VLAN tag is added to the data packets received on the ONU and the VLAN tag is removed from the data packets transmitted from the ONU.
FTTB	An ONU is installed in a building and is connected to a layer-2 switch which provides multiple Ethernet ports for providing subscribers with access services.	● When configuring the home Internet access service, if multiple subscribers connected to the ONU must not interconnect with each other and each subscriber needs to be authenticated individually, you need to configure the subscribers on each ONU port with different VLANs. ● When the ONU is connected to a layer-2 switch, the packets that reach the ONU carry VLAN tags. You do not need to configure the native VLAN for the ONU port, but you need to make sure that the subscriber-side VLANs are consistent with the VLAN tags of the packets.

Application Scenario	General Networking	Description
FTTC	The ONU is installed in the cabinet at the curb and is connected to a Mini DSLAM or a Mini DSLAM with the EPON uplink function to provide subscribers with access services.	You only need to configure the service port for the OLT according to the upstream VLAN of the Mini DSLAM.

The EPON access service is provided through the EPON access service card. Each service card on the OLT provides four or eight EPON ports. Each port supports the split ratio of 1:64. Each card provides up to 256 ONU accesses.

Figure 8-1 shows the flowchart for configuring the EPON access service.

Figure 8-1 Flowchart for configuring the EPON access service


Start
Add a VLAN
Configure an upstream port for the VLAN
Configure the MEF IP traffic profile
Configure the EPON profiles
Configure an ONU
Configure service ports
Save the data
End

8.2.1 Configuring an ONU

This topic describes how to add an ONU and set the basic attributes of the ONU. It is mainly used for adding an ONU and configuring services when the ONU is offline. When the ONU is online, the configuration data is applied to the ONU through the ONU management protocol.

Prerequisites

- The DBA profile must be configured in the system. For details, see **8.1.2 Configuring a DBA Profile**.
- The EPON line profile must be configured in the system. For details, see **8.1.3 Configuring an EPON Line Profile**.
- The EPON service profile must be configured in the system. For details, see **8.1.4 Configuring an EPON Service Profile**.

Procedure

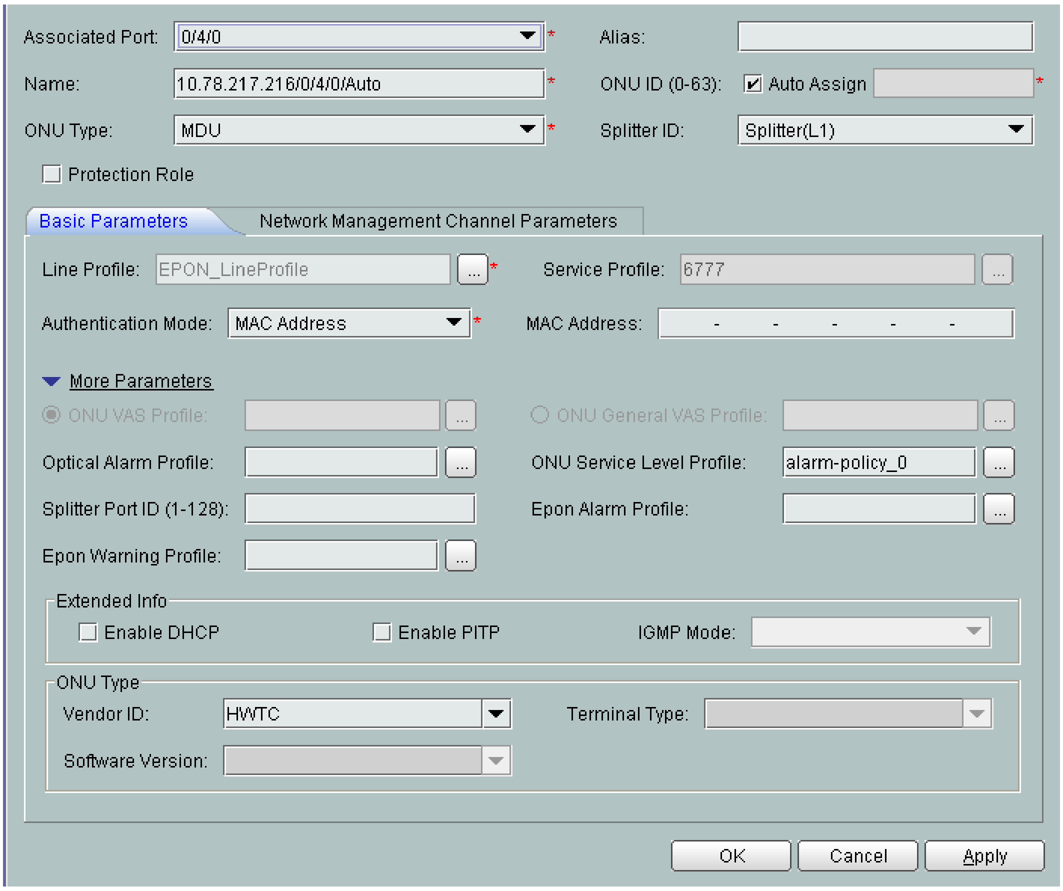
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **EPON** > **EPON Management** from the navigation tree.

Step 3 On the **EPON ONU** tab page, set the filter criteria or click ⏬ to display the EPON ONUs.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



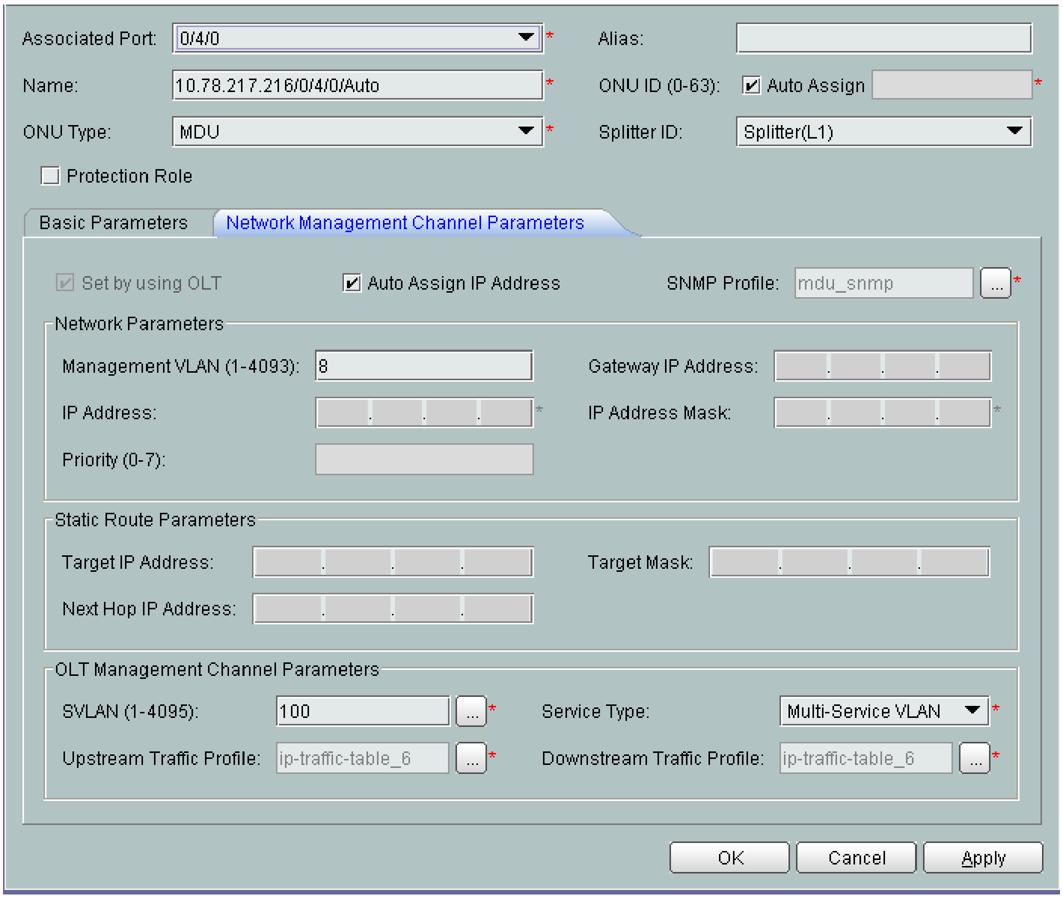
Associated Port: 0/4/0 *
Alias:
Name: 10.78.217.216/0/4/0/Auto *
ONU ID (0-63): ☑ Auto Assign *
ONU Type: MDU *
Splitter ID: Splitter(L1)
☐ Protection Role

Line Profile: EPON_LineProfile *
Service Profile: 6777
Authentication Mode: MAC Address *
MAC Address: - - - - -

More Parameters
● ONU VAS Profile:
○ ONU General VAS Profile:
Optical Alarm Profile:
ONU Service Level Profile: alarm-policy_0
Splitter Port ID (1-128):
Epon Alarm Profile:
Epon Warning Profile:

Extended Info
☐ Enable DHCP
☐ Enable PITP
IGMP Mode:

ONU Type
Vendor ID: HWTC
Terminal Type:
Software Version:



Associated Port: 0/4/0 *
Alias:
Name: 10.78.217.216/0/4/0/Auto *
ONU ID (0-63): ☑ Auto Assign *
ONU Type: MDU *
Splitter ID: Splitter(L1)
☐ Protection Role

☑ Set by using OLT
☑ Auto Assign IP Address
SNMP Profile: mdu_snmp *

Network Parameters
Management VLAN (1-4093): 8
Gateway IP Address:
IP Address: *
IP Address Mask: *
Priority (0-7):

Static Route Parameters
Target IP Address:
Target Mask:
Next Hop IP Address:

OLT Management Channel Parameters
SVLAN (1-4095): 100 *
Service Type: Multi-Service VLAN *
Upstream Traffic Profile: ip-traffic-table_6 *
Downstream Traffic Profile: ip-traffic-table_6 *

NOTE

- The **Rate Type** parameter can be specified and modified in an EPON ONU when you add the ONU or modify the ONU. Only the MA5600 V800R008C03 and MA5600 V800R013C00 support this configuration.
- **Terminal Type** and **Software Version** that you set must be the same as the version of the actual ONT.
- When the **Set by using OLT** check box is cleared, ONUs are configured and managed remotely on the OLT through the OMCI protocol.
- When the **Set by using OLT** check box is selected, ONUs are configured and managed remotely on the OLT through the SNMP protocol.
- Do not add SNMP parameters on the ONU through the CII, but issue the SNMP profile from the OLT to the ONU.
- If **ONU Type** is **MDU** and the **Set by using OLT** check box is selected, OLT management channel parameters must be set.

Step 6 Click **OK**.

----End

8.2.2 Configuring a Service Port

This topic describes how to configure a service port to provide the EPON access service.

Prerequisites

- The VLAN to which the service port will be added must be available: **4.1.2.2 Adding a VLAN**.

Copyright © Huawei Technologies Co., Ltd.

- The VLAN must have been configured with an upstream port. **5.3 Configuring the Upstream Port of a VLAN**.
- An appropriate MEF IP traffic profile must have been configured: **5.2 Configuring an MEF IP Traffic Profile**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

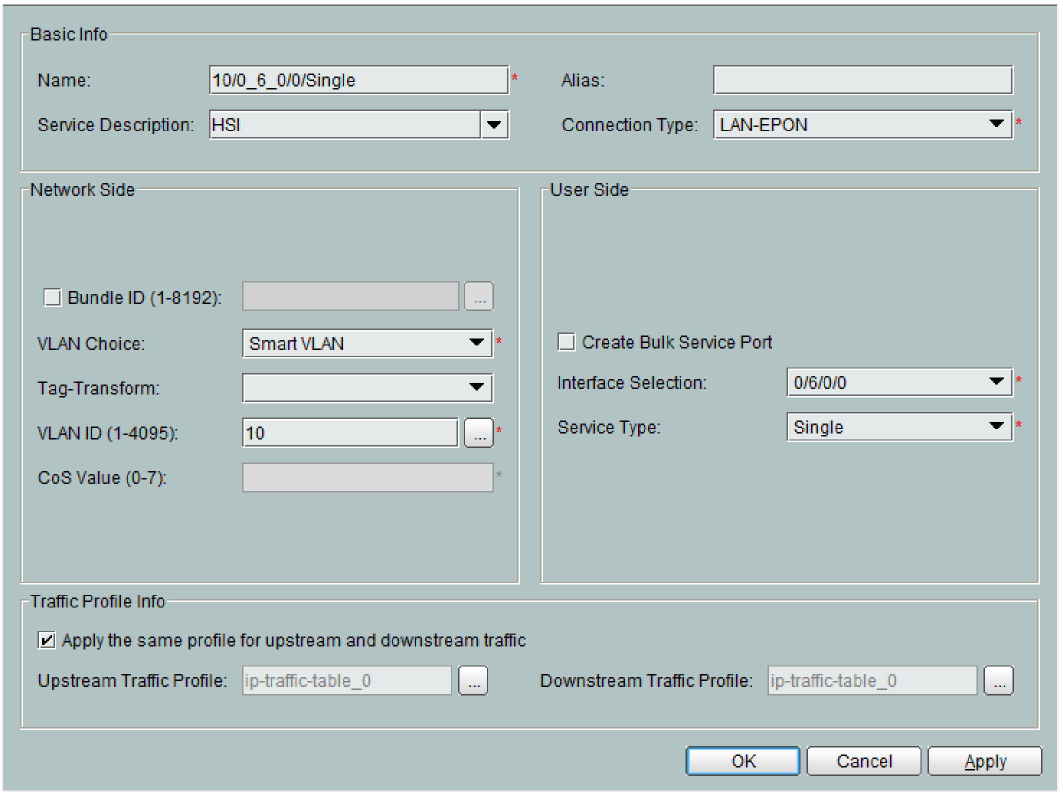
Step 2 Choose **EPON** > **EPON Management** from the navigation tree.

Step 3 On the **EPON UNI Port** tab page, set the filter criteria or click ⌄ to display the EPON UNI ports.

Step 4 Select a record from the EPON port list, and click the **ServicePort Info.** tab in the lower pane.

Step 5 Right-click the list, and then choose **Add**.

Step 6 In the dialog box that is displayed, configure the service port.



Basic Info
Name: 10/0_6_0/0/Single *
Alias:
Service Description: HSI
Connection Type: LAN-EPON *

Network Side
☐ Bundle ID (1-8192):
VLAN Choice: Smart VLAN *
Tag-Transform:
VLAN ID (1-4095): 10 *
CoS Value (0-7):

User Side
☐ Create Bulk Service Port
Interface Selection: 0/6/0/0 *
Service Type: Single *

Traffic Profile Info
☑ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile: ip-traffic-table_0
Downstream Traffic Profile: ip-traffic-table_0

Step 7 Click **OK**.

----End

8.3 Provisioning a EPON FTTH Service

This topic uses gigabit-capable passive optical network (EPON) as an example to describe how to quickly provision an EPON fiber to the home (FTTH) service . In this scenario, users can configure service channels for an OLT PON port in a window, including channels for Internet access, voice over IP (VoIP), and multicast services.

Prerequisites

- The OLT has been added to the U2000 and ONTs have been connected to the OLT by fibers. In addition, the ONT communicates with the OLT successfully.
- The corresponding virtual local area network (VLAN) has been added to the system. For details on how to add a VLAN, see **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN has been configured. For details on how to configure the upstream port of a VLAN, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MEF IP traffic profile has been already configured on the system. For details on how to configure the MEF IP traffic profile, see **5.2 Configuring an MEF IP Traffic Profile**.

Procedure

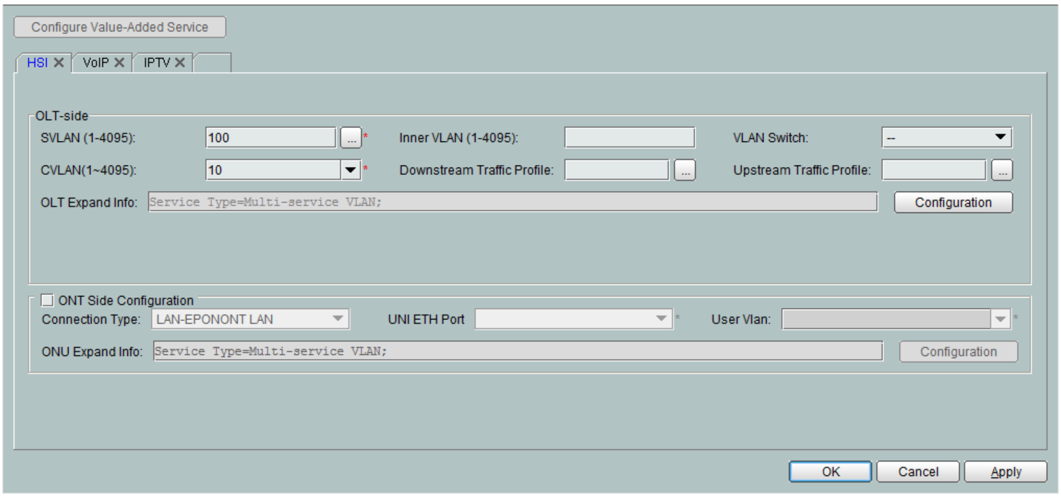
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **EPON** > **EPON Management** from the navigation tree.

Step 3 Click the **EPON ONU Details** tab.

Step 4 Click ... next to **Name**. In the dialog box that is displayed, select the required ONT and click **OK**.

Step 5 In the lower part of **ONU Details** tab page, click **Provisioning Service**. In the dialog box that is displayed, configure the EPON FTTH service.



OLT-side
SVLAN (1-4095): 100
CVLAN(1~4095): 10
Inner VLAN (1-4095):
VLAN Switch: --
Downstream Traffic Profile:
Upstream Traffic Profile:
OLT Expand Info: Service Type=Multi-service VLAN;

☐ ONT Side Configuration
Connection Type: LAN-EPONONT LAN
UNI ETH Port:
User Vlan:
ONU Expand Info: Service Type=Multi-service VLAN;

Copyright © Huawei Technologies Co., Ltd.

NOTE

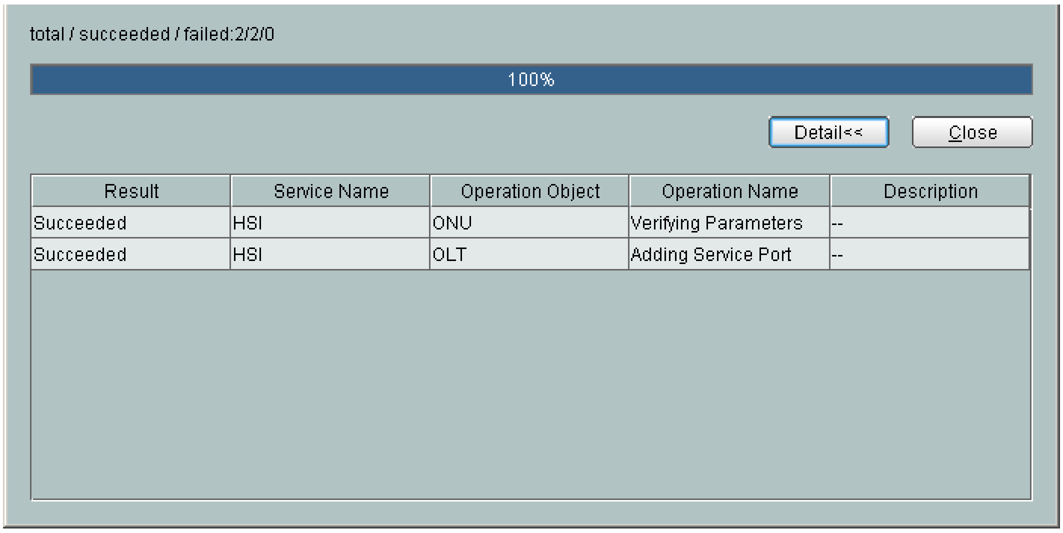
- **SVLAN** refers to the upstream VLAN on the OLT side.
- **CVLAN** refers to the downstream VLAN on the OLT side. It can also be called a customer VLAN. The value of this parameter must be the same as the **VLAN ID(1-4094)** value of the GEM connection in the line profile to which the ONT is bound.

The following functions are provided to optimize certain operations:

- Provisioning other FTTH services by adding tab pages, including but are not limited to Internet access, voice, and multicast services. On a new tab page, you can set **Service Type**, **Service Name** to provision a service. **Service Name** is a character string consisting of a maximum of four bytes.
- Storing certain information. When you click **OK** to complete the configuration, certain parameter settings are stored. The stored settings are displayed for reference when you set the same parameters next time.
- Configuring ONT value-added services by clicking **Configure Value-Added Service** or switching to the **Add Service** mode by clicking **Switch** on the upper right corner.
- Displaying important parameter settings in the blank area. You can click certain buttons to display a dialog box. After you set the parameters in the dialog box, the dialog box is closed and the parameter settings are displayed in the blank area of the preceding window.

Step 6 Click **OK**.

Step 7 In the **Progress** dialog box, check the operation result.



total / succeeded / failed:2/2/0

100%

Result	Service Name	Operation Object	Operation Name	Description
Succeeded	HSI	ONU	Verifying Parameters	--
Succeeded	HSI	OLT	Adding Service Port	--

----End

Result

The EPON FTTH service is provisioned successfully.

8.4 Provisioning a EPON FTTB Service

This topic describes how to quickly provision an EPON FTTB service. In an EPON FTTB network, the OLT, functioning as an OLT, connects MDUs or ONUs over the ODN network. The ONUs or MDUs then provide services for users. Depending on the access modes of MDUs, users can access an MDU in LAN mode or xDSL mode to access composite services, including VOIP, Internet access, and multicast services.

Prerequisites

- The OLT communicates successfully with MDUs.
- The corresponding VLAN has been added to the system. For details on how to add a VLAN, see **4.1.2.2 Adding a VLAN**.
- The upstream port of the VLAN has been configured. For details on how to configure the upstream port of a VLAN, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MEF IP traffic profile has been configured on the system. For details on how to configure the MEF IP traffic profile, see **5.2 Configuring an MEF IP Traffic Profile**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

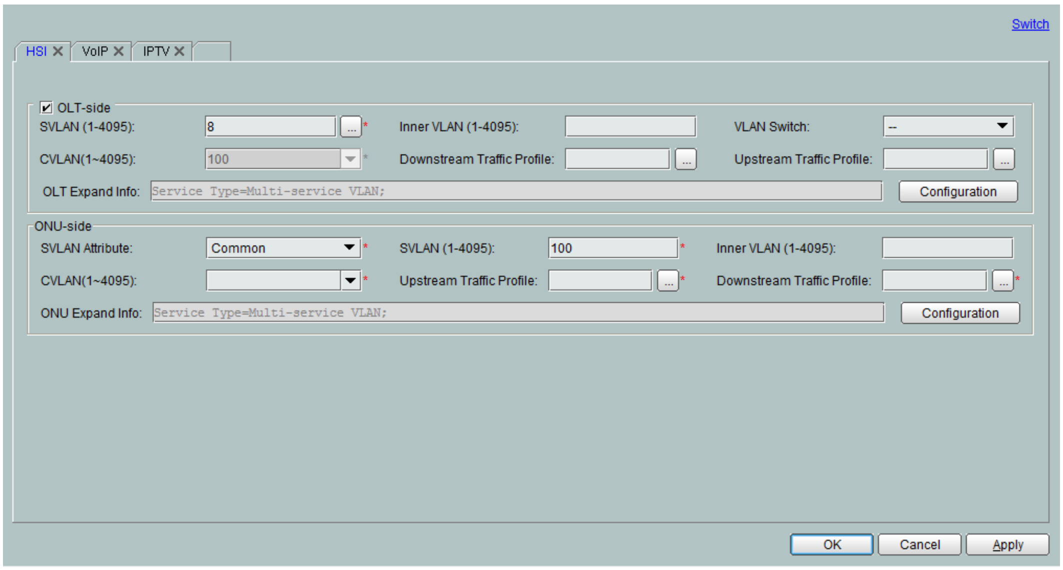
Step 2 Choose **EPON** > **EPON Management** from the navigation tree.

Step 3 Click the **EPON ONU Details** tab.

Step 4 Click ... next to **Name**. In the dialog box that is displayed, select the required MDU and click **OK**.

Step 5 In the lower part of the **ONU Details** tab page, click the **Ethernet Port** tab. Then, specify the filter criteria or click ⩔ to display the required Ethernet ports.

Step 6 In the Ethernet port list, select a record and click **Provisioning Service**. In the dialog box that is displayed, configure the EPON FTTB service.



☑ OLT-side
SVLAN (1-4095): 8 *
Inner VLAN (1-4095):
VLAN Switch: --
CVLAN(1~4095): 100 *
Downstream Traffic Profile:
Upstream Traffic Profile:
OLT Expand Info: Service Type=Multi-service VLAN;

ONU-side
SVLAN Attribute: Common *
SVLAN (1-4095): 100 *
Inner VLAN (1-4095):
CVLAN(1~4095): *
Upstream Traffic Profile: *
Downstream Traffic Profile: *
ONU Expand Info: Service Type=Multi-service VLAN;

NOTE

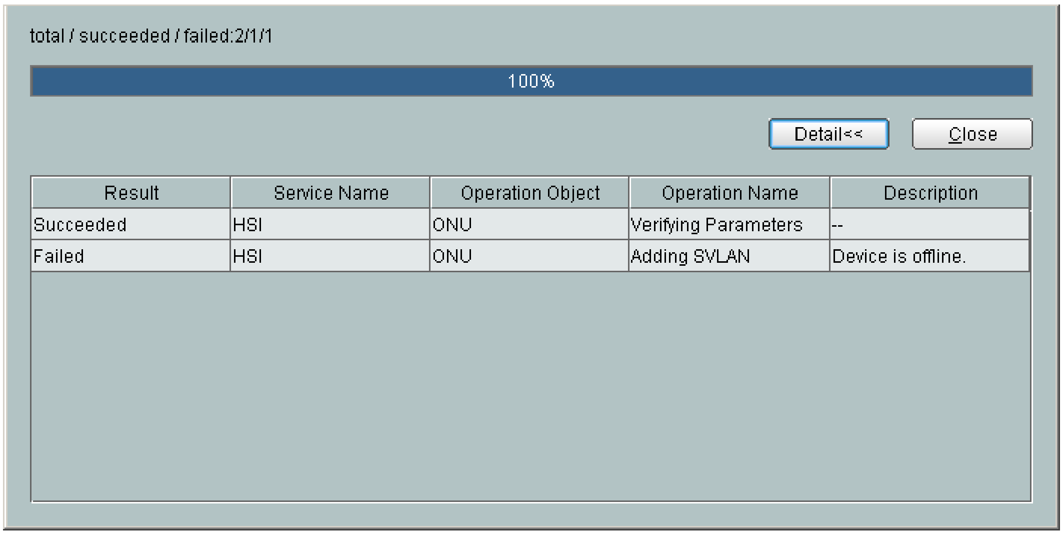
- In the **OLT Side Configuration** area:
  - **SVLAN** refers to the upstream VLAN of the OLT.
  - **CVLAN** is associated with **SVLAN** in the **ONU Side Configuration** area.
- In the **ONU Side Configuration** area:
  - **SVLAN** refers to the downstream VLAN of the OLT. It can also be called a customer VLAN. The value of this parameter must be the same as the value of the **VLAN ID(1-4094)** parameter for GEM connection in the bound line profile.
  - **CVLAN** refers to the downstream VLAN of the ONU. It is used to identify users.

The following functions are provided to optimize certain operations:

- Provisioning other FTTB services such as Internet access, voice, and multicast services by adding tab pages. On a new tab page, you can set **Service Type**, **Service Name** to provision a service. **Service Name** is a character string consisting of a maximum of 4 bytes.
- Storing certain information. When you click **OK** to complete the configuration, certain parameter settings are stored. The stored settings are displayed for reference the next time you set the same parameters.
- Configuring ONT value-added services by clicking **Configure Value-Added Service** or switching to the **Add Service** mode by clicking **Switch** on the upper right corner.
- Displaying important parameter settings in the blank area. You can click certain buttons to display a dialog box. After you set the parameters in the dialog box, the dialog box is closed and the parameter settings are displayed in the blank area of the preceding window.

Step 7 Click **OK**.

Step 8 In the **Progress** dialog box, check the operation result.



total / succeeded / failed:2/1/1

Result	Service Name	Operation Object	Operation Name	Description
Succeeded	HSI	ONU	Verifying Parameters	--
Failed	HSI	ONU	Adding SVLAN	Device is offline.

----End

Result

The EPON FTTB service is provisioned successfully.

8.5 Configuring the EPON Upstream Service

This topic describes how to configure the EPON upstream service. As a multi-dwelling unit (MDU), the MA5600T, MA5603T or MA5606T takes advantage of the wide coverage, flexible networking, and low maintenance cost of the GPON network. The MA5600T, MA5603T or MA5606T, with the OLT, provides high-bandwidth broadband access for subscribers. In addition, the MA5600T, MA5603T or MA5606T improves the user density of the OLT.

Prerequisites

- The corresponding VLAN must have been created in the system. For details on adding a VLAN, see **4.1.2.2 Adding a VLAN**.
- The Ethernet access service must have been configured in the system. For details on configuring the Ethernet access service, see **5 Configuring the Ethernet Access**.

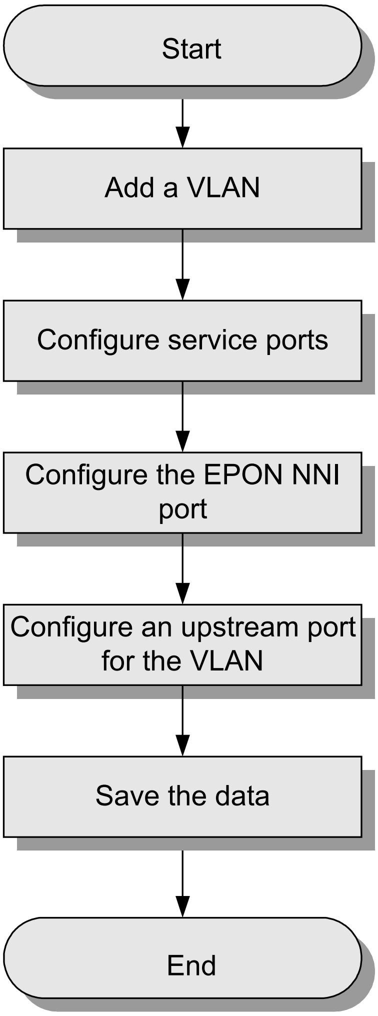
Context

This topic describes only the configuration on the ONU side when the MA5600T, MA5603T or MA5606T is taken as a MDU. For the configuration on the OLT side, refer to **8.2 Configuring the EPON Access Service**.

The MA5600T, MA5603T or MA5606T provides the EPON upstream port and forms an EPON network with the optical line terminal (OLT).

Figure 8-2 shows the flowchart for configuring the EPON upstream service.

Figure 8-2 Flowchart for configuring the EPON upstream service


Start
Add a VLAN
Configure service ports
Configure the EPON NNI port
Configure an upstream port for the VLAN
Save the data
End

8.5.1 Configuring an EPON NNI Port

This topic describes how to set the alias of an EPON upstream port, which helps you remember the EPON upstream port interconnected to the upper layer OLT.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **EPON** > **EPON NNI Port** from the navigation tree.

Step 3 On the **EPON NNI Port** tab page, set the filter criteria or click ︾ to display the EPON NNI ports.

Step 4 Select a record from the port list, right-click, and then choose **Modify**.

Step 5 In the dialog box that is displayed, set the alias.

Step 6 Click **OK**.

----End

8.5.2 Configuring the Upstream Port of a VLAN

This topic describes how to add an EPON upstream port to a VLAN so that the EPON upstream port can communicate with the other ports in the VLAN. To enable an upstream port to forward the user packets that carry a VLAN tag, you need to add the upstream port to the corresponding VLAN. After the upstream port is added to the VLAN, the upstream port forwards the user packets carrying the corresponding VLAN tag.

Prerequisites

The corresponding VLAN must have been created in the system. For details on adding a VLAN, see **4.1.2.2 Adding a VLAN**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.

Step 4 Select a record from the VLAN list, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, click **Subport**, and add the port of the 0/9/0 to the subport list.

Step 6 Click **OK**.

----End

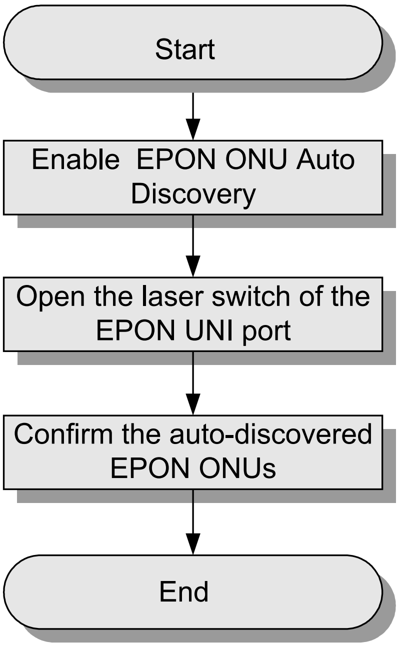
8.6 Configuring the ONU Auto Discovery Function

This topic describes how to configure the ONU auto discovery function. If the ONU auto discovery function is enabled on the OLT, the OLT obtains the registration information about the ONU when an ONU goes online and then the ONU is in the auto discovered state. By default, the ONU auto discovery function of an EPON port is disabled.

Context

Figure 8-3 shows the flowchart for configuring the ONU auto discovery function.

Figure 8-3 Flowchart for configuring the ONU auto discovery function


Start
Enable EPON ONU Auto Discovery
Open the laser switch of the EPON UNI port
Confirm the auto-discovered EPON ONUs
End

8.6.1 Enable EPON ONU Auto Discovery

This topic describes how to configure the ONT auto-discovery function of an EPON UNI port.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **EPON** > **EPON Management** from the navigation tree.

Step 3 On the **EPON UNI Port** tab page, set the filter criteria or click ⌄ to display the EPON UNI ports.

Step 4 Select a record from the port list, right-click, and then choose **Enable ONU Auto Discovery**.

Step 5 Click **OK**.

----End

8.6.2 Enabling the Laser of an EPON UNI Port

This topic describes how to enable the laser of an EPON UNI port so that the ONTs of the EPON port can automatically go online.

Context

- To prevent the ONTs of an EPON port from going online when commissioning the EPON port, disable the laser of the EPON port.
- None of the ONTs of an EPON port can go online after the laser of the EPON port is disabled.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **EPON** > **EPON Management** from the navigation tree.

Step 3 On the **EPON UNI Port** tab page, set the filter criteria or click ⏬ to display the EPON UNI ports.

Step 4 Select a record from the EPON port list, right-click, and then choose **Enable EPON UNI Port**.

Step 5 Click **Yes**.

----End

8.6.3 Confirming an Auto-Discovered EPON ONU

This topic describes how to confirm an auto-discovered ONU of an EPON port. When an ONU is automatically discovered, it is in the auto-discovered state. The ONU can work in the normal state only after it is confirmed.

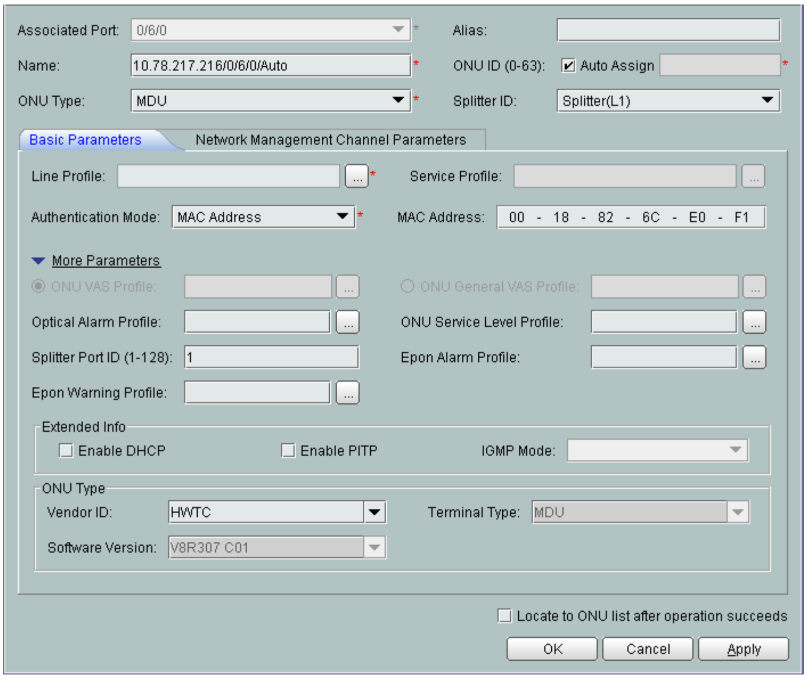
Procedure

- **Path one:**
  1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
  2. Choose **EPON** > **EPON Management** from the navigation tree.
  3. On the **EPON UNI Port** tab page, set the filter criteria or click ⏬ to display the EPON UNI ports.
  4. Select a EPON UNI port from the list, and click the **ONU Info** tab in the lower part of the page.
  5. On the **ONU Info** tab page, click the **Auto Discover ONUs**.
  6. In the dialog box that is displayed, select an ONU that needs to be confirmed, and then click **Confirm**.

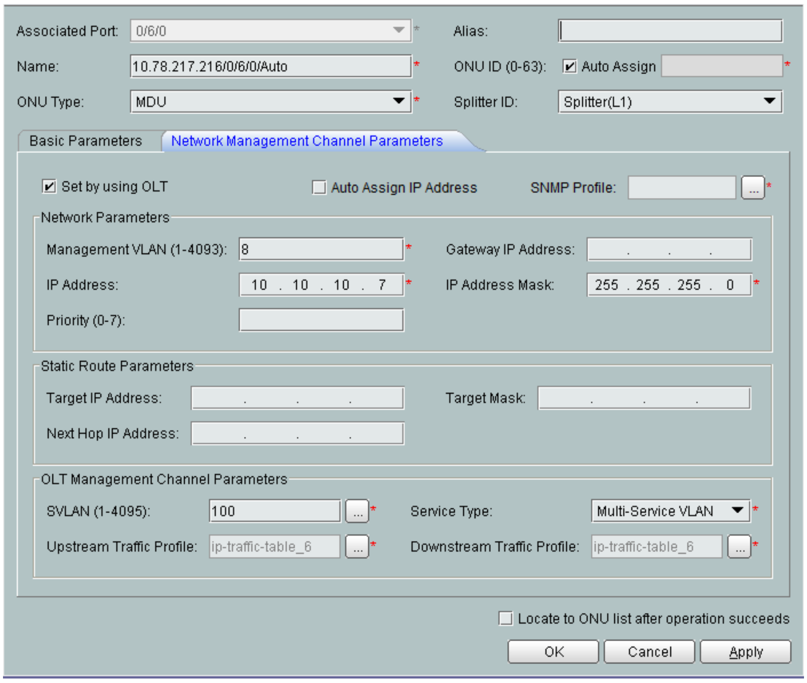
NOTE

Click the **Refresh** to obtain the ONUs in real time.

7. In the dialog box that is displayed, set the parameters on the **Basic Parameters** and **Network Management Channel Parameters** tab pages.



Associated Port: 0/6/0
Alias:
Name: 10.78.217.216/0/6/0/Auto
ONU ID (0-63): ☑ Auto Assign
ONU Type: MDU
Splitter ID: Splitter(L1)
Line Profile:
Service Profile:
Authentication Mode: MAC Address
MAC Address: 00 - 18 - 82 - 6C - E0 - F1
● ONU VAS Profile:
○ ONU General VAS Profile:
Optical Alarm Profile:
ONU Service Level Profile:
Splitter Port ID (1-128): 1
Epon Alarm Profile:
Epon Warning Profile:
Extended Info: ☐ Enable DHCP ☐ Enable PITP IGMP Mode:
ONU Type: Vendor ID: HWTC Terminal Type: MDU Software Version: V8R307 C01
☐ Locate to ONU list after operation succeeds



Associated Port: 0/6/0
Alias:
Name: 10.78.217.216/0/6/0/Auto
ONU ID (0-63): ☑ Auto Assign
ONU Type: MDU
Splitter ID: Splitter(L1)
☑ Set by using OLT ☐ Auto Assign IP Address SNMP Profile:
Network Parameters
Management VLAN (1-4093): 8
Gateway IP Address: . . .
IP Address: 10 . 10 . 10 . 7
IP Address Mask: 255 . 255 . 255 . 0
Priority (0-7):
Static Route Parameters
Target IP Address: . . .
Target Mask: . . .
Next Hop IP Address: . . .
OLT Management Channel Parameters
SVLAN (1-4095): 100
Service Type: Multi-Service VLAN
Upstream Traffic Profile: ip-traffic-table_6
Downstream Traffic Profile: ip-traffic-table_6
☐ Locate to ONU list after operation succeeds

NOTE

- The MA5600 V800R008C03 and MA5600 V800R013C00 support configuring the **Rate Type**.
- When **ONU Type** is set to **MDU** and the **Set by using OLT** check box is cleared, ONUs are configured and managed remotely on the OLT through the SNMP protocol.
- Do not add the SNMP parameters on the ONU through the serial port, but issue the SNMP profile from the OLT to the ONU only.

8. Click **OK**.

- **Path two:**
  1. Choose **Configuration** > **Access Service Management** > **EPON ONU** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Service Management** > **EPON ONU** from the main menu (application style).
  2. Choose the **EPON ONU Auto Discovery** tab, click **Filter**, and set parameters in the dialog box that is displayed.
  3. Select an ONU that needs to be confirmed, right-click, and then chooose**Confirm ONU**.
  4. In the dialog box that is displayed, set the parameters on the **Basic Parameters** and **Network Management Channel Parameters** tab pages.
  5. Click **OK**.

----End

9 Configuring the Multicast Service

About This Chapter

This topic describes how to configure the multicast service on a standalone NE, and on the NE in a subtending network.

9.1 Configuring the Multicast Services
Multicast is a point-to-multipoint communication mode in which the source transmits messages to a subset of nodes on the network. The OLT uses the multicast technology to provide IPTV services for carriers. The controlled multicast technology allows carriers to manage and control multicast users on the network equipment, and to provision broadband video services according to the requirements. In this case, multicast services are operable and manageable.

9.2 Configuring the Multicast Services of Subtending Devices
The OLT provides various types of Ethernet ports, which can be used to subtend devices. This topic describes how to configure multicast services when the OLT is in a subtending network.

9.1 Configuring the Multicast Services

Multicast is a point-to-multipoint communication mode in which the source transmits messages to a subset of nodes on the network. The OLT uses the multicast technology to provide IPTV services for carriers. The controlled multicast technology allows carriers to manage and control multicast users on the network equipment, and to provision broadband video services according to the requirements. In this case, multicast services are operable and manageable.

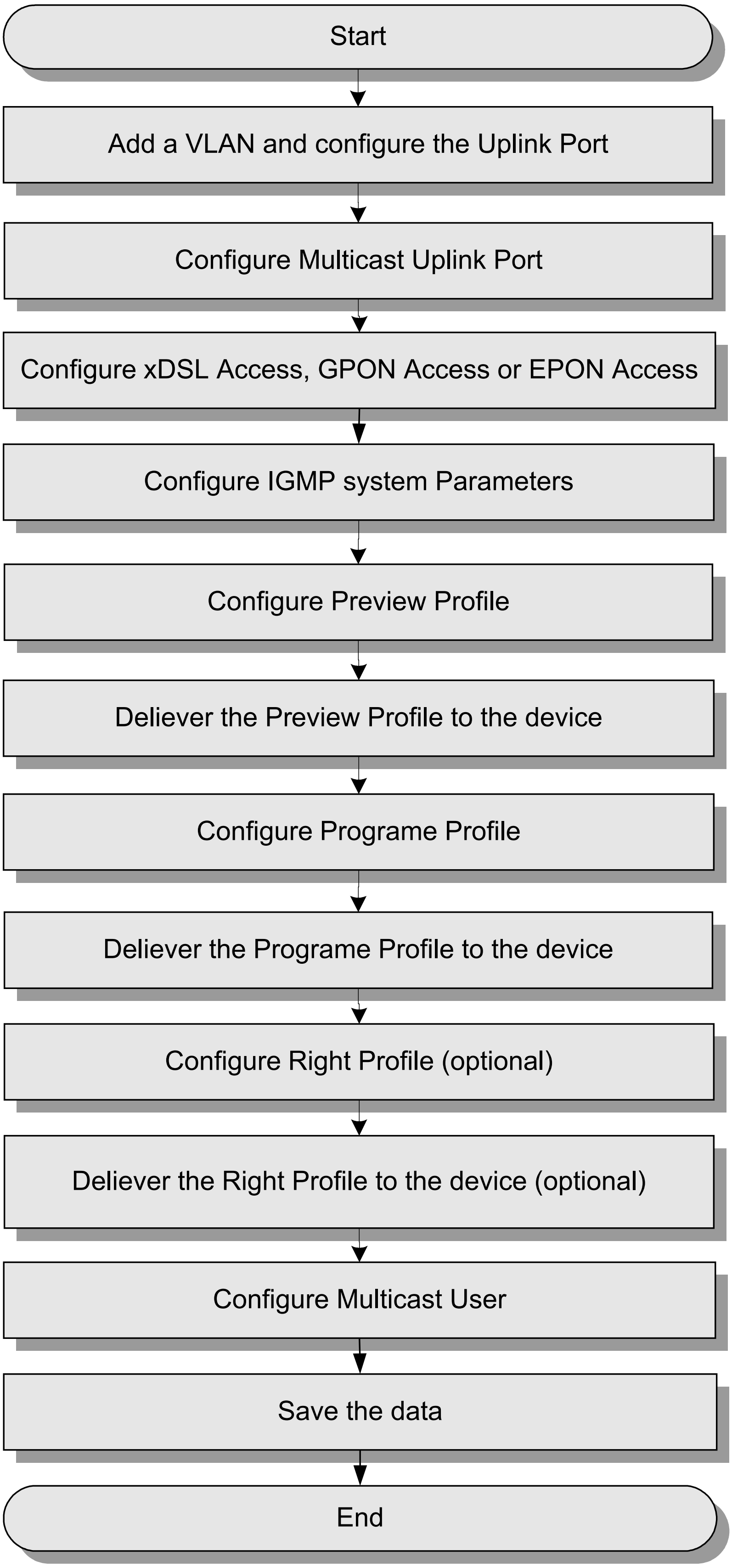
Prerequisites

- The required VLAN must be added. For details, see **4.1.2.2 Adding a VLAN**.
- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- The system parameter profile must be configured with multicast system parameters. For details, see **9.1.2.4 Configuring the Multicast Parameters**.
- The xDSL access mode or xPON access mode must be configured.
  - For details on how to configure the xDSL access mode, see **6.3 Configuring the xDSL Access Services**.
  - For details on how to configure the GPON access mode, see **7.2 Configuring the GPON Access Service - Distributed Mode** and **7.3 Configuring the GPON Access Service - Profile Mode**.
  - For details on how to configure the EPON access mode, see **8.2 Configuring the EPON Access Service**.

Context

The principles and configurations of multicast services in different xDSL access modes, GPON access mode or EPON access mode are similar, except for the access mode and parameter settings. **Figure 9-1** shows the flowchart for configuring multicast services.

Figure 9-1 Flowchart for configuring multicast services


Start
Add a VLAN and configure the Uplink Port
Configure Multicast Uplink Port
Configure xDSL Access, GPON Access or EPON Access
Configure IGMP system Parameters
Configure Preview Profile
Delierver the Preview Profile to the device
Configure Programe Profile
Deliever the Programe Profile to the device
Configure Right Profile (optional)
Deliever the Right Profile to the device (optional)
Configure Multicast User
Save the data
End

9.1.1 Introduction to the Multicast Service

As the streaming media such as multimedia videos and data warehouses are emerging in the IP network, the multicast applications become more and more popular. The multicast technology is used in the point-to-multipoint data transmission applications, such as the streaming media, distance learning, video conferencing, video multicasting (such as Web TV), online games, and Internet data center (IDC).

Context

The OLT provides the operable and manageable multicast service. It supports the IGMP V2/V3, IGMP proxy, and IGMP snooping.

- It supports the program preview function. Users can preview a program for a specific period. The preview times, preview duration, and preview interval are configurable.
- It supports the audience statistics function.
- It provides the controlled multicast function to control the multicast programs that multicast users can join in. It supports the rights profile mode. The rights are classified into three types: watchable, previewable, and forbidden. The rights profile mode satisfies the carriers' different requirements for multicast services.
- IPv6 multicast applies to the MA5600V800R009 and later versions.

9.1.2 Configuring an IGMP Profile

The Internet Group Management Protocol (IGMP) profile contains the parameters required for configuring the multicast service.

Context

The IGMP profiles of the OLT consist of the program profile, the rights profile and the preview profile.

- The program profile is used for adding static multicast programs to a multicast VLAN. Before watching a multicast program, you need to add the program to the multicast program library.
- The rights profile is used for managing the permission to a series of programs.
- The preview profile contains preview parameters. The profile can be applied to multiple devices. This simplifies the parameter configuration process.

9.1.2.1 Configuring a Preview Profile

The preview profile helps you to have a basic understanding of a program but has no permission to the complete program by controlling the times, duration and interval for you to watch the program. After a user with the preview right is online, the user is restricted by the preview duration. When the preview time is ended, the device forces the user to be offline. You can demand the program after the previous preview interval expires. The times for demanding the program in a day are restricted by the preview times. The preview profile contains preview parameters. The profile can be applied to multiple devices. This simplifies the parameter configuration process.

Procedure

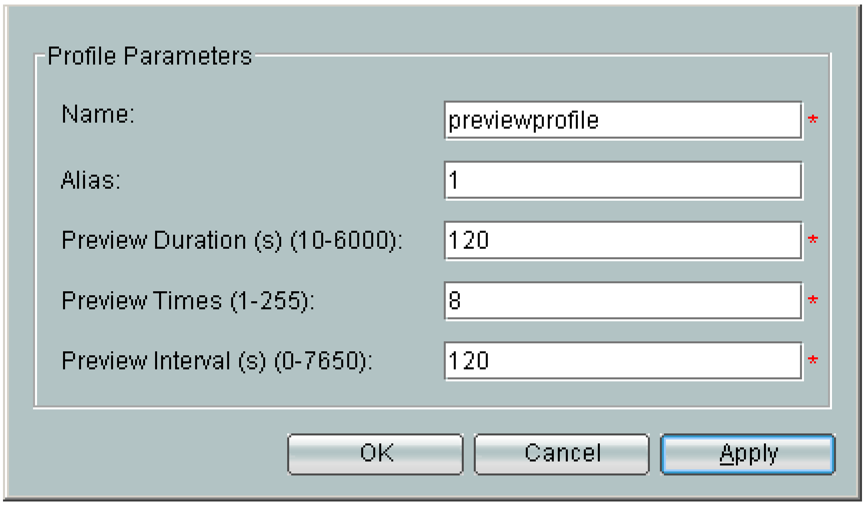
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

Step 3 Click the **Preview Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: previewprofile *

Alias: 1

Preview Duration (s) (10-6000): 120 *

Preview Times (1-255): 8 *

Preview Interval (s) (0-7650): 120 *

Step 6 Click **OK**.

----End

9.1.2.2 Configuring a Program Profile

The program profile is used for adding static multicast programs to a multicast VLAN. Before watching a multicast program, you need to add the program to the multicast program library. If a program profile is referenced by a multicast VLAN, the multicast VLAN is automatically configured with the parameter values of the attributes contained in the program profile.

Prerequisites

The multicast preview profile must be configured.

Procedure

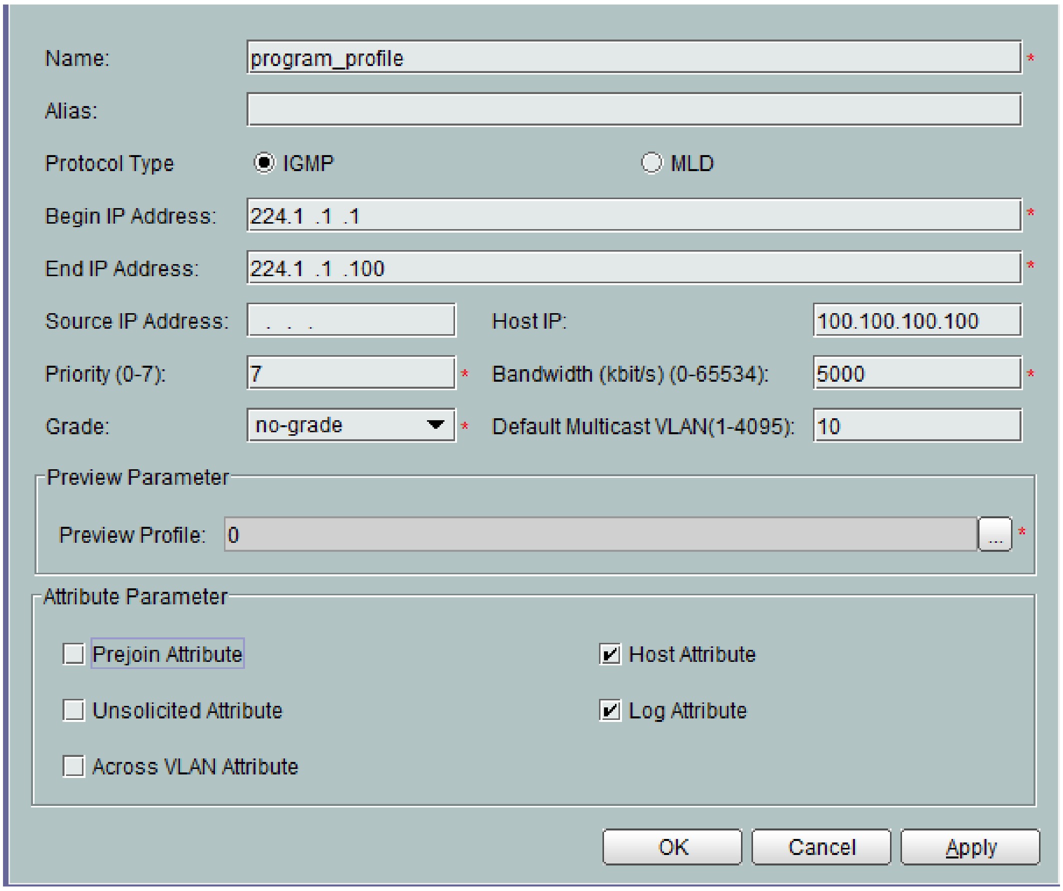
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

Step 3 Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: program_profile *
Alias:
Protocol Type ● IGMP ○ MLD
Begin IP Address: 224.1 .1 .1 *
End IP Address: 224.1 .1 .100 *
Source IP Address: . . .
Host IP: 100.100.100.100
Priority (0-7): 7 *
Bandwidth (kbit/s) (0-65534): 5000 *
Grade: no-grade *
Default Multicast VLAN(1-4095): 10

Preview Parameter
Preview Profile: 0 *

Attribute Parameter
☐ Prejoin Attribute
☑ Host Attribute
☐ Unsolicited Attribute
☑ Log Attribute
☐ Across VLAN Attribute

Step 6 Click **OK**.

----End

9.1.2.3 Configuring a Rights Profile

The rights profile is used for managing the permission to a series of programs. Program rights are classified into three types: watch, preview, and forbid. In a rights profile, set the permission to different programs, and then bind the rights profile to the users that require authentication. In this way, the permission of the users to the programs is limited. The users that do not require authentication can watch all the programs on the device.

Procedure

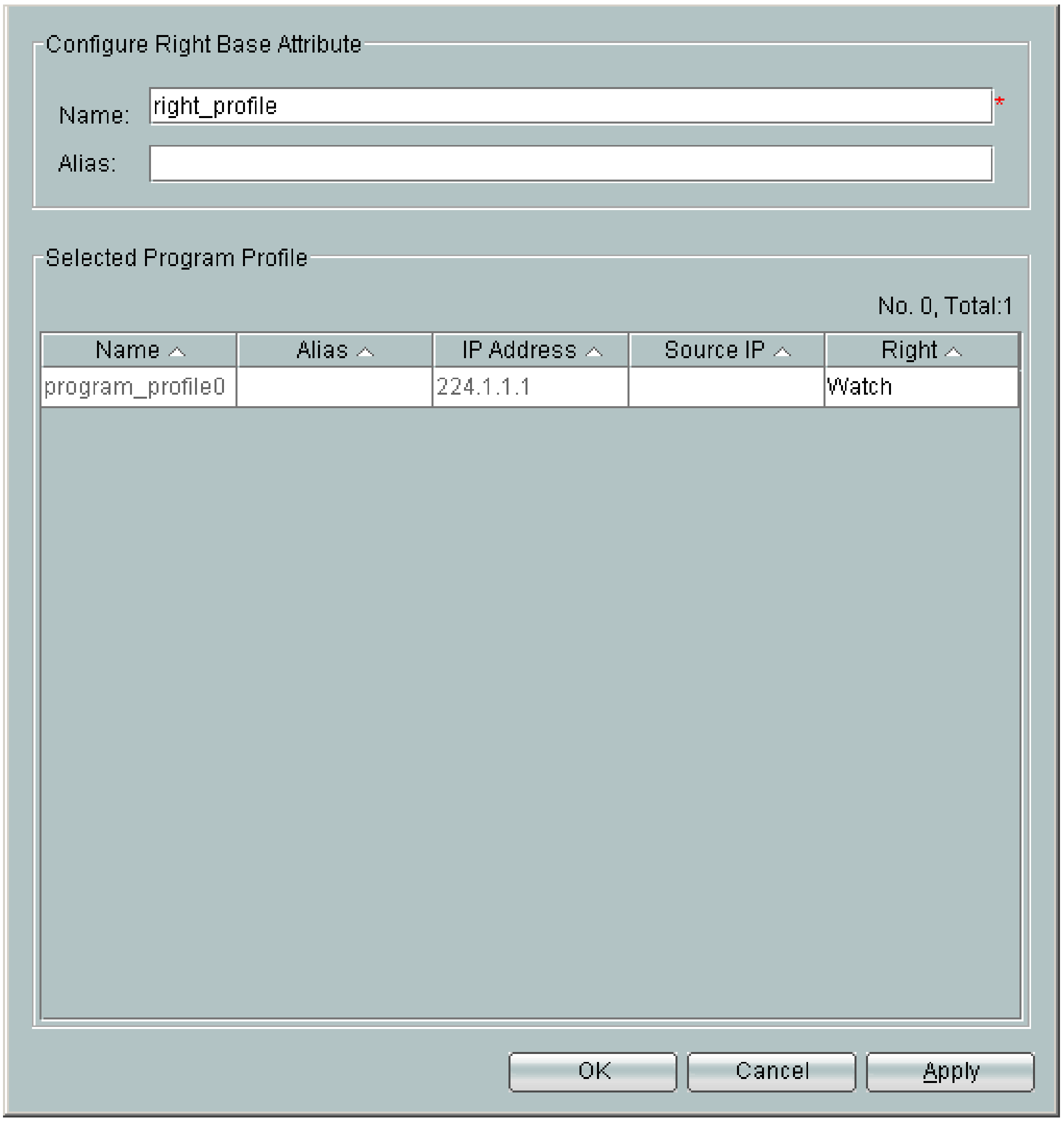
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

Step 3 Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the name of the rights profile. In the **Selected Program Profile** list, right-click, and choose **Select Profile**. In the dialog box that is displayed, select the program profile required for configuring the rights profile. Click **OK**.



Name: right_profile *
Alias:

Name	Alias	IP Address	Source IP	Right
program_profile0		224.1.1.1		Watch

Step 6 In the **Selected Program Profile** list, select a program profile, and then set the **Right** parameter.

Step 7 Click **OK**.

----End

9.1.2.4 Configuring the Multicast Parameters

Before you provision services for multicast, you can configure the multicast parameters according to the global data plan. The parameters consist of the Internet Group Management Protocol parameters and NTV mode. The Internet Group Management Protocol (IGMP) defines the mechanism used to set up and maintain the relationship of multicast group members between the host and the router.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.

Step 3 On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 4 In the dialog box that is displayed, enter the name of the system parameter profile. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters** navigation tree, and then click **Next**.

Step 5 Select **Protocol** > **IGMP** on the **System Parameter Settings** navigation tree. In the right pane, set the related parameters according to the plan.

Step 6 Select **NTV** on the **System Parameter Settings** navigation tree. In the right pane, set the related parameters according to the plan.

Step 7 Click **Finish**.

Step 8 Select the required record of the system parameter profile, right-click, and then choose **Download to NE**.

Step 9 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

9.1.3 Configuring the Multicast VLAN

One or more multicast VLANs are used to separate the multicast service from other services. After configuring the multicast user, you need to add the user to a multicast VLAN so that the user can watch the programs in the multicast VLAN.

Prerequisites

The corresponding VLAN must exist. For details, see **4.1.2.2 Adding a VLAN**.

Procedure

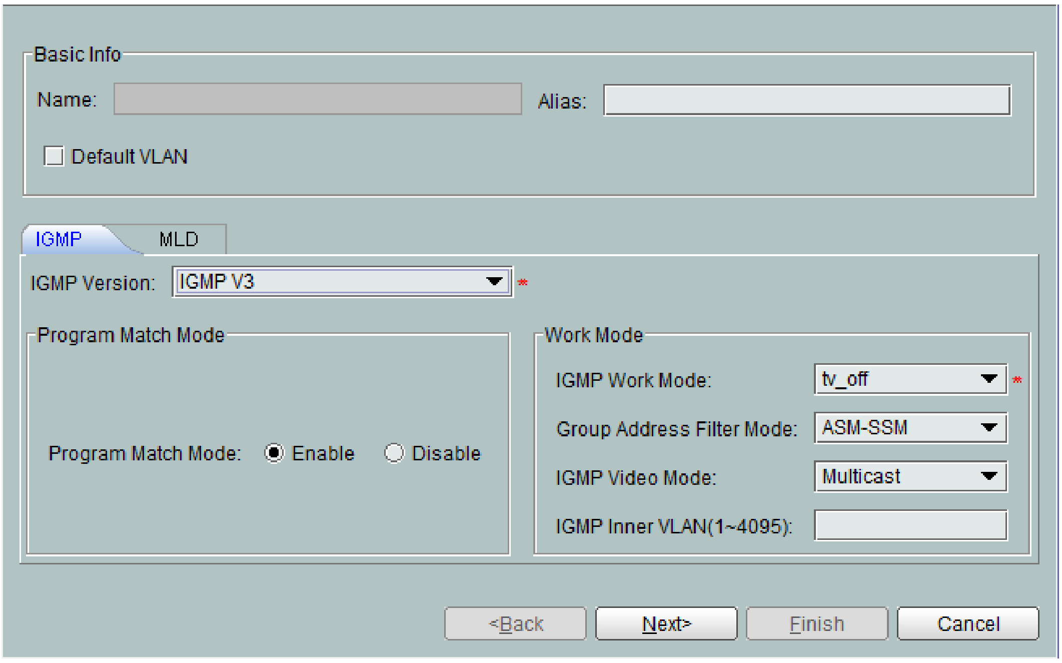
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Multicast** > **Multicast VLAN** from the navigation tree.

Step 3 On the **Multicast VLAN** tab page, set the filter criteria to display the required multicast VLANs.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Basic Info

Name:

Alias:

☐ Default VLAN

IGMP | MLD

IGMP Version: IGMP V3 *

Program Match Mode

Program Match Mode: ● Enable ○ Disable

Work Mode

IGMP Work Mode: tv_off *

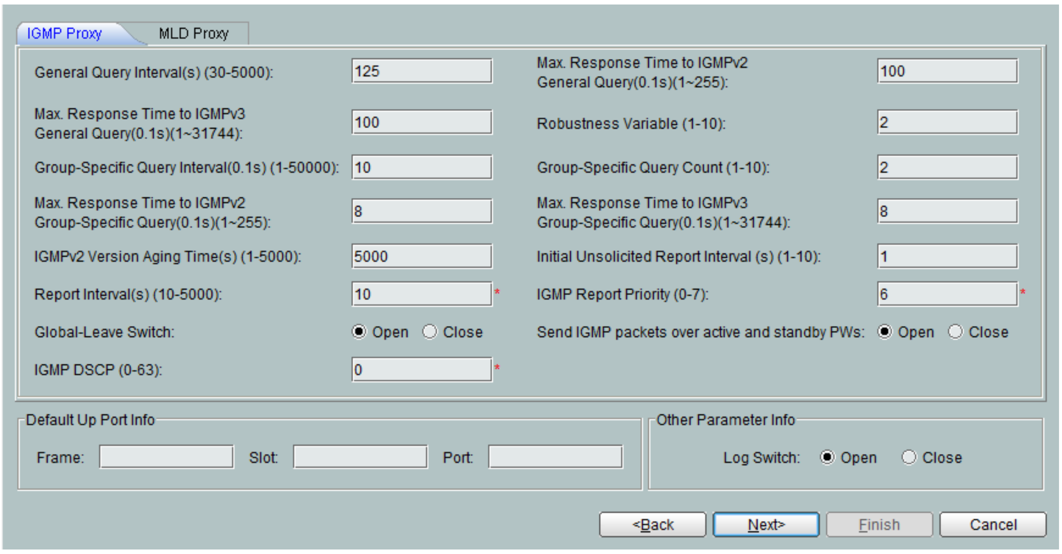
Group Address Filter Mode: ASM-SSM

IGMP Video Mode: Multicast

IGMP Inner VLAN(1~4095):

Step 6 Click **Next**.

Step 7 In the dialog box that is displayed, set the parameters.



IGMP Proxy | MLD Proxy

General Query Interval(s) (30-5000): 125

Max. Response Time to IGMPv2 General Query(0.1s)(1~255): 100

Max. Response Time to IGMPv3 General Query(0.1s)(1~31744): 100

Robustness Variable (1-10): 2

Group-Specific Query Interval(0.1s) (1-50000): 10

Group-Specific Query Count (1-10): 2

Max. Response Time to IGMPv2 Group-Specific Query(0.1s)(1~255): 8

Max. Response Time to IGMPv3 Group-Specific Query(0.1s)(1~31744): 8

IGMPv2 Version Aging Time(s) (1-5000): 5000

Initial Unsolicited Report Interval (s) (1-10): 1

Report Interval(s) (10-5000): 10 *

IGMP Report Priority (0-7): 6 *

Global-Leave Switch: ● Open ○ Close

Send IGMP packets over active and standby PWs: ● Open ○ Close

IGMP DSCP (0-63): 0 *

Default Up Port Info

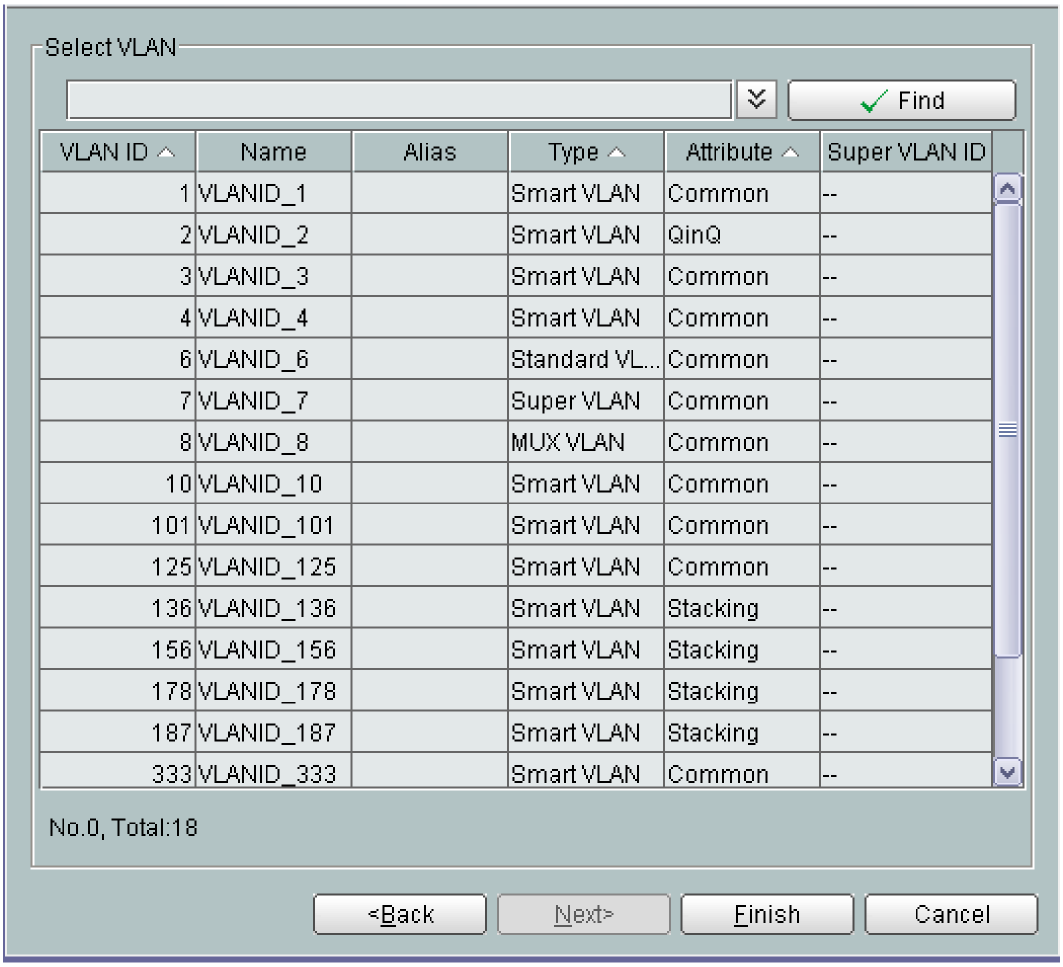
Frame: Slot: Port:

Other Parameter Info

Log Switch: ● Open ○ Close

Step 8 Click **Next**.

Step 9 Select the required VLAN from the list, and then click **Finish**.



VLAN ID	Name	Alias	Type	Attribute	Super VLAN ID
1	VLANID_1		Smart VLAN	Common	--
2	VLANID_2		Smart VLAN	QinQ	--
3	VLANID_3		Smart VLAN	Common	--
4	VLANID_4		Smart VLAN	Common	--
6	VLANID_6		Standard VL...	Common	--
7	VLANID_7		Super VLAN	Common	--
8	VLANID_8		MUX VLAN	Common	--
10	VLANID_10		Smart VLAN	Common	--
101	VLANID_101		Smart VLAN	Common	--
125	VLANID_125		Smart VLAN	Common	--
136	VLANID_136		Smart VLAN	Stacking	--
156	VLANID_156		Smart VLAN	Stacking	--
178	VLANID_178		Smart VLAN	Stacking	--
187	VLANID_187		Smart VLAN	Stacking	--
333	VLANID_333		Smart VLAN	Common	--

No.0, Total:18

----End

9.1.4 Configuring the Virtual Multicast Upstream Port

To provide demand services when the upstream port is not working in the MSTP mode, you need to configure a virtual multicast upstream port to transmit and receive the multicast packets (including the protocol packets and data packets). After the virtual multicast upstream port is added, the multicast packets are transmitted and received through this port.

Prerequisites

The **Uplink port mode** parameter cannot be configured with **MSTP**. For details, see Setting NTV Parameters.

Procedure

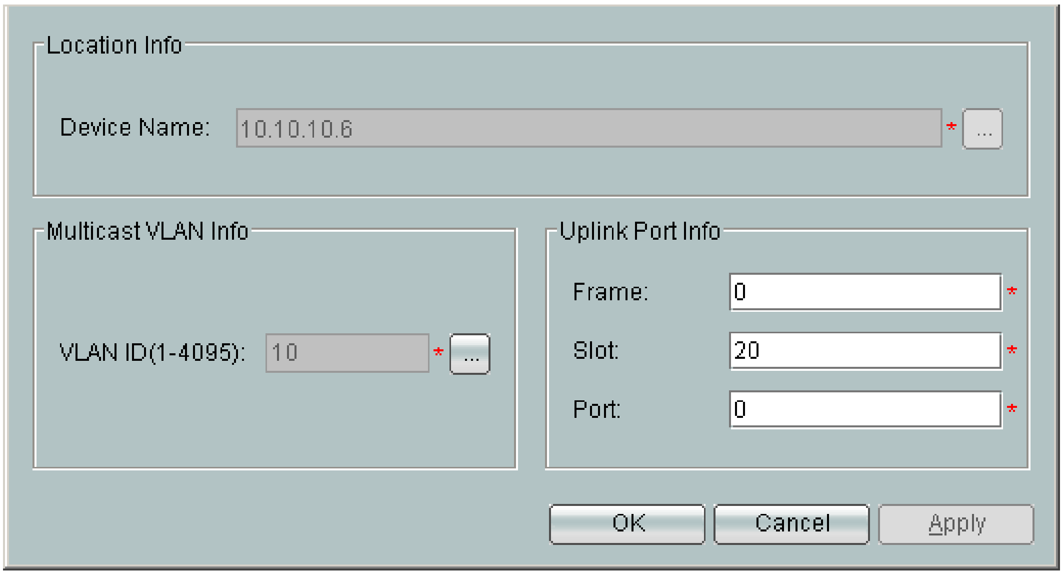
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Multicast** > **Uplink Port** from the navigation tree.

Step 3 Click **Find** to display the required virtual multicast upstream port records according to the filter criteria that you specify.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, configure the VLAN ID,the shelf, slot, and port of the upstream port.


Location Info
Device Name: 10.10.10.6 *
Multicast VLAN Info
VLAN ID(1-4095): 10 *
Uplink Port Info
Frame: 0 *
Slot: 20 *
Port: 0 *

Step 6 Click **OK**.

----End

9.1.5 (Optional) Applying a Preview Profile to a Device

This topic describes how to apply a configured preview profile to a device and make the preview profile take effect on the device.

Prerequisites

The multicast preview profile must be configured. For details, see **9.1.2.1 Configuring a Preview Profile**.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

Step 3 Click the **Preview Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 Click **Filter** to display the required preview profiles according to the filter criteria that you specify.

Step 5 Select the required profile, right-click, and then choose **Download to NE**.

Step 6 In the dialog box that is displayed, select the required devices in the left pane, set the task attributes in the right pane, and then click **OK**.

----End

9.1.6 Applying a Program Profile to a Device

This topic describes how to apply a configured program profile to a device and make the program profile take effect on the device.

Prerequisites

The multicast program profile must be configured. For details, see **9.1.2.2 Configuring a Program Profile**.

The VLAN must be configured. For details, see **4.1.2.2 Adding a VLAN**.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

Step 3 Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 Click **Filter** to display the required program profiles according to the filter criteria that you specify.

Step 5 Select the required profile, right-click, and then choose **Download to NE**.

Step 6 In the **Delivering Program Profile** dialog box, select the required devices in the left pane, set the task attributes in the right pane, and then click **Next**.

Step 7 In the dialog box that is displayed, set the **Up Port** and **VLAN ID**, and then click **Finish**.

----End

9.1.7 Applying a Rights Profile to a Device

This topic describes how to apply a configured rights profile to a device and make the rights profile take effect on the device.

Prerequisites

The multicast rights profile must be configured. For details, see **9.1.2.3 Configuring a Rights Profile**.

The VLAN must be configured. For details, see **4.1.2.2 Adding a VLAN**.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

Step 3 Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.

Step 4 Click **Filter** to display the required rights profiles according to the filter criteria that you specify.

Step 5 Select the required profile, right-click, and then choose **Download to NE**.

Step 6 In the **Delivering Right Profile** dialog box, select the required devices in the left pane, set the task attributes in the right pane, and then click **Next**.

Step 7 In the dialog box that is displayed, set the **Up Port** and **VLAN ID**, and then click **Finish**.

NOTE

If the selected program profile has been applied to an NE, you need not enter a VLAN ID.

----End

9.1.8 Configuring a Multicast User

This topic describes how to add a multicast user. Only multicast users can watch multicast programs.

Prerequisites

The corresponding service virtual port must exist. For details, see the following topics:

- For details on how to configure the service virtual port in the xDSL access mode, see Configuring a Service Port.
- For details on how to configure the service virtual port in the GPON access mode, see **7.2.5 Configuring the Service Port**.
- For details on how to configure the service virtual port in the EPON access mode, see **8.2.2 Configuring a Service Port**.

Context

- When adding a multicast user, you must specify a service virtual port.
- An authentication user must be bound to a rights profile to obtain relevant rights. A non-authentication user can watch all the programs configured on the device.

Procedure

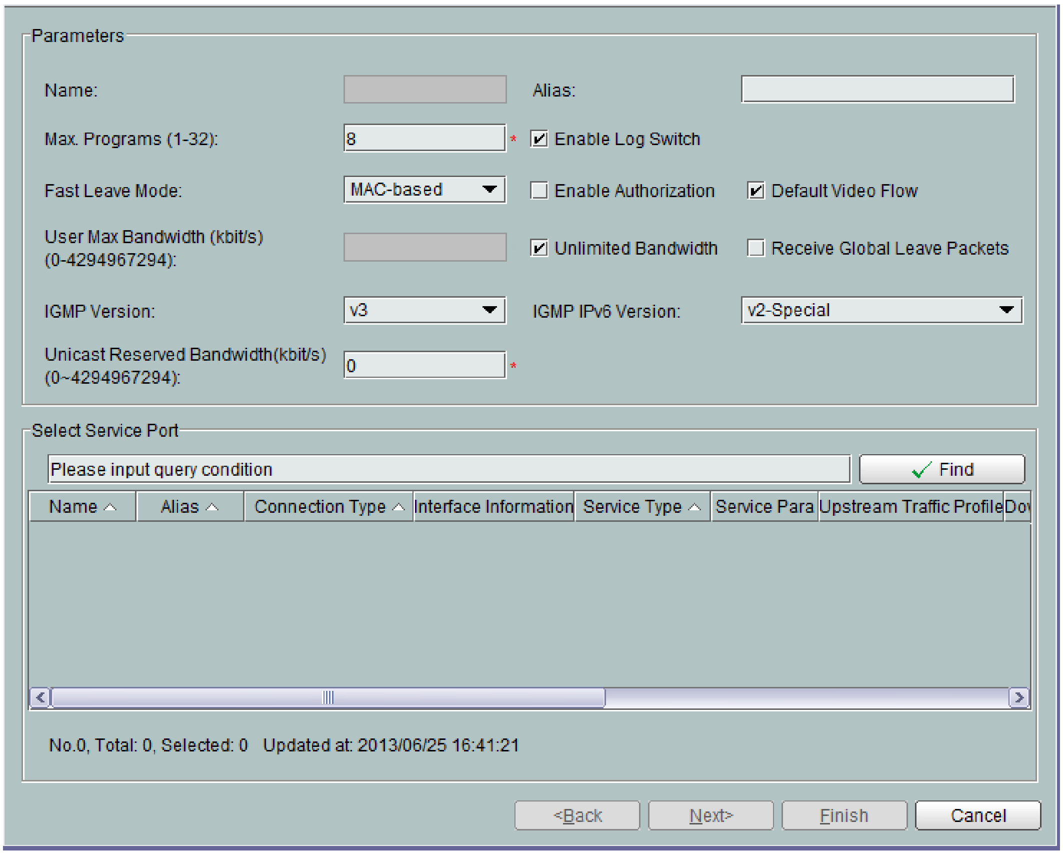
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Multicast** > **Multicast User** from the navigation tree.

Step 3 On the **Multicast User** tab page, set the filter criteria to display the required multicast users.

Step 4 On the **Multicast User** interface, right-click, and then choose **Add**.

Step 5 In the dialog box that is displayed, set the parameters.



Parameters

Name:

Alias:

Max. Programs (1-32): 8 *

☑ Enable Log Switch

Fast Leave Mode: MAC-based

☐ Enable Authorization

☑ Default Video Flow

User Max Bandwidth (kbit/s) (0-4294967294):

☑ Unlimited Bandwidth

☐ Receive Global Leave Packets

IGMP Version: v3

IGMP IPv6 Version: v2-Special

Unicast Reserved Bandwidth(kbit/s) (0~4294967294): 0 *

Select Service Port

Please input query condition

Name	Alias	Connection Type	Interface Information	Service Type	Service Para	Upstream Traffic Profile	Do

No.0, Total: 0, Selected: 0 Updated at: 2013/06/25 16:41:21

NOTE

After selecting **Enable Authorization**, click **Next**. In the dialog box that is displayed, configure the rights profile that is applied to the multicast user.

Step 6 Click **Finish**.

Step 7 Select a record from the multicast user list, and then click the **User Multicast VLAN** tab below the list. Right-click the list, and then choose **Add**.

Step 8 In the dialog box that is displayed, select the required multicast VLAN, and then click **OK**.

----End

9.2 Configuring the Multicast Services of Subtending Devices

The OLT provides various types of Ethernet ports, which can be used to subtend devices. This topic describes how to configure multicast services when the OLT is in a subtending network.

Prerequisites

- The multicast source must exist in the network.
- The service card must be in the normal state.

Context

Figure 9-2 shows the flowchart for configuring the multicast service of the upper-layer subtending device (Device A).

Figure 9-2 Flowchart for configuring the multicast service of the subtending device (Device A)

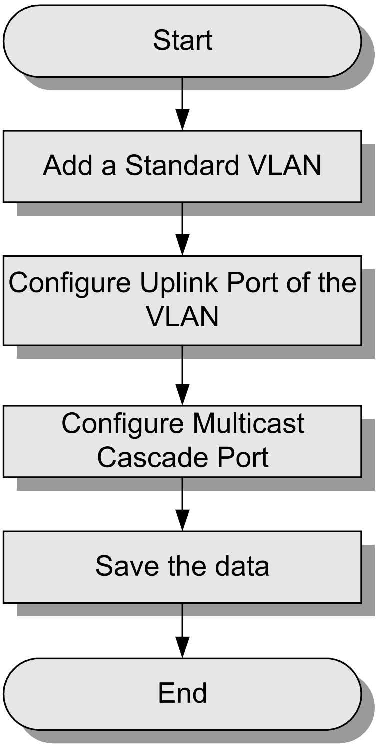
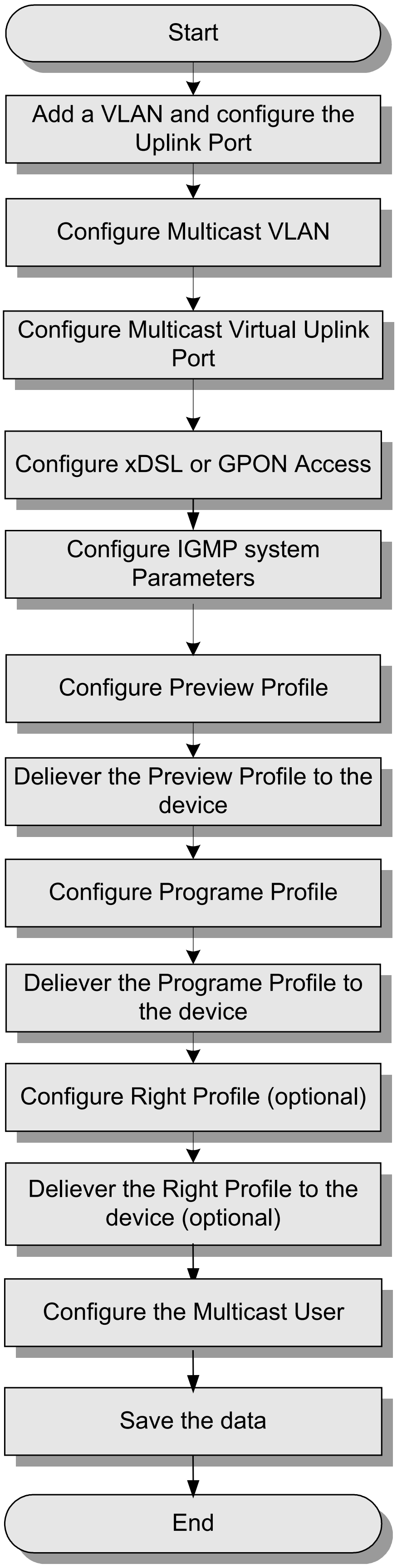

Start
Add a Standard VLAN
Configure Uplink Port of the VLAN
Configure Multicast Cascade Port
Save the data
End

Figure 9-3 shows the flowchart for configuring the multicast service of the lower-layer subtending device (Device B).

Figure 9-3 Flowchart for configuring the multicast service of the subtending device (Device B)


Start
Add a VLAN and configure the Uplink Port
Configure Multicast VLAN
Configure Multicast Virtual Uplink Port
Configure xDSL or GPON Access
Configure IGMP system Parameters
Configure Preview Profile
Deliever the Preview Profile to the device
Configure Programe Profile
Deliever the Programe Profile to the device
Configure Right Profile (optional)
Deliever the Right Profile to the device (optional)
Configure the Multicast User
Save the data
End

9.2.1 Introduction to the Multicast Services of Subtend Devices

The OLT provides various types of Ethernet ports. These ports are used to subtend other devices and implement multicast service access.

Context

In a subtend network, the access devices are directly interconnected to each other through the FE or GE ports. Subtend networks can extend the network coverage and support a large number of users. Subtend networks make networking more flexible by using the OLT products. The subtend networking saves the upstream link resources of the access points, reduces the number of local convergence devices, and simplifies the complex networking.

9.2.2 Configuration Example of the Multicast Services of Subtend Devices

This topic provides an example for configuring the multicast services of subtend devices.

Prerequisites

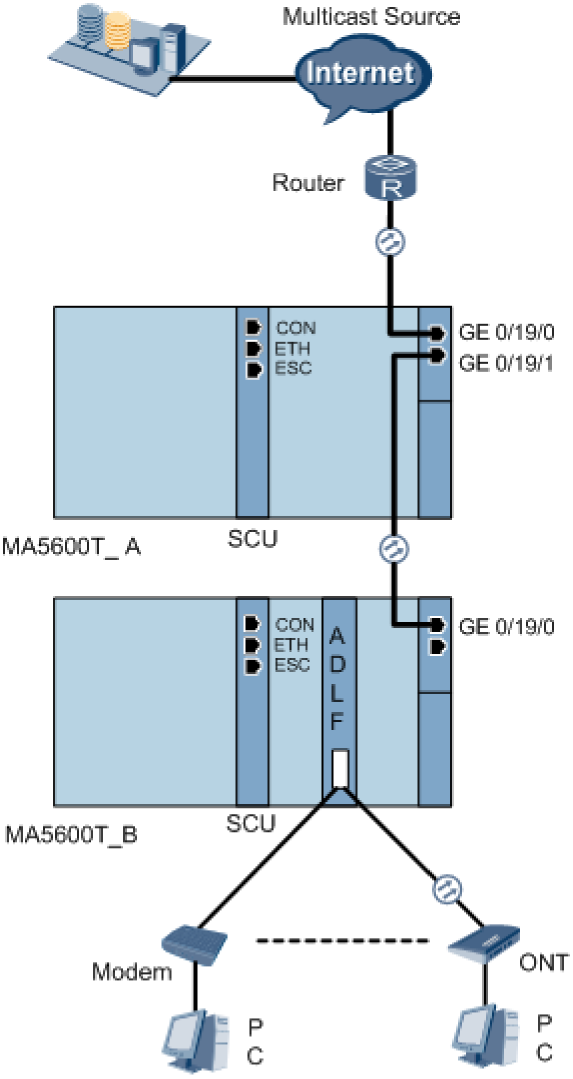
- The networking as shown in **Figure 9-4** must be completed. The devices on the network must work in the normal state.
- The multicast source must exist in the network.
- Ethernet port 0/19/1 on OLT_A and Ethernet port 0/19/0 on OLT_B are of the same type. The port rates of the two Ethernet ports are set to the self-sensing mode. The duplex modes of the two Ethernet ports are set to the self-negotiation mode.

The principles and configurations of the multicast services of subtend devices in the xDSL and GPON and EPON access modes are similar, except for the access mode and parameter configuration. This topic considers the ADSL access mode as an example.

Example Network

Figure 9-4 shows the example network in which the multicast service of the subtend OLT is configured.

Figure 9-4 Example network of the multicast service of subtend device



Data Plan

Table 9-1 provides the data plan.

Table 9-1 Data plan for the multicast service in subtend mode

Item	Data	Remarks
Device A		
IP address of the upper layer multicast router	10.0.0.254	-
VLAN	VLAN ID: 30 VLAN type: Standard VLAN	-

Item	Data	Remarks
Multicast VLAN	● Alias: IGMP_VLAN ● VLAN ID: 30 ● VLAN type: Standard VLAN	-
Virtual upstream port	Upstream port: 0/19/0 and 0/19/1	The upstream ports are also the subports of the standard VLAN 30.
Subtend port	0/19/1	-
Program profile	The multicast server provides three programs. Three programs use the default preview profile of the system. ● Name of the program profiles: BTV-1, BTV-2, and BTV-3 ● Range of multicast addresses: 224.0.1.2-224.0.1.4 ● Source IP address of the programs: 10.10.10.10 ● Accept the default values for other parameters.	-
Device B		
ADSL access mode	Service port: 0/11/0 and 0/11/1	-
MEF IP traffic profile	● Name: ip_profile ● CIR: 2048 kbit/s ● Accept the default values for other parameters.	These are the traffic profiles of the transmit and receive ends of the service virtual port.
VLAN	VLAN ID: 30 VLAN type: Standard VLAN	The VLAN ID is the same as the VLAN ID of device A.
Multicast VLAN	● Alias: IGMP_VLAN ● Default upstream port: 0/19/0 ● VLAN ID: 30 ● VLAN type: Standard VLAN	-
Virtual upstream port	Upstream port: 0/19/0	The upstream ports are also the subports of the Standard VLAN 30.

Item	Data	Remarks
IGMP global parameter	● Default video VPI/VCI: 0/35 ● Upstream port mode: Default ● NTV mode: IGMP_proxy ● Rights profile mode: Profile ● Accept the default values for other parameters.	-
Program profile	The multicast server provides three programs. Three programs use the default preview profile of the system. ● Name of the program profiles: BTV-1, BTV-2, and BTV-3 ● Range of multicast addresses: 224.0.1.2-224.0.1.4 ● Source IP address of the programs: 10.10.10.10 ● Accept the default values for other parameters.	-
Rights profile	Name: profile1 Available programs: BTV-1 and BTV-2	-
Multicast user	Use A: ● Port: 0/11/0 ● The use who requires no authentication. ● Maximum number of available programs: 6 Use B: ● Port: 0/11/1 ● The user who requires authentication. The rights profile is profile1. ● Maximum number of available programs: 2	-

Procedure

- To configure the multicast service of the subtend device A, do as follows.
  1. Add a VLAN and configure the upstream port of the VLAN.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **VLAN** from the navigation tree.
     c. In the information list, right-click and choose **Add** from the shortcut menu.

   d. In the dialog box that is displayed, set the parameters.
      - VLAN ID: 30
      - Type: Standard VLAN
      - Attribute: Common
   e. Click **Next**.
   f. In the **Sub Port** tab, select 0/19/0 and 0/19/1 as the upstream port(s).
   g. Click **Done**.
2. Add a multicast VLAN.
   a. Choose **Multicast** > **Multicast VLAN** from the navigation tree.
   b. On the **Multicast VLAN** tab page, set the filter criteria to display the required multicast VLANs.
   c. In the information list, right-click and choose **Add** from the shortcut menu.
   d. In the dialog box that is displayed, select the device name, and set the parameters as follows:
      - **IGMP Version**: **IGMP V3**
      - **IGMP Work Mode**: **igmp_proxy**
   e. Set the default upstream port to 0/19/0. Set **IGMP Report Priority** to **6** and **Report Interval** to **10s**.
   f. Click **Next**.
   g. Select the VLANID_30 whose type is Standard VLAN from the list.
   h. Click **Finish**.
3. Configure the multicast virtual upstream port.
   a. Choose **Multicast** > **Virtual Uplink Port** from the navigation tree.
   b. On the **Virtual Uplink Port** tab page, set the filter criteria to display the required virtual upstream ports.
   c. In the information list, right-click and choose **Add** from the shortcut menu.
   d. In the dialog box that is displayed, select the device name. Set the multicast VLAN ID to **30** and upstream port to 0/19/0.
   e. Click **OK**.
4. **Configure the multicast program profile**. Set the parameters as follows:
   - Name of the program profiles: BTV-1, BTV-2, and BTV-3
   - Range of multicast addresses: 224.0.1.2-224.0.1.4
   - Source IP address of the programs: 10.10.10.10
   - Accept the default values for other parameters.
5. **Apply a program profile to a device**. Set the VLAN ID to 30.
6. Configure the multicast subtend ports.
   a. Choose **Multicast** > **Cascading Port** from the navigation tree.
   b. On the **Cascading Port** tab page, set the filter criteria to display the required subtend ports.
   c. In the information list, right-click and choose **Add** from the shortcut menu.

    d. In the dialog box that is displayed, set the subtend port to 0/19/1.
    e. Click **OK**.

- To configure the multicast service of the subtend device B, do as follows.
  1. Add a VLAN and configure the upstream port of the VLAN.
     a. Choose **VLAN** from the navigation tree.
     b. In the information list, right-click and choose **Add** from the shortcut menu.
     c. In the dialog box that is displayed, set the parameters.
        - VLAN ID: 30
        - Type: Standard VLAN
        - Attribute: Common
     d. Click **Next**.
     e. In the **Sub Port** tab, select 0/19/0 and 0/19/1 as the upstream port(s).
     f. Click **Done**.
  2. Add a multicast VLAN.
     a. Choose **Multicast** > **Multicast VLAN** from the navigation tree.
     b. On the **Multicast VLAN** tab page, set the filter criteria to display the required multicast VLANs.
     c. In the information list, right-click and choose **Add** from the shortcut menu.
     d. In the dialog box that is displayed, select the device name, and set the parameters as follows:
        - **IGMP Version**: **IGMP V3**
        - **IGMP Work Mode**: **igmp_proxy**
     e. Set the default upstream port to 0/19/0. Set **IGMP Report Priority** to **6** and **Report Interval** to **10s**.
     f. Click **Next**.
     g. Select the VLANID_30 whose type is Standard VLAN from the list.
     h. Click **Finish**.
  3. Configure the multicast virtual upstream port.
     a. Choose **Multicast** > **Virtual Uplink Port** from the navigation tree.
     b. On the **Virtual Uplink Port** tab page, set the filter criteria to display the required virtual upstream ports.
     c. In the information list, right-click and choose **Add** from the shortcut menu.
     d. In the dialog box that is displayed, select the device name. Set the multicast VLAN ID to **30** and upstream port to 0/19/0.
     e. Click **OK**.
  4. Add a traffic profile.
     a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

   b. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
   c. Click the **MEF IP Traffic Profile** tab.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
   e. In the dialog box that is displayed, set the name of the MEF IP traffic profile to **ip_profile**, and CIR to **2048kbit/s**. Use the default values for other parameters.
   f. Click **OK**.
5. Configure the service virtual port.
   a. Choose **Connection** > **Service Port** from the navigation tree.
   b. Right-click the list, and then choose **Add**.
   c. In the dialog box that is displayed, set the parameters of the service virtual port as follows:
      - Connection Type: ADSL
      - Traffic profile of the transmit/receive end: ip_profile
      - VLAN information:
        - **VLAN Choice**: Standard VLAN
        - **VLAN ID**: 30
      - Port information: 0/11/0 and 0/11/1
      - VPI/VCI: 0/35
6. **9.1.2.4 Configuring the Multicast Parameters** and Adding the System Parameter Profile to a Device. Set the parameters as follows:
   - **Default VPI for VOD**: **0**
   - **Default VCI for VOD**: **35**
   - **NTV mode**: **IGMP_proxy**
   - **Uplink port mode**: **Default**
   - **Right profile mode**: **Profile based mode**
   - Accept the default values for other parameters.
7. **Configure the multicast program profile**. Set the parameters as follows:
   - Name of the program profiles: BTV-1, BTV-2, and BTV-3
   - Range of multicast addresses: 224.0.1.2-224.0.1.4
   - Source IP address of the programs: 10.10.10.10
   - Accept the default values for other parameters.
8. **Apply a program profile to a device**.
9. **Configure the rights profile**. Set the parameters as follows:
   - Name: profile1
   - Available programs: BTV-1 and BTV-2
10. **Apply a rights profile to a device**.
11. **Configure multicast users**. Set the parameters as follows:
    - Use A:

    - Port: 0/11/0
    - The use who requires no authentication.
    - Maximum number of available programs: 6
  - User B:
    - Port: 0/11/1
    - The user who requires authentication. The rights profile is profile1.
    - Maximum number of available programs: 2
- **Save the data**.

----End

Result

User A of device B is a non-authentication user who can watch all programs. User B is an authentication user who can only watch programs BTV-1 and BTV-2.

10 Configuring the Triple Play Service

About This Chapter

By the powerful service processing capability, the OLT provides users with the voice service, data service, and video service at the same time, that is, the triple play service. In addition, the quality of service (QoS) is guaranteed.

Context

Figure 10-1 shows the flowchart for configuring the triple play service of xDSL access mode.

Figure 10-1 Flowchart for configuring the triple play service-xDSL access

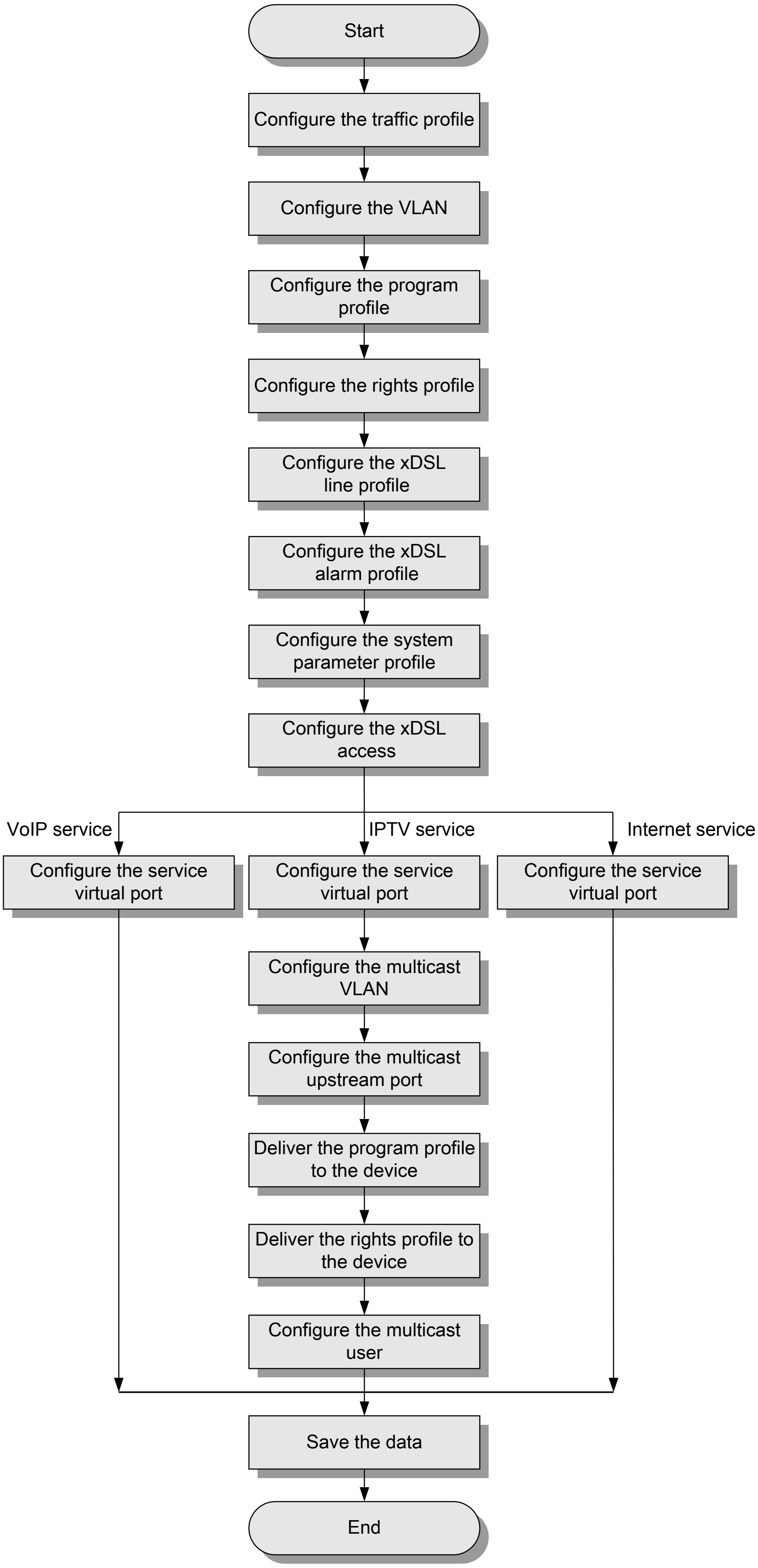

Start
Configure the traffic profile
Configure the VLAN
Configure the program profile
Configure the rights profile
Configure the xDSL line profile
Configure the xDSL alarm profile
Configure the system parameter profile
Configure the xDSL access
VoIP service
IPTV service
Internet service
Configure the service virtual port
Configure the service virtual port
Configure the service virtual port
Configure the multicast VLAN
Configure the multicast upstream port
Deliver the program profile to the device
Deliver the rights profile to the device
Configure the multicast user
Save the data
End

Figure 10-2 shows the flowchart for configuring the triple play service of GPON access mode.

Figure 10-2 Flowchart for configuring the triple play service-GPON access

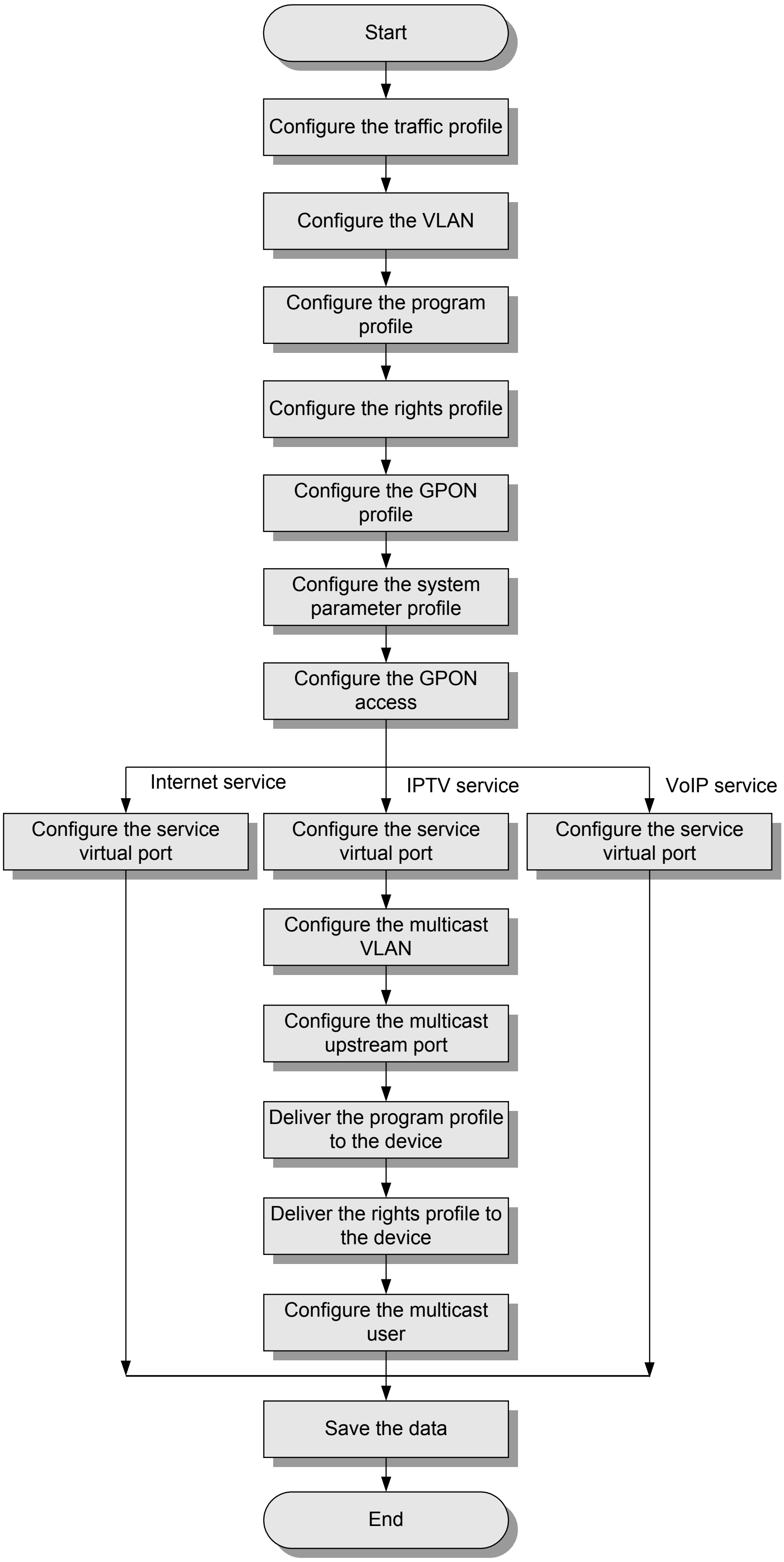
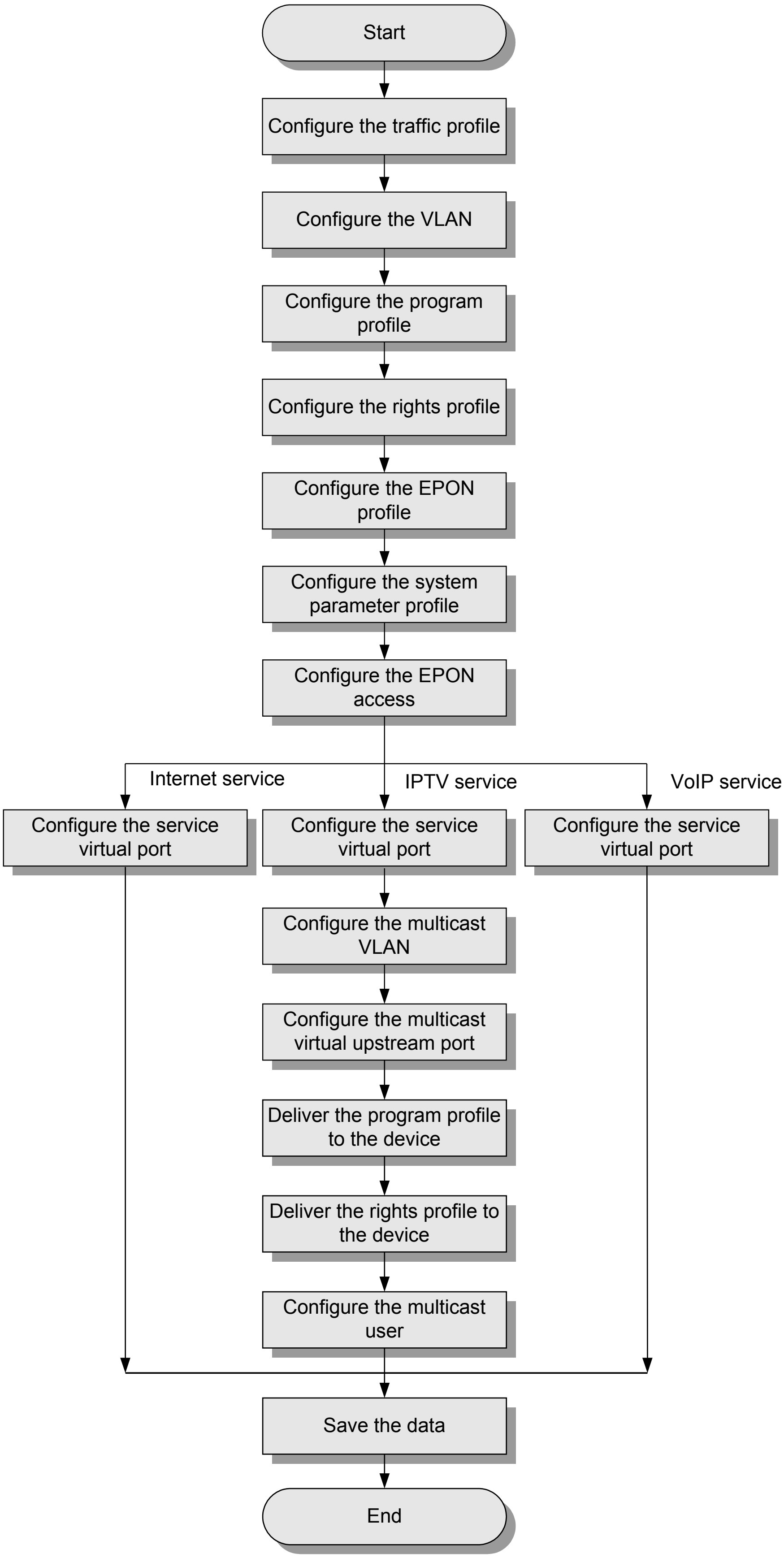

Start
Configure the traffic profile
Configure the VLAN
Configure the program profile
Configure the rights profile
Configure the GPON profile
Configure the system parameter profile
Configure the GPON access
Internet service
IPTV service
VoIP service
Configure the service virtual port
Configure the service virtual port
Configure the service virtual port
Configure the multicast VLAN
Configure the multicast upstream port
Deliver the program profile to the device
Deliver the rights profile to the device
Configure the multicast user
Save the data
End

Figure 10-3 shows the flowchart for configuring the triple play service of EPON access mode.

Figure 10-3 Flowchart for configuring the triple play service-EPON access


Start
Configure the traffic profile
Configure the VLAN
Configure the program profile
Configure the rights profile
Configure the EPON profile
Configure the system parameter profile
Configure the EPON access
Internet service
IPTV service
VoIP service
Configure the service virtual port
Configure the service virtual port
Configure the service virtual port
Configure the multicast VLAN
Configure the multicast virtual upstream port
Deliver the program profile to the device
Deliver the rights profile to the device
Configure the multicast user
Save the data
End

10.1 Introduction to the Triple Play Service
The triple play service provides subscribers with various service access methods concurrently over one subscriber line. Currently, the high-speed Internet access service, VoIP service, and IPTV service are supported.

10.2 Configuration Example of the Triple Play Service-xDSL Access
This topic provides an example for configuring the triple play service. On the user side, the VoIP, IPTV, and Internet services are accessed through different service virtual ports. At least three service virtual ports must be configured for each xDSL port. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

10.3 Configuration Example of the Triple Play Service-GPON Access (Distributed Mode)
This topic provides an example for configuring the triple play service. On the user side, the VoIP, IPTV, and Internet services are accessed through different GEM ports. At least three GEM ports must be configured for each GPON terminal. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

10.4 Configuration Example of the Triple Play Service - GPON Access (Profile Mode)
This topic provides an example for configuring the triple play service. On the user side, the VoIP, IPTV, and Internet services are accessed through different GEM ports. At least three GEM ports must be configured for each GPON terminal. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

10.5 Configuration Example of the Triple Play Service - EPON Access
This topic provides an example for configuring the triple play service. On the user side, the VoIP service, IPTV service, and Internet service are identified by different service virtual ports. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

10.1 Introduction to the Triple Play Service

The triple play service provides subscribers with various service access methods concurrently over one subscriber line. Currently, the high-speed Internet access service, VoIP service, and IPTV service are supported.

Context

The major concerns of the triple play service are how to process various services on one service port based on the priorities, and how to lessen the interaction among the services to the utmost extent.

- VoIP service:

  The VoIP service uses low bandwidth and has high requirements on the delay. If the delay is long, the problems such as echo may exist, thus affecting the voice quality. Therefore, the VoIP service has the highest priority among the three types of services.

- IPTV service:

  The IPTV service uses high bandwidth and has high requirements on the bit error rate and the packet loss ratio. If the bit error rate or the packet loss ratio is too high, the video frames are lost, which results in the mosaic of the picture or even the screen mess. Therefore, among the three types of services, the priority of the IPTV service is lower than that of the VoIP service, but higher than that of the high-speed Internet service.

- Internet service:

  Most users of the high-speed Internet service often browse the websites, so the service has low requirements on the real-time feature. In addition, the requirement on the packet loss ratio is not as high as that of the IPTV service, because the system supports the retransmission mechanism to ensure the transmission reliability. Therefore, among the three types of services, the high-speed Internet service has the lowest priority.

For convenient management of the three types of services on one port, three VLANs are used on the upstream port of the OLT. Each service has one VLAN.

NOTE

If the services are differentiated by the Ethernet type (IPoE/PPPoE), only two VLANs are needed for upstream transmission.

For the xDSL access, two methods can be used to implement the triple play service, as shown in **Table 10-1**. The following considers the multi-PVC multi-service mode as an example.

Table 10-1 Triple play implementation - xDSL access

Implementation Mode	Difference
Multi-PVC multi-service mode	Multiple PVCs are set up between the OLT and each xDSL terminal to bear various services. Different PVCs are used to differentiate the service flow.

Implementation Mode	Difference
Single-PVC multi-service mode	Only one PVC is set up between the OLT and each xDSL terminal to bear various services. ● The Ethernet type (IPoE/PPPoE) is used to differentiate the services. ● The VLAN ID from the xDSL terminal is used to differentiate the services. ● The 802.1p value from the xDSL terminal is used to differentiate the services. ● The combination of the 802.1p value (Ethernet packet) with the VLAN ID is used to differentiate the services. ● The combination of the Ethernet type (IPoE/PPPoE) with the VLAN ID is used to differentiate the services.

For the GPON access, two methods can be used to implement the triple play service, as shown in **Table 10-2**. The following considers the multi-GEM port multi-service mode as an example.

Table 10-2 Triple play implementation - GPON access

Implementation Mode	Difference
Multi-GEM port multi-service mode	Each GPON terminal uses multiple GEM ports to bear various services. Different GEM ports are used to differentiate the service flow.

Implementation Mode	Difference
Single-GEM port multi-service mode	Each GPON terminal uses one GEM port to bear various services. ● The Ethernet type (IPoE/PPPoE) is used to differentiate the services. ● The VLAN ID from the GPON terminal is used to differentiate the services. ● The 802.1p value from the GPON terminal is used to differentiate the services. ● The combination of the 802.1p value (Ethernet packet) with the VLAN ID is used to differentiate the services. ● The combination of the Ethernet type (IPoE/PPPoE) with the VLAN ID is used to differentiate the services. The single-GEM port multi-service mode can be used in the following two application scenarios. ● The GPON terminal cannot identify multiple services, and all services have to be mapped into one GEM port. In this case, the OLT identifies the multiple services inside the GEM port, and processes the services. ● The GEM port resource of the GPON terminal is limited. In this case, one GEM port needs to bear multiple services when one service cannot be mapped to one GEM port.

10.2 Configuration Example of the Triple Play Service-xDSL Access

This topic provides an example for configuring the triple play service. On the user side, the VoIP, IPTV, and Internet services are accessed through different service virtual ports. At least three service virtual ports must be configured for each xDSL port. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

Context

Table 10-3 provides the data plan for the triple play service.

Table 10-3 Data plan for the triple play service

Item	Data
Upstream port	0/19/0

Item	Data
Service card	● Port: 0/11/0 ● VoIP service: VPI/VCI = 0/35 ● IPTV service: VPI/VCI = 0/36 ● Internet service: VPI/VCI = 0/37
ADSL profiles	Line profile ● Name: adsl_lineprofile ● Accept the default values for the other parameters. Alarm profile ● Name: alarm_profile ● Accept the default values for the other parameters.
MEF IP traffic profile	VoIP service ● Name: profile_voip ● CIR: 2048 kbit/s ● Priority: 6 ● Accept the default values for the other parameters. IPTV service ● Name: profile_iptv ● CIR: 2048 kbit/s ● Priority: 5 ● Accept the default values for the other parameters. Internet service ● Name: profile_internet ● CIR: 2048 kbit/s ● Priority: 1 ● Accept the default values for the other parameters.
VLAN	VoIP service ● VLAN type: Smart VLAN ● VLAN ID: 11 IPTV service ● VLAN type: Smart VLAN ● VLAN ID: 12 Internet service ● VLAN type: Smart VLAN ● VLAN ID: 13
System parameter profile	● Name: systemprofile ● The profile is already bound to the device.

Item	Data
Program profile	● Name: BTV-1 ● Begin IP Address: 224.1.1.1 ● End IP Address: 224.1.1.1 ● Source IP Address: 10.10.10.10 ● Preview Profile: 0 (the default value)
Rights profile	● Name: profile1 ● The user with the rights can watch BTV-1 in the program library.
Multicast user	● Port: 0/11/0 ● Name: IGMPUserA ● Accept the default values for the other parameters.

Procedure

- Pre-configure the parameters for service provisioning.
  1. Set MEF IP traffic profile.
     a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
     b. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
     c. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
     d. In the dialog box that is displayed, set the parameters.

        VoIP service
        - Name: profile_voip
        - CIR: 2048 kbit/s
        - Priority: 6

        IPTV service
        - Name: profile_iptv
        - CIR: 2048 kbit/s
        - Priority: 5

        Internet service
        - Name: profile_internet
        - CIR: 2048 kbit/s
        - Priority: 1
     e. Click **OK**.

   f. Select the traffic profile, right-click, and then choose **Download to NE**.
   g. In the dialog box that is displayed, select the required NE(s), and click **OK**.
2. Add a program profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.
      - Name: BTV-1
      - Begin IP Address: 224.1.1.1
      - End IP Address: 224.1.1.1
      - Source IP Address: 10.10.10.10
      - Preview Profile: 0 (the default value)
   e. Click **OK**.
3. Add a rights profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.
   c. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.
      - Name: profile1
      - Program list: BTV-1
      - Accept the default values for the other parameters.
   d. Click **OK**.
4. Configure an ADSL line profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **DSL Profile** > **ADSL Profile** from the navigation tree.
   c. Click the **ADSL Line Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

   e. In the dialog box that is displayed, set the parameters.
      - Name: adsl_lineprofile
      - Accept the default values for the other parameters.
   f. Click **Next**.
   g. Click **Finish**.
   h. Select the line profile, right-click, and then choose **Download to NE**.
   i. In the dialog box that is displayed, select the required device, and then click **OK**.

5. Configure an ADSL alarm profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **DSL Profile** > **ADSL Profile** from the navigation tree.
   c. Click the **ADSL Alarm Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
   e. In the dialog box that is displayed, set the parameters.
      - Name: alarm_profile
      - Accept the default values for the other parameters.
   f. Click **Next**.
   g. Click **OK**.
   h. Select the alarm profile, right-click, and then choose **Download to NE**.
   i. In the dialog box that is displayed, select the required device, and then click **OK**.
6. Configure a system parameter profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.
   c. On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
   e. In the dialog box that is displayed, set the name of the system parameter profile to **systemprofile**. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters**, and then click **Next**.
   f. Set related parameters, and then click **Finish**.

   g. Select the system parameter profile whose name is **systemprofile**, right-click, and then choose **Download to NE**.
   h. In the dialog box that is displayed, select a device name.
   i. Click **OK**.
7. Configure a VLAN.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **VLAN** from the navigation tree.
   c. On the **VLAN** tab page, right-click, and then choose **Add**.
   d. In the dialog box that is displayed, set the parameters.

      On the **Base Info** interface, set the parameters as follows.
      - VLAN ID: 11 (Add VLAN IDs 12 and 13 in turn.)
      - Type: Smart VLAN

      On the **Sub Port** tab page of the **Configure VLAN** interface, add 0/19/0 as the upstream port of the VLAN.
   e. Click **Finish**.

- Configure the ADSL access.
  1. Bind an ADSL port with the related profile.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **DSL** > **ADSL Port** from the navigation tree.
     c. On the **ADSL** tag page, select ADSL port 0/11/0, right-click, and then choose **Configure Attributes**.
     d. In the dialog box that is displayed, set the parameters.
        - Line Profile: adsl_lineprofile
        - Alarm Profile: alarm_profile
     e. Click **OK**.
  2. Activate an ADSL port.

     On the **ADSL** tag page, select ADSL port 0/11/00/2/00/1/0, right-click, and then choose **Activate**.
- Configure the VoIP service.
  1. Configure a service virtual port.
     a. Choose **Connection** > **Service Port** from the navigation tree.
     b. On the **Service Port** tab page, right-click, and then choose **Add**.
     c. In the dialog box that is displayed, set the parameters.
        - Connection Type: LAN-ADSL
        - Traffic profile name: profile_voip
        - VLAN ID: 11
        - VPI/VCI: 0/35
        - Interface Selection: 0/11/0

   d. Click **OK**.

- Configure the IPTV service.
  1. Configure a service virtual port. For details, see the steps of configuring a service virtual port when configuring the VoIP service.
     - Connection Type: LAN-ADSL
     - Traffic profile name: profile_iptv
     - VLAN ID: 12
     - VPI/VCI: 0/36
     - Interface Selection: 0/11/0
  2. Configure a multicast VLAN.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **Multicast** > **Multicast VLAN** from the navigation tree.
     c. In the information list, right-click and choose **Add** from the shortcut menu.
     d. In the dialog box that is displayed, set the parameters.
        - IGMP Work Mode: igmp_proxy
        - VLAN ID: 12
     e. Click **OK**.
  3. Configure a multicast upstream port.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **Multicast** > **Virtual Uplink Port** from the navigation tree.
     c. On the **Virtual Uplink Port** tab page, set the filter criteria to display the required virtual upstream ports.
     d. On the tab page, right-click, and then choose **Add**.
     e. In the dialog box that is displayed, set **VLAN ID** to **12** and **Uplink Port Info** to 0/19/0.
     f. Click **OK**.
  4. Apply a program profile to the device.
     a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
     b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
     c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.
     d. Select the program profile whose **Program IP Address** is **224.1.1.1** from the list, right-click, and then choose **Download to NE**.
     e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **Up Port** to 0/19/0 and **VLAN ID** to **12**.

   f. Click **OK**.

5. Apply a rights profile to a device.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. Select the rights profile whose **Name** is **profile1** from the list, right-click, and then choose **Download to NE**.
   e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **Up Port** to 0/19/0 and **VLAN ID** to **12**.
   f. Click **OK**.
6. Configure a multicast user.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **Multicast** > **Multicast User** from the navigation tree.
   c. On the **Multicast User** tab page, right-click, and then choose **Add**.
   d. In the dialog box that is displayed, set the parameters.
      - Alias: IGMPUserA
      - Select **Enable Authorization**.
      - Select the configured service virtual port.
      - Rights profile: profile1
   e. Click **Finish**.
   f. Select a record from the multicast user list, and then click the **User Multicast VLAN** tab below the list. Right-click the list, and then choose **Add**.
   g. In the dialog box that is displayed, select the multicast VLAN 12, and then click **OK**.

- Configure the Internet service.

  Configure a service virtual port. For details, see the steps of configuring a service virtual port when configuring the VoIP service.
  - Connection Type: LAN-ADSL
  - Traffic profile name: profile_internet
  - VLAN ID: 13
  - VPI/VCI: 0/37
  - Interface Selection: 0/11/0
- Save the data.

1. In the **Main Topology**, select the NE in the navigation tree, right-click, and then choose **Save Data Immediately**.
2. Click **OK**.

----End

Result

- The VoIP user can make calls successfully.
- The multicast user whose service port is 0/11/0 can watch the program whose IP address is 224.1.1.1.
- The Internet user can access the Internet in PPPoE dialing mode.

10.3 Configuration Example of the Triple Play Service-GPON Access (Distributed Mode)

This topic provides an example for configuring the triple play service. On the user side, the VoIP, IPTV, and Internet services are accessed through different GEM ports. At least three GEM ports must be configured for each GPON terminal. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

Context

Table 10-4 provides the data plan for the triple play service.

Table 10-4 Data plan for the triple play service

Item	Data
Upstream port	0/19/0
GPON profiles	DBA profile ● Name: dba_profile ● DBA type: Fixed bandwidth ● Fixed bandwidth: 1024 kbit/s ● Accept the default values for the other parameters. ONT capability profile ● Name: ont_profile ● Number of FE ports: 32 ● Accept the default values for the other parameters.

Item	Data
GPON access parameters	ONT - ONT ID: 0 - Authentication mode: SN - SN: ABC02F123456789F GEM port - VoIP service - GEM port ID: 128 - T-CONT ID: 0 - DBA name: dba_profile - Priority queue: 3 - IPTV service - GEM port ID: 129 - T-CONT ID: 0 - DBA name: dba_profile - Priority queue: 2 - Internet service - GEM port ID: 130 - T-CONT ID: 0 - DBA name: dba_profile - Priority queue: 1
MEF IP traffic profile	VoIP service - Name: profile_voip - CIR: 2048 kbit/s - Priority: 6 - Accept the default values for the other parameters. IPTV service - Name: profile_iptv - CIR: 2048 kbit/s - Priority: 5 - Accept the default values for the other parameters. Internet service - Name: profile_internet - CIR: 2048 kbit/s - Priority: 1 - Accept the default values for the other parameters.

Item	Data
VLAN	VoIP service ● VLAN type: Smart VLAN ● VLAN ID: 11 IPTV service ● VLAN type: Smart VLAN ● VLAN ID: 12 Internet service ● VLAN type: Smart VLAN ● VLAN ID: 13
Service Port	VoIP service ● Connection Type: LAN-GPON ● VLAN Choice: Smart VLAN ● VLAN ID: 11 ● Interface Selection: 0/11/0/128 ● Service Type: Single ● Upstream Traffic Profile: profile_voip ● Downstream Traffic Profile: profile_voip IPTV service ● Connection Type: LAN-GPON ● VLAN Choice: Smart VLAN ● VLAN ID: 12 ● Interface Selection: 0/11/0/129 ● Service Type: Single ● Upstream Traffic Profile: profile_iptv ● Downstream Traffic Profile: profile_iptv Internet service ● Connection Type: LAN-GPON ● VLAN Choice: Smart VLAN ● VLAN ID: 13 ● Interface Selection: 0/11/0/130 ● Service Type: Single ● Upstream Traffic Profile: profile_internet ● Downstream Traffic Profile: profile_internet
System parameter profile	● Name: systemprofile ● The profile is already bound to the device.

Item	**Data**
Program profile	● Name: BTV1 ● IP address: 224.1.1.1 ● Source IP address of the program: IP address of the ISP1 (10.10.10.10)
Rights profile	● Name: profile1 ● The user with the rights can watch BTV-1 in the program library.
Multicast user	● Port: 0/11/0 ● Name: IGMPUserA ● Accept the default values for the other parameters.

Procedure

- Pre-configure the parameters for service provisioning.
  1. Configure an MEF IP traffic profile.
     a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
     b. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
     c. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
     d. In the dialog box that is displayed, set the parameters.

        VoIP service
        - Name: profile_voip
        - CIR: 2048 kbit/s
        - Priority: 6

        IPTV service
        - Name: profile_iptv
        - CIR: 2048 kbit/s
        - Priority: 5

        Internet service
        - Name: profile_internet
        - CIR: 2048 kbit/s
        - Priority: 1

     e. Click **OK**.
  2. Configure a VLAN.

   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **VLAN** from the navigation tree.
   c. On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs. Right-click the list, and then choose **Batch Add**.
   d. In the dialog box that is displayed, set the parameters.

      On the **Base Info** tab page, set the parameters as follows.

      - Start ID: 10
      - End ID: 12
      - Type: Smart VLAN

      On the **Sub Port** tab page, set upstream port 0/19/0 as the upstream port of the VLAN.
   e. Click **OK**.
   f. Select VLANs 10, 11, and 12 from the VLAN list, right-click, and then choose **Configure**.
   g. In the dialog box that is displayed, set the parameters.

      On the **L3 Interface** tab page, set **Management Status** to **UP** and **IP Address** to **10.1.1.10**.
   h. Click **OK**.

3. Configure a program profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.
      - Name: BTV1
      - Begin IP Address: 224.0.1.1
      - End IP Address: 224.0.1.1
      - Source IP Address: 10.10.10.10
      - Preview Profile: 0
   e. Click **OK**.
4. Configure a rights profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.
      - Name: profile1
      - Program list: BTV1
      - Accept the default values for the other parameters.
   e. Click **OK**.
5. Configure a DBA profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.
   c. Click the **DBA Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
   d. In the dialog box that is displayed, set the parameters.
      - Name: dba_profile
      - DBA type: Fixed Bandwidth
      - Fixed Bandwidth: 1024 kbit/s
      - Accept the default values for the other parameters.
   e. Click **OK**.
6. Configure an ONT capability profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.
   c. Click the **GPON ONT Capacity Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
   d. In the dialog box that is displayed, set the parameters.
      - Name: ont_profile
      - Number of FE ports: 32
      - Do not select the check box next to **Number of ETH ports**, accept the default values for the other parameters.
   e. Click **OK**.
7. Configure a system parameter profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration**

in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

b. On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.

c. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

d. In the dialog box that is displayed, enter the name of the system parameter profile. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters** navigation tree, and then click **Next**.

NOTE

Set the name of the system parameter profile to **systemprofile**.

e. Click **Finish**.

f. Select the **systemprofile** record, right-click, and then choose **Download to NE**.

g. In the dialog box that is displayed, select the required devices in the left pane, set the task attributes in the right pane, and then click **OK**.

h. Click **OK**.

- Configure the GPON access.

1. Configure an ONT.

a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

b. Choose **GPON** > **GPON Management** from the navigation tree.

c. On the **GPON ONU** tab page, set the filter criteria or click ︾ to display the required GPON ONUs.

d. In the information list, right-click and choose **Add** from the shortcut menu.

e. In the dialog box that is displayed, set the parameters. Click **OK**.

- ONU ID: 0
- capability profile : ont_profile
- Authentication mode: SN
- SN: ABC02F123456789F

f. Select the ONT from the ONT list. Click the **Current ONU: UNI Port Info** tab in the lower pane.

VoIP service

- Select the UNI Port whose **UNI ID** is **1** from the UNI port list, right-click, and then choose **Modify**, set **Defaul VLAN ID** to **11**. Click **OK**. .

IPTV service

- Select the UNI Port whose **UNI ID** is **2** from the UNI port list, right-click, and then choose **Modify**, set **Defaul VLAN ID** to **12**. Click **OK**. .

Internet service

- Select the UNI Port whose **UNI ID** is **3** from the UNI port list, right-click, and then choose **Modify**, set **Defaul VLAN ID** to **13**. Click **OK**. .

   g. Click the **T-CONT Info** tab in the lower pane, right-click, and then choose **Bind**.

   h. In the dialog box that is displayed, set **T-CONT ID** to **0**, and then click ... next to **DBA Name**. In the dialog box that is displayed, select profile **dba_profile**.

   i. Click **OK**.

2. Configure a GEM port.

   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

   b. Choose **GPON** > **GEM Port** from the navigation tree.

   c. In the information list, right-click and choose **Add** from the shortcut menu.

      NOTE

      Add three GEM ports for the VoIP service, IPTV service, and Internet service.

   d. In the dialog box that is displayed, set the parameters. Click **OK**.

      - Shelf/Slot/Port: 0/11/0
      - GEM port ID: 128 (VoIP service), 129 (IPTV service), and 130 (Internet service)

   e. Select the GEM port whose **GEM Port ID** is **128** from the GEM port list, right-click, and then choose **Bind ONT**. In the dialog box that is displayed, set the parameters.

      - Bound ONT: 0/11/0/0
      - T-CONT ID: 0
      - Service Type: ETH
      - Priority queue: 3

   f. Select the GEM port whose **GEM Port ID** is **129** from the GEM port list, right-click, and then choose **Bind ONT**. In the dialog box that is displayed, set the parameters.

      - Bound ONT: 0/11/0/0
      - T-CONT ID: 0
      - Service Type: ETH
      - Priority queue: 2

   g. Select the GEM port whose **GEM Port ID** is **130** from the GEM port list, right-click, and then choose **Bind ONT**. In the dialog box that is displayed, set the parameters.

      - Bound ONT: 0/11/0/0
      - T-CONT ID: 0
      - Service Type: ETH
      - Priority queue: 1

3. Configure a GEM connection.

   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

   b. Choose **GPON** > **GPON Management** from the navigation tree.

c. On the **GPON ONU** tab page, set the filter criteria or click ⌄ to display the required GPON ONUs.

d. Select ONT 0/11/0/0. Click the **Current ONU: UNI Port Info** tab in the lower pane.

NOTE

Add three GEM connections for the VoIP service, IPTV service, and Internet service.

VoIP service

- Right-click, and then choose **Add**, click ... next to **GEM Port ID**, In the dialog box that is displayed, Select the GEM Port whose **GEM Port ID** is **128** from the GEM Port list, Click **OK**. Set **VLAN ID** to **11**. Click **OK**. .

IPTV service

- Right-click, and then choose **Add**, click ... next to **GEM Port ID**, In the dialog box that is displayed, Select the GEM Port whose **GEM Port ID** is **129** from the GEM Port list, Click **OK**. Set **VLAN ID** to **12**. Click **OK**. .

Internet service

- Right-click, and then choose **Add**, click ... next to **GEM Port ID**, In the dialog box that is displayed, Select the GEM Port whose **GEM Port ID** is **130** from the GEM Port list, Click **OK**. Set **VLAN ID** to **13**. Click **OK**. .

e. In the dialog box that is displayed, set the parameters.
  - GEM Port ID: 128 (VoIP service), 129 (IPTV service), and 130 (Internet service)
  - VLAN ID: 11 (VoIP service), 12 (IPTV service), and 13 (Internet service)

f. Click **OK**.

- Configure the VoIP service.
  1. Configure a service virtual port.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **Connection** > **Service Port** from the navigation tree.
     c. In the information list, right-click and choose **Add** from the shortcut menu.
     d. In the dialog box that is displayed, set the parameters.
        - Connection Type: LAN-GPON
        - VLAN Choice: Smart VLAN
        - VLAN ID: 11
        - Interface Selection: 0/11/0/128
        - Service Type: Single
        - Upstream Traffic Profile: profile_voip
        - Downstream Traffic Profile: profile_voip
     e. Click **OK**.
- Configure the IPTV service.
  1. Configure a service virtual port. For details, see the section Configure the VoIP service.

   - Connection Type: LAN-GPON
   - VLAN Choice: Smart VLAN
   - VLAN ID: 12
   - Interface Selection: 0/11/0/129
   - Service Type: Single
   - Upstream Traffic Profile: profile_iptv
   - Downstream Traffic Profile: profile_iptv
2. Configure a DHCP server. For details, see the section Configure the VoIP service.
   - DHCP server group number: 3
   - Primary IP address: 10.2.2.2
   - Secondary IP address: 10.2.2.3
   - Domain name: video
3. Configure a multicast VLAN.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **Multicast** > **Multicast VLAN** from the navigation tree.
   c. On the **Multicast VLAN** tab page, set the filter criteria to display the required multicast VLANs.
   d. In the information list, right-click and choose **Add** from the shortcut menu.
   e. In the dialog box that is displayed, set the parameters.
      - IGMP working mode: igmp_proxy
      - VLAN ID: 12
   f. Click **OK**.
4. Configure a multicast upstream port.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **Multicast** > **Virtual Uplink Port** from the navigation tree.
   c. On the **Virtual Uplink Port** tab page, set the filter criteria to display the required virtual upstream ports.
   d. In the information list, right-click and choose **Add** from the shortcut menu.
   e. In the dialog box that is displayed, set **VLAN ID** to **12** and **Uplink Port Info** to 0/19/0.
   f. Click **OK**.
5. Apply a program profile to the device.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

   c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. Select the program profile whose **IP Address** is **224.0.1.1** from the list, right-click, and then choose **Download to NE**.
   e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **VLAN ID** to **12**.
   f. Click **OK**.

6. Apply a rights profile to a device.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. Select the rights profile whose **Name** is **profile1** from the list, right-click, and then choose **Download to NE**.
   e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **VLAN ID** to **12**.
   f. Click **OK**.
7. Configure a multicast user.
   a. Choose **Multicast** > **Multicast User** from the navigation tree.
   b. On the **Multicast User** tab page, set the filter criteria to display the required multicast users.
   c. In the information list, right-click and choose **Add** from the shortcut menu.
   d. In the dialog box that is displayed, set the parameters.
      - Alias: IGMPUserA
      - Select **Enable Authentication**.
      - Select the configured service virtual port.
      - Rights profile: profile1
   e. Click **Finish**.
   f. Select a record from the multicast user list, and then click the **User Multicast VLAN** tab below the list. Right-click the list, and then choose **Add**.
   g. In the dialog box that is displayed, select the multicast VLAN 12, and then click **OK**.

- Configure the Internet service.

  Configure a service virtual port. For details, see the section Configure the VoIP service.
  - Connection Type: LAN-GPON
  - VLAN Choice: Smart VLAN

  - VLAN ID: 13
  - Interface Selection: 0/11/0/130
  - Service Type: Single
  - Upstream Traffic Profile: profile_internet
  - Downstream Traffic Profile: profile_internet
- Save the data.
  1. On the tab page that is displayed, choose **NE Properties** > **Auto Save Configuaration**> from the navigation tree.
  2. In the right pane, set **Save Type** to **all**, select the **Enable Auto Save** check box, and then set **Absolute Period** or **Relative Period**.
  3. Click **Apply**.

----End

Result

- The VoIP user can make calls successfully.
- The multicast user whose service port is 0/11/0 can watch the program whose IP address is 224.1.1.1.
- The Internet user can access the Internet in PPPoE dialing mode.

10.4 Configuration Example of the Triple Play Service - GPON Access (Profile Mode)

This topic provides an example for configuring the triple play service. On the user side, the VoIP, IPTV, and Internet services are accessed through different GEM ports. At least three GEM ports must be configured for each GPON terminal. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

Context

Table 10-5 provides the data plan for the triple play service.

Table 10-5 Data plan for the triple play service

Item	Data
Upstream port	0/19/0

Item	Data
GPON profiles	DBA profile - Name: dba_profile - DBA type: Fixed bandwidth - Fixed bandwidth: 1024 kbit/s - Use the default values for the other parameters. Line profile - Name: ont_lineprofile - T-CONT ID: 0 - DBA profile: dba_profile - GEM port: - VoIP service: - GEM port ID: 125 - Upstream Priority queue: 3 - IPTV service: - GEM port ID: 126 - Upstream Priority queue: 2 - Internet service: - GEM port ID: 127 - Upstream Priority queue: 1 Service profile - Name: ont_srvprofile - Ethernet port ID: 3 - MAC addresses learning switch: ON - Use the default values for other parameters
GPON access parameters	ONT - ONT ID: 0 - Authentication mode: SN - SN: ABC02F123456789F
MEF IP traffic profile	- Name: profile_voip - CIR: 2048 kbit/s - Priority: 6 - Use the default values for the other parameters.

Item	Data
VLAN	VoIP service ● VLAN type: Smart VLAN ● VLAN ID: 11 IPTV service ● VLAN type: Smart VLAN ● VLAN ID: 12 Internet service ● VLAN type: Smart VLAN ● VLAN ID: 13
Service Port	VoIP service ● Connection Type: LAN-GPON ● VLAN Choice: Smart VLAN ● VLAN ID: 11 ● Interface Selection: 0/11/0/0/125 ● Service Type: Single ● Upstream Traffic Profile: profile_voip ● Downstream Traffic Profile: profile_voip IPTV service ● Connection Type: LAN-GPON ● VLAN Choice: Smart VLAN ● VLAN ID: 12 ● Interface Selection: 0/11/0/0/126 ● Service Type: Single ● Upstream Traffic Profile: profile_iptv ● Downstream Traffic Profile: profile_iptv Internet service ● Connection Type: LAN-GPON ● VLAN Choice: Smart VLAN ● VLAN ID: 13 ● Interface Selection: 0/11/0/0/127 ● Service Type: Single ● Upstream Traffic Profile: profile_internet ● Downstream Traffic Profile: profile_internet
System parameter profile	● Name: systemprofile ● The profile is already bound to the device.

Item	Data
Program profile	● Name: BTV1 ● IP address: 224.1.1.1 ● Source IP address of the program: IP address of the ISP1 (10.10.10.10)
Rights profile	● Name: profile1 ● The user with the rights can watch BTV-1 in the program library.
Multicast user	● Port: 0/11/0 ● Name: IGMPUserA ● Use the default values for the other parameters.

Procedure

- Pre-configure the parameters for service provisioning.
  1. Configure the MEF IP traffic profile.
     a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
     b. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
     c. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
     d. In the dialog box that is displayed, set the parameters.
        - Name: ip_profile
        - CIR: 2048 kbit/s
        - Priority: 6
     e. Click **OK**.
     f. Right-click the traffic profile and choose **Download to NE** from the shortcut menu.
     g. Click **OK**.
  2. Configure the VLAN.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **VLAN** from the navigation tree.
     c. On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs. Right-click in the list and choose **Batch Add** from the shortcut menu.
     d. In the dialog box that is displayed, set the parameters.

        On the **Basic Info** tab page,

- Start VLAN ID: 10
- End VLAN ID: 12
- VLAN type: Smart VLAN

On the **Subport** tab page, add the 0/19/0 upstream port as the upstream port for the VLAN.

e. Click **OK**.

3. Add the program profile.

a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.

d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.

- Name: BTV1
- Start IP address: 224.0.1.1
- End IP address: 224.0.1.1
- Source IP address: 10.10.10.20
- Preview Profile: 0

e. Click **OK**.

4. Add the rights profile.

a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

c. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.

d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.

- Name: profile1
- Program list: BTV1
- Use the default values for other parameters

e. Click **OK**.

5. Configure the DBA profile.

a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration**

in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

b. In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

c. Click the **DBA Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

d. In the dialog box that is displayed, set the parameters.
   - Name: dba_profile
   - DBA type: Fixed bandwidth
   - Fixed bandwidth: 1024 kbit/s
   - Use the default values for other parameters

e. Click **OK**.

f. Right-click the DBA profile and choose **Download to NE** from the shortcut menu.

g. In the dialog box that is displayed, select the required device, and then click **OK**.

6. Configure the line profile.

   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

   b. In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

   c. Click the **GPON Line Profile** tab page.In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

   d. In the dialog box that is displayed, set the parameters.

      a. Choose **Basic Info** from the navigation tree, and then set the basic parameters of the profile.

      b. Choose **T-CONT Info** > **T-CONT0** in the navigation tree and set **DBA Profile** to **dba_profile**.

      c. Right-click **T-CONT0** in the navigation tree and choose **ADD GEM Port** from the shortcut menu. In the dialog box that is displayed, set **GEM Port Index** to **125** and **Upstream Priority Queue** to **3**.

      NOTE

      Repeat the preceding steps to set **GEM Port Index** to **126** and**127**, and **Upstream Priority Queue** to **2** and **1**.

   e. Click **OK**.

   f. Right-click the line profile and choose **Download to NE** from the shortcut menu.

   g. In the dialog box that is displayed, select the required device, and then click **OK**.

7. Configure the service profile.

   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration**

in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

b. In the dialog box that is displayed, choose **PON Profile** > **GPON Profile** from the navigation tree.

c. Click the **GPON Service Profile** tab page.In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

d. In the dialog box that is displayed, set the parameters.

    a. Choose **Basic Info** from the navigation tree, and then set the basic parameters of the profile.
        - Name: ont_srvprofile
        - Number of ETH ports: 3
        - Use the default values for other parameters

    b. Choose **UNI Port** from the navigation tree. In the right pane, right-click a record in the Ethernet port list and choose **UNI Port Configuation Properties** from the shortcut menu.

    c. In the dialog box that is displayed, select the required **Default VLAN ID**, and then click **OK**.

    NOTE

    The Default VLAN IDs for the VoIP service, IPTV service, and Internet service are set to 11, 12, and 13 respectively.

e. Click **OK**.

f. Right-click the line profile and choose **Download to NE** from the shortcut menu.

g. In the dialog box that is displayed, select the required device, and then click **OK**.

8. Configure the system parameter profile.

    a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

    b. In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.

    c. On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.

    d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

    e. In the dialog box that is displayed, enter the name of the system parameter profile. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters** navigation tree, and then click **Next**.

    NOTE

    Set the name of the system parameter profile to **systemprofile**.

    f. Click **Finish**.

g. In the system parameter profile list, right-click **systemprofile** and choose **Download to NE** from the shortcut menu.

h. In the dialog box that is displayed, select the device name.

NOTE

If you select the **Show window of task manager after finished** check box in the dialog box that is displayed, and then click **OK**, the scheduling center window is displayed.

i. Click **OK**.

- Configure the GPON access.

  Configure the ONT.

  1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
  2. Choose **GPON** > **GPON Management** from the navigation tree.
  3. On the **GPON ONU** tab page, set the filter criteria or click ⌄ to display the required GPON ONUs.
  4. Right-click in the list and choose **Add** from the shortcut menu.
  5. In the dialog box that is displayed, set the parameters. Click **OK**.
     - ONT ID: 0
     - Line profile: ont_lineprofile
     - Service profile: ont_srvprofile
     - Authorization mode: SN
     - SN: ABC02F123456789F
  6. Click **OK**.

- Configure the VoIP service.

  Configure the service virtual port.

  1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
  2. Choose **Connection** > **Service Port** from the navigation tree.
  3. Right-click in the list and then choose **Add** from the shortcut menu.
  4. In the dialog box that is displayed, set the parameters.
     - Connection Type: LAN-GPON
     - VLAN Choice: Smart VLAN
     - VLAN ID: 11
     - Interface Selection: 0/11/0/0/125
     - Service Type: Single
     - Upstream Traffic Profile: profile_voip
     - Downstream Traffic Profile: profile_voip
  5. Click **OK**.

- Configure the IPTV service.

  1. Configure the service virtual port. For details, see Configure the service virtual port in Configure the VoIP Service.

  - Connection Type: LAN-GPON
  - VLAN Choice: Smart VLAN
  - VLAN ID: 12
  - Interface Selection: 0/11/0/0/126
  - Service Type: Single
  - Upstream Traffic Profile: profile_iptv
  - Downstream Traffic Profile: profile_iptv

2. Configure the multicast VLAN.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **Multicast** > **Multicast VLAN** from the navigation tree.
   c. In the information list, right-click and choose **Add** from the shortcut menu.
   d. In the dialog box that is displayed, set the parameters.
      - IGMP work mode: igmp_proxy
      - VLAN ID: 12
   e. Click **OK**.
3. Configure a multicast upstream port.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **Multicast** > **Virtual Uplink Port** from the navigation tree.
   c. On the **Virtual Uplink Port** tab page, set the filter criteria to display the required virtual upstream ports.
   d. In the information list, right-click and choose **Add** from the shortcut menu.
   e. In the dialog box that is displayed, set **Multicast VLAN ID** to **12** and **Uplink Port** to 0/19/0.
   f. Click **OK**.
4. Apply a program profile to the device.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the list, right-click the program profile whose **IP Address** is **224.0.1.1** and choose **Download to NE** from the shortcut menu.
   e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **VLAN ID** to **12**.
   f. Click **OK**.
5. Apply a rights profile to a device.

   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the list, right-click the rights profile whose **Name** is **profile1** and choose **Download to NE** from the shortcut menu.
   e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **VLAN ID** to **12**.
   f. Click **OK**.

6. Configure a multicast user.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. Choose **Multicast** > **Multicast User** from the navigation tree.
   c. In the information list, right-click and choose **Add** from the shortcut menu.
   d. In the dialog box that is displayed, set the parameters.
      - Alias: IGMPUserA
      - **Enable Authorization** check box: selected
      - Select Service Port: configured service virtual port
      - Rights profile: profile1
   e. Click **Finish**.
   f. Select a record from the multicast user list, and then click the **User Multicast VLAN** tab below the list. Right-click in the list and choose **Add** from the shortcut menu.
   g. In the dialog box that is displayed, select the multicast VLAN 12, and then click **OK**.

- Configure the Internet service.

  Configure the service virtual port. For details, see Configure the service virtual port in Configure the VoIP Service.
  - Connection Type: LAN-GPON
  - VLAN Choice: Smart VLAN
  - VLAN ID: 13
  - Interface Selection: 0/11/0/0/127
  - Service Type: Single
  - Upstream Traffic Profile: profile_internet
  - Downstream Traffic Profile: profile_internet
- Save the data.

1. On the tab page that is displayed, choose **NE Attribute** > **Auto Save Configuration** from the navigation tree.
2. In the right pane, set **Save Type** to **all**, select the **Enable Auto Save** check box, and then set **Absolute Period** or **Relative Period**.
3. Click **Apply**.

----End

Result

- The VoIP users make calls successfully.
- The multicast user of service port 0/11/0 can watch the program whose IP address is 224.1.1.1.
- The Internet user can access the Internet in PPPoE dialing mode.

10.5 Configuration Example of the Triple Play Service - EPON Access

This topic provides an example for configuring the triple play service. On the user side, the VoIP service, IPTV service, and Internet service are identified by different service virtual ports. On the network side, the upstream port must be configured so that the three types of services are transmitted upstream through different VLANs.

Context

Table 10-6 provides the data plan for the triple play service.

Table 10-6 Data plan for the triple play service

Item	Data
Upstream port	0/19/0

Item	Data
EPON profiles	DBA profile ● Name: dba_profile ● DBA type: Fixed bandwidth ● Fixed bandwidth: 1024 kbit/s ● Use the default values for other parameters Line profile ● Name: ont_lineprofile ● CAR profile: ip_profile ● DBA profile: dba_profile ● Use the default values for other parameters Service profile ● Name: ont_srvprofile ● Ethernet port ID: 3 ● Use the default values for other parameters
ONT	● ONT ID: 0 ● Authentication mode: SN ● SN: ABC02F123456789F
MEF IP traffic profile	VoIP service ● Name: profile_voip ● CIR: 2048 kbit/s ● Priority: 6 ● Use the default values for other parameters IPTV service ● Name: profile_iptv ● CIR: 2048 kbit/s ● Priority: 5 ● Use the default values for other parameters Internet service ● Name: profile_iptv ● CIR: 2048 kbit/s ● Priority: 1 ● Use the default values for other parameters

Item	Data
VLAN	VoIP service - VLAN type: Smart VLAN - VLAN ID: 11 IPTV service - VLAN type: Smart VLAN - VLAN ID: 12 Internet service - VLAN type: Smart VLAN - VLAN ID: 13
System parameter profile	- Name: systemprofile - The profile is already bound to the device.
Program profile	- Name: BTV1 - Begin IP Address: 224.1.1.1 - End IP Address: 224.1.1.1 - Source IP Address: 10.10.10.10 - Preview Profile: 0 (the default value)
Rights profile	- Name: profile1 - The user with the rights can watch BTV1 in the program library.
Multicast user	- Port: 0/1/0 - Name: IGMPUserA - Use the default values for other parameters

Procedure

- Pre-configure the parameters for service provisioning.
  1. Configure the MEF IP traffic profile.
     a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
     b. In the dialog box that is displayed, choose **Traffic Profile** from the navigation tree.
     c. Click the **MEF IP Traffic Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
     d. In the dialog box that is displayed, set the parameters.

        VoIP service

        - Name: profile_voip

  - CIR: 2048 kbit/s
  - Priority: 6

  IPTV service

  - Name: profile_iptv
  - CIR: 2048 kbit/s
  - Priority: 5

  Internet service

  - Name: profile_iptv
  - CIR: 2048 kbit/s
  - Priority: 1

e. Click **OK**.

f. Right-click the MEF IP traffic profile and choose **Download to NE** from the shortcut menu.

g. In the dialog box that is displayed, select the required device, and then click **OK**.

2. Configure the VLAN.

   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

   b. Choose **VLAN** from the navigation tree.

   c. On the **VLAN** tab page, set the filter criteria or click ⏬ to display the VLANs. Right-click in the list and choose **Batch Add** from the shortcut menu.

   d. In the dialog box that is displayed, set the parameters.

      On the **Base Info** tab page, set the parameters as follows.

      - Start VLAN ID: 11
      - End VLAN ID: 13
      - VLAN type: Smart VLAN

      On the **Sub Port Info** tab page, set upstream port 0/19/0 as the upstream port of the VLAN.

   e. Click **OK**.

3. Add the program profile.

   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.

   c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.

   d. In the information list, right-click and choose **Add** from the shortcut menu. In the dialog box that is displayed, set the parameters.

      - Name: BTV1

    - Start IP address: 224.1.1.1
    - End IP address: 224.1.1.1
    - Source IP address: 10.10.10.10
    - Preview Profile: 0 (the default value)
  e. Click **OK**.

4. Add the rights profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.
      - Name: profile1
      - Program list: BTV1
      - Use the default values for other parameters
   e. Click **OK**.

5. Configure the DBA profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.
   c. Click the **DBA Profile** tab. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
   d. In the dialog box that is displayed, set the parameters.
      - Name: dba_profile
      - DBA type: Fixed bandwidth
      - Fixed bandwidth: 1024 kbit/s
      - Use the default values for other parameters
   e. Click **OK**.
   f. Right-click the DBA profile and choose **Download to NE** from the shortcut menu.
   g. In the dialog box that is displayed, select the required device, and then click **OK**.

6. Configure the line profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration**

in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

b. In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.

c. Click the **EPON Line Profile** tab.In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

d. In the dialog box that is displayed, set the parameters.
   - Name: ont_lineprofile
   - CAR profile: ip_profile
   - DBA profile: dba_profile
   - Use the default values for other parameters

e. Click **OK**.

f. Right-click the line profile and choose **Download to NE** from the shortcut menu.

g. In the dialog box that is displayed, select the required device, and then click **OK**.

7. Configure the traffic profile.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **PON Profile** > **EPON Profile** from the navigation tree.
   c. Click the **EPON Service Profile** tab.In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
   d. In the dialog box that is displayed, set the parameters.
      a. Choose **Basic Info** from the navigation tree, and then set the basic parameters of the profile.
         - Name: ont_srvprofile
         - Number of ETH ports: 3
         - Use the default values for other parameters
      b. Choose **UNI Port** from the navigation tree. In the right pane, select the Ethernet port whose **ETH ID** is **1** from the list, right-click, and then choose **Config VLAN Switch of UNI Port** from the shortcut menu.
      c. In the dialog box that is displayed, set **VLAN Type** to **Transparent** and **CVLAN** to **11**, and then click **OK**.

         NOTE

         Repeat the preceding steps to configure the ports whose **ETH ID** is **2** and **3**.
   e. Click **OK**.
   f. Right-click the service profile and choose **Download to NE** from the shortcut menu.
   g. In the dialog box that is displayed, select the required device, and then click **OK**.

8. Configure the system parameter profile.
    a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
    b. In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.
    c. On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.
    d. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
    e. In the dialog box that is displayed, set the name of the system parameter profile to **systemprofile**. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters**, and then click **Next**.
    f. Set related parameters, and then click **Finish**.
    g. In the system parameter profile list, right-click **systemprofile** record and choose **Download to NE** from the shortcut menu.
    h. In the dialog box that is displayed, select the system parameter profile whose **Profile Name** is **systemprofile**, and then configure the attributes of the task.

    NOTE

    If you select **Show window of task manager after finished** in the dialog box, and then click **OK**, the **Scheduling Center** window is displayed.

    i. Click **OK**.

- Configure the EPON access service.

  Configure the ONT.

  1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
  2. Choose **EPON** > **EPON Management** from the navigation tree.
  3. On the **EPON ONU** tab page, set the filter criteria or click ︾ to display the EPON ONUs.
  4. In the information list, right-click and choose **Add** from the shortcut menu.
  5. In the dialog box that is displayed, set the parameters. Click **OK**.
     - ONT ID: 0
     - Authentication mode: SN
     - Line profile: ont_lineprofile
     - Traffic profile: ont_srvprofile
     - SN: ABC02F123456789F
  6. Click **OK**.

- Configure the VoIP service.

  Configure the service virtual port.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **Connection** > **Service Port** from the navigation tree.
3. In the information list, right-click and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters.
   - Traffic profile name: profile_voip
   - VLAN ID: 11
   - Port: 0/1/0
5. Click **OK**.

- Configure the IPTV service.
  1. Configure the service virtual port. For details, see section "Configure the VoIP service".
     - Traffic profile name: profile_iptv
     - VLAN ID: 12
     - Port: 0/1/0
  2. Configure the multicast VLAN.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **Multicast** > **Multicast VLAN** from the navigation tree.
     c. On the **Multicast VLAN** tab page, set the filter criteria to display the required multicast VLANs.
     d. In the information list, right-click and choose **Add** from the shortcut menu.
     e. In the dialog box that is displayed, set the parameters.
        - IGMP working mode: igmp_proxy
        - VLAN ID: 12
     f. Click **OK**.
  3. Configure the multicast upstream port.
     a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
     b. Choose **Multicast** > **Virtual Uplink Port** from the navigation tree.
     c. On the **Virtual Uplink Port** tab page, set the filter criteria to display the required virtual upstream ports.
     d. In the information list, right-click and choose **Add** from the shortcut menu.
     e. In the dialog box that is displayed, set **VLAN ID** to **12** and **Uplink Port Info** to 0/19/0.
     f. Click **OK**.
  4. Apply a program profile to a device.
     a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Program Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. Right-click the program profile whose **Program IP Address** is **224.1.1.1** and choose **Download to NE** from the shortcut menu.
   e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **VLAN ID** to **12**.
   f. Click **OK**.
5. Apply the rights profile to a device.
   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
   b. In the dialog box that is displayed, choose **IGMP Profile** from the navigation tree.
   c. Click the **Right Profile** tab, and select the required device type from the **Device Type** drop-down list.
   d. Right-click the rights profile whose **Name** is **profile1** and choose **Download to NE** from the shortcut menu.
   e. In the dialog box that is displayed, select the required device, set the task attributes in the right pane, and then click **Next**. In the dialog box that is displayed, set **VLAN ID** to **12**.
   f. Click **OK**.
6. Configure the multicast user.
   a. Choose **Multicast** > **Multicast User** from the navigation tree.
   b. In the information list, right-click and choose **Add** from the shortcut menu.
   c. In the dialog box that is displayed, set the parameters.
      - Alias: IGMPUserA
      - Select **Enable Authentication**.
      - Select the configured service virtual port.
      - Rights profile: profile1
   d. Click **Finish**.
   e. Select a record from the multicast user list, and then click the **User Multicast VLAN** tab below the list. Right-click in the list and choose **Add** from the shortcut menu.
   f. In the dialog box that is displayed, select the multicast VLAN 12, and then click **OK**.

- Configure the Internet service.

  Configure the service virtual port. For details, see the section "Configure the VoIP service".
  - Traffic profile name: profile_internet

  - VLAN ID: 13
  - Port: 0/1/0
- Save the data.
  1. On the tab page that is displayed, choose **NE Attribute** > **Auto Save Configuration** from the navigation tree.
  2. In the right pane, set **Save Type** to **all**, select the **Enable Auto Save** check box, and then set **Absolute Period** or **Relative Period**.
  3. Click **Apply**.

----End

Result

- The VoIP user make calls successfully.
- The multicast user whose service port is 0/1/0 can watch the program whose IP address is 224.1.1.1.
- The Internet user can access the Internet in PPPoE dialing mode.

11 Configuring the Private Line Service

About This Chapter

A private line service refers to a service carried over a true or virtual private line on the public network for transparent transmission and for access of private network services.

11.1 Configuring the VLAN Stacking Wholesale Services
VLAN stacking allows batches of users to access the services provided by their respective ISPs according to certain rules.

11.2 Configuring the QinQ VLAN Private Line Service
QinQ VLAN is used in the private line services of enterprise private networks to provide safe channels for the data transmission between the enterprise private networks.

11.1 Configuring the VLAN Stacking Wholesale Services

VLAN stacking allows batches of users to access the services provided by their respective ISPs according to certain rules.

Prerequisites

- The MEF IP traffic profile must be configured. For details, see **5.2 Configuring an MEF IP Traffic Profile** and .
- The required VLAN must be added. For details, see **4.1.2.2 Adding a VLAN**.
- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- The corresponding access services must be configured. For details, see **6.3 Configuring the xDSL Access Services**, **7.2 Configuring the GPON Access Service - Distributed Mode**, **7.3 Configuring the GPON Access Service - Profile Mode**, and **8.2 Configuring the EPON Access Service**.

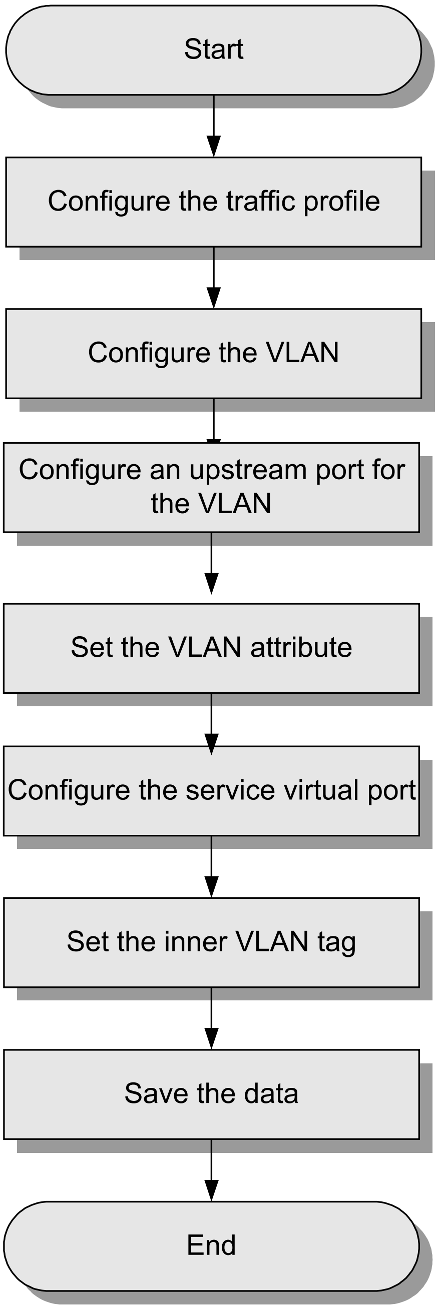
Context

When there are multiple ISPs in the layer 2 metropolitan area network (MAN), the wholesale service allows batches of user to access the services provided by their ISPs according to certain rules.

A stacking VLAN packet has inner and outer VLAN tags that are allocated by the OLT. The upper layer BRAS device authenticates the packet based on the two VLAN tags. Two VLAN tags increases the number of access users.

Figure 11-1 shows the flowchart for configuring the wholesale service.

Figure 11-1 Flowchart for configuring the wholesale service


Start
Configure the traffic profile
Configure the VLAN
Configure an upstream port for the VLAN
Set the VLAN attribute
Configure the service virtual port
Set the inner VLAN tag
Save the data
End

11.1.1 Introduction to VLAN Stacking Wholesale Services

VLAN stacking refers to the stack of the 802.1q tags. It allows the device to add two 802.1q VLAN tags to an untagged user packet or change a tagged user packet into a packet with two 802.1q VLAN tags. The packet with two VLAN tags can be transmitted over the backbone network of the service provider. When the packet reaches the BRAS, the BRAS authenticates the packet based on the two VLAN tags, or removes the outer VLAN tag and identifies the user by the inner VLAN tag.

Copyright © Huawei Technologies Co., Ltd.

Background

The VLAN stacking feature allows the OLT to add an inner 802.1q VLAN tag and an outer 802.1q VLAN tag to an access user packet. The packet with two VLAN tags is transmitted to the layer 2 switching network, and forwarded to the ISP network according to the outer VLAN tag.

Wholesale service: In a layer 2 MAN, there may be multiple Internet service providers (ISPs). The services of these ISPs need to be provisioned to their users quickly. Therefore, the outer VALN tag is used to identify the ISP and the inner VLAN tag is used to identify the user. In this manner, different user groups with different outer VLAN tags can gain access to the specified ISP networks and obtain the services provided by the ISPs.

The broadband service of users 1 and 2 and the broadband service of users 3 and 4 are provided by different ISPs. The VLAN stacking feature allows the OLT to add two VLAN tags to a user packet and forward the user packet to the layer 2 network. The outer VLAN tag is used to identify the ISP and the inner VLAN tag is used to identify the user. The layer 2 switch forwards the user packet to the specified ISP BRAS according to the outer VLAN tag. The ISP BRAS removes the outer VLAN tag and identifies the user by the inner VLAN tag. After being authenticated by the ISP BRAS, the user can access the services provided by the ISP.

11.1.2 Configuring the VLAN Stacking Attribute

Stacking is an attribute of the VLAN. VLAN stacking is mainly used in the wholesale service.

Prerequisites

To set the stacking attribute for the VLAN, make sure that the VLAN must be added. For details, see **4.1.2.2 Adding a VLAN**.

Context

The following VLANs cannot be configured with the stacking attribute:

- Super VLAN
- Sub VLAN
- Standard VLAN
- VLAN with a layer-3 interface
- VLAN with a service virtual port
- Default VLAN
- Reserved VLAN

Procedure

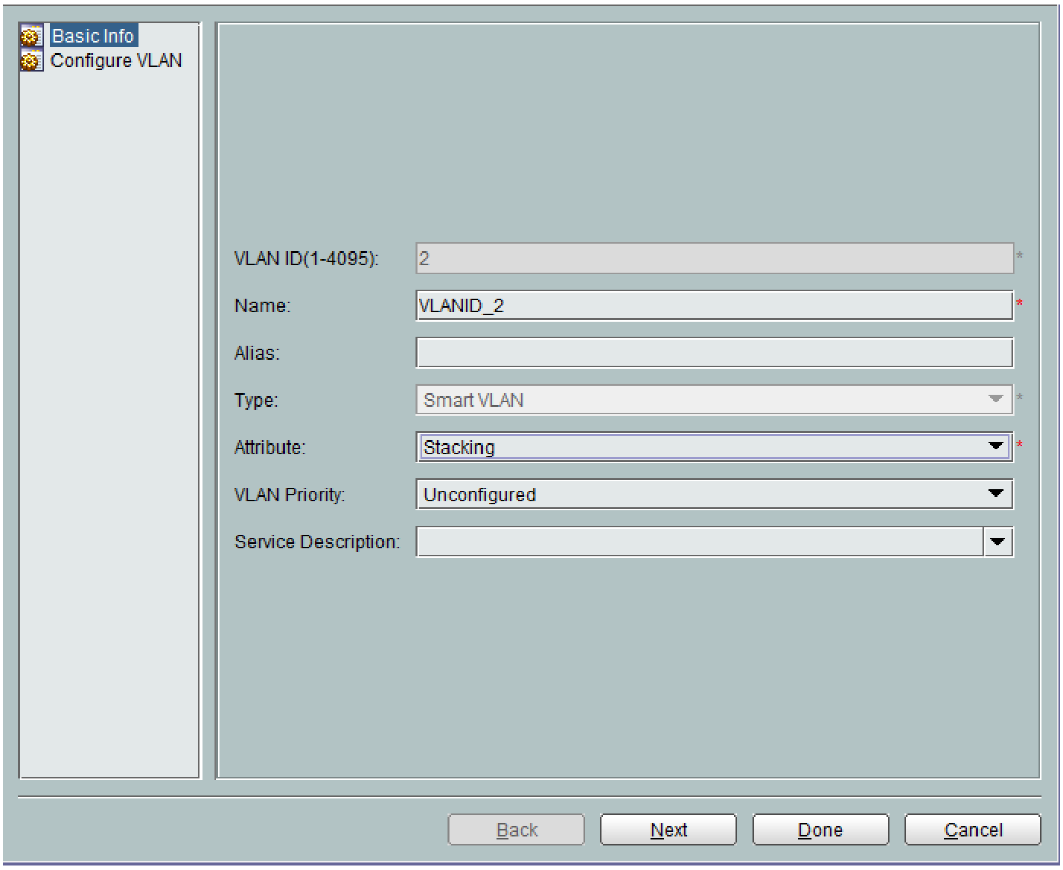
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⏬ to display the VLANs.

Step 4 Select the VLAN to be configured, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, set **Attribute** to **Stacking**.



VLAN ID(1-4095): 2 *
Name: VLANID_2 *
Alias:
Type: Smart VLAN *
Attribute: Stacking *
VLAN Priority: Unconfigured
Service Description:

Step 6 Click **Done**.

----End

11.1.3 Configuring the Inner VLAN Tag

The packet of a VLAN with the stacking attribute has an inner VLAN tag and an outer VLAN tag. The inner VLAN tag is used to identify the user.

Prerequisites

Service virtual ports must be configured for the VLAN with the stacking attribute.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

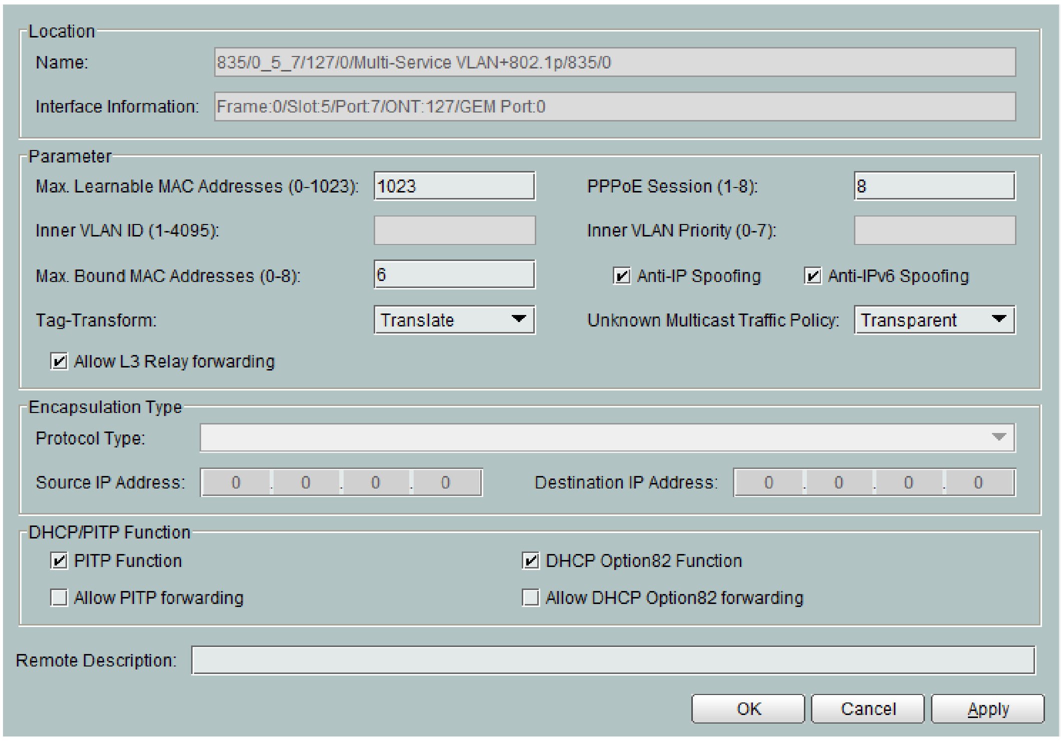
Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.

Step 4 Select the stacking VLAN to be configured, and click the **Service Port** tab in the lower pane.

Step 5 Select a record from the service virtual port list, right-click, and then choose **Configure Extended Properties**.

Step 6 In the dialog box that is displayed, set **Inner VLAN ID**.



Location

Name: 835/0_5_7/127/0/Multi-Service VLAN+802.1p/835/0

Interface Information: Frame:0/Slot:5/Port:7/ONT:127/GEM Port:0

Parameter

Max. Learnable MAC Addresses (0-1023): 1023

PPPoE Session (1-8): 8

Inner VLAN ID (1-4095):

Inner VLAN Priority (0-7):

Max. Bound MAC Addresses (0-8): 6

☑ Anti-IP Spoofing ☑ Anti-IPv6 Spoofing

Tag-Transform: Translate

Unknown Multicast Traffic Policy: Transparent

☑ Allow L3 Relay forwarding

Encapsulation Type

Protocol Type:

Source IP Address: 0 . 0 . 0 . 0

Destination IP Address: 0 . 0 . 0 . 0

DHCP/PITP Function

☑ PITP Function

☑ DHCP Option82 Function

☐ Allow PITP forwarding

☐ Allow DHCP Option82 forwarding

Remote Description:

Step 7 Click **OK**.

----End

11.2 Configuring the QinQ VLAN Private Line Service

QinQ VLAN is used in the private line services of enterprise private networks to provide safe channels for the data transmission between the enterprise private networks.

Prerequisites

- The MEF IP traffic profile must be configured. For details, see **5.2 Configuring an MEF IP Traffic Profile**.
- The corresponding VLAN must exist. For details, see **4.1.2.2 Adding a VLAN**.
- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- The corresponding access services must be configured. For details, see **5 Configuring the Ethernet Access**, **6.3 Configuring the xDSL Access Services**, **7.2 Configuring the GPON Access Service - Distributed Mode**, and **8.2 Configuring the EPON Access Service**.

Context

The private line service allows the private network services to be transparently transmitted to the peer end, for example, on an Intranet.

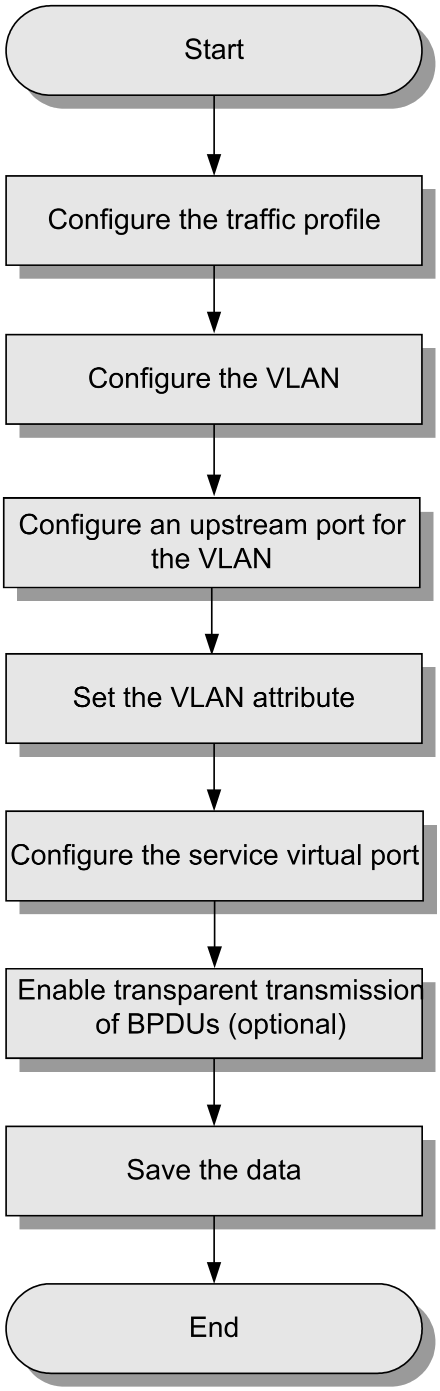
To communicate with each other, users that are on the same private network but at different locations are connected to the public network through the OLT. On the OLT, configure the

Copyright © Huawei Technologies Co., Ltd.

upstream VLAN for user packets from the private network to have the QinQ attribute. In this way, the packet has two VLAN tags: an inner VLAN tag from the private network and an outer VLAN tag from the public network. Through the outer VLAN tag, the packet is transparently transmitted to the peer private network user. In this way, private network users can communicate with each other.

Figure 11-2 shows the flowchart for configuring the private line service.

Figure 11-2 Flowchart for configuring the private line service


Start
Configure the traffic profile
Configure the VLAN
Configure an upstream port for the VLAN
Set the VLAN attribute
Configure the service virtual port
Enable transparent transmission of BPDUs (optional)
Save the data
End

11.2.1 Introduction to the QinQ VLAN Private Line Service

QinQ VLAN is a tunnel protocol based on the 802.1Q encapsulation. QinQ VLAN adds an 802.1Q tag to a VLAN packet that already has an 802.1Q tag from the private network so that this VLAN packet can be transparently transmitted from the private network to the layer-2 VPN through the public network.

Background

The OLT receives a packet with a private VLAN tag and uses the QinQ (802.1Q in 802.1Q) feature to add a public VLAN tag (that is, the QinQ VLAN tag) to the packet. The packet with the private VLAN tag is forwarded to the peer OLT over the public network according to its outer public VLAN tag. The peer OLT removes the outer VLAN tag and transmits the packet to the peer private network.

The OLT also supports the transparent transmission of BPDU packets from a private network to its peer private network by using the QinQ VLAN private line service.

11.2.2 Configuring the VLAN QinQ Attribute

QinQ is an attribute of the VLAN. QinQ VLAN is mainly used in the private line service.

Prerequisites

To set the QinQ attribute for one VLAN, make sure that the VLAN must be added. For details, see **4.1.2.2 Adding a VLAN**.

Context

When adding VLANs in batches, set the QinQ attribute for the VLANs directly.

The following VLANs cannot be configured with the QinQ attribute:

- Super VLAN
- Sub VLAN
- VLAN with a layer-3 interface
- VLAN with a service virtual port
- Default VLAN
- Reserved VLAN

Procedure

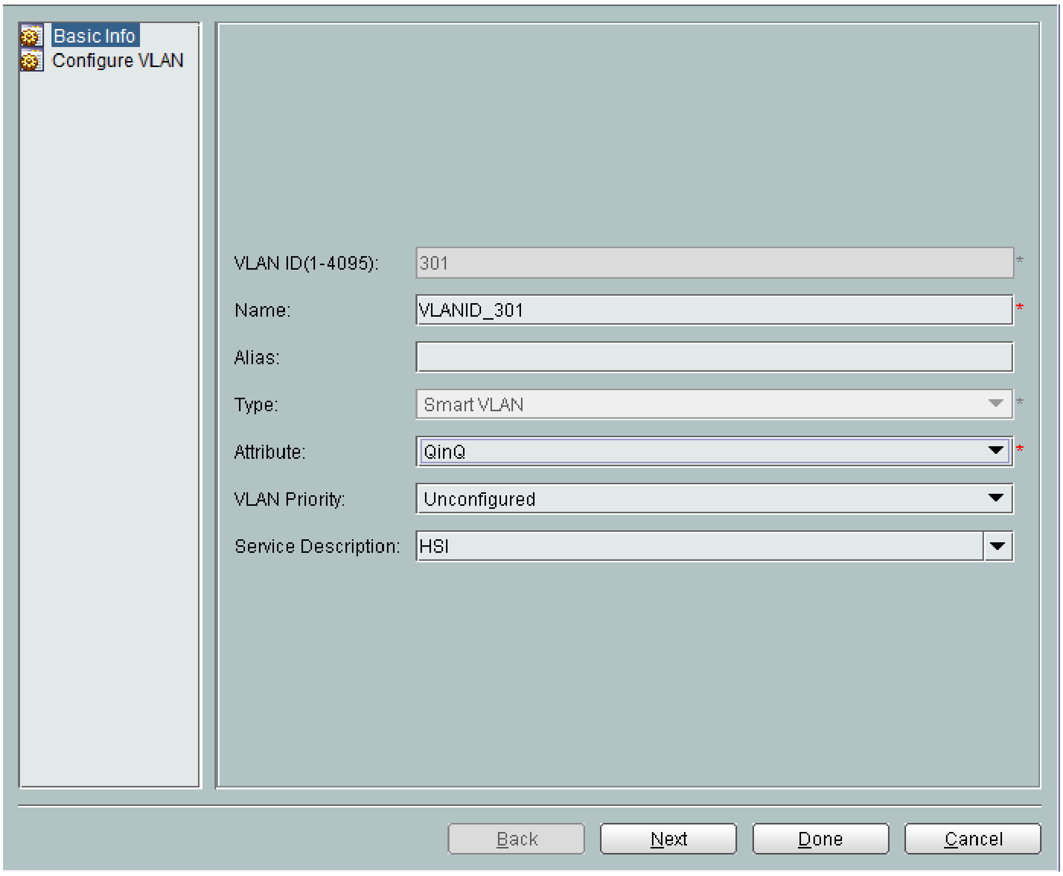
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ▼ to display the VLANs.

Step 4 Select the VLAN to be configured, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, set **Attribute** to **QinQ**.



VLAN ID(1-4095): 301 *

Name: VLANID_301 *

Alias:

Type: Smart VLAN *

Attribute: QinQ *

VLAN Priority: Unconfigured

Service Description: HSI

Step 6 Click **Done**.

----End

11.2.3 Enabling Transparent Transmission of BPDU Packets

This topic describes how to enable the transparent transmission of BPDU packets so that the BPDU packets of a private network can be transparently transmitted over a public network based on the QinQ VLAN feature.

Prerequisites

The QinQ VLAN must be configured. For details, see **11.2.2 Configuring the VLAN QinQ Attribute**.

Context

The transparent transmission of BPDU packets is based on VLAN and realized only through QinQ VLANs.

The private network BPDU packets that can be transparently transmitted refer to the upstream and downstream packets whose MAC addresses range from 01-80-c2-00-00-00 to 01-80-c2-00-00-2f. Note that the BPDU packets whose MAC addresses are 01-80-c2-00-00-00, 01-80-c2-00-00-08, or 01-80-c2-00-00-11 cannot be transmitted transparently.

Procedure

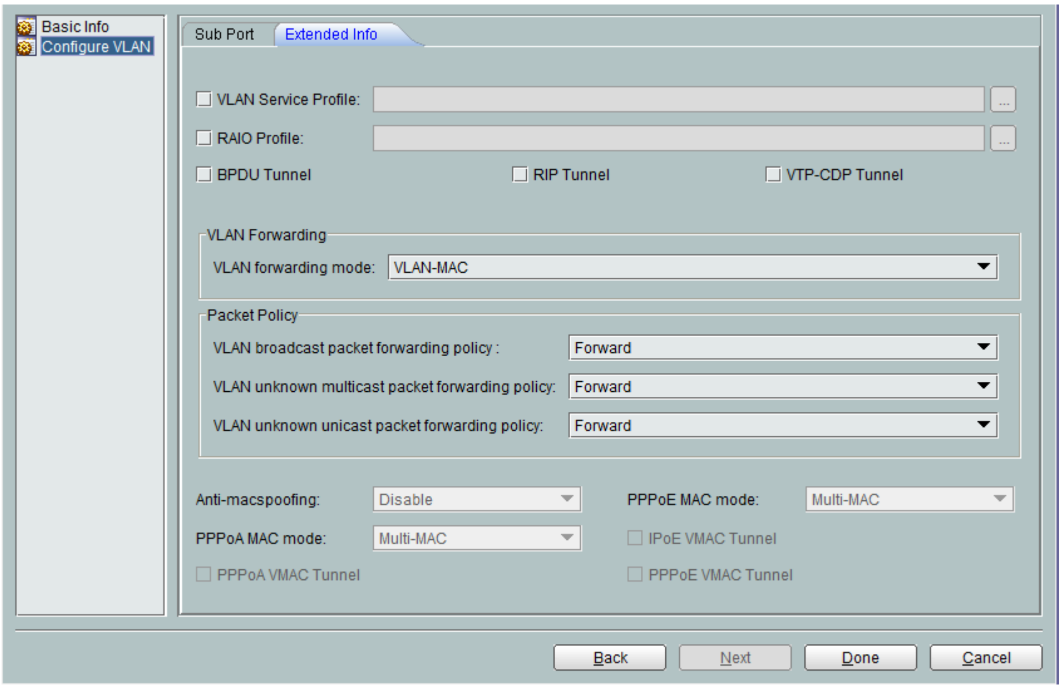
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⇊ to display the VLANs.

Step 4 Select a record from the QinQ VLAN list, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, click the **Extended Info** tab, and select **VLAN Service Profile**, click ... next to **VLAN Service Profile** and then select the required VLAN service profile.



☐ VLAN Service Profile:
☐ RAIO Profile:
☐ BPDU Tunnel ☐ RIP Tunnel ☐ VTP-CDP Tunnel

VLAN Forwarding
VLAN forwarding mode: VLAN-MAC

Packet Policy
VLAN broadcast packet forwarding policy : Forward
VLAN unknown multicast packet forwarding policy: Forward
VLAN unknown unicast packet forwarding policy: Forward

Anti-macspoofing: Disable
PPPoE MAC mode: Multi-MAC
PPPoA MAC mode: Multi-MAC
☐ IPoE VMAC Tunnel
☐ PPPoA VMAC Tunnel
☐ PPPoE VMAC Tunnel

Step 6 Click **Done**.

----End

12 Configuring VPWS Services

About This Chapter

VPWS is a Layer 2 service bearer technology that emulates the basic behaviors and characteristics of services such as ATM, FR, Ethernet, lower-rate TDM and SONET/SDH on a PSN. VPWS is short for virtual private wire service. SONET is short for synchronous optical network. SDH is short for synchronous digital hierarchy. PSN is short for packet switched network.

Context

The IP-oriented networks have strong capabilities to expand and upgrade, and coexist and exchange with other networks. By contrast, limited by transmission modes and service types, traditional ATM networks are hard to share resources and interact with newly deployed networks for management. Therefore, you should determine whether to establish same networks or use existing or public network resources during traditional communication network upgrade and expansion. To provide a solution to this dilemma, many technologies emerge to address the interconnection and interoperability between traditional telecommunication networks and PSNs, and VPWS is one of the technologies.

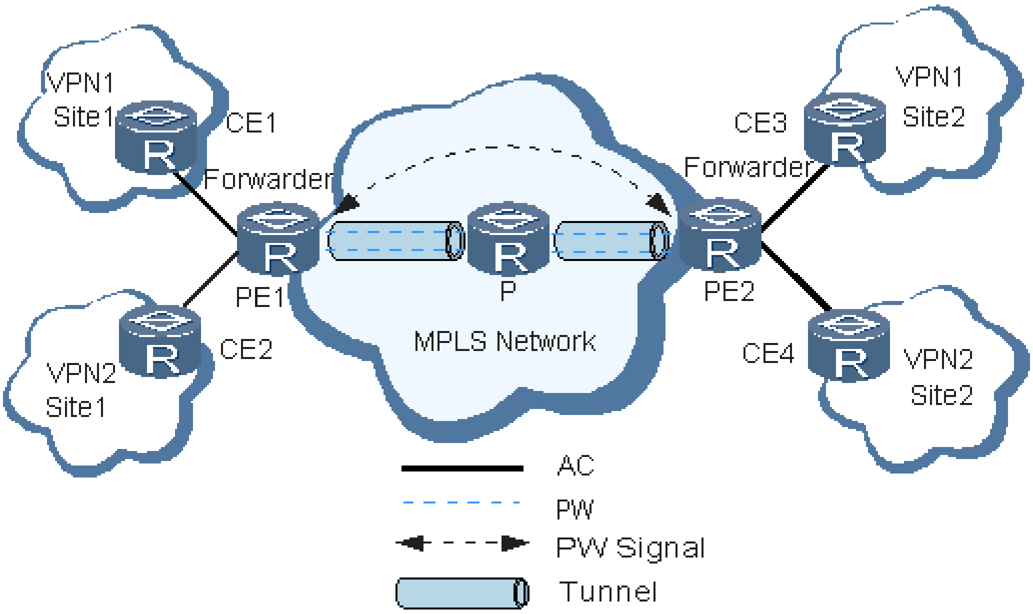
VPWS is a type of point-to-point Layer 2 virtual private network (L2VPN) technology. In addition to sharing some fixed advantages of MPLS L2VPN, VPWS can also interconnect traditional networks and PSNs to share resources and expand networks.

VPWS uses label distribution protocol (LDP) as the signaling protocol, carries various Layer 2 services (such as Layer 2 data packets) at customer edges (CEs) through tunnels (such as MPLS LSP tunnels), and transparently transmits Layer 2 data at CE. A VPWS network consists of the following transmission components:

- Attachment circuit (AC)
- Pseudo wire (PW)
- Forwarder
- Tunnels
- PW signal

The shows the networking of a VPWS service.

Figure 12-1 Networking of a VPWS service



VPN1 packet flow from CE1 to CE3 is used as an example to describe the trend of the basic data flow:

- Layer 2 packets are uploaded at CE1 and access PE1 through AC.
- The forwarder selects a PW to transmit packets after the PE1 receives packets.
- Based on forwarding table entries of the PW, PE1 generates two-layer MPLS labels: the private network label marks the PW and the public network label is used to transmit packets to PE2 through tunnels.
- The private network label is popped out when the Layer 2 packets are transmitted to PE2 through public network tunnels. The public network label is popped out on the penultimate hop on device PE.
- The forwarder of PE2 selects an AC to transmit the Layer 2 packets to CE3.

Static PW

The static PW does not use signal protocol to negotiate parameters but uses commands to manually specify related information, and data is transmitted between PEs through tunnels.

Dynamic PW

Dynamic PWs are established using signal protocols. U-PEs use LDP to exchange PW labels and use PW-ID to bind relevant CEs. After a tunnel is set up and label exchange and binding is implemented between two PEs, a PW is established once when ACs of the two PEs are up.

Dynamic PWs have the following types of information packets:

- Request: requests the peer end to allocate labels.
- Mapping: informs the remote end of local labels and determine whether to carry status words (default Martini mode does not support status words) based on default signal behaviors.

- Notification: notifies of status and negotiate PW status to decrease exchanged packets.
- Withdraw: carries mapping labels and status to notify the peer end to withdraw labels.
- Release: is a response message to withdraw message and notifies the peer end which sends withdraw message to withdraw labels.

PWE3 service expansion on the control plane

Signaling expansion

The notification mode is added to the LDP signaling, notifying of PW status and removing signaling only when PW configurations are deleted or the LDP is interrupted. This mode decreases signaling control packets exchanged between PEs, reduce signal overheads, and is compatible with LDP and Martini modes.

TDM interface expansion

More low-rate TDM interfaces are supported. TDM packet sorting, clock extraction and synchronization is introduced using control words (CWs) and the Real-time Transport Protocol (RTP).

Supporting lower-rate TDM interfaces brings the following benefits:

- Adding encapsulation types (lower-rate TDM packets can be encapsulated.)
- Supporting network triple-play (PSTN, television network, and data network)
- A new way to replace traditional DDN services

Other expansion

PWE3 service expansion on the control plane also includes:

- Adding negotiation mechanism for fragmentation
- Adding PW connectivity detection, such as virtual circuit connectivity verification (VCCV), operation administration and maintenance (OAM), to increase the fast convergence capability and reliability
- Completing the management information base (MIB) function to facilitate MIB maintenance

PWE3 service expansion on the data plane

- Real-time information expansion
- Adding RTP to extract and synchronize clocks
- Ensuring bandwidth, jitter, and delay of telecommunication signals
- Retransmitting orderless packets

12.1 VPWS Configuration Process
The configuration process of the VPWS consists of configure the TDM services, ATM services and Ethernet services. This section describes the operation tasks for configuring the services, and relations between the tasks. When configure and managing the VPWS service, follow the configuration process.

12.2 Configuring an IP Address for the Interface
The loopback interface retains Up after it was created and it works as the source interface of MPLS packets for application protocols, such as MPLS, route protocols, and SNMP. The IP

address of the loopback interface is planned by carriers and must be the same as the value of **Specify LSR(Label Switched Router) identifier**.

12.3 Configuring Global MPLS Parameters
Enable MPLS functions on network-wide NEs by setting global parameters, such as MPLS capability, LDP capability, and specify LSR identifier. Other VPWS configurations take effect only after global MPLS parameters are set.

12.4 Adding a VLAN
Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

12.5 Configuring a Service Port
After being configured successfully, the xDSL service port can carry service streams of various types. The way for configuring other service ports is similar to that for configuring an ADSL service port. The following uses the ADSL port configuration as an example.

12.6 Adding an MPLS VLAN
Before provisioning services to NEs, add an MPLS VLAN. The local peer communicates with the remote peer through the uplink port of the MPLS VLAN.

12.7 Adding an MPLS Interface
The MPLS interface is a Layer 3 interface bound to the MPLS VLAN. The local peer can communicate with the remote peer using LSP after an MPLS interface is added and MPLS LDP is enabled.

12.8 Adding a Remote LDP Peer
The remote peer is a remote label switching router (LSR) which establishes a session with the local LSR. The MPLS discovers the remote peer through LDP extension mechanism. The local peer periodically sends messages in UDP packets to the specified remote peer.

12.9 Adding a Tunnel Policy
A tunnel may carry multiple PWs which are data transmission channels within a tunnel. By default, a VPN instance uses LSPs for service transmission on the backbone network. To use other types of tunnels or configure load balancing for service transmission of the VPN instance, you need to apply a tunnel policy to the VPN instance.

12.10 Adding a PW
Different types of PWs are set up to emulate end-to-end ATM or Ethernet services. Bind the PW to the service VLAN, add the PW label to service VLAN packets, and transmit them through label switched paths (LSPs).

12.11 ATM VPWS Application Case
This topic describes the configuration of ATM VPWS services.

12.12 TDM VPWS Application Case
This topic describes the configuration of TDM VPWS services.

12.1 VPWS Configuration Process

The configuration process of the VPWS consists of configure the TDM services, ATM services and Ethernet services. This section describes the operation tasks for configuring the services, and relations between the tasks. When configure and managing the VPWS service, follow the configuration process.

Figure 12-2 shows the flowchart for configuring an ATM service or an Ethernet service. For details of each step, see the relevant section.

Figure 12-2 ATM VPWS service configuration process

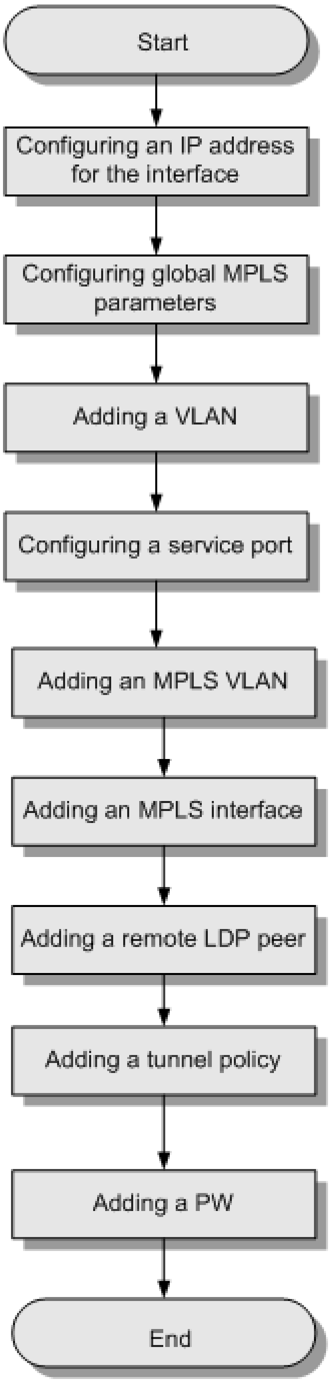
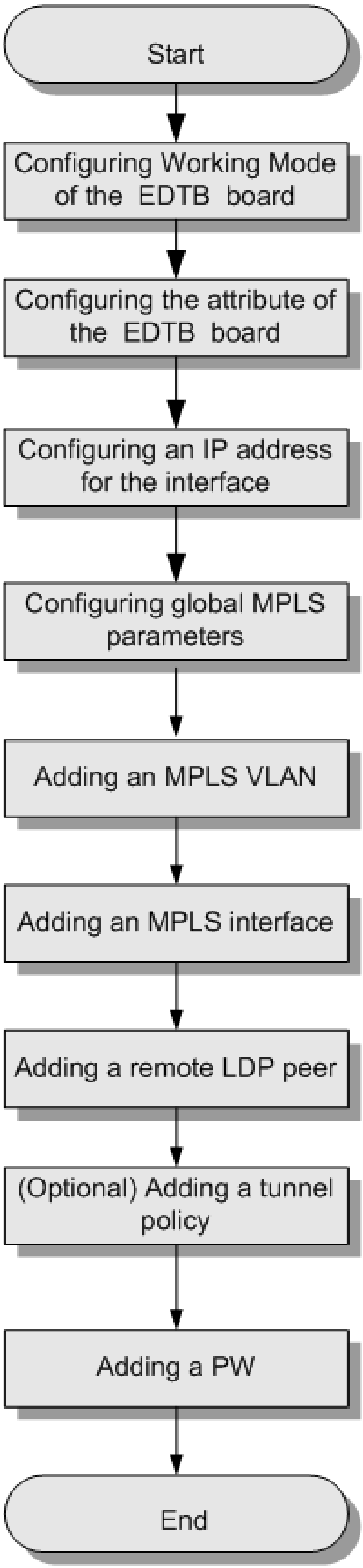


Figure 12-3 shows the flowchart for configuring a TDM service.

Figure 12-3 TDM VPWS service configuration process


Start
Configuring Working Mode of the EDTB board
Configuring the attribute of the EDTB board
Configuring an IP address for the interface
Configuring global MPLS parameters
Adding an MPLS VLAN
Adding an MPLS interface
Adding a remote LDP peer
(Optional) Adding a tunnel policy
Adding a PW
End

12.2 Configuring an IP Address for the Interface

The loopback interface retains Up after it was created and it works as the source interface of MPLS packets for application protocols, such as MPLS, route protocols, and SNMP. The IP address of the loopback interface is planned by carriers and must be the same as the value of **Specify LSR(Label Switched Router) identifier**.

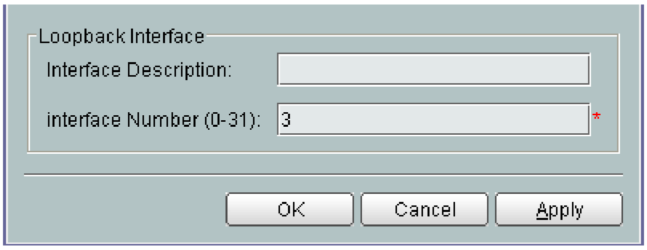
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **LookBack Interface** from the navigation tree.

Step 3 In the information list, right-click in a blank area and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters.



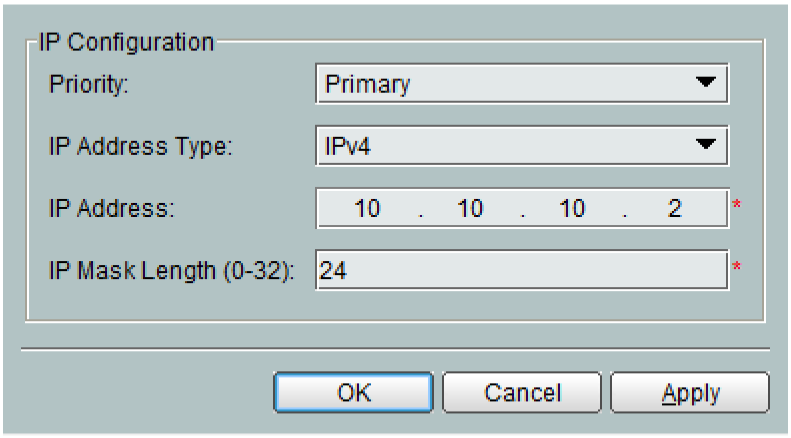
Loopback Interface
Interface Description:
interface Number (0-31): 3 *

Step 5 Click **OK**.

Step 6 Select the loopback and click the **IP Address** tab in the lower pane.

Step 7 In the information list, right-click in a blank area and choose **Add** from the shortcut menu.

Step 8 In the dialog box that is displayed, set the parameters.



IP Configuration
Priority: Primary
IP Address Type: IPv4
IP Address: 10 . 10 . 10 . 2 *
IP Mask Length (0-32): 24 *

Step 9 Click **OK**.

----End

12.3 Configuring Global MPLS Parameters

Enable MPLS functions on network-wide NEs by setting global parameters, such as MPLS capability, LDP capability, and specify LSR identifier. Other VPWS configurations take effect only after global MPLS parameters are set.

Context

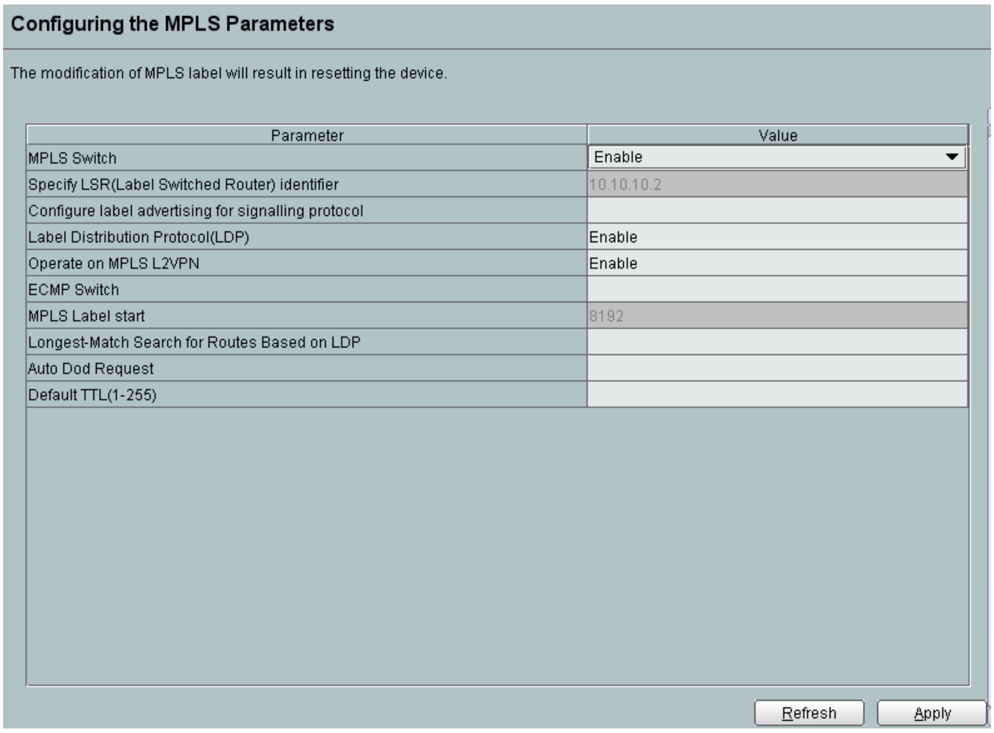
All routers that transmit MPLS services must be configured with basic MPLS settings on MPLS networks.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Properties** > **Protocol** > **MPLS** from the navigation tree.

Step 3 Configure global MPLS parameters in the **Value** column.



Configuring the MPLS Parameters

The modification of MPLS label will result in resetting the device.

Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.2
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

Step 4 Click **Apply**.

----End

12.4 Adding a VLAN

Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

Context

Table 12-1 describes VLAN types and their applications.

Table 12-1 VLAN types and their applications

VLAN Type	Description	Application
Standard VLAN	Ethernet ports in a standard VLAN are interconnected with each other. Ethernet ports in different standard VLANs are isolated from each other. In the standard VLAN, the ports on the same service card are isolated from each other. The ports on different service cards can communicate with each other. Ethernet ports in a standard VLAN are interconnected with each other. Ethernet ports in different standard VLANs are isolated from each other. The standard VLAN and the smart VLAN are mutually exclusive. That is, ports on the same service card cannot be added to a smart VLAN and a standard VLAN concurrently.	Only available for Ethernet ports. Applied to network management and subtending.
Smart VLAN	A smart VLAN contains multiple service virtual ports. In addition, traffic streams on these ports are isolated from each other and traffic streams on different VLANs are isolated from each other. A smart VLAN provides access for multiple users, saving the VLAN resources.	Applied to the access service, such as the residential community access.
MUX VLAN	A MUX VLAN contains only one service virtual port. In addition, traffic streams on different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. In this case, a MUX VLAN can uniquely identify an access user.	Applied to the access service, such as scenarios where users are distinguished based on VLANs.
Super VLAN	The super VLAN is a L3-based VLAN. It consists of multiple sub VLANs. Through ARP proxy, a super VLAN realizes L3 interconnection for these sub VLANs. A sub VLAN can be a standard VLAN, smart VLAN, or a MUX VLAN.	Applied to save IP address resources so that the utilization of the IP address is improved.

Copyright © Huawei Technologies Co., Ltd.

Table 12-2 describes the VLAN attributes.

Table 12-2 VLAN attributes

VLAN Attribute	Application
Common	A VLAN with the common attribute can be used as a L2 VLAN or to create a L3 interface.
QinQ	A QinQ VLAN packet contains two layers of VLAN tags: inner VLAN tag from the private network and outer VLAN tag from the OLT. Through the outer VLAN, a L2 VPN tunnel can be set up to transparently transmit the service between private networks.
Stacking	A stacking VLAN packet contains two layers of VLAN tags: inner VLAN tag and outer VLAN tag from the OLT. With this attribute, the upper layer BRAS device authenticates users based on the two VLAN tags, thus increasing the number of access users. In an upper network in the L2 working mode, you can forward packets according to the "VLAN + MAC", thus providing the wholesale service provisioning function for ISPs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

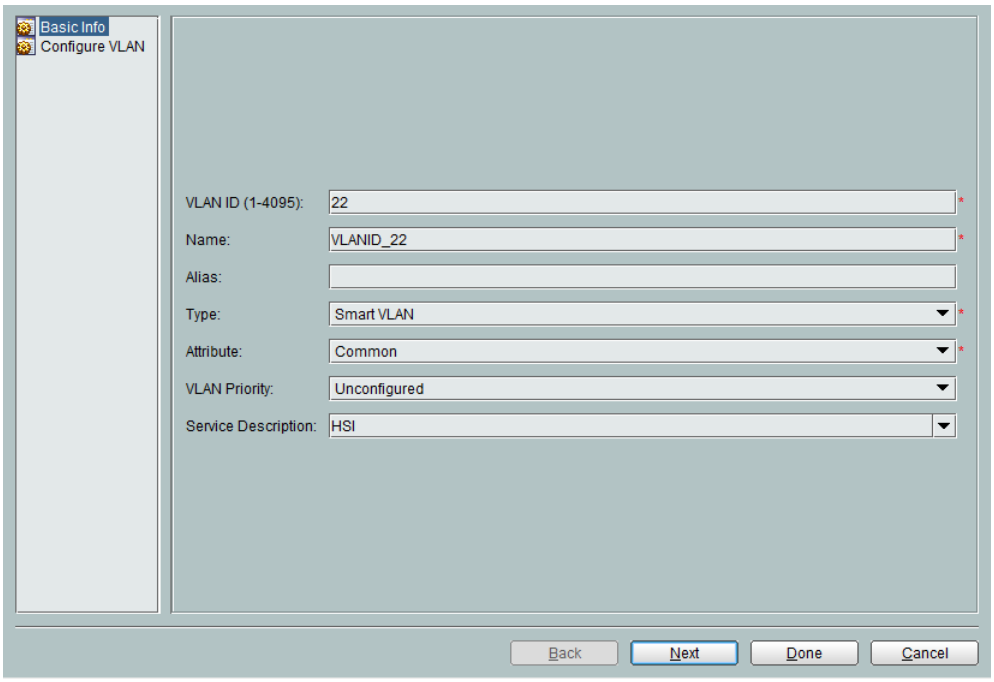
Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⏬ to display the VLANs.

Step 4 Right-click the list, and then choose **Add** or **Batch Add**.

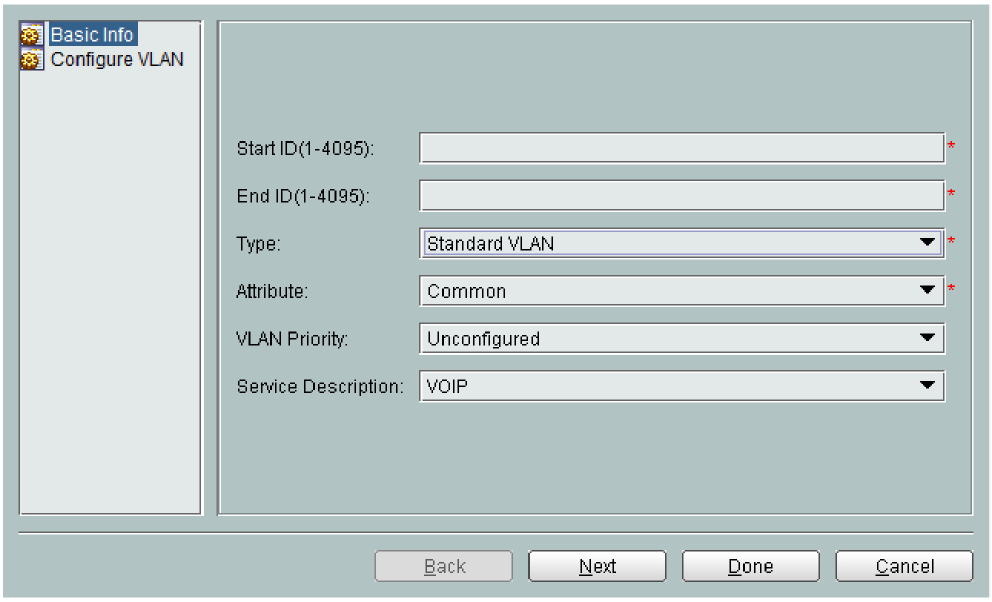
Step 5 In the dialog box that is displayed, set the parameters.

- When you add a VLAN, and then set the parameters as follows:
  - **VLAN ID**
  - **Name**
  - **Alias**
  - **Type**
  - **VLAN Priority**

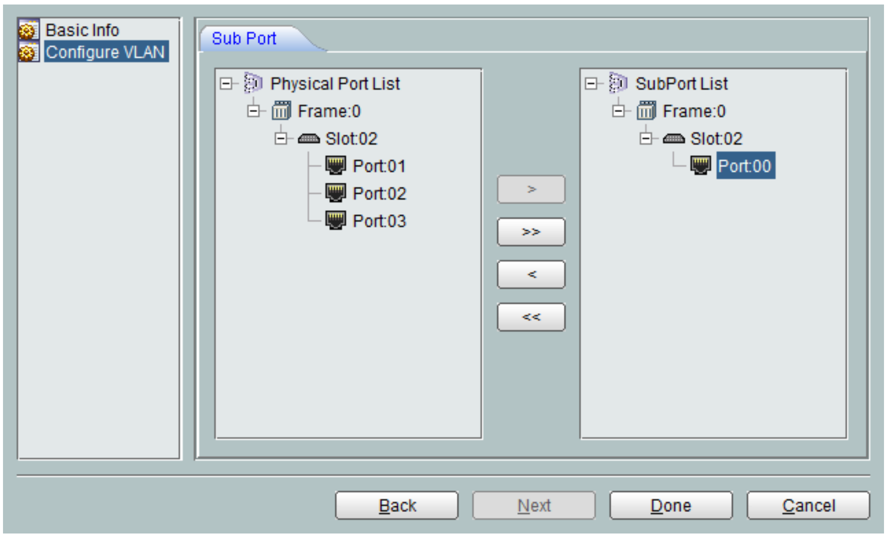


VLAN ID (1-4095): 22 *
Name: VLANID_22 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI

- When you add VLANs in batches, and then set the parameters as follows:
  - **Start ID**
  - **End ID**
  - **Type**
  - **VLAN Priority**



Start ID(1-4095): *
End ID(1-4095): *
Type: Standard VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: VOIP



Step 6 Click **Finish**.

----End

12.5 Configuring a Service Port

After being configured successfully, the xDSL service port can carry service streams of various types. The way for configuring other service ports is similar to that for configuring an ADSL service port. The following uses the ADSL port configuration as an example.

Procedure

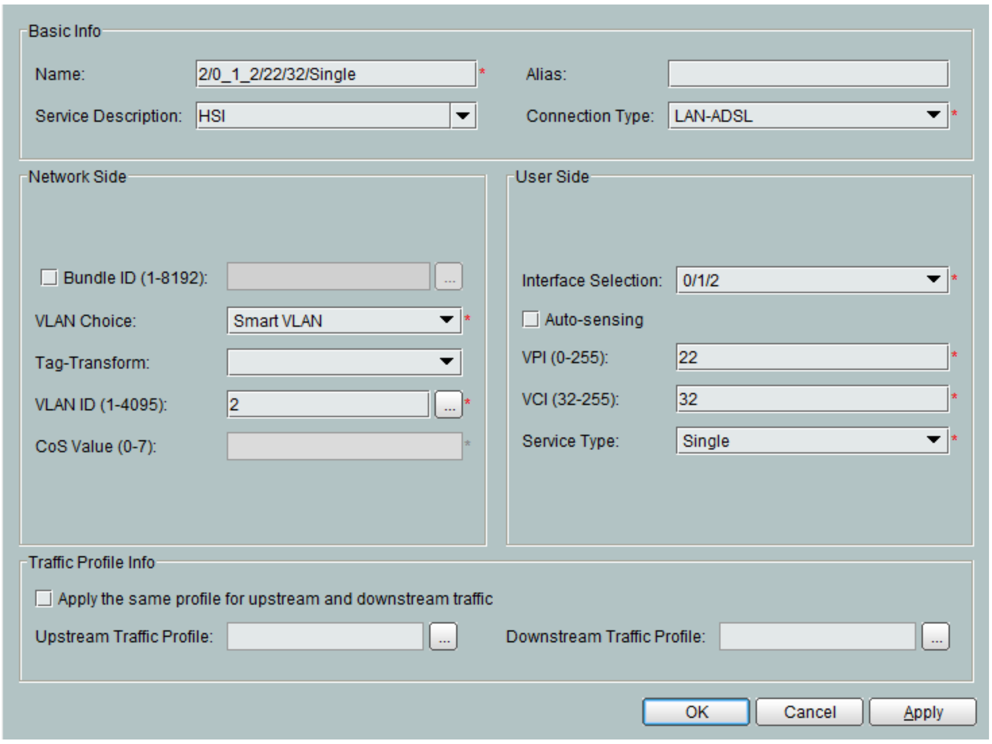
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ≚ to display the ADSL ports.

Step 4 In the information list, select an ADSL port record. On the **Service Port Info** tab page in the lower pane, right-click, and then choose **Add**.

Step 5 In the dialog box that is displayed, input or choose the proper parameters.



Basic Info

Name: 2/0_1_2/22/32/Single *

Alias:

Service Description: HSI

Connection Type: LAN-ADSL *

Network Side

☐ Bundle ID (1-8192):

VLAN Choice: Smart VLAN *

Tag-Transform:

VLAN ID (1-4095): 2 *

CoS Value (0-7):

User Side

Interface Selection: 0/1/2 *

☐ Auto-sensing

VPI (0-255): 22 *

VCI (32-255): 32 *

Service Type: Single *

Traffic Profile Info

☐ Apply the same profile for upstream and downstream traffic

Upstream Traffic Profile:

Downstream Traffic Profile:

NOTE

- The configuration of VLAN ID must be the same as that in **12.4 Adding a VLAN**.
- Select only the MEF IP Traffic Profile that exists on the device. Otherwise, the system reports an error.

Step 6 Click **OK**.

----End

12.6 Adding an MPLS VLAN

Before provisioning services to NEs, add an MPLS VLAN. The local peer communicates with the remote peer through the uplink port of the MPLS VLAN.

Procedure

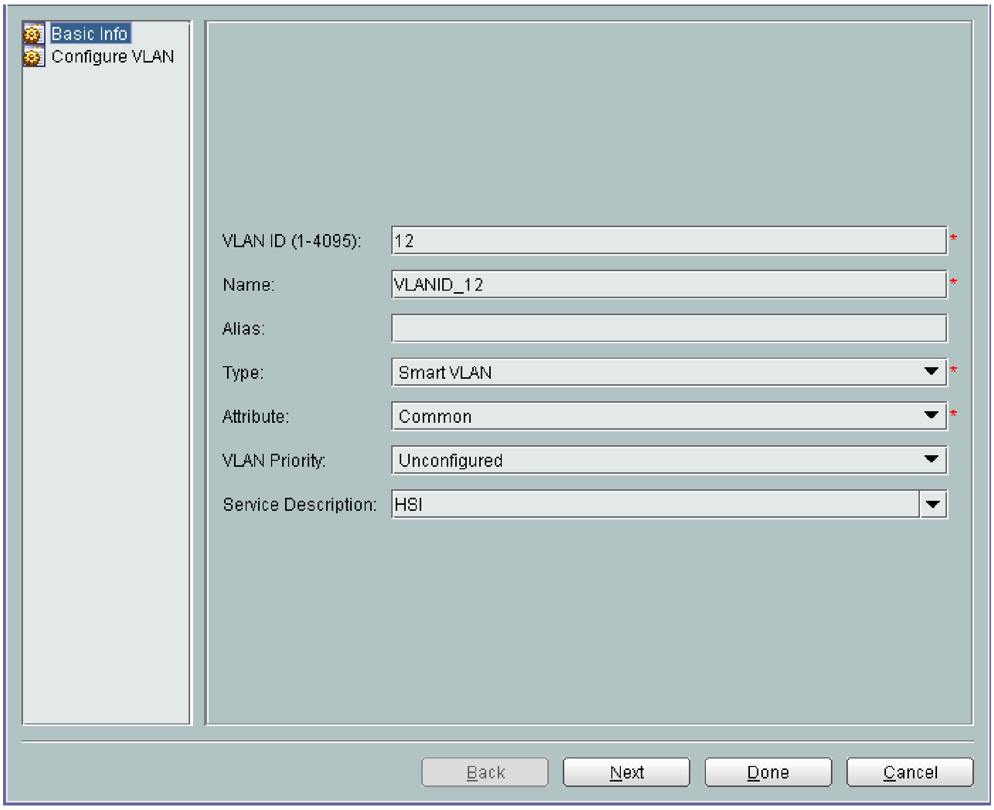
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

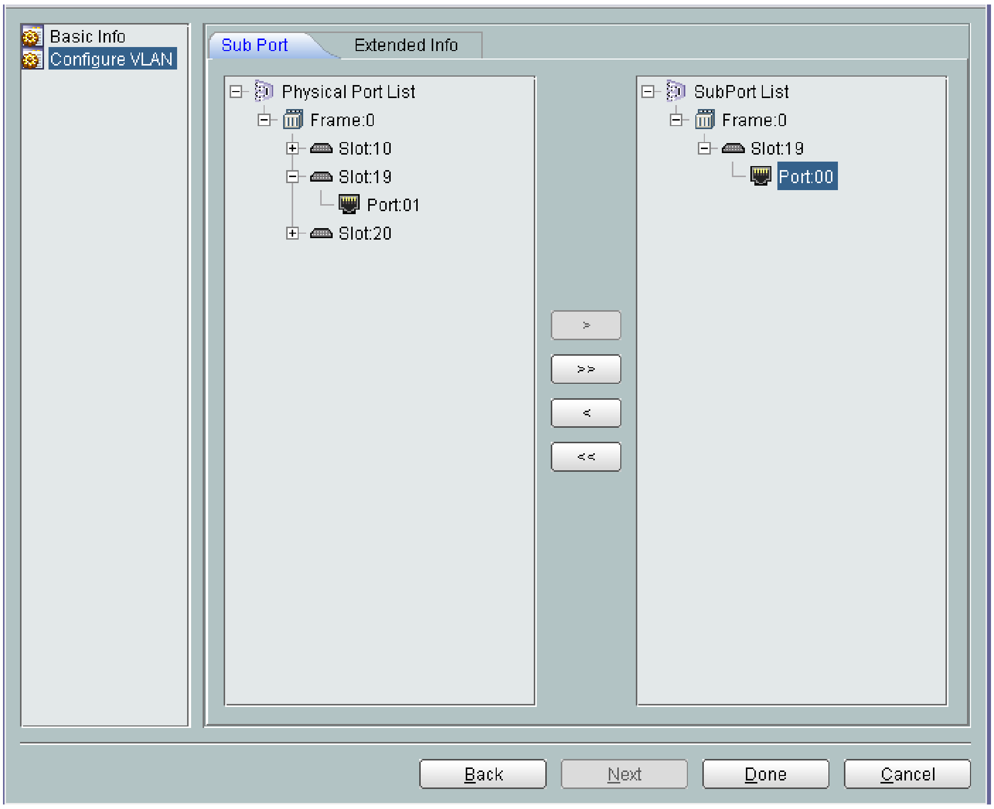
Step 3 On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.

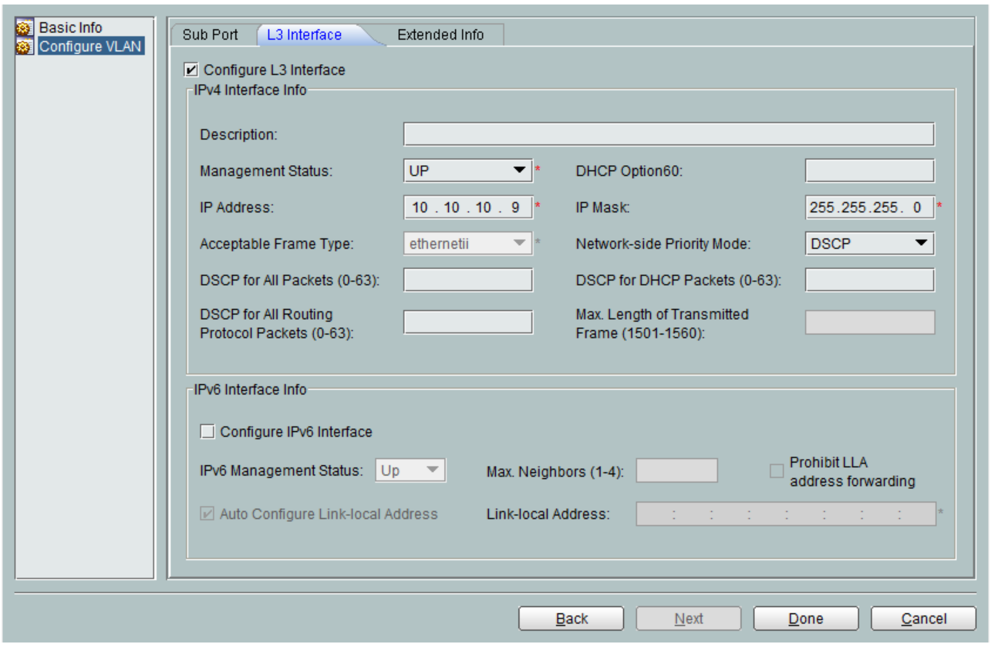
Step 4 In the information list, right-click in a blank area and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12 *
Name: VLANID_12 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI





☑ Configure L3 Interface

IPv4 Interface Info

Description:

Management Status: UP *

DHCP Option60:

IP Address: 10 . 10 . 10 . 9 *

IP Mask: 255 .255 .255 . 0 *

Acceptable Frame Type: ethernetii *

Network-side Priority Mode: DSCP

DSCP for All Packets (0-63):

DSCP for DHCP Packets (0-63):

DSCP for All Routing Protocol Packets (0-63):

Max. Length of Transmitted Frame (1501-1560):

IPv6 Interface Info

☐ Configure IPv6 Interface

IPv6 Management Status: Up

Max. Neighbors (1-4):

☐ Prohibit LLA address forwarding

☑ Auto Configure Link-local Address

Link-local Address: : : : : : : : *

Step 6 Click **Finish**.

----End

12.7 Adding an MPLS Interface

The MPLS interface is a Layer 3 interface bound to the MPLS VLAN. The local peer can communicate with the remote peer using LSP after an MPLS interface is added and MPLS LDP is enabled.

Procedure

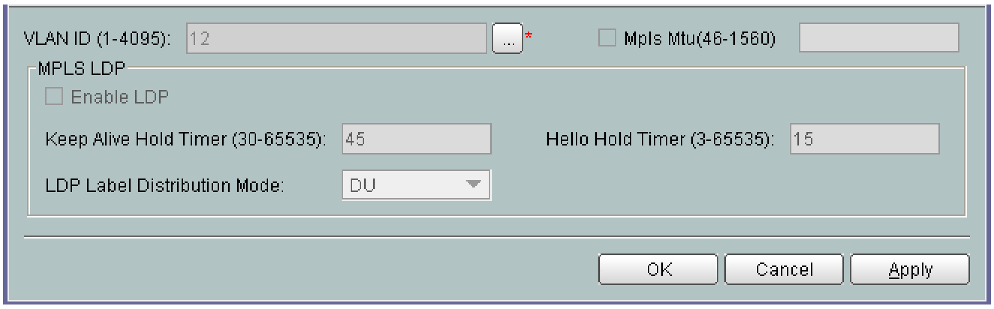
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **MPLS Management** from the navigation tree.

Step 3 Click the **MPLS Interface** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12 *

☐ Mpls Mtu(46-1560)

MPLS LDP

☐ Enable LDP

Keep Alive Hold Timer (30-65535): 45

Hello Hold Timer (3-65535): 15

LDP Label Distribution Mode: DU

Step 6 Click **OK**.

----End

12.8 Adding a Remote LDP Peer

The remote peer is a remote label switching router (LSR) which establishes a session with the local LSR. The MPLS discovers the remote peer through LDP extension mechanism. The local peer periodically sends messages in UDP packets to the specified remote peer.

Procedure

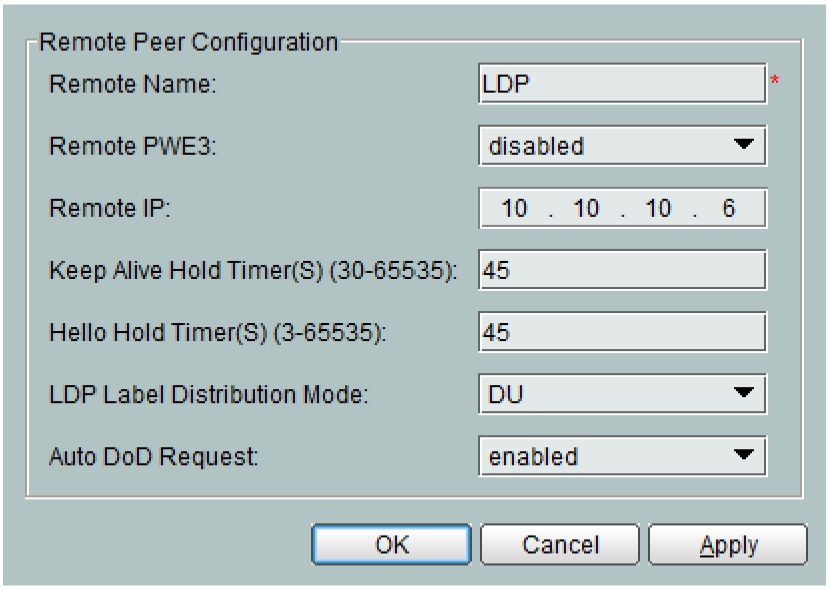
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **MPLS Management** from the navigation tree.

Step 3 Click the **LDP Remote Peer** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: disabled
Remote IP: 10 . 10 . 10 . 6
Keep Alive Hold Timer(S) (30-65535): 45
Hello Hold Timer(S) (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled

Step 6 Click **OK**.

----End

12.9 Adding a Tunnel Policy

A tunnel may carry multiple PWs which are data transmission channels within a tunnel. By default, a VPN instance uses LSPs for service transmission on the backbone network. To use other types of tunnels or configure load balancing for service transmission of the VPN instance, you need to apply a tunnel policy to the VPN instance.

Procedure

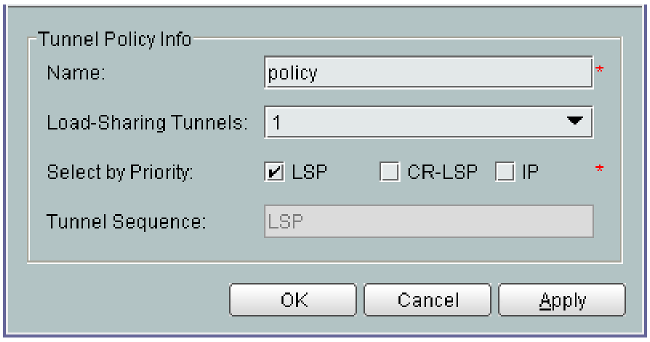
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **MPLS Management** from the navigation tree.

Step 3 Click the **Tunnel Policy** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Tunnel Policy Info
Name: policy *
Load-Sharing Tunnels: 1
Select by Priority: ☑ LSP ☐ CR-LSP ☐ IP *
Tunnel Sequence: LSP

Step 6 Click**OK**.

----End

12.10 Adding a PW

Different types of PWs are set up to emulate end-to-end ATM or Ethernet services. Bind the PW to the service VLAN, add the PW label to service VLAN packets, and transmit them through label switched paths (LSPs).

Procedure

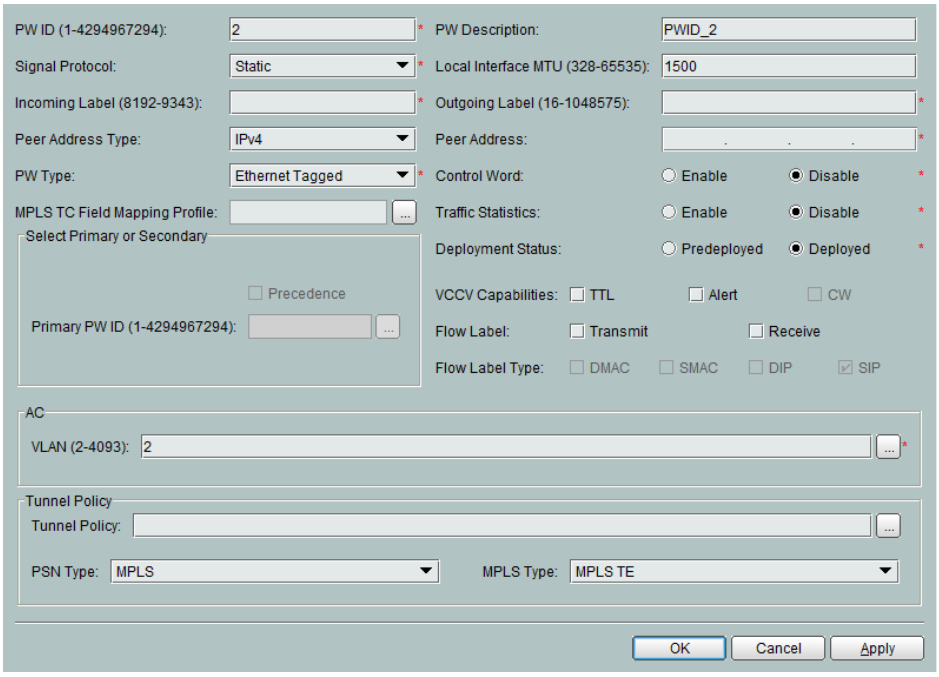
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **VPWS Management** from the navigation tree.

Step 3 Click the **Layer 2 multicast CAC on a PW** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



PW ID (1-4294967294): 2 *
PW Description: PWID_2
Signal Protocol: Static *
Local Interface MTU (328-65535): 1500
Incoming Label (8192-9343): *
Outgoing Label (16-1048575): *
Peer Address Type: IPv4
Peer Address: . . . *
PW Type: Ethernet Tagged *
Control Word: ○ Enable ● Disable *
MPLS TC Field Mapping Profile:
Traffic Statistics: ○ Enable ● Disable *
Select Primary or Secondary
☐ Precedence
Primary PW ID (1-4294967294):
Deployment Status: ○ Predeployed ● Deployed *
VCCV Capabilities: ☐ TTL ☐ Alert ☐ CW
Flow Label: ☐ Transmit ☐ Receive
Flow Label Type: ☐ DMAC ☐ SMAC ☐ DIP ☑ SIP
AC
VLAN (2-4093): 2 *
Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: MPLS TE

Step 6 Click **OK**.

----End

12.11 ATM VPWS Application Case

This topic describes the configuration of ATM VPWS services.

Prerequisites

- The networking shown in **Figure 12-4**has been completed.
- The network devices and lines are functioning properly.
- Service boards are online.

NOTE

Networkings for ATM VPWS and Ethernet VPWS services are described. The networking modes for the two types of services are the same except for differences in the board types of the OLTs and the upstream port types of the ONUs. Therefore, the procedure for configuring ATM VPWS services is described only. Procedures for configuring Ethernet VPWS services are similar to that for configuring ATM VPWS services.

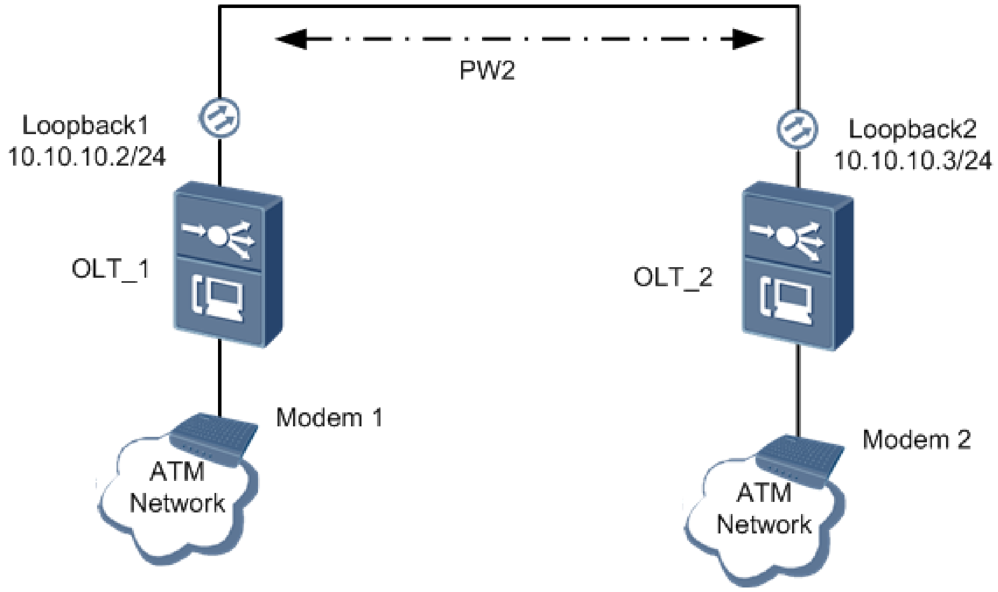
ATM VPWS Networking Description

On carriers' existing access networks, both upstream and downstream of many earlier access devices (such as DSLAM) are in the ATM mode. The IP-oriented networks have strong capabilities to expand and upgrade, and coexist and exchange with other networks. By contrast, limited by transmission modes and service types, traditional ATM networks are hard to share resources and interact with newly deployed networks for management. How can carriers use existing resources to upgrade traditional ATM networks, expand applications and exchange with other networks so that traditional communication networks and PSNs are interconnected?

Transparent ATM transmission is used to migrate existing ATM networks through PSNs. In this manner, carriers do not need to add ATM device to the ISP network and change configurations of ATM CE devices. Traditional ATM services can be emulated to the maximum when traversing PSNs so that end users will not experience differences. Therefore, users' and carriers' existing investment are protected during network integration and construction.

Figure 12-4 shows the networking of an ATM VPWS service. On actual networks, there are multiple routers between two OLTs. The following figure does not show the routers because this case does not require router configuration.

Figure 12-4 Networking of an ATM VPWS service



As shown in **Figure 12-4**, the local CE devices (Modem 1 and Modem 2) carry ATM services and access the MPLS network through OLT. To transparently transmit ATM signals between Modem 1 and Modem 2, set up a PW between two OLT.

On the NMS, ATM VPWS services are implemented in the following way:

- An ATM VPWS service needs to be established between OLT_1 and OLT_2 to emulate ATM services that connect two remote modems.
- The PW is required to connect ATM interfaces of modems for transparently transmitting ATM signals through ISP networks. In this manner, ATM signals do not need to be processed and exchanged at VPC/VCC layer. VPC is short for virtual path connection. VCC is short for virtual channel connection.

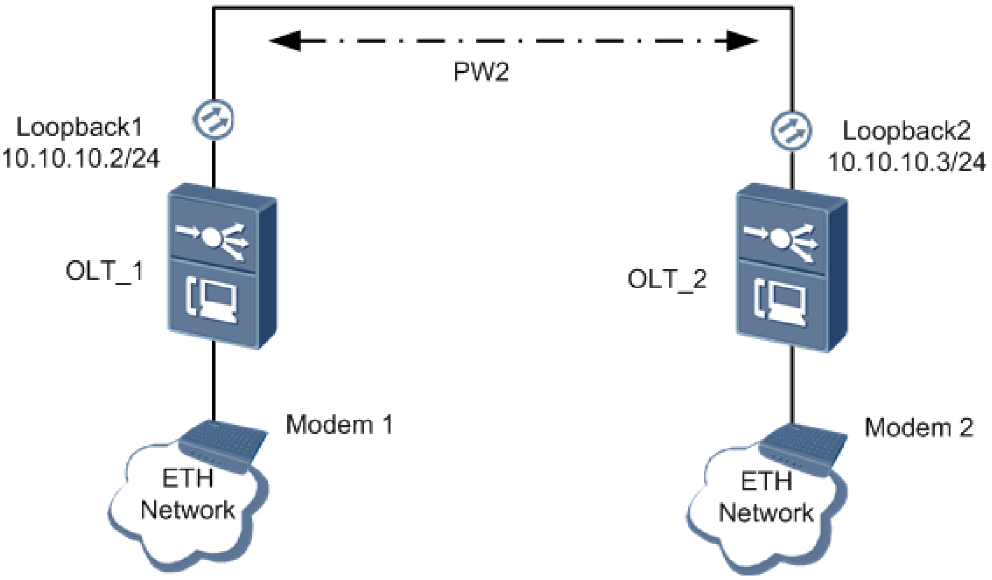
ETH VPWS Networking Description

With the development of IP-based networks, Ethernet is widely used. An enterprise usually uses Ethernet as its intranet. If the enterprise has branches in different places, how can the branches use existing public resources to communicate with each other and be separated from other enterprises?

The VPWS technology is developed to set up an L2VPN so that Ethernet services can be emulated to the maximum when they are transmitted over PSNs. Therefore, Ethernet in different places interconnects with each other.

The shows the networking of an Ethernet VPWS service. On actual networks, there are multiple routers between two OLTs. The following figure does not show the routers because this case does not require router configuration.

Figure 12-5 Networking of an ETH VPWS service



As shown in **Figure 12-5**, CE1 and CE2 are respectively connected to OLT_1 and OLT_2 through GE. VPWS must be configured to transparently transmit service data between CE1 and CE2.

An Ethernet PWE3 service needs to be established between OLT_1 and OLT_2 to emulate Ethernet services that connect two remote CEs.

Data Plan

Table 12-3 Data plan for ATM VPWS configuration

Configuration Item	Data	Remarks
Loopback interface and IP address	OLT_1: ● Interface Number: 3 ● IP Address: 10.10.10.2 ● Ip Mask Length: 24 ● The other parameters use the default values. OLT_2: ● Interface Number: 3 ● IP Address: 10.10.10.3 ● Ip Mask Length: 24 ● The other parameters use the default values.	-
Configuring the MPLS Parameters	OLT_1: ● MPLS Switch: Enable ● Specify LSR(Label Switched Router) identifier: 10.10.10.2 ● Label Distribution Protocol(LDP): Enable ● Operate on MPLS L2VPN: Enable ● The other parameters use the default values. OLT_2: ● MPLS Switch: Enable ● Specify LSR(Label Switched Router) identifier: 10.10.10.3 ● Label Distribution Protocol(LDP): Enable ● Operate on MPLS L2VPN: Enable ● The other parameters use the default values.	**Specify LSR(Label Switched Router) identifier** must be the same as **Ip Address**.

Configuration Item	Data	Remarks
Service VLAN	OLT_1 or OLT_2: ● VLAN ID: 10 ● Type: Smart VLAN ● Attribute: QinQ ● Sub Port: 0/9/0 ● The other parameters use the default values.	-
Service-port	OLT_1 or OLT_2: ● Connection Type: LAN-ADSL ● Interface Selection: 0/16/0 ● VLAN Choice: Smart VLAN ● VLAN ID: 10 ● Auto-sensing: selected **Auto-sensing** check box ● Service Type: Single ● Upstream Traffic Profile/ Downstream Traffic Profile: ip-traffic-table_2 ● The other parameters use the default values.	**VLAN ID** must be the same as the **VLAN ID** of the service VLAN.
MPLS VLAN	OLT_1: ● VLAN ID: 12 ● Type: Smart VLAN ● Attribute: Common ● Sub Port: 0/9/0 ● Management Status: UP ● IP addresses: 10.10.10.6 ● The other parameters use the default values. OLT_2: ● VLAN ID: 12 ● Type: Smart VLAN ● Attribute: Common ● Sub Port: 0/9/0 ● Management Status: UP ● IP Address: 10.10.10.7 ● The other parameters use the default values.	-

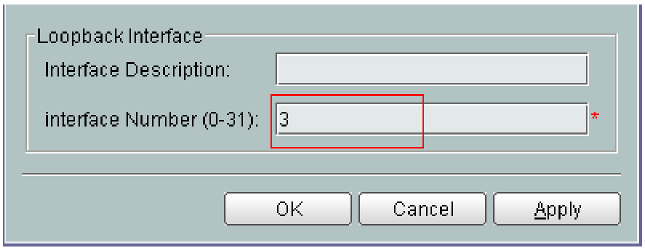
Configuration Item	Data	Remarks
MPLS interface	OLT_1 or OLT_2: ● VLAN ID: 12 ● Mpls Mtu: 60 ● Enable LDP: selected **Enable LDP** check box ● The other parameters use the default values.	**VLAN ID** must be the same as the **VLAN ID** of the MPLS VLAN.
Remote Peer Configuration	OLT_1: ● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.3 ● The other parameters use the default values. OLT_2: ● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.2 ● The other parameters use the default values.	-
PW	OLT_1: ● PW ID: 2 ● Signal Protocol: LDP ● Peer Address: 10.10.10.3 ● VLAN ID: 10 ● MPLS Type: mplsNonTe ● The other parameters use the default values. OLT_2: ● PW ID: 2 ● Signal Protocol: LDP ● Peer Address: 10.10.10.2 ● VLAN ID: 10 ● MPLS Type: mplsNonTe ● The other parameters use the default values.	**Virtual local area network (VLAN)** must be the same as the **VLAN ID** of the service VLAN.

Procedure

Step 1 Configure an IP address for the interface.

As the source interface of MPLS packets, the loopback interface retains Up after it was created. The IP address of the loopback interface is planned by carriers and must be the same as the value of **Specify LSR(Label Switched Router) identifier**. Configure OLT_1 and OLT_2 as follows:

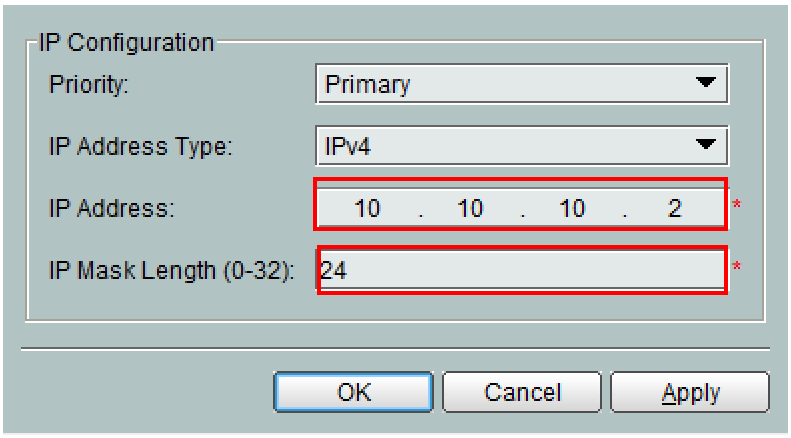
1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **LookBack Interface** from the navigation tree.
3. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters.



Interface Description:
interface Number (0-31): 3 *

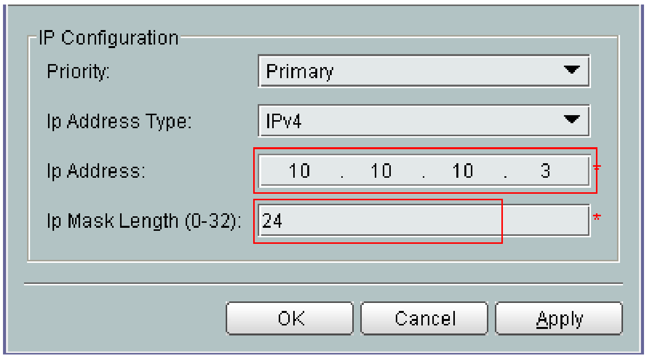
5. Click **OK**.
6. Select the loopback and click the **IP Address** tab in the lower pane.
7. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
8. In the dialog box that is displayed, set the parameters.

Configuring parameters for OLT_1



Priority: Primary
IP Address Type: IPv4
IP Address: 10 . 10 . 10 . 2 *
IP Mask Length (0-32): 24 *

Configuring parameters for OLT_2



Priority: Primary

Ip Address Type: IPv4

Ip Address: 10 . 10 . 10 . 3 *

Ip Mask Length (0-32): 24 *

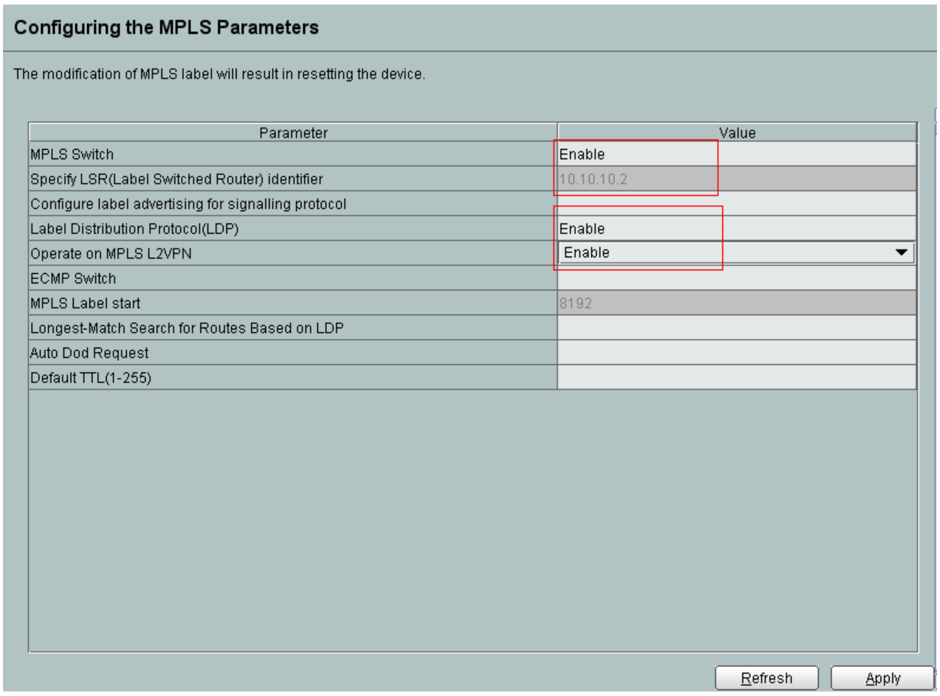
9. Click **OK**.

Step 2 Configure the global MPLS parameters.

Enable MPLS functions on network-wide NEs by setting global parameters, such as MPLS capability, LDP capability, and specify LSR identifier. Other VPWS configurations take effect only after global MPLS parameters are set. Configure OLT_1 and OLT_2 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **NE Properties** > **Protocol** > **MPLS** from the navigation tree.
3. Configure global MPLS parameters in the **Value** column.

Configuring parameters for OLT_1

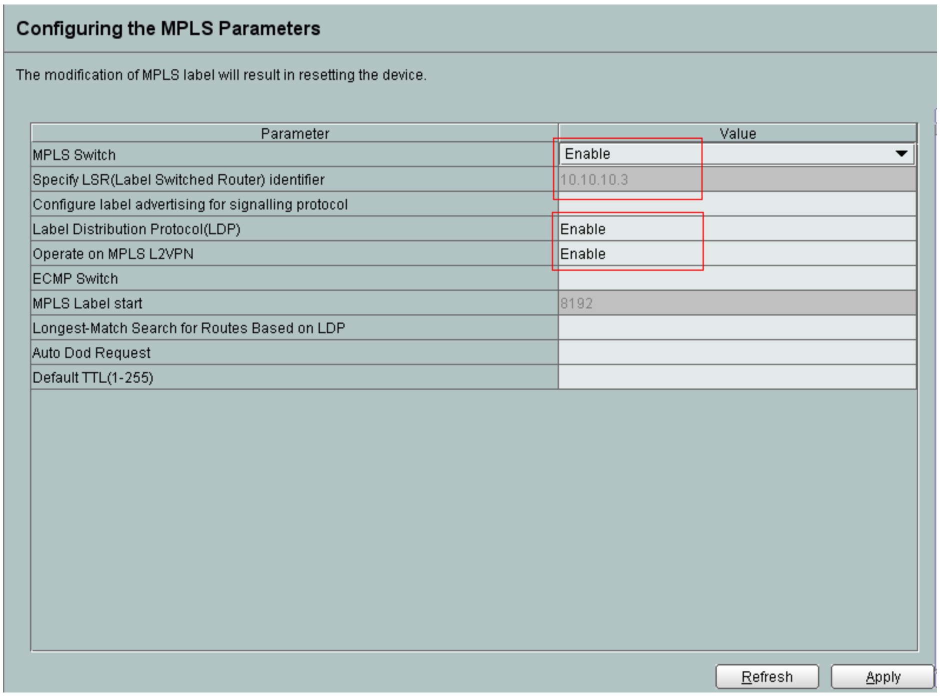


Configuring the MPLS Parameters

The modification of MPLS label will result in resetting the device.

Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.2
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

Configuring parameters for OLT_2



Configuring the MPLS Parameters

The modification of MPLS label will result in resetting the device.

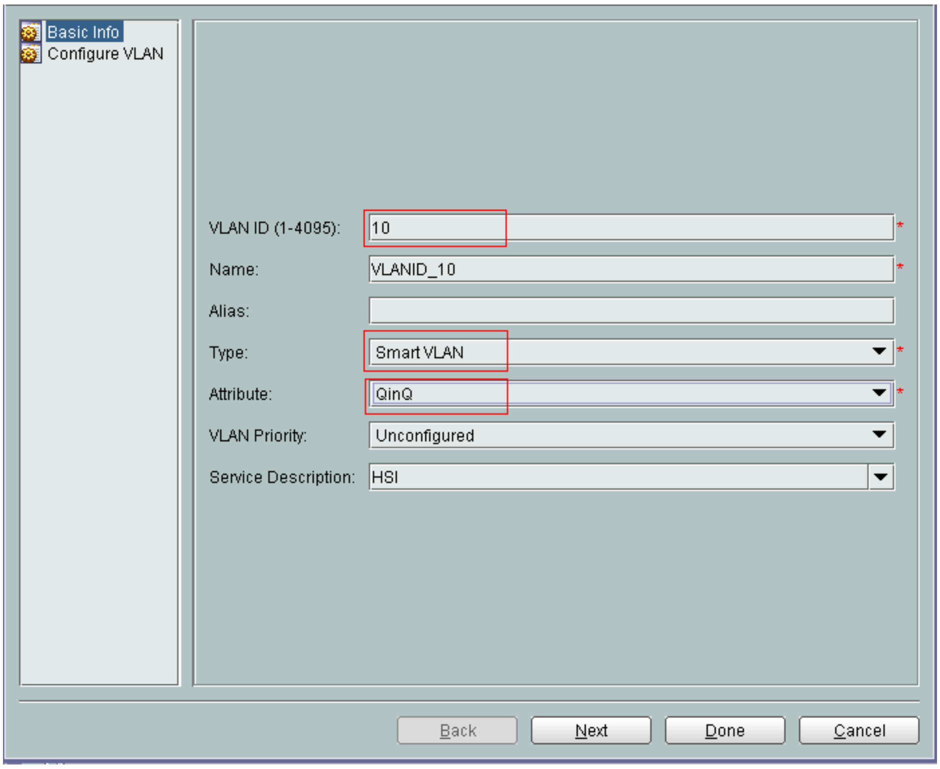
Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.3
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

4. Click **Apply**.

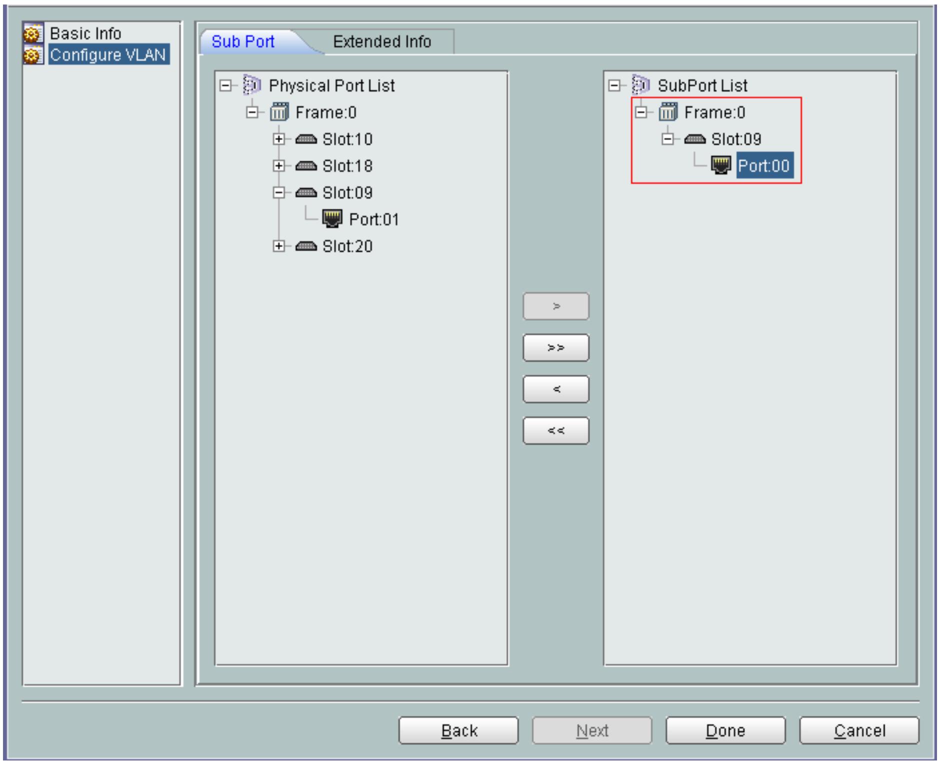
Step 3 Add a service VLAN.

Configure OLT_1 and OLT_2 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.
4. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 10 *
Name: VLANID_10 *
Alias:
Type: Smart VLAN *
Attribute: QinQ *
VLAN Priority: Unconfigured
Service Description: HSI

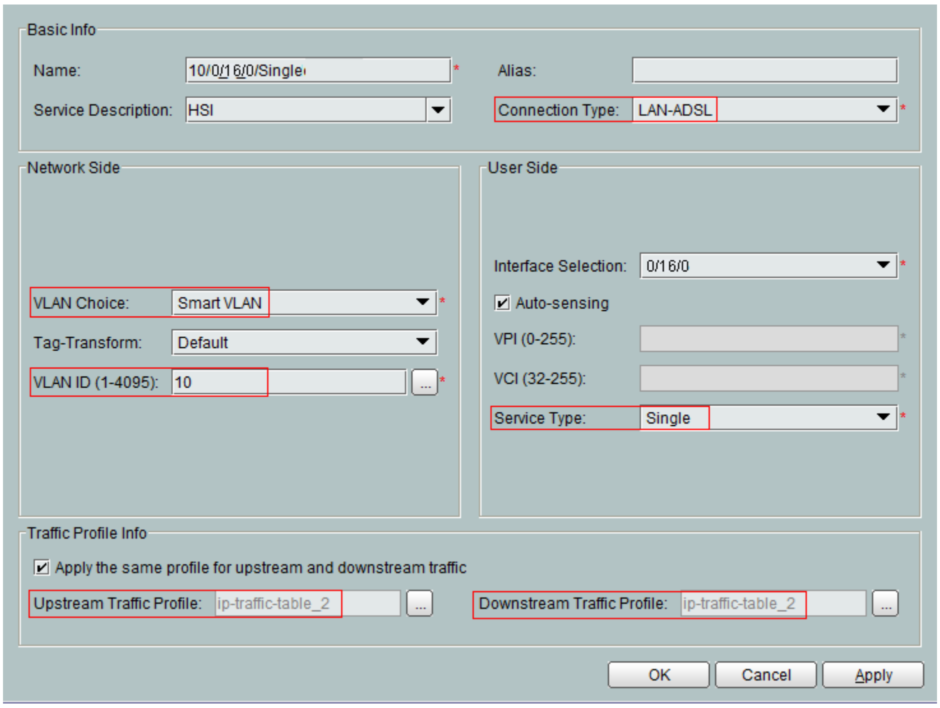


6. Click **Finish**.

Step 4 Add a service port.

The service port can carry various service flows after it is configured. Configure MA5600T_1 and MA5600T_2 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **ADSL Port** from the navigation tree.
3. On the **ADSL** tab page, set the filter criteria or click ⩔ to display the ADSL ports.
4. In the information list, select an ADSL port record and click the **Service Port Info** tab. On the tab, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



Basic Info
Name: 10/0/16/0/Single *
Alias:
Service Description: HSI
Connection Type: LAN-ADSL *

Network Side
VLAN Choice: Smart VLAN *
Tag-Transform: Default
VLAN ID (1-4095): 10 *

User Side
Interface Selection: 0/16/0 *
☑ Auto-sensing
VPI (0-255):
VCI (32-255):
Service Type: Single *

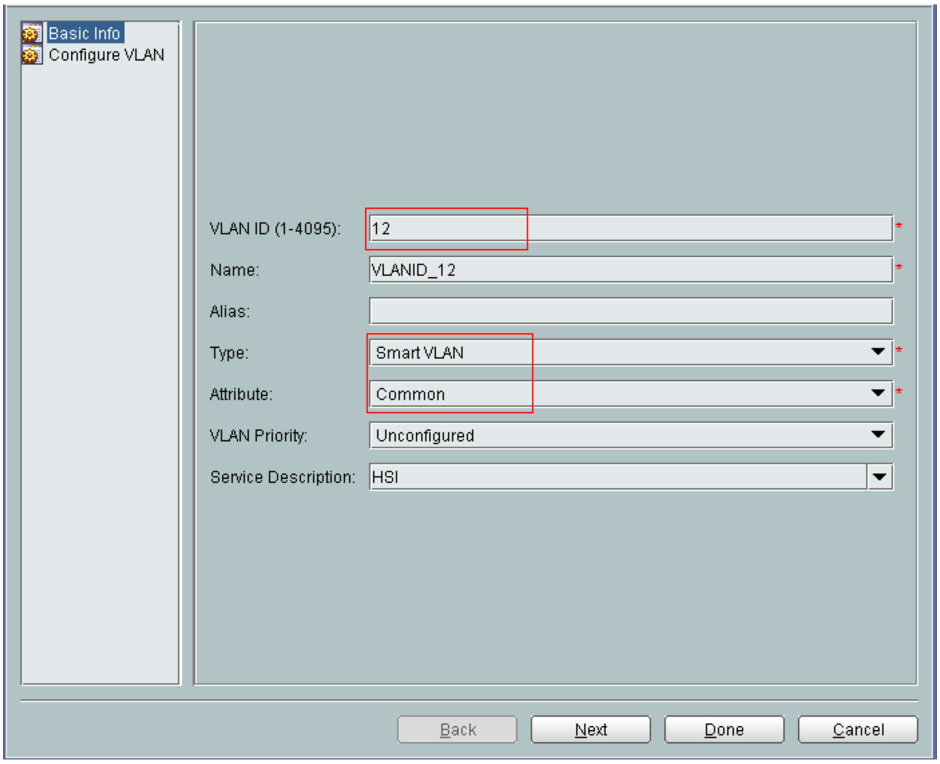
Traffic Profile Info
☑ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile: ip-traffic-table_2
Downstream Traffic Profile: ip-traffic-table_2

6. Click **OK**.

Step 5 Add an MPLS VLAN.

Before provisioning services to NEs, add an MPLS VLAN. The local peer communicates with the remote peer through the uplink port of the MPLS VLAN. Configure OLT_1 and OLT_2 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. On the **VLAN** tab page, set the filter criteria or click ⩔ to display the VLANs.
4. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12

Name: VLANID_12

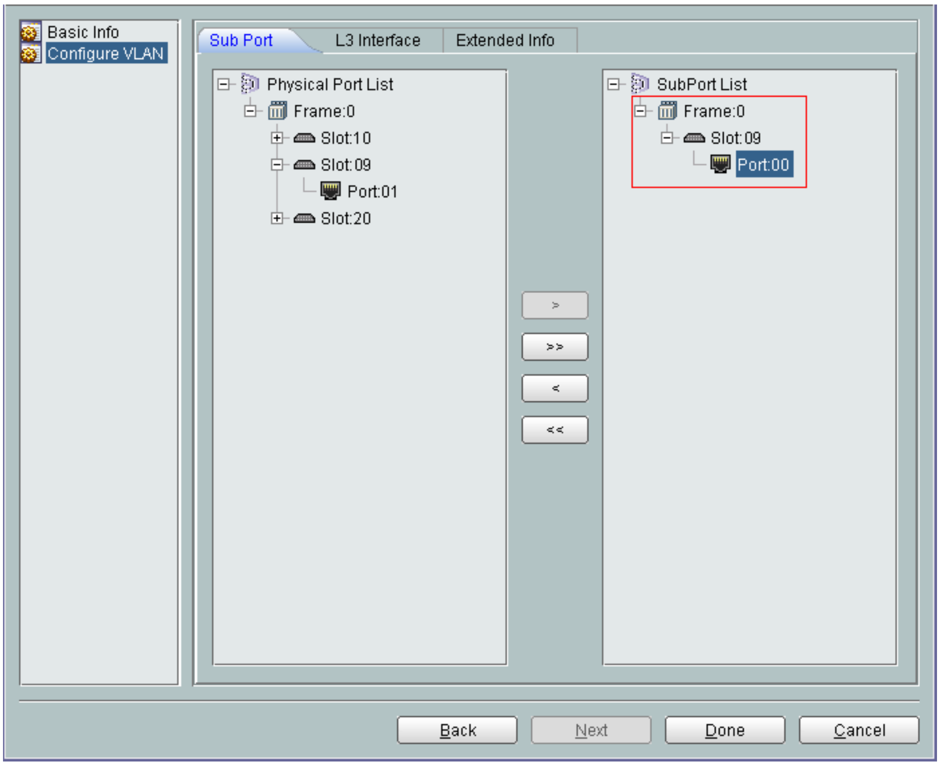
Alias:

Type: Smart VLAN

Attribute: Common

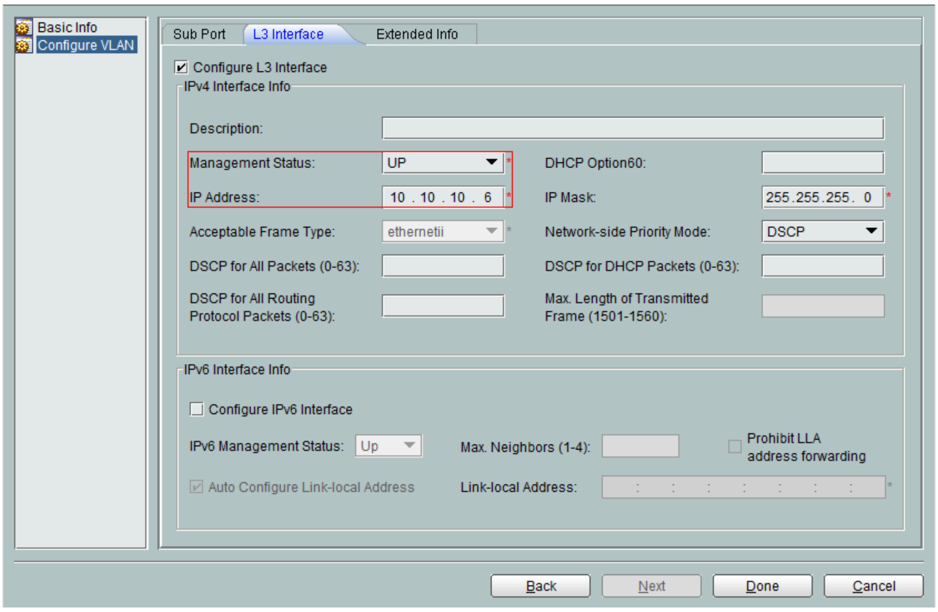
VLAN Priority: Unconfigured

Service Description: HSI



6. Click **Next**.
7. Click the **L3 Interface** tab.
8. In the dialog box that is displayed, set the parameters.

   Configuring parameters for OLT_1



☑ Configure L3 Interface

IPv4 Interface Info

Description:

Management Status: UP

IP Address: 10 . 10 . 10 . 6

DHCP Option60:

IP Mask: 255.255.255. 0

Acceptable Frame Type: ethernetii

Network-side Priority Mode: DSCP

DSCP for All Packets (0-63):

DSCP for DHCP Packets (0-63):

DSCP for All Routing Protocol Packets (0-63):

Max. Length of Transmitted Frame (1501-1560):

IPv6 Interface Info

☐ Configure IPv6 Interface

IPv6 Management Status: Up

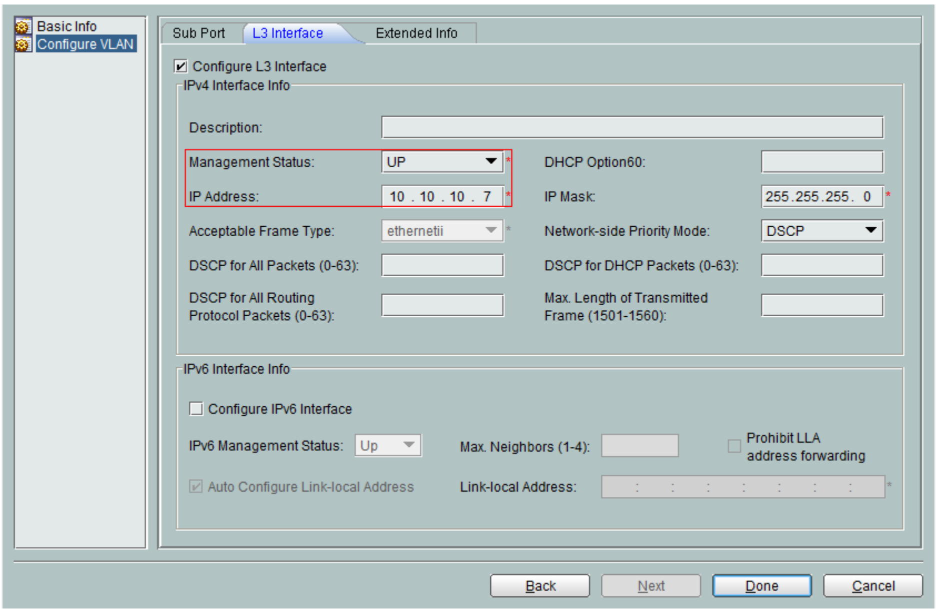
Max. Neighbors (1-4):

☐ Prohibit LLA address forwarding

☑ Auto Configure Link-local Address

Link-local Address: : : : : : : :

Configuring parameters for OLT_2



☑ Configure L3 Interface

IPv4 Interface Info

Description:

Management Status: UP

IP Address: 10 . 10 . 10 . 7

DHCP Option60:

IP Mask: 255.255.255. 0

Acceptable Frame Type: ethernetii

Network-side Priority Mode: DSCP

DSCP for All Packets (0-63):

DSCP for DHCP Packets (0-63):

DSCP for All Routing Protocol Packets (0-63):

Max. Length of Transmitted Frame (1501-1560):

IPv6 Interface Info

☐ Configure IPv6 Interface

IPv6 Management Status: Up

Max. Neighbors (1-4):

☐ Prohibit LLA address forwarding

☑ Auto Configure Link-local Address

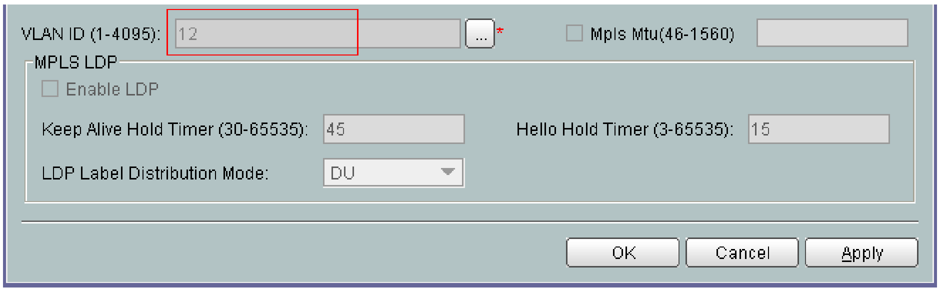
Link-local Address: : : : : : : :

9. Click **Finish**.

Step 6 Add an MPLS interface.

The MPLS interface is a Layer 3 interface bound to the MPLS VLAN. The local peer can communicate with the remote peer using LSP after an MPLS interface is added and MPLS LDP is enabled. Configure OLT_1 and OLT_2 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **MPLS Interface** tab.
4. Right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.


VLAN ID (1-4095): 12 ... *
☐ Mpls Mtu(46-1560)
MPLS LDP
☐ Enable LDP
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 15
LDP Label Distribution Mode: DU

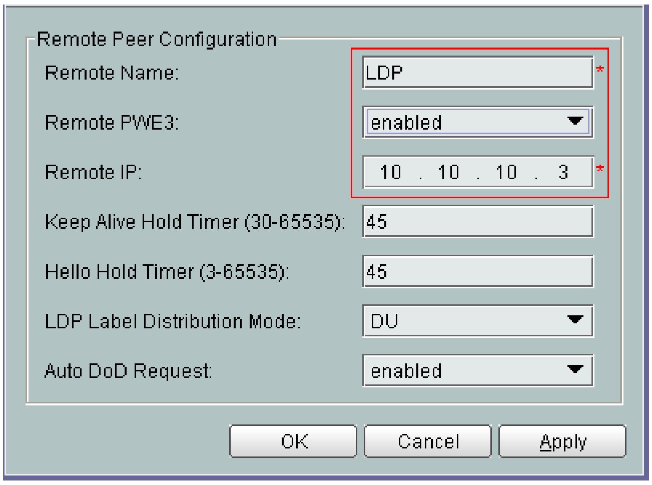
6. Click **OK**.

Step 7 Add a remote peer.

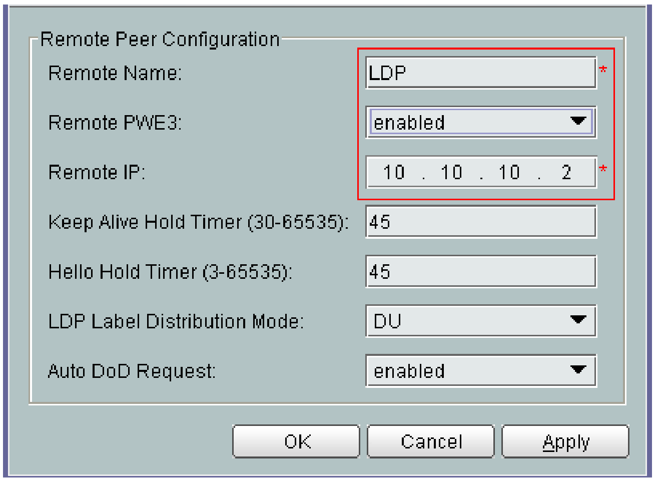
The remote peer is a remote label switching router (LSR) which establishes a session with the local LSR. The MPLS discovers the remote peer through LDP extension mechanism. The local peer periodically sends messages in UDP packets to the specified remote peer.In **Figure 12-4**, the two OLTs are the remote peers for each other. Configure OLT_1 and OLT_2 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **LDP Remote Peer** tab.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.

Configuring parameters for OLT_1


Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: enabled
Remote IP: 10 . 10 . 10 . 3 *
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled

Configuring parameters for OLT_2



Remote Peer Configuration

Remote Name: LDP *

Remote PWE3: enabled

Remote IP: 10 . 10 . 10 . 2 *

Keep Alive Hold Timer (30-65535): 45

Hello Hold Timer (3-65535): 45

LDP Label Distribution Mode: DU

Auto DoD Request: enabled

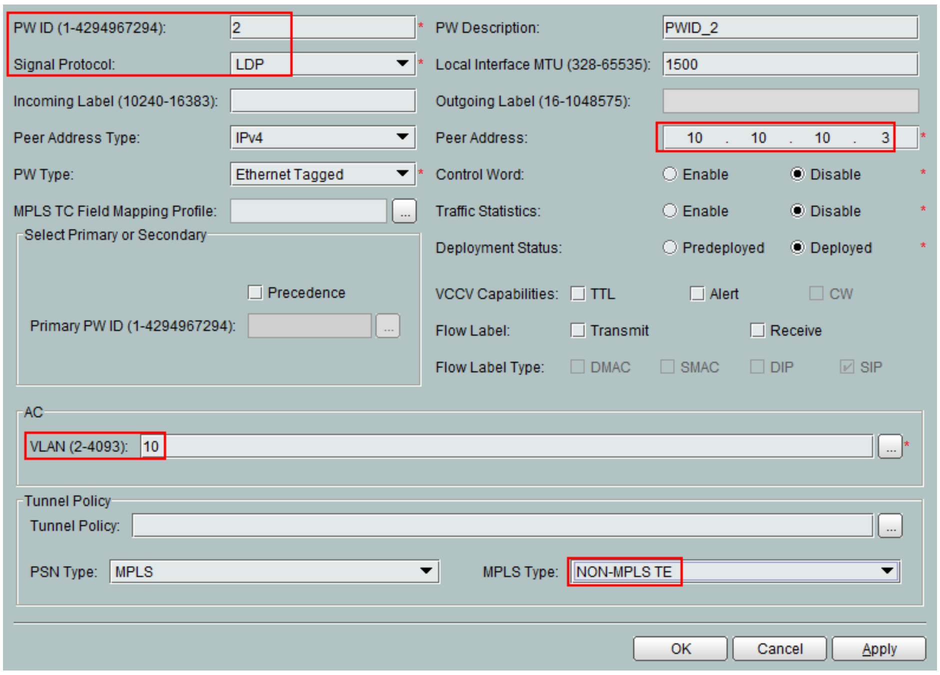
6. Click **OK**.

Step 8 Add a PW.

A PW is added to emulate end-to-end ATM links. Bind the PW to the service VLAN, add the PW label to service VLAN packets, and transmit them through label switched paths (LSPs). Configure OLT_1 and OLT_2 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPWS Management** from the navigation tree.
3. Click the **PW** tab.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.

Configuring parameters for OLT_1



PW ID (1-4294967294): 2 *

Signal Protocol: LDP *

Incoming Label (10240-16383):

Peer Address Type: IPv4

PW Type: Ethernet Tagged *

MPLS TC Field Mapping Profile:

Select Primary or Secondary

☐ Precedence

Primary PW ID (1-4294967294):

PW Description: PWID_2

Local Interface MTU (328-65535): 1500

Outgoing Label (16-1048575):

Peer Address: 10 . 10 . 10 . 3 *

Control Word: ○ Enable ● Disable *

Traffic Statistics: ○ Enable ● Disable *

Deployment Status: ○ Predeployed ● Deployed *

VCCV Capabilities: ☐ TTL ☐ Alert ☐ CW

Flow Label: ☐ Transmit ☐ Receive

Flow Label Type: ☐ DMAC ☐ SMAC ☐ DIP ☑ SIP

AC

VLAN (2-4093): 10 *

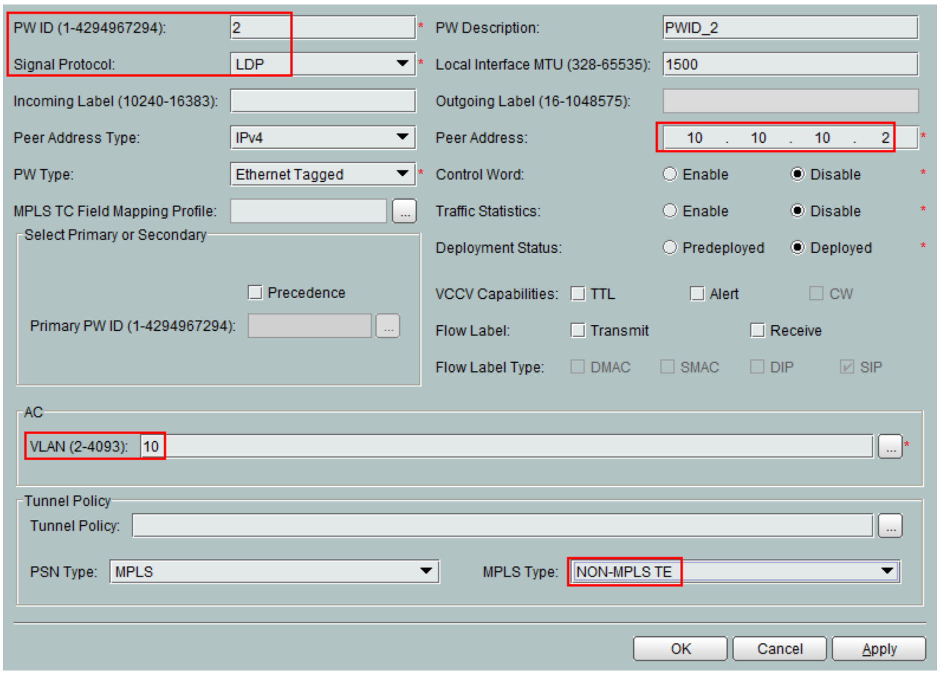
Tunnel Policy

Tunnel Policy:

PSN Type: MPLS

MPLS Type: NON-MPLS TE

Configuring parameters for OLT_2



PW ID (1-4294967294): 2 *
Signal Protocol: LDP *
Incoming Label (10240-16383):
Peer Address Type: IPv4
PW Type: Ethernet Tagged *
MPLS TC Field Mapping Profile:
Select Primary or Secondary
☐ Precedence
Primary PW ID (1-4294967294):
PW Description: PWID_2
Local Interface MTU (328-65535): 1500
Outgoing Label (16-1048575):
Peer Address: 10 . 10 . 10 . 2 *
Control Word: ○ Enable ● Disable *
Traffic Statistics: ○ Enable ● Disable *
Deployment Status: ○ Predeployed ● Deployed *
VCCV Capabilities: ☐ TTL ☐ Alert ☐ CW
Flow Label: ☐ Transmit ☐ Receive
Flow Label Type: ☐ DMAC ☐ SMAC ☐ DIP ☑ SIP
AC
VLAN (2-4093): 10 *
Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: NON-MPLS TE

6. Click **OK**.

----End

Result

After the preceding configuration is completed, OLT_1 and OLT_2 can communicate with each other on the ATM network if the ATM network configurations are correct.

12.12 TDM VPWS Application Case

This topic describes the configuration of TDM VPWS services.

Prerequisites

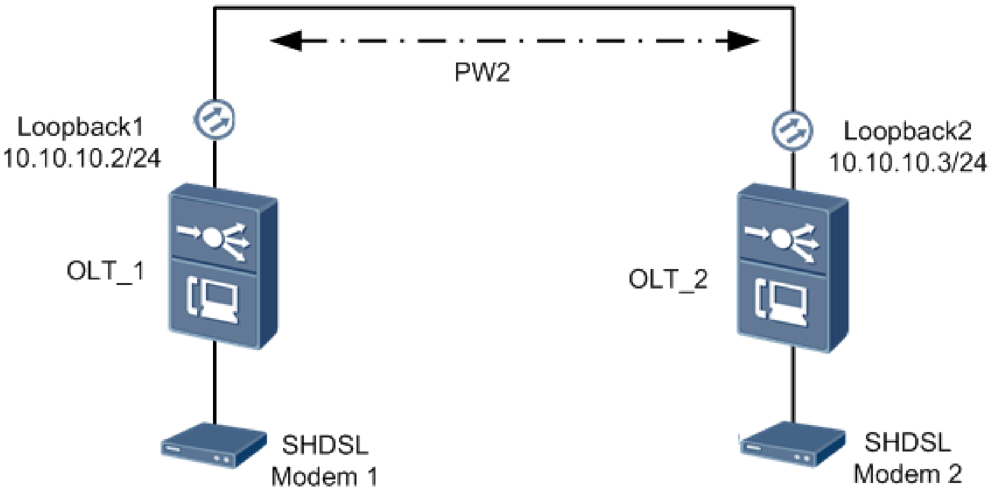
- The network devices and lines are functioning properly.
- Service boards are online.
- A static route or dynamic route is successfully configured on each device over the network so that the IP routes between LSRs are reachable.

TDM VPWS Networking Description

The TDM VPWS technology is used to emulate TDM services. VPWS packet headers carry information about frame formats, alarms, signaling, and synchronous timing in the TDM service flow. Encapsulated PW packets are transmitted on the PSN. After arriving at the PW egress, the packets are decapsulated and restored to TDM CS services.

The **Figure 12-6** shows the networking of a TDM VPWS service. On actual networks, there are multiple routers between two OLTs. The following figure does not show the routers because this case does not require router configuration.

Figure 12-6 Networking of a TDM VPWS service



As shown in **Figure 12-6**, the local CE SHDSL modems that carry TDM services are respectively connected to OLT_1 and OLT_2 through E1 interfaces. VPWS must be configured to transparently transmit service data between CEs.

A TDM VPWS service needs to be established between OLT_1 and OLT_2 to emulate TDM services that connect two remote CEs.

Data Plan

Table 12-4 Data plan for TDM VPWS configuration

Configuration Item	Data	Remarks
EDTB Board	Board Work Mode: *SATOP*	-
	Access Mode: *E1*	
	E1 Port: *0/2/0*	
Loopback interface and IP address	OLT_1: ● Interface Number: 3 ● IP Address: 10.10.10.2 ● Ip Mask Length: 24 ● The other parameters use the default values. OLT_2: ● Interface Number: 3 ● IP Address: 10.10.10.3 ● Ip Mask Length: 24 ● The other parameters use the default values.	-

Configuration Item	Data	Remarks
Configuring the MPLS Parameters	OLT_1: - MPLS Switch: Enable - Specify LSR(Label Switched Router) identifier: 10.10.10.2 - Label Distribution Protocol(LDP): Enable - Operate on MPLS L2VPN: Enable - The other parameters use the default values. OLT_2: - MPLS Switch: Enable - Specify LSR(Label Switched Router) identifier: 10.10.10.3 - Label Distribution Protocol(LDP): Enable - Operate on MPLS L2VPN: Enable - The other parameters use the default values.	**Specify LSR(Label Switched Router) identifier** must be the same as **Ip Address**.
MPLS VLAN	OLT_1: - VLAN ID: 12 - Type: Smart VLAN - Attribute: Common - Sub Port: 0/9/0 - Management Status: UP - IP addresses: 10.10.10.6 - The other parameters use the default values. OLT_2: - VLAN ID: 12 - Type: Smart VLAN - Attribute: Common - Sub Port: 0/9/0 - Management Status: UP - IP Address: 10.10.10.7 - The other parameters use the default values.	-

Configuration Item	Data	Remarks
MPLS interface	OLT_1 or OLT_2: ● VLAN ID: 12 ● Mpls Mtu: 60 ● Enable LDP: selected **Enable LDP** check box ● The other parameters use the default values.	**VLAN ID** must be the same as the **VLAN ID** of the MPLS VLAN.
Remote Peer Configuration	OLT_1: ● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.3 ● The other parameters use the default values. OLT_2: ● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.2 ● The other parameters use the default values.	-
PW	OLT_1: ● PW ID: 2 ● Signal Protocol: LDP ● Peer Address: 10.10.10.3 ● PW Type: *TDM SAToP E1* ● Port Type: *Local E1/T1* ● MPLS Type: mplsNonTe ● The other parameters use the default values. OLT_2: ● PW ID: 2 ● Signal Protocol: LDP ● Peer Address: 10.10.10.2 ● PW Type: *TDM SAToP E1* ● Port Type: *Local E1/T1* ● MPLS Type: mplsNonTe ● The other parameters use the default values.	**Virtual local area network (VLAN)** must be the same as the **VLAN ID** of the service VLAN.

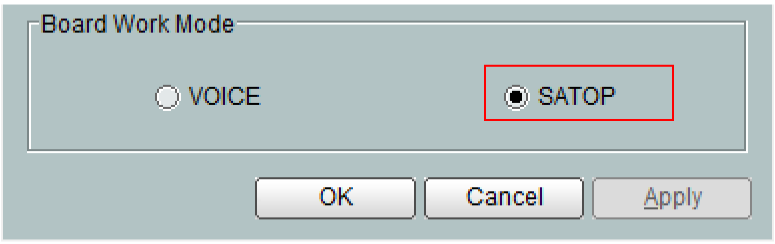
NOTE

Take the configuration on the OLT_1 for example. To configure the service on OLT_2 based on the data plan using the same steps.

Procedure

Step 1 Configure the working mode of the EDTB board.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. In the NE Explorer, choose **NE Panel** from the navigation tree.
3. Right-click the desired EDTB board and choose **Configure Board Work Mode** from the shortcut menu.
4. In the dialog box that is displayed, set **Board Work Mode** to **SATOP**.



Board Work Mode

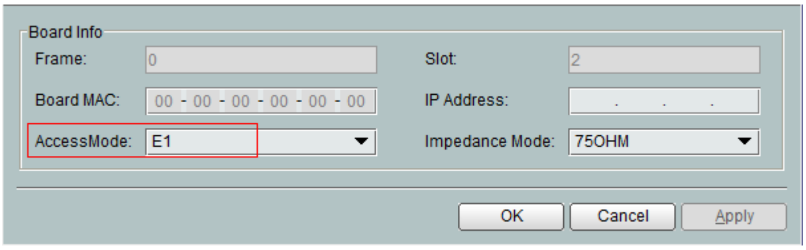
○ VOICE

● SATOP

5. Click **OK**.

Step 2 Configure the access mode of EDTB board

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. In the NE Explorer, choose **NE Panel** from the navigation tree.
3. Right-click the desired EDTB board and choose **Config Board** from the shortcut menu.
4. In the dialog box that is displayed, set **Access Mode** to **E1**.



Board Info

Frame: 0

Slot: 2

Board MAC: 00 - 00 - 00 - 00 - 00 - 00

IP Address: . . .

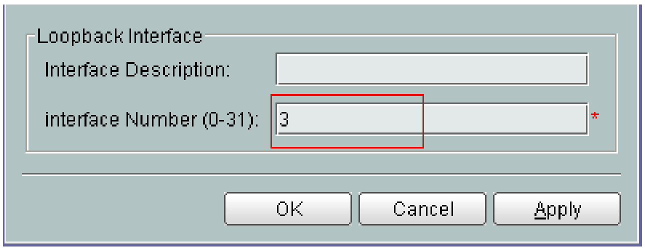
AccessMode: E1

Impedance Mode: 75OHM

5. Click **OK**.

Step 3 Configure an IP address for the interface.

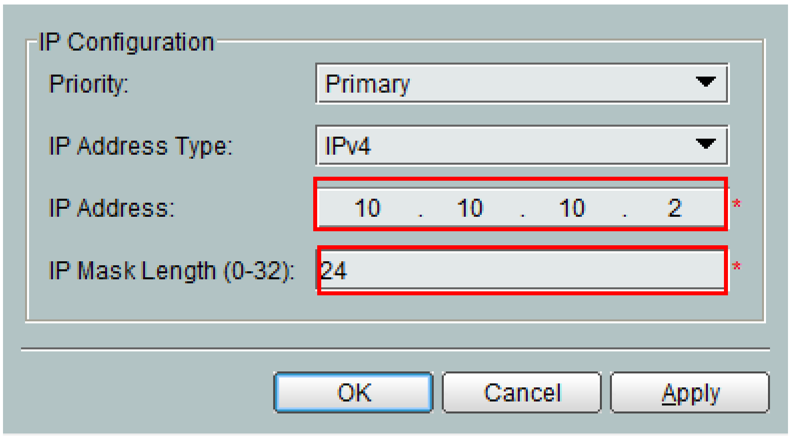
1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **LookBack Interface** from the navigation tree.
3. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters.



Interface Description:

interface Number (0-31): 3 *

5. Click **OK**.
6. Select the loopback and click the **IP Address** tab in the lower pane.
7. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
8. In the dialog box that is displayed, set the parameters.



Priority: Primary

IP Address Type: IPv4

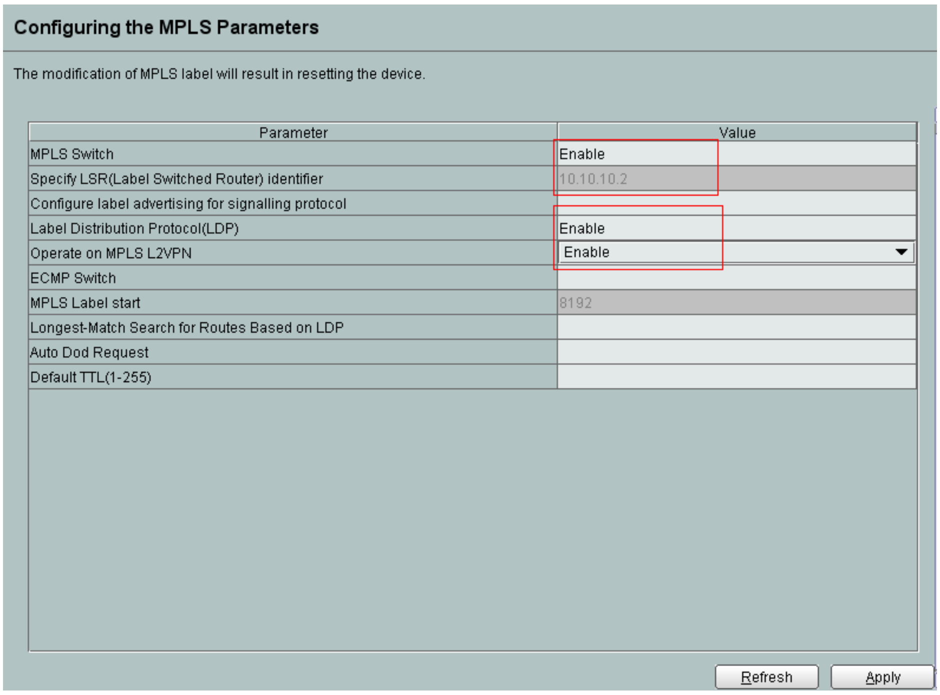
IP Address: 10 . 10 . 10 . 2 *

IP Mask Length (0-32): 24 *

9. Click **OK**.

Step 4 Configure the global MPLS parameters.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **NE Properties** > **Protocol** > **MPLS** from the navigation tree.
3. Configure global MPLS parameters in the **Value** column.



Configuring the MPLS Parameters

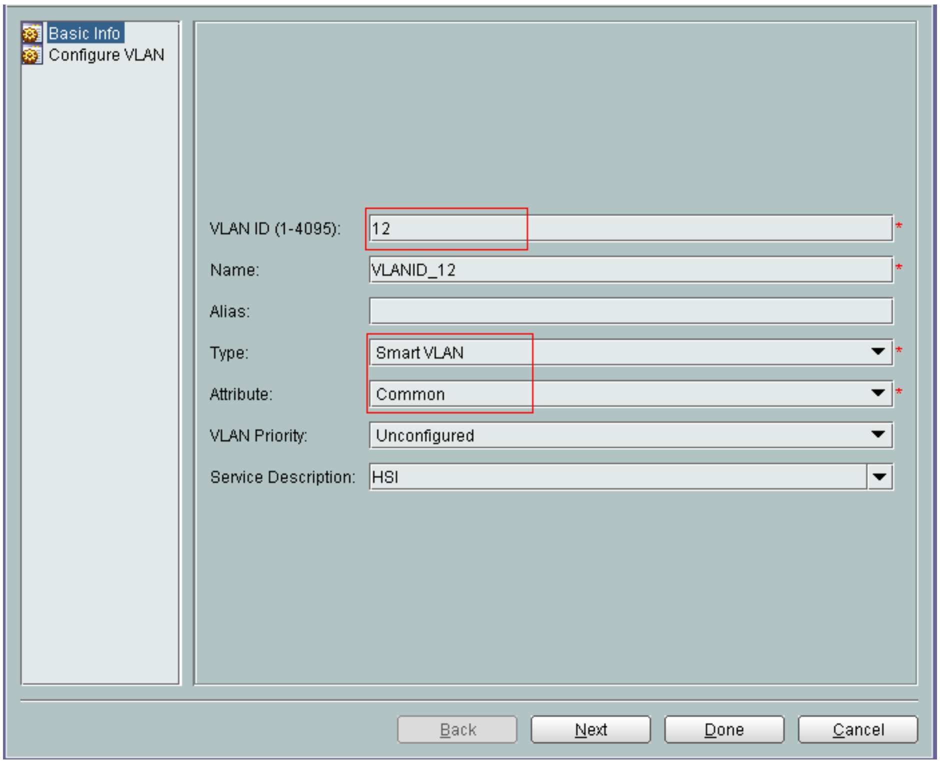
The modification of MPLS label will result in resetting the device.

Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.2
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

4. Click **Apply**.

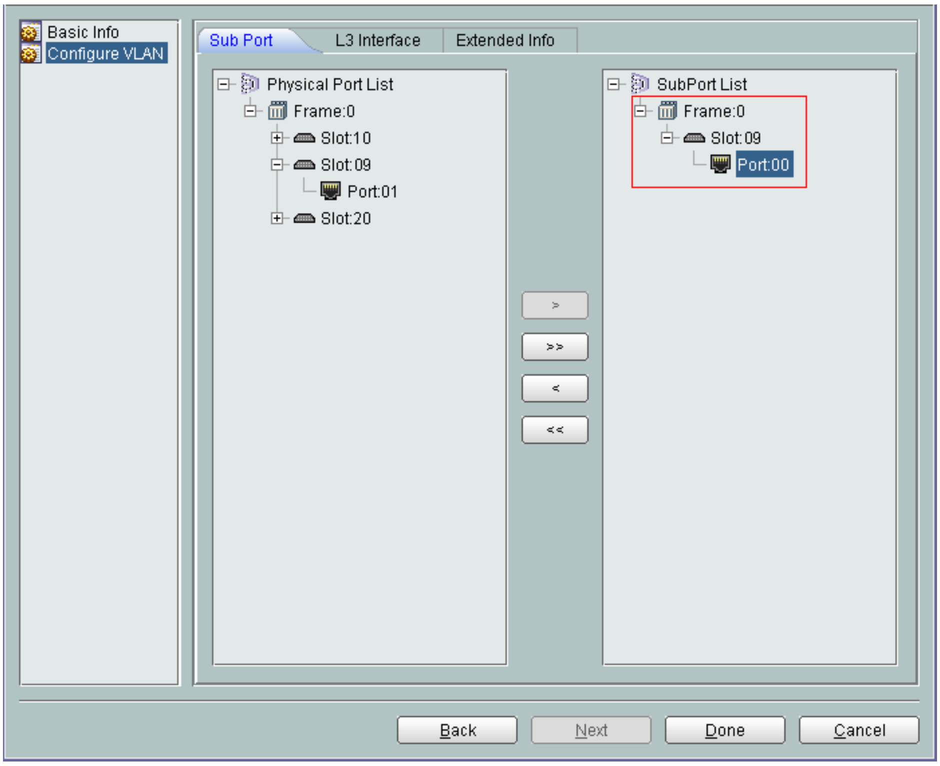
Step 5 Add an MPLS VLAN.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. On the **VLAN** tab page, set the filter criteria or click ⏬ to display the VLANs.
4. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.

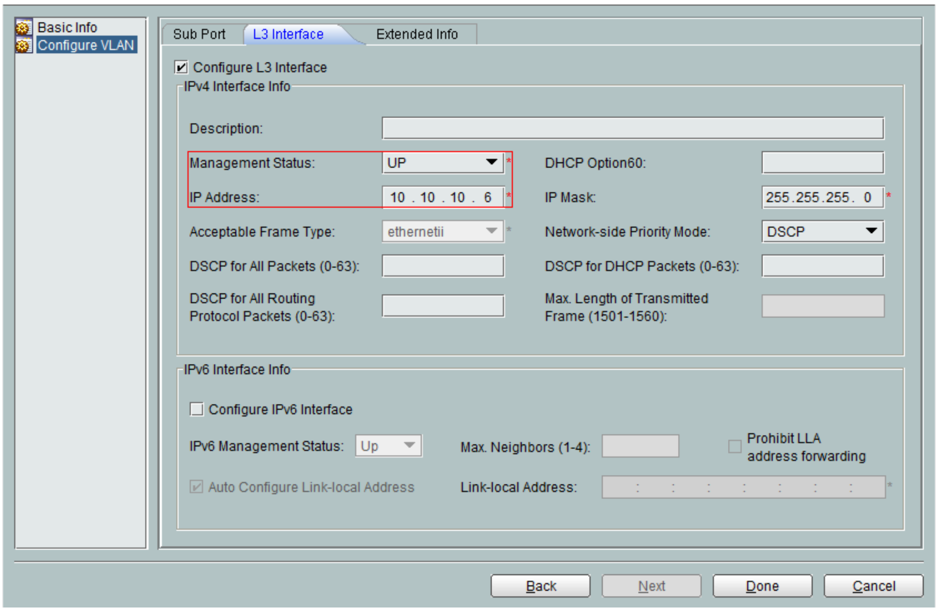


VLAN ID (1-4095): 12 *
Name: VLANID_12 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI

6. Click **Next**.
7. Click the **Sub Port** tab.



8. Click the **L3 Interface** tab.
9. In the dialog box that is displayed, set the parameters.


Basic Info
Configure VLAN
Sub Port
L3 Interface
Extended Info
IPv4 Interface Info
Description:
DHCP Option60:
DSCP for All Packets (0-63):
DSCP for DHCP Packets (0-63):
DSCP for All Routing Protocol Packets (0-63):
Max. Length of Transmitted Frame (1501-1560):
IPv6 Interface Info
☐ Configure IPv6 Interface
Max. Neighbors (1-4):
☐ Prohibit LLA address forwarding
Link-local Address:
Back
Next
Done
Cancel

☑ Configure L3 Interface

Management Status: UP

IP Address: 10 . 10 . 10 . 6

IP Mask: 255.255.255. 0

Acceptable Frame Type: ethernetii

Network-side Priority Mode: DSCP

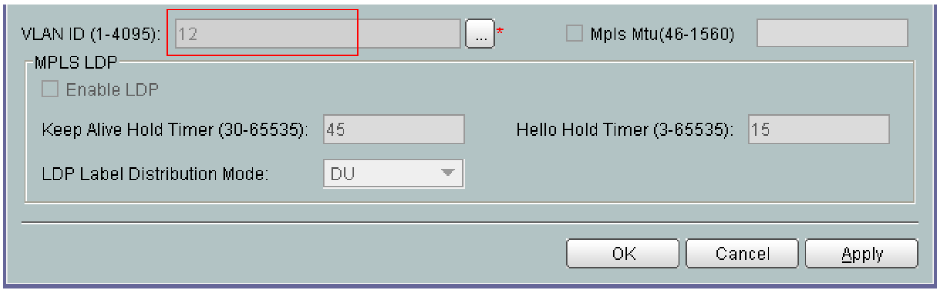
IPv6 Management Status: Up

☑ Auto Configure Link-local Address

10. Click **Finish**.

Step 6 Add an MPLS interface.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **MPLS Interface** tab.
4. Right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12

Keep Alive Hold Timer (30-65535): 45

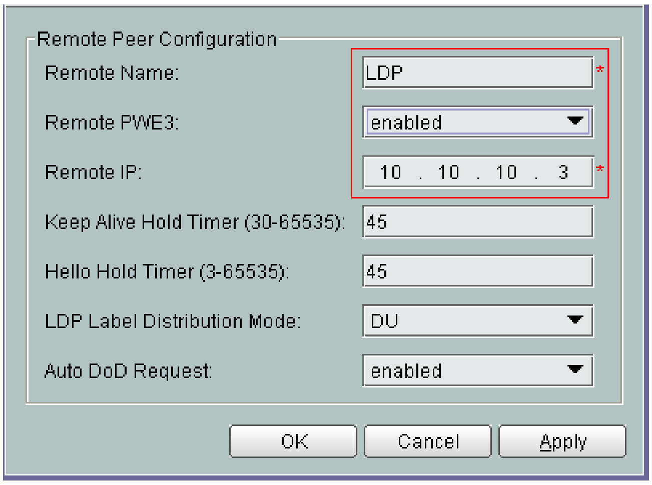
Hello Hold Timer (3-65535): 15

LDP Label Distribution Mode: DU

6. Click **OK**.

Step 7 Add a remote peer.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **LDP Remote Peer** tab.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.

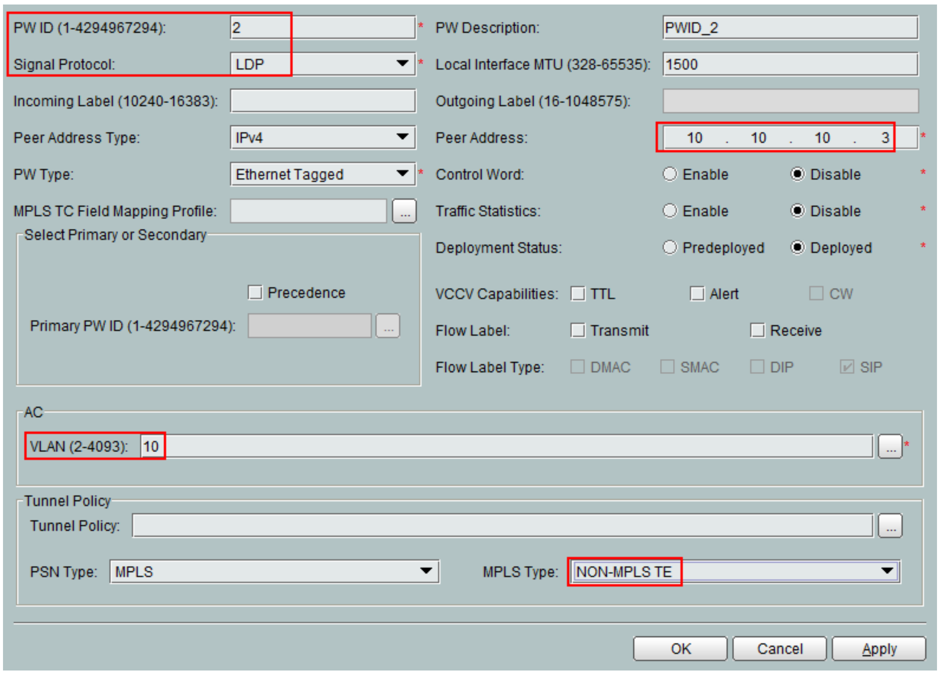


Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: enabled
Remote IP: 10 . 10 . 10 . 3 *
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled

6. Click **OK**.

Step 8 Add a PW.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPWS Management** from the navigation tree.
3. Click the **PW** tab.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



PW ID (1-4294967294): 2 *
Signal Protocol: LDP *
Incoming Label (10240-16383):
Peer Address Type: IPv4
PW Type: Ethernet Tagged *
MPLS TC Field Mapping Profile:
Select Primary or Secondary
☐ Precedence
Primary PW ID (1-4294967294):
PW Description: PWID_2
Local Interface MTU (328-65535): 1500
Outgoing Label (16-1048575):
Peer Address: 10 . 10 . 10 . 3 *
Control Word: ○ Enable ● Disable *
Traffic Statistics: ○ Enable ● Disable *
Deployment Status: ○ Predeployed ● Deployed *
VCCV Capabilities: ☐ TTL ☐ Alert ☐ CW
Flow Label: ☐ Transmit ☐ Receive
Flow Label Type: ☐ DMAC ☐ SMAC ☐ DIP ☑ SIP
AC
VLAN (2-4093): 10 *
Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: NON-MPLS TE

6. Click **OK**.

----End

Result

After the preceding configuration is completed, services of the customer can be provisioned normally.

Copyright © Huawei Technologies Co., Ltd.

13 Configuring VPLS Services

About This Chapter

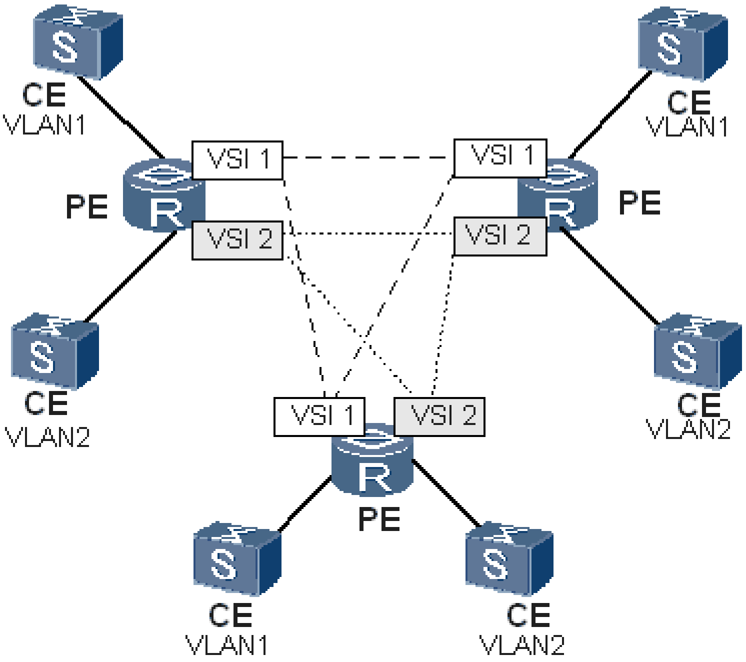
The virtual private LAN segment (VPLS) is a L2VPN technology that is based on MPLS and Ethernet technologies. It support multipoint-to-multipoint VPN networking and provides a better solution for carriers who supplied point-to-point L2VPN services.

Context

The VPLS interconnects multiple Ethernet LANs through the packet switched network (PSN) so that they can work as one LAN. The VPLS supports multipoint-to-multipoint VPN networking. Internet service providers can use the VPLS technology to provide users with multipoint services through MPLS backbone networks. The MPLS solution which uses PWs as Ethernet bridge links allows LAN services to be transparently transmitted through MPLS networks.

The **Figure 13-1** shows a VPLS forwarding model, in which the PE uses virtual switch instances (VSIs) to perform MPLS forwarding. PEs forward Ethernet frames across full-connected Ethernet emulated circuits or PWs.

Figure 13-1 VPLS forwarding model networking



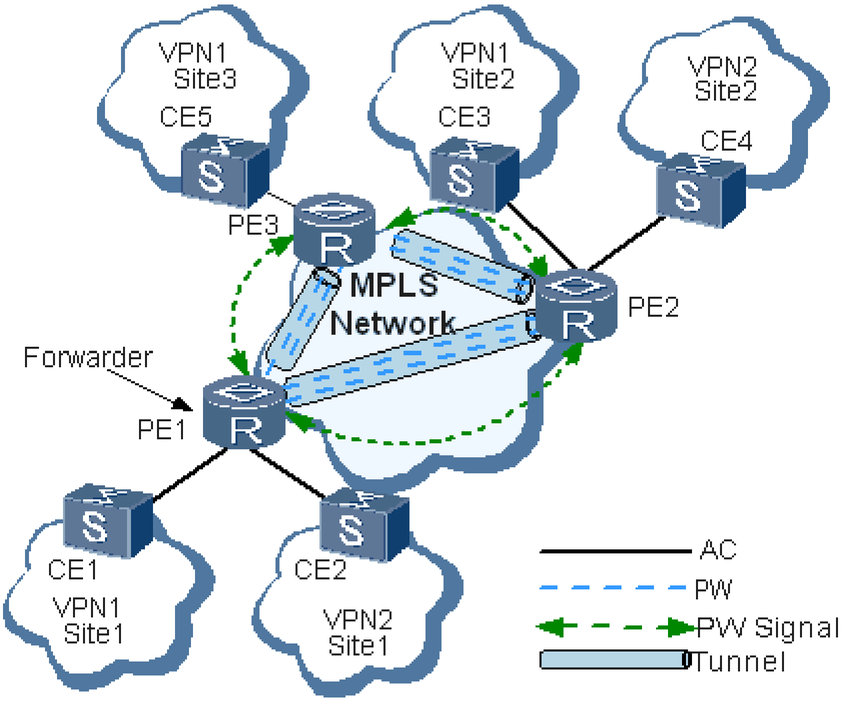
Basic VPLS Transport Components

The whole VPLS network is similar to a switch. In the VPLS network, PWs are set up between VPN sites of each VPN through MPLS tunnels, and Layer 2 packets are transparently transmitted between sites; PEs learn the source MAC addresses and create MAC forwarding entries when forwarding packets, and then maps the MAC addresses to attachment circuits (ACs) and PWs.

The basic VPLS transport components include ACs, virtual circuits (VCs), forwarders, tunnels, encapsulation, PW signaling protocol, and Quality of Service (QoS).

The **Figure 13-2** shows the location of each basic VPLS transport component in the VPLS network.

Figure 13-2 VPLS forwarding model networking



The following takes the flow direction of VPN1 packets from CE1 to CE3 as an example to show the basic direction of the data flow. CE1 forwards Layer 2 packets to PE1. After PE1 receives these packets, the forwarder selects a PW to forward these packets to PE2. Then the forwarder of PE2 forwards these packets to CE3.

13.1 VPLS Configuration Process

The configuration process of the VPLS consists of configure the Full-Mesh services and H-Mesh services. This section describes the operation tasks for configuring the services, and relations between the tasks. When configure and managing the VPLS service, follow the configuration process.

13.2 Configuring an IP Address for the Interface

The loopback interface retains Up after it was created and it works as the source interface of MPLS packets for application protocols, such as MPLS, route protocols, and SNMP. The IP address of the loopback interface is planned by carriers and must be the same as the value of **Specify LSR(Label Switched Router) identifier**.

13.3 Configuring Global MPLS Parameters

Enable MPLS functions on network-wide NEs by setting global parameters, such as MPLS capability, LDP capability, and specify LSR identifier. Other VPWS configurations take effect only after global MPLS parameters are set.

13.4 Adding a VLAN

Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

13.5 Configuring a Service Port

After being configured successfully, the xDSL service port can carry service streams of various types. The way for configuring other service ports is similar to that for configuring an ADSL service port. The following uses the ADSL port configuration as an example.

13.6 Adding an MPLS VLAN
Before provisioning services to NEs, add an MPLS VLAN. The local peer communicates with the remote peer through the uplink port of the MPLS VLAN.

13.7 Adding an MPLS Interface
The MPLS interface is a Layer 3 interface bound to the MPLS VLAN. The local peer can communicate with the remote peer using LSP after an MPLS interface is added and MPLS LDP is enabled.

13.8 Adding a Remote LDP Peer
The remote peer is a remote label switching router (LSR) which establishes a session with the local LSR. The MPLS discovers the remote peer through LDP extension mechanism. The local peer periodically sends messages in UDP packets to the specified remote peer.

13.9 Adding a Tunnel Policy
A tunnel may carry multiple PWs which are data transmission channels within a tunnel. By default, a VPN instance uses LSPs for service transmission on the backbone network. To use other types of tunnels or configure load balancing for service transmission of the VPN instance, you need to apply a tunnel policy to the VPN instance.

13.10 Adding a PW
Different types of PWs are set up to emulate end-to-end ATM or Ethernet services. Bind the PW to a VLAN and access the VLAN to the PW.

13.11 Adding a PW Protection Group (Optional)
After a PW protection group is added, the service can be quickly switched to another PW when the PW which carries the service is faulty (for example, the tunnel of the PW is deleted).

13.12 Adding a VSI
The virtual switch instance (VSI) is the core of VPLS services. It can map links that access VPLS networks to PWs.

13.13 Binding a VSI to a PW
Packet forwarding is limited to a scope after the virtual switch instance (VSI) is bound to a PW. Therefore, packets can be transmitted only over the PW to which the VSI is bound.

13.14 Binding a VSI to an AC
Packet forwarding is limited to a scope after the virtual switch instance (VSI) is bound to an AC. AC packets can be transmitted over the PW only after they are bound to a VSI.

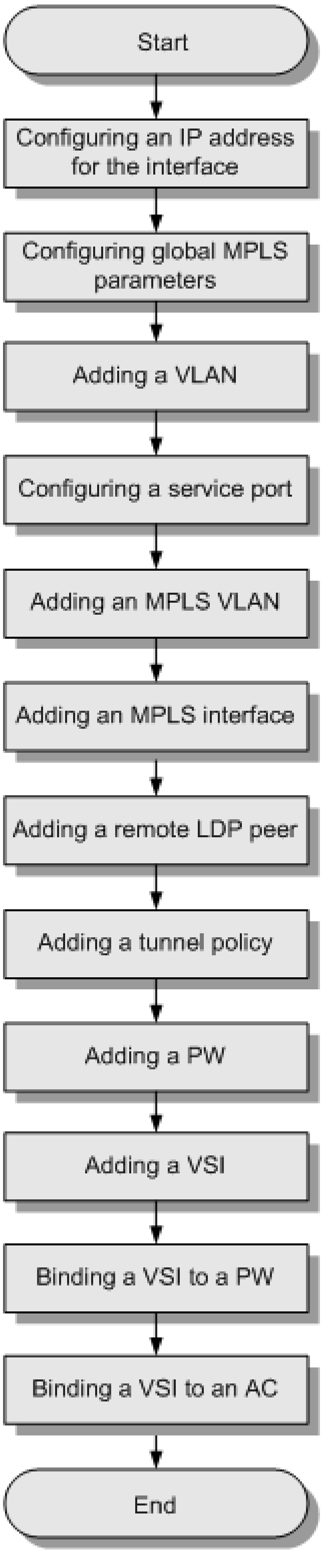
13.15 VPLS Application Case
VPLS application cases include the H-VPLS configuration case and the Full-Mesh network configuration case.

13.1 VPLS Configuration Process

The configuration process of the VPLS consists of configure the Full-Mesh services and H-Mesh services. This section describes the operation tasks for configuring the services, and relations between the tasks. When configure and managing the VPLS service, follow the configuration process.

Figure 13-3 shows the flowchart for configuring an VPLS service. For details of each step, see the relevant section.

Figure 13-3 VPLS service configuration process



13.2 Configuring an IP Address for the Interface

The loopback interface retains Up after it was created and it works as the source interface of MPLS packets for application protocols, such as MPLS, route protocols, and SNMP. The IP address of the loopback interface is planned by carriers and must be the same as the value of **Specify LSR(Label Switched Router) identifier**.

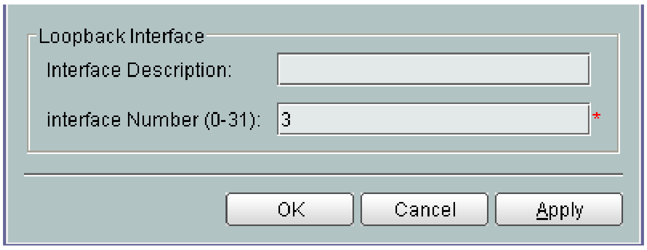
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **LookBack Interface** from the navigation tree.

Step 3 In the information list, right-click in a blank area and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters.



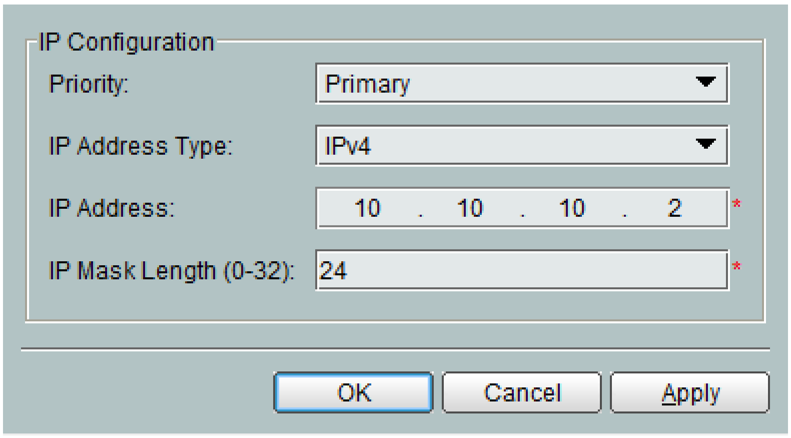
Loopback Interface
Interface Description:
interface Number (0-31): 3 *

Step 5 Click **OK**.

Step 6 Select the loopback and click the **IP Address** tab in the lower pane.

Step 7 In the information list, right-click in a blank area and choose **Add** from the shortcut menu.

Step 8 In the dialog box that is displayed, set the parameters.



IP Configuration
Priority: Primary
IP Address Type: IPv4
IP Address: 10 . 10 . 10 . 2 *
IP Mask Length (0-32): 24 *

Step 9 Click **OK**.

----End

13.3 Configuring Global MPLS Parameters

Enable MPLS functions on network-wide NEs by setting global parameters, such as MPLS capability, LDP capability, and specify LSR identifier. Other VPWS configurations take effect only after global MPLS parameters are set.

Context

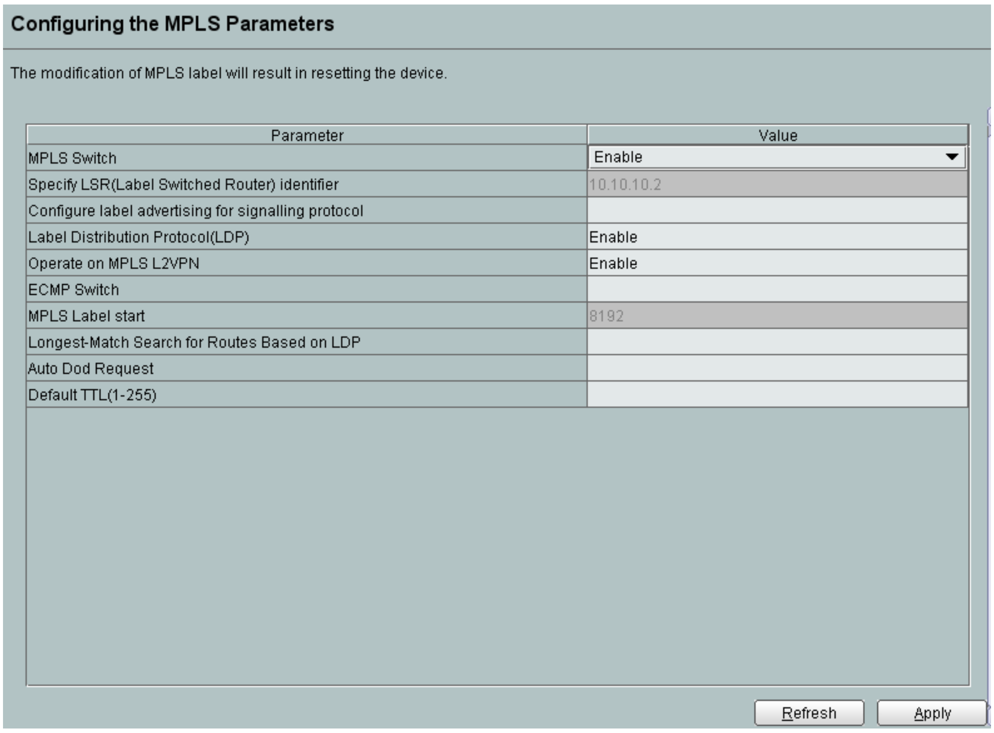
All routers that transmit MPLS services must be configured with basic MPLS settings on MPLS networks.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Properties** > **Protocol** > **MPLS** from the navigation tree.

Step 3 Configure global MPLS parameters in the **Value** column.



Configuring the MPLS Parameters

The modification of MPLS label will result in resetting the device.

Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.2
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

Step 4 Click **Apply**.

----End

13.4 Adding a VLAN

Before you provision services for network elements, you can add a VLAN or add VLANs in batches according to the global data plan. When VLANs with continuous IDs and the VLAN type is consistent with the VLAN attribute, these VLANs can be added in batches. In addition, the names of the VLANs that are added in batches are generated automatically.

Context

Table 13-1 describes VLAN types and their applications.

Table 13-1 VLAN types and their applications

VLAN Type	Description	Application
Standard VLAN	Ethernet ports in a standard VLAN are interconnected with each other. Ethernet ports in different standard VLANs are isolated from each other. In the standard VLAN, the ports on the same service card are isolated from each other. The ports on different service cards can communicate with each other. Ethernet ports in a standard VLAN are interconnected with each other. Ethernet ports in different standard VLANs are isolated from each other. The standard VLAN and the smart VLAN are mutually exclusive. That is, ports on the same service card cannot be added to a smart VLAN and a standard VLAN concurrently.	Only available for Ethernet ports. Applied to network management and subtending.
Smart VLAN	A smart VLAN contains multiple service virtual ports. In addition, traffic streams on these ports are isolated from each other and traffic streams on different VLANs are isolated from each other. A smart VLAN provides access for multiple users, saving the VLAN resources.	Applied to the access service, such as the residential community access.
MUX VLAN	A MUX VLAN contains only one service virtual port. In addition, traffic streams on different VLANs are isolated from each other. One-to-one mapping can be set up between a MUX VLAN and an access user. In this case, a MUX VLAN can uniquely identify an access user.	Applied to the access service, such as scenarios where users are distinguished based on VLANs.
Super VLAN	The super VLAN is a L3-based VLAN. It consists of multiple sub VLANs. Through ARP proxy, a super VLAN realizes L3 interconnection for these sub VLANs. A sub VLAN can be a standard VLAN, smart VLAN, or a MUX VLAN.	Applied to save IP address resources so that the utilization of the IP address is improved.

Table 13-2 describes the VLAN attributes.

Table 13-2 VLAN attributes

VLAN Attribute	Application
Common	A VLAN with the common attribute can be used as a L2 VLAN or to create a L3 interface.
QinQ	A QinQ VLAN packet contains two layers of VLAN tags: inner VLAN tag from the private network and outer VLAN tag from the OLT. Through the outer VLAN, a L2 VPN tunnel can be set up to transparently transmit the service between private networks.
Stacking	A stacking VLAN packet contains two layers of VLAN tags: inner VLAN tag and outer VLAN tag from the OLT. With this attribute, the upper layer BRAS device authenticates users based on the two VLAN tags, thus increasing the number of access users. In an upper network in the L2 working mode, you can forward packets according to the "VLAN + MAC", thus providing the wholesale service provisioning function for ISPs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

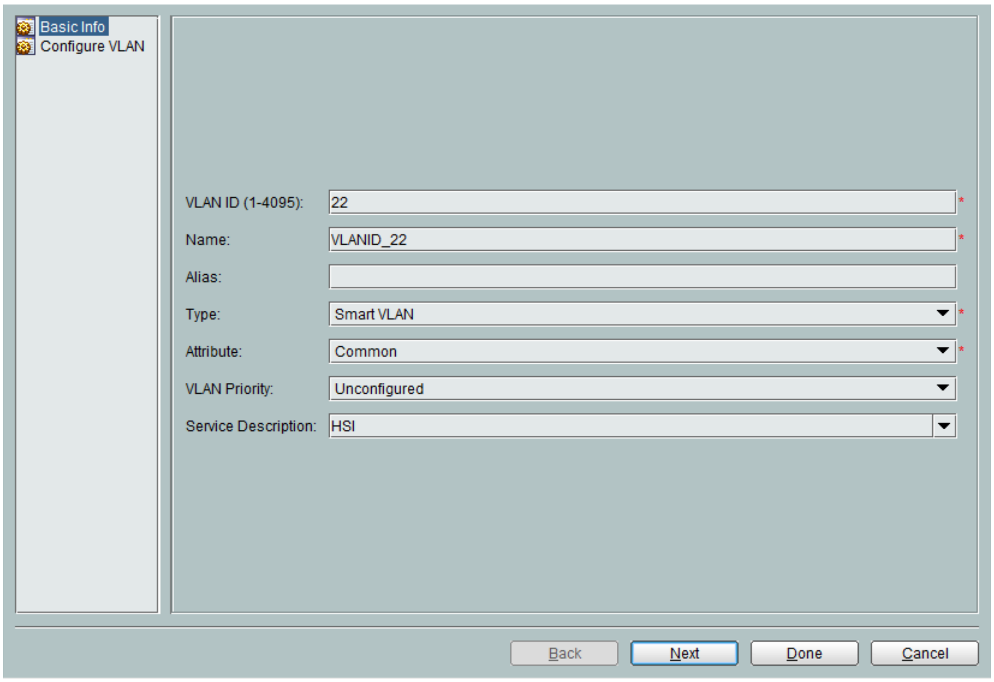
Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ⏬ to display the VLANs.

Step 4 Right-click the list, and then choose **Add** or **Batch Add**.

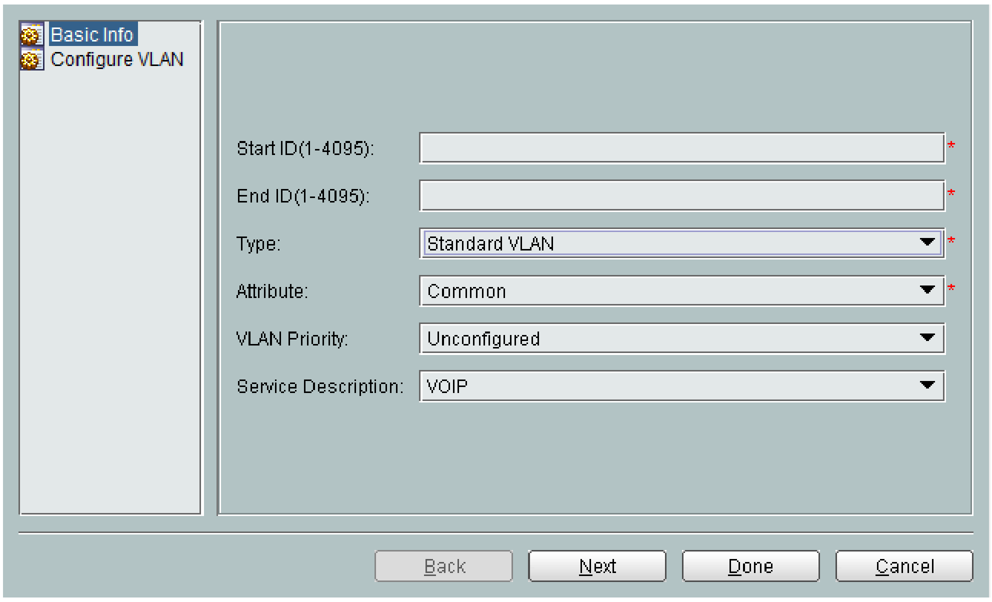
Step 5 In the dialog box that is displayed, set the parameters.

- When you add a VLAN, and then set the parameters as follows:
  - **VLAN ID**
  - **Name**
  - **Alias**
  - **Type**
  - **VLAN Priority**

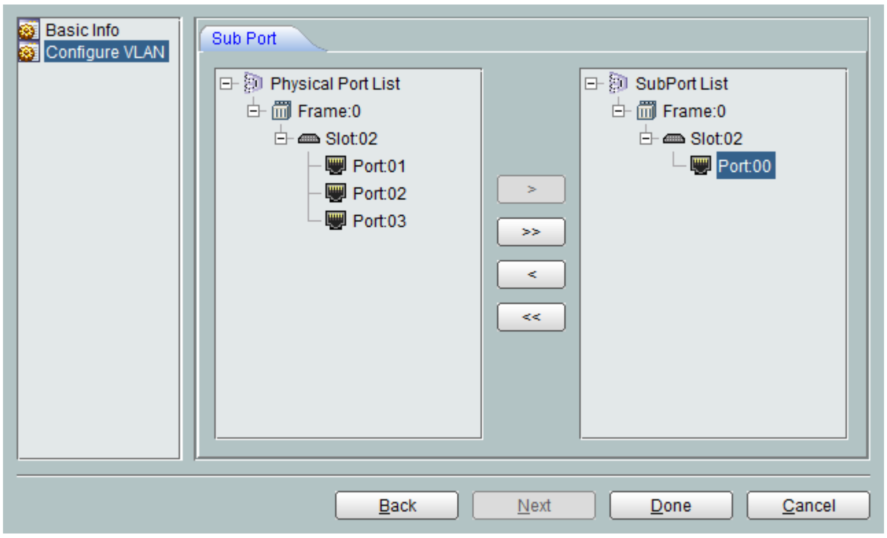


VLAN ID (1-4095): 22
Name: VLANID_22
Alias:
Type: Smart VLAN
Attribute: Common
VLAN Priority: Unconfigured
Service Description: HSI

- When you add VLANs in batches, and then set the parameters as follows:
  - **Start ID**
  - **End ID**
  - **Type**
  - **VLAN Priority**



Start ID(1-4095):
End ID(1-4095):
Type: Standard VLAN
Attribute: Common
VLAN Priority: Unconfigured
Service Description: VOIP



Step 6 Click **Finish**.

----End

13.5 Configuring a Service Port

After being configured successfully, the xDSL service port can carry service streams of various types. The way for configuring other service ports is similar to that for configuring an ADSL service port. The following uses the ADSL port configuration as an example.

Procedure

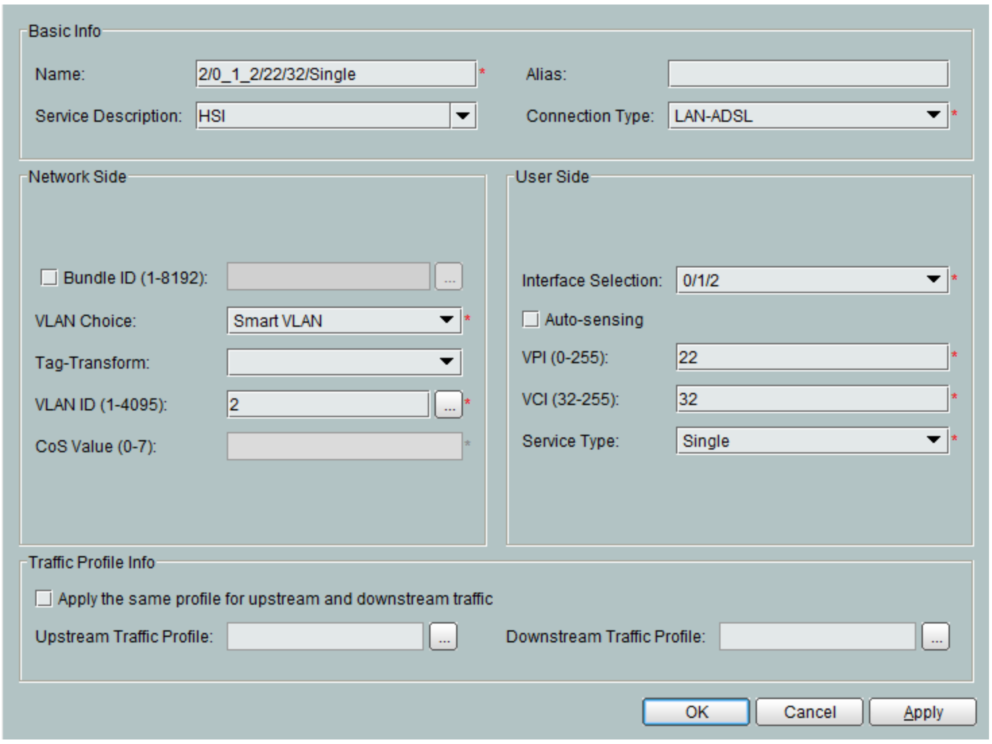
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ADSL Port** from the navigation tree.

Step 3 On the **ADSL** tab page, set the filter criteria or click ⌄ to display the ADSL ports.

Step 4 In the information list, select an ADSL port record. On the **Service Port Info** tab page in the lower pane, right-click, and then choose **Add**.

Step 5 In the dialog box that is displayed, input or choose the proper parameters.



Name: 2/0_1_2/22/32/Single *
Alias:
Service Description: HSI
Connection Type: LAN-ADSL *
☐ Bundle ID (1-8192):
VLAN Choice: Smart VLAN *
Tag-Transform:
VLAN ID (1-4095): 2 *
CoS Value (0-7):
Interface Selection: 0/1/2 *
☐ Auto-sensing
VPI (0-255): 22 *
VCI (32-255): 32 *
Service Type: Single *
☐ Apply the same profile for upstream and downstream traffic
Upstream Traffic Profile:
Downstream Traffic Profile:

NOTE

- The configuration of VLAN ID must be the same as that in **13.4 Adding a VLAN**.
- Select only the MEF IP Traffic Profile that exists on the device. Otherwise, the system reports an error.

Step 6 Click **OK**.

----End

13.6 Adding an MPLS VLAN

Before provisioning services to NEs, add an MPLS VLAN. The local peer communicates with the remote peer through the uplink port of the MPLS VLAN.

Procedure

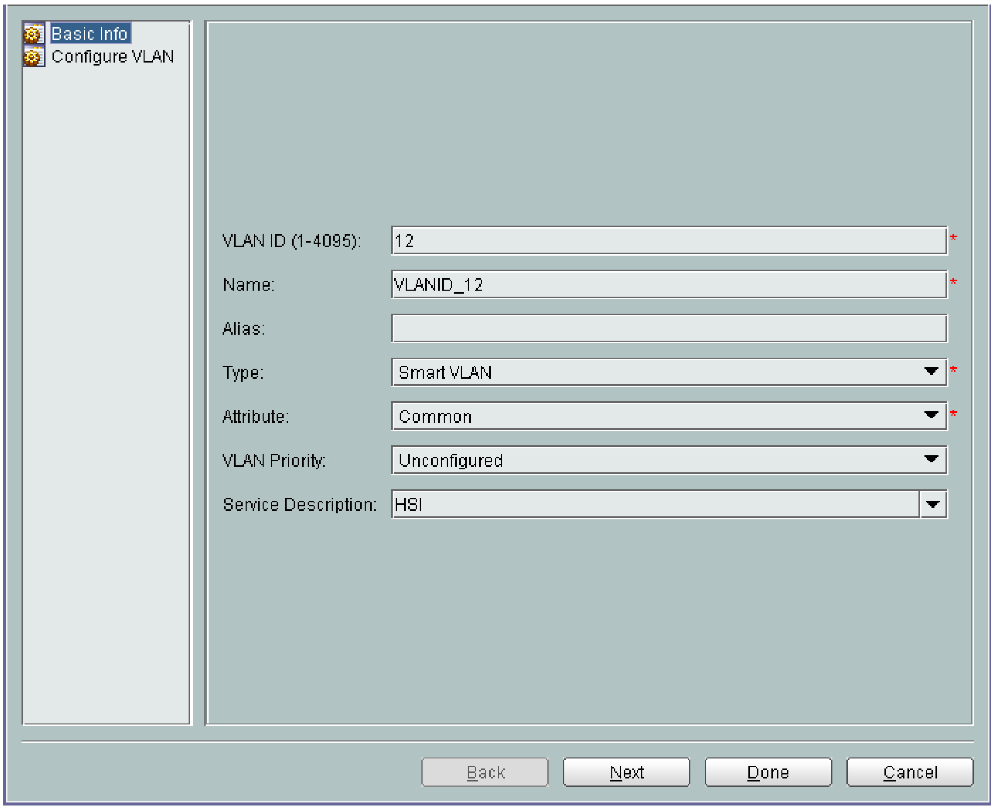
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

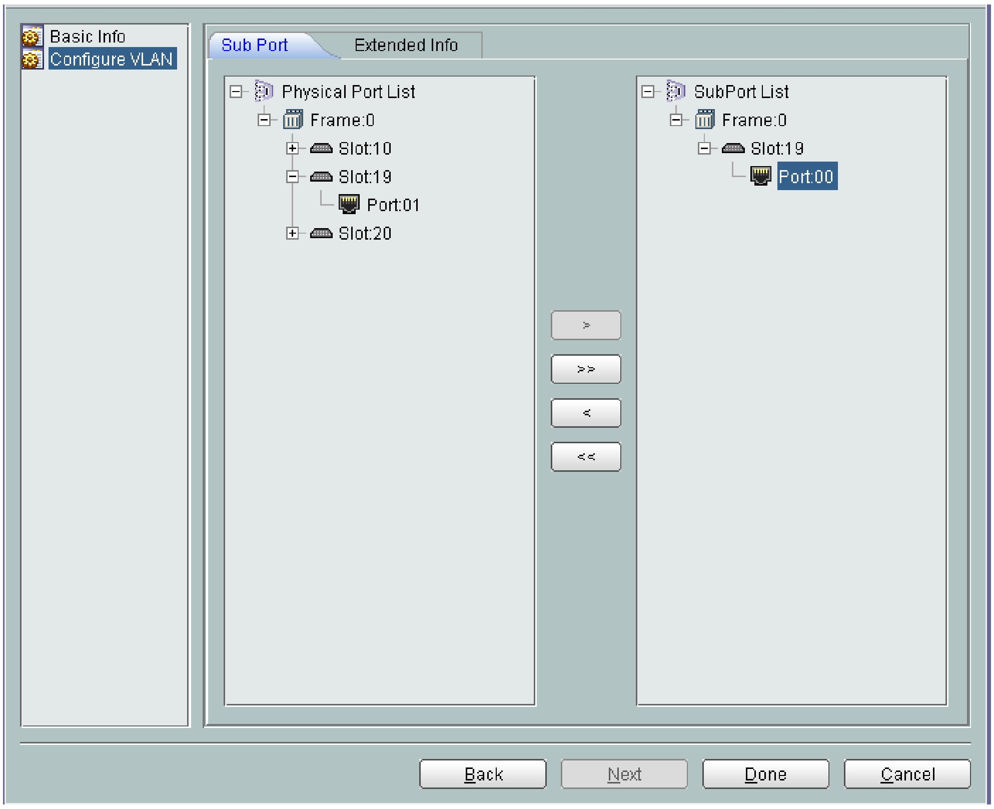
Step 3 On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.

Step 4 In the information list, right-click in a blank area and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.

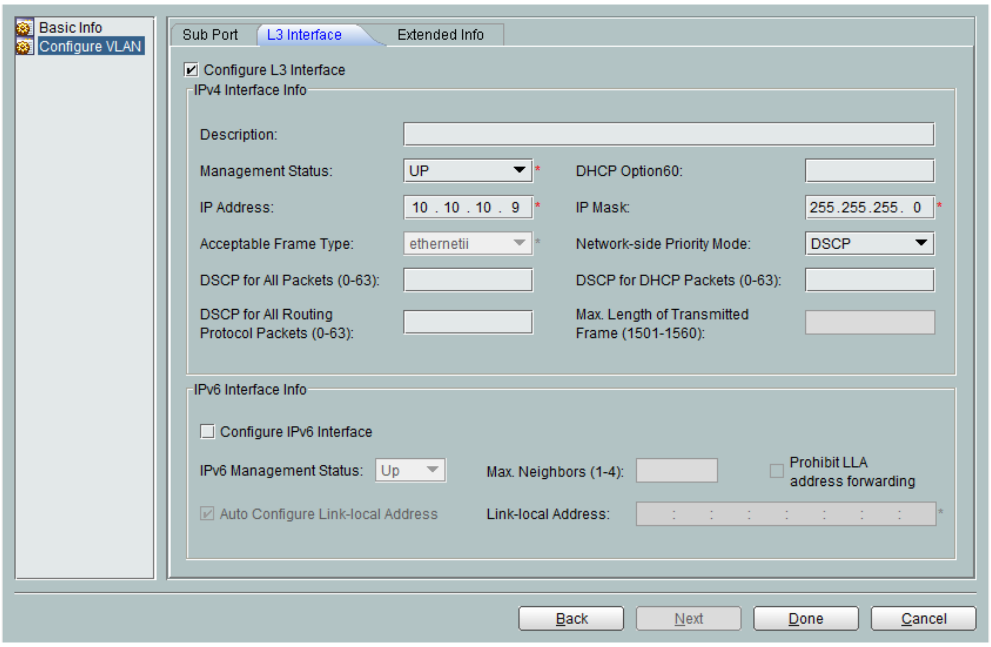


VLAN ID (1-4095): 12 *
Name: VLANID_12 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI



- Physical Port List
  - Frame:0
    - Slot:10
    - Slot:19
      - Port:01
    - Slot:20

- SubPort List
  - Frame:0
    - Slot:19
      - Port:00



☑ Configure L3 Interface

Management Status: UP

IP Address: 10 . 10 . 10 . 9

IP Mask: 255 .255 .255 . 0

Acceptable Frame Type: ethernetii

Network-side Priority Mode: DSCP

☐ Configure IPv6 Interface

IPv6 Management Status: Up

☐ Prohibit LLA address forwarding

☑ Auto Configure Link-local Address

Step 6 Click **Finish**.

----End

13.7 Adding an MPLS Interface

The MPLS interface is a Layer 3 interface bound to the MPLS VLAN. The local peer can communicate with the remote peer using LSP after an MPLS interface is added and MPLS LDP is enabled.

Procedure

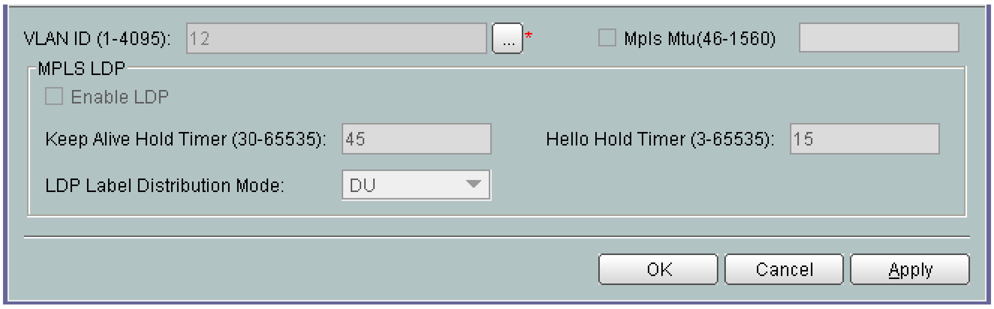
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **MPLS Management** from the navigation tree.

Step 3 Click the **MPLS Interface** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12

☐ Mpls Mtu(46-1560)

☐ Enable LDP

Keep Alive Hold Timer (30-65535): 45

Hello Hold Timer (3-65535): 15

LDP Label Distribution Mode: DU

Step 6 Click **OK**.

----End

13.8 Adding a Remote LDP Peer

The remote peer is a remote label switching router (LSR) which establishes a session with the local LSR. The MPLS discovers the remote peer through LDP extension mechanism. The local peer periodically sends messages in UDP packets to the specified remote peer.

Procedure

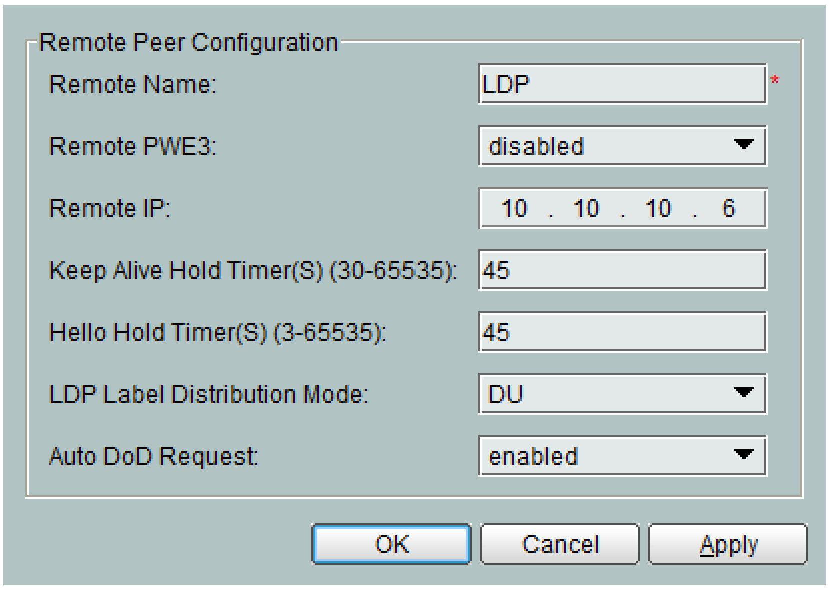
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **MPLS Management** from the navigation tree.

Step 3 Click the **LDP Remote Peer** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Remote Peer Configuration

Remote Name:	LDP *
Remote PWE3:	disabled
Remote IP:	10 . 10 . 10 . 6
Keep Alive Hold Timer(S) (30-65535):	45
Hello Hold Timer(S) (3-65535):	45
LDP Label Distribution Mode:	DU
Auto DoD Request:	enabled

Step 6 Click **OK**.

----End

13.9 Adding a Tunnel Policy

A tunnel may carry multiple PWs which are data transmission channels within a tunnel. By default, a VPN instance uses LSPs for service transmission on the backbone network. To use other types of tunnels or configure load balancing for service transmission of the VPN instance, you need to apply a tunnel policy to the VPN instance.

Procedure

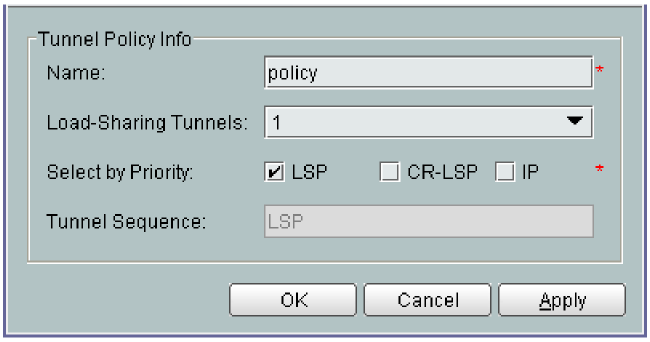
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **MPLS Management** from the navigation tree.

Step 3 Click the **Tunnel Policy** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Tunnel Policy Info

Name: policy *

Load-Sharing Tunnels: 1

Select by Priority: ☑ LSP ☐ CR-LSP ☐ IP *

Tunnel Sequence: LSP

Step 6 Click**OK**.

----End

13.10 Adding a PW

Different types of PWs are set up to emulate end-to-end ATM or Ethernet services. Bind the PW to a VLAN and access the VLAN to the PW.

Procedure

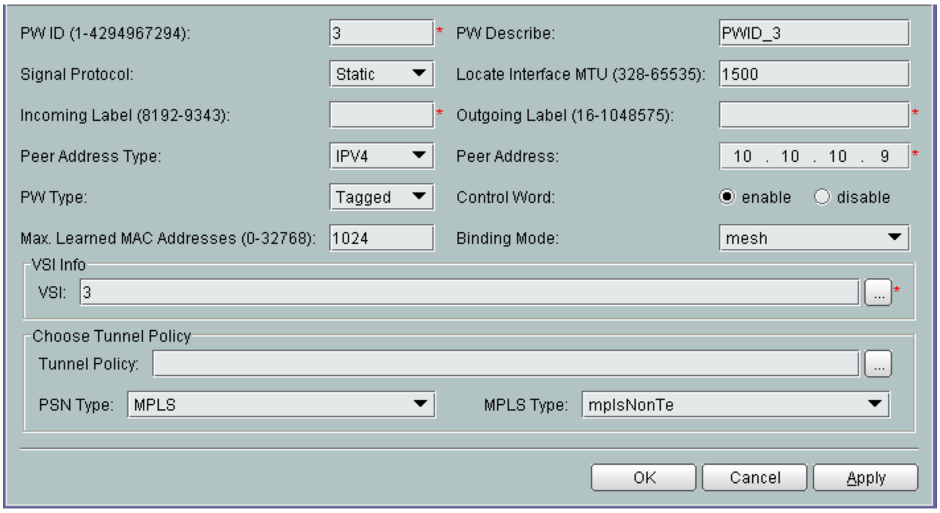
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **VPLS Management** from the navigation tree.

Step 3 Click the **PW** tab.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



PW ID (1-4294967294): 3 *
PW Describe: PWID_3
Signal Protocol: Static
Locate Interface MTU (328-65535): 1500
Incoming Label (8192-9343): *
Outgoing Label (16-1048575): *
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 9 *
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh

VSI Info
VSI: 3 *

Choose Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe

Step 6 Click **OK**.

----End

13.11 Adding a PW Protection Group (Optional)

After a PW protection group is added, the service can be quickly switched to another PW when the PW which carries the service is faulty (for example, the tunnel of the PW is deleted).

Procedure

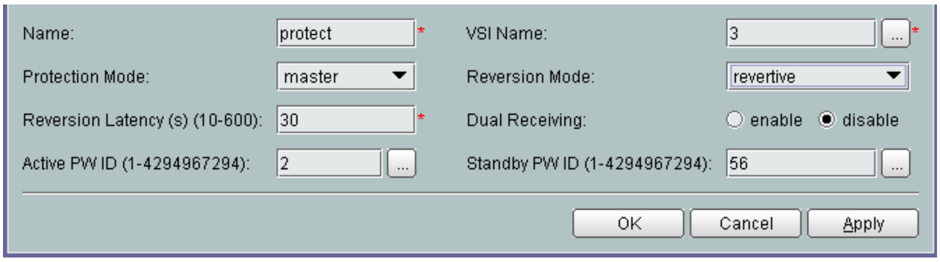
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **VPLS Management** from the navigation tree.

Step 3 On the **Protection Group** tab page, set the filter criteria or click ⌄ to display the PW protect groups.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: protect *
VSI Name: 3 *
Protection Mode: master
Reversion Mode: revertive
Reversion Latency (s) (10-600): 30 *
Dual Receiving: ○ enable ● disable
Active PW ID (1-4294967294): 2
Standby PW ID (1-4294967294): 56

Step 6 Click **OK**.

----End

13.12 Adding a VSI

The virtual switch instance (VSI) is the core of VPLS services. It can map links that access VPLS networks to PWs.

Procedure

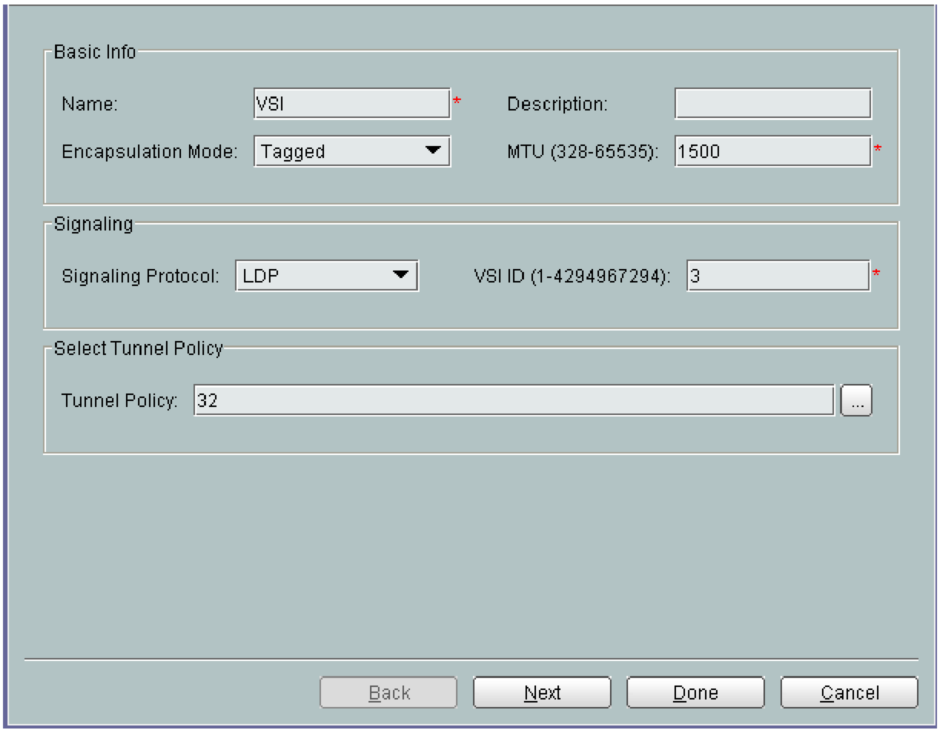
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **VPLS Management** from the navigation tree.

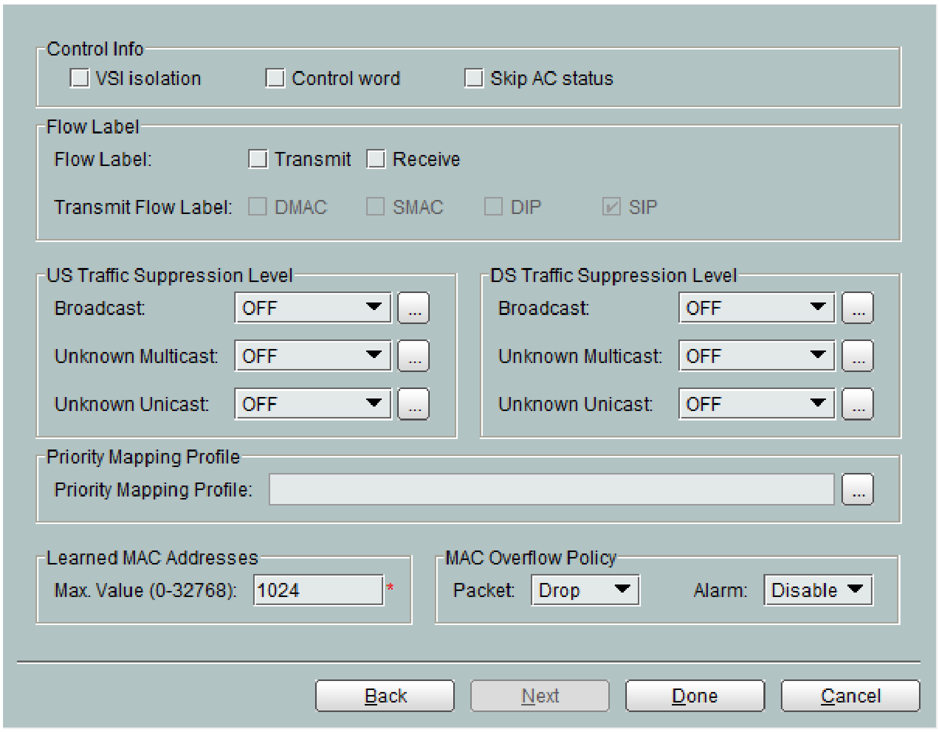
Step 3 On the **VSI** tab page, set the filter criteria or click ⌄ to display the VSIs.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Name: VSI *
Description:
Encapsulation Mode: Tagged
MTU (328-65535): 1500 *
Signaling Protocol: LDP
VSI ID (1-4294967294): 3 *
Tunnel Policy: 32



Control Info
☐ VSI isolation ☐ Control word ☐ Skip AC status

Flow Label
Flow Label: ☐ Transmit ☐ Receive
Transmit Flow Label: ☐ DMAC ☐ SMAC ☐ DIP ☑ SIP

US Traffic Suppression Level
Broadcast: OFF
Unknown Multicast: OFF
Unknown Unicast: OFF

DS Traffic Suppression Level
Broadcast: OFF
Unknown Multicast: OFF
Unknown Unicast: OFF

Priority Mapping Profile
Priority Mapping Profile:

Learned MAC Addresses
Max. Value (0-32768): 1024 *

MAC Overflow Policy
Packet: Drop Alarm: Disable

Step 6 Click **Done**.

----End

13.13 Binding a VSI to a PW

Packet forwarding is limited to a scope after the virtual switch instance (VSI) is bound to a PW. Therefore, packets can be transmitted only over the PW to which the VSI is bound.

Procedure

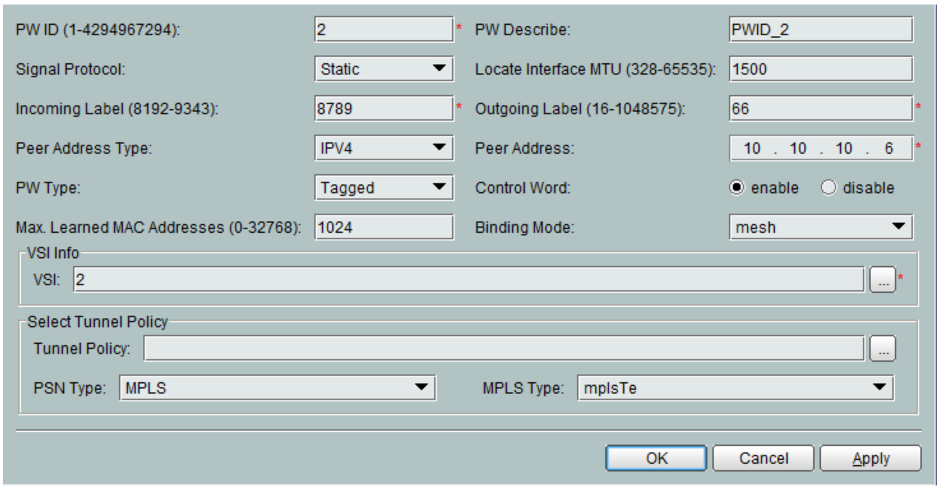
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **VPLS Management** from the navigation tree.

Step 3 Click the **PW** tab, set the filter criteria or click to display the PWs.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



PW ID (1-4294967294): 2 *
PW Describe: PWID_2
Signal Protocol: Static
Locate Interface MTU (328-65535): 1500
Incoming Label (8192-9343): 8789 *
Outgoing Label (16-1048575): 66 *
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 6 *
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh

VSI Info
VSI: 2 *

Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsTe

Step 6 Click **OK**.

----End

13.14 Binding a VSI to an AC

Packet forwarding is limited to a scope after the virtual switch instance (VSI) is bound to an AC. AC packets can be transmitted over the PW only after they are bound to a VSI.

Procedure

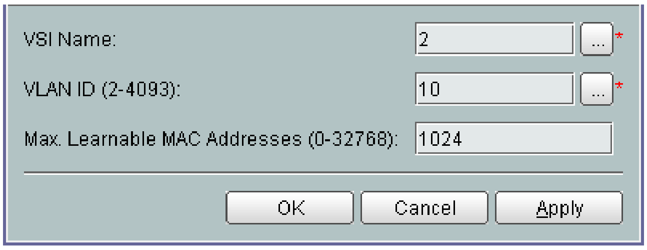
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VPN** > **VPLS Management** from the navigation tree.

Step 3 On the **AC** tab page, set the filter criteria or click ⌄ to display the ACs.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



VSI Name: 2 *
VLAN ID (2-4093): 10 *
Max. Learnable MAC Addresses (0-32768): 1024

Step 6 Click **OK**.

----End

13.15 VPLS Application Case

VPLS application cases include the H-VPLS configuration case and the Full-Mesh network configuration case.

13.15.1 H-VPLS Configuration Case

This case describes how to configure VPLS services on an H-VPLS network. VPLS is short for virtual private LAN service.

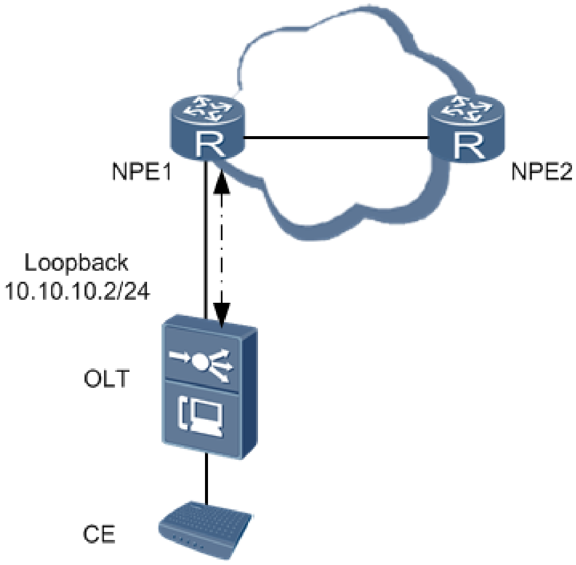
Prerequisites

- The networking shown in **Figure 13-4** has been completed.
- The network devices and lines are functioning properly.
- Service boards are online.

Networking Description

Figure 13-4 shows the networking of an H-VPLS service. On an H-VPLS network, each OLT connects to the basic VPLS full-mesh network directly to enable OLTs to communicate with each other. Therefore, you do not need to configure a PW between two OLTs , reducing PWs and maintenance costs.

Figure 13-4 H-VPLS networking



NPEs are NEs on the network side, such as general routers. CEs are Layer 2 network devices (such as a modem) on the lower layer of OLTs. CEs are connected to OLTs through the service ports on ADLF boards. OLTs are interconnected through GE uplink ports on the SCC board.

Data Plan

Table 13-3 Data plan for H-VPLS configuration

Configuration Item	Data	Remarks
Loopback interface and IP address	● Interface Number: 3 ● IP Address: 10.10.10.2 ● Ip Mask Length: 24 ● The other parameters use the default values.	-
Configuring the MPLS Parameters	● MPLS Switch: Enable ● Specify LSR(Label Switched Router) identifier: 10.10.10.2 ● Label Distribution Protocol(LDP): Enable ● Operate on MPLS L2VPN: Enable ● The other parameters use the default values.	**Specify LSR(Label Switched Router) identifier** must be the same as **Ip Address**.
Service VLAN	● VLAN ID: 10 ● Type: Smart VLAN ● Attribute: QinQ ● Sub Port: 0/9/0 ● The other parameters use the default values.	-
Service-port	● Connection Type: LAN-ADSL ● Interface Selection: 0/16/0 ● VLAN Choice: Smart VLAN ● VLAN ID: 10 ● Auto-sensing: selected **Auto-sensing** check box ● Service Type: Single ● Upstream Traffic Profile/ Downstream Traffic Profile: ip-traffic-table_2 ● The other parameters use the default values.	**VLAN ID** must be the same as the **VLAN ID** of the service VLAN.

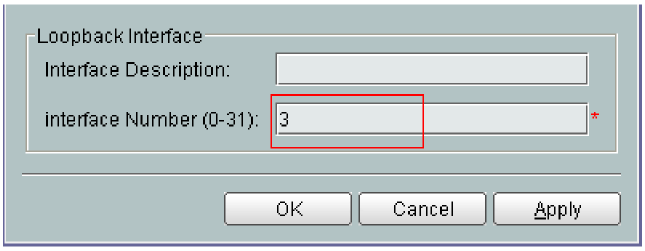
Configuration Item	Data	Remarks
MPLS VLAN	● VLAN ID: 12 ● Type: Smart VLAN ● Attribute: Common ● Sub Port: 0/9/0 ● Management Status: UP ● IP Address: 10.10.10.6 ● The other parameters use the default values.	-
MPLS interface	● VLAN ID: 12 ● Mpls Mtu: 60 ● Enable LDP: selected **Enable LDP** check box ● The other parameters use the default values.	**VLAN ID** must be the same as the **VLAN ID** of the MPLS VLAN.
Remote Peer Configuration	● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.3 ● The other parameters use the default values.	-
PW	● PW ID: 2 ● Signal Protocol: LDP ● Peer Address: 10.10.10.3 ● VLAN ID: 10 ● MPLS Type: mplsNonTe ● The other parameters use the default values.	**Virtual local area network (VLAN)** must be the same as the **VLAN ID** of the service VLAN.

Procedure

Step 1 Configure an IP address for the interface.

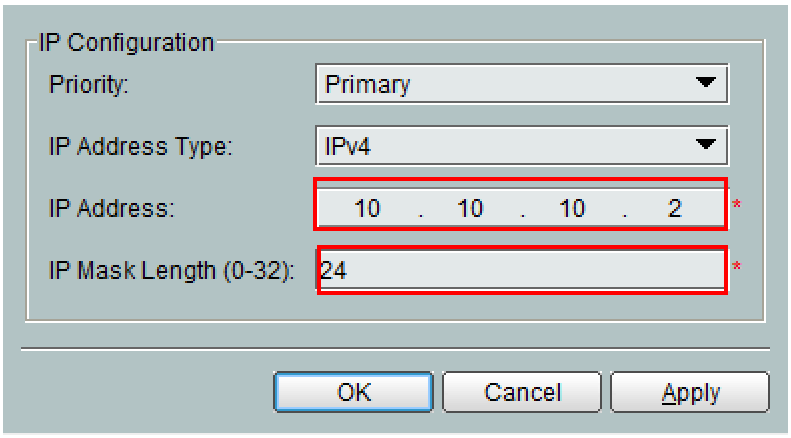
As the source interface of MPLS packets, the loopback interface retains Up after it was created. The IP address of the loopback interface is planned by carriers and must be the same as the value of **Specify LSR(Label Switched Router) identifier**. Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **LookBack Interface** from the navigation tree.
3. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters.



Interface Description:
interface Number (0-31): 3 *

5. Click **OK**.
6. Select the loopback and click the **IP Address** tab in the lower pane.
7. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
8. In the dialog box that is displayed, set the parameters.



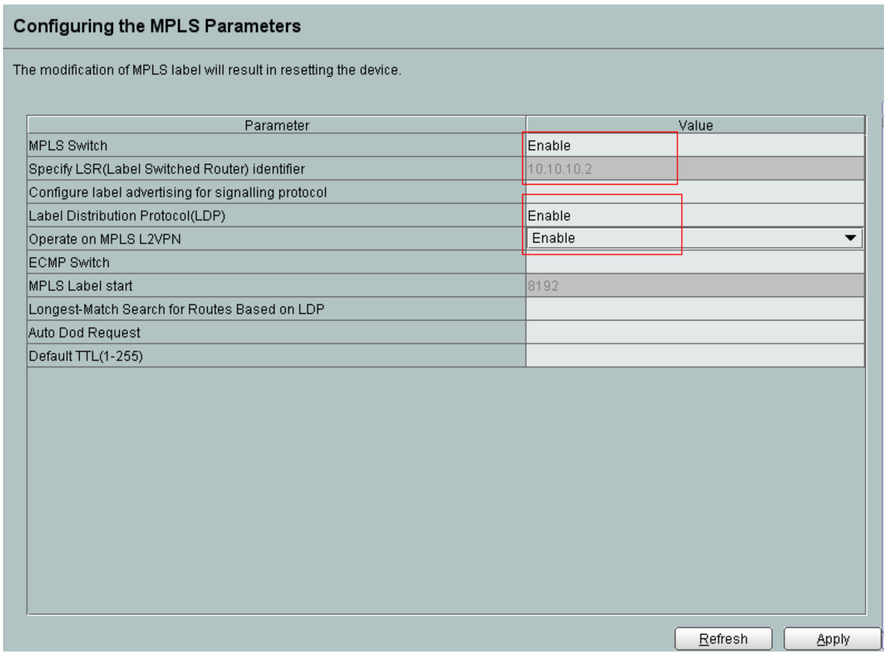
Priority: Primary
IP Address Type: IPv4
IP Address: 10 . 10 . 10 . 2 *
IP Mask Length (0-32): 24 *

9. Click **OK**.

Step 2 Configure the global MPLS parameters.

Enable MPLS functions on network-wide NEs by setting global parameters, such as MPLS capability, LDP capability, and specify LSR identifier. Other VPWS configurations take effect only after global MPLS parameters are set. Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **NE Properties** > **Protocol** > **MPLS** from the navigation tree.
3. Configure global MPLS parameters in the Value column.



Configuring the MPLS Parameters

The modification of MPLS label will result in resetting the device.

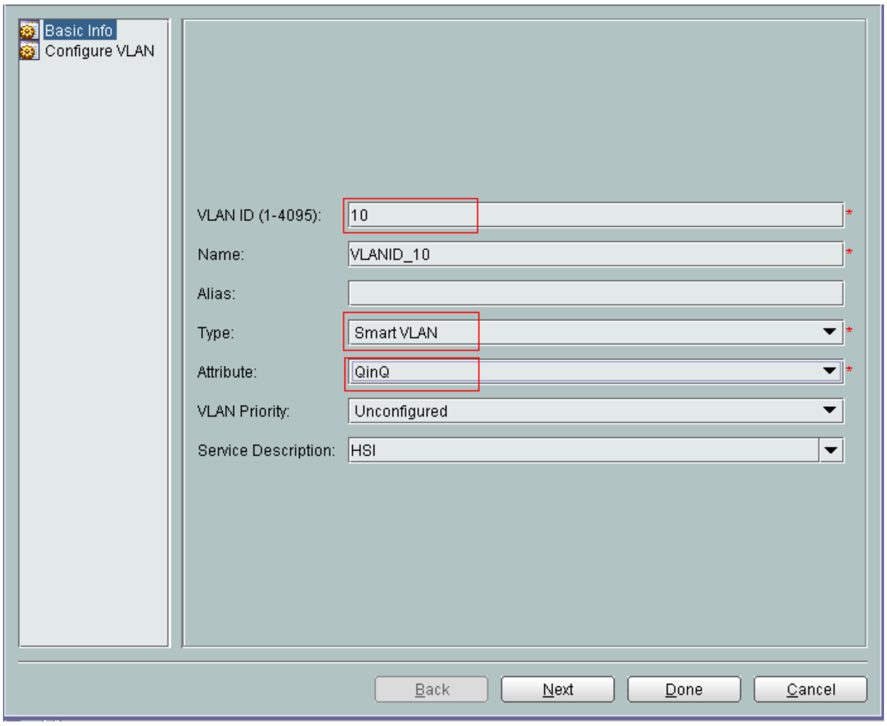
Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.2
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

4. Click **Apply**.

Step 3 Add a service VLAN.

Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.
4. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 10

Name: VLANID_10

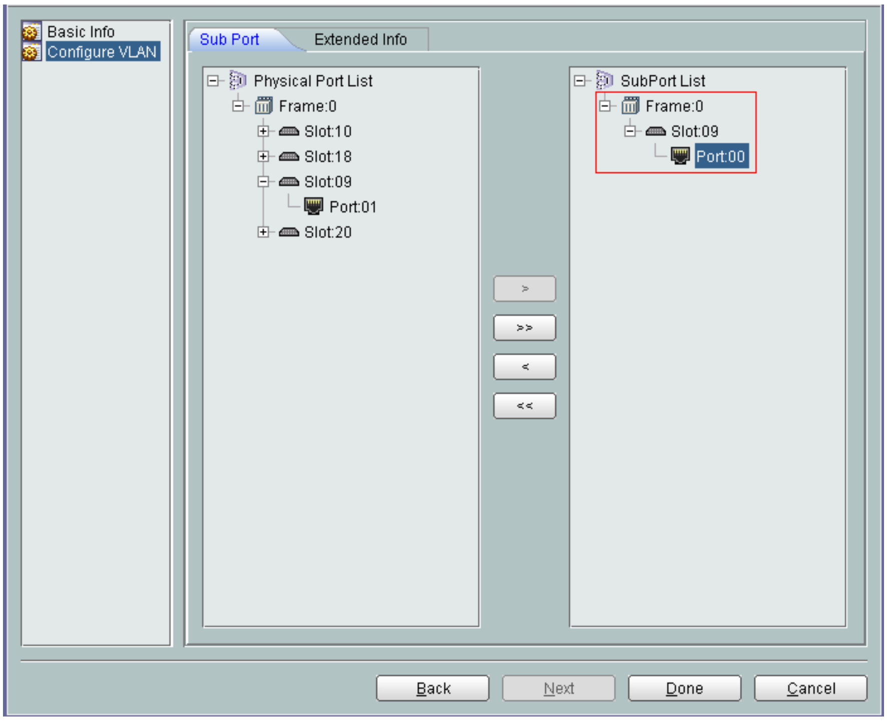
Alias:

Type: Smart VLAN

Attribute: QinQ

VLAN Priority: Unconfigured

Service Description: HSI



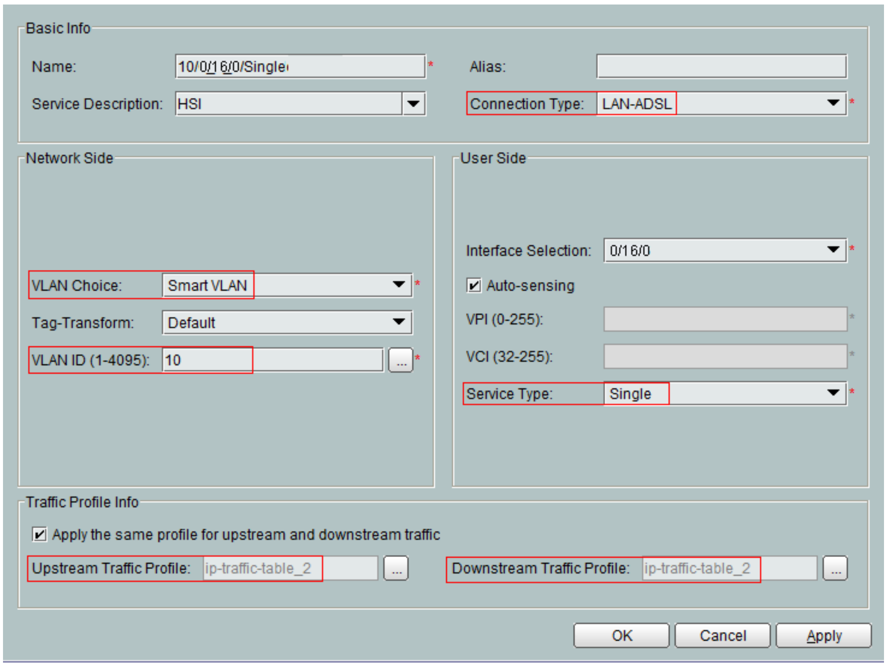
6. Click **Finish**.

Step 4 Add a service port.

The service port can carry various service flows after it is configured. Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **DSL** > **ADSL Port** from the navigation tree.

3. On the **ADSL** tab page, set the filter criteria or click to display the ADSL ports.
4. In the information list, select an ADSL port record and click the **Service Port Info** tab. On the tab, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



Basic Info

Name: 10/0/16/0/Single

Alias:

Service Description: HSI

Connection Type: LAN-ADSL

Network Side

VLAN Choice: Smart VLAN

Tag-Transform: Default

VLAN ID (1-4095): 10

User Side

Interface Selection: 0/16/0

☑ Auto-sensing

VPI (0-255):

VCI (32-255):

Service Type: Single

Traffic Profile Info

☑ Apply the same profile for upstream and downstream traffic

Upstream Traffic Profile: ip-traffic-table_2

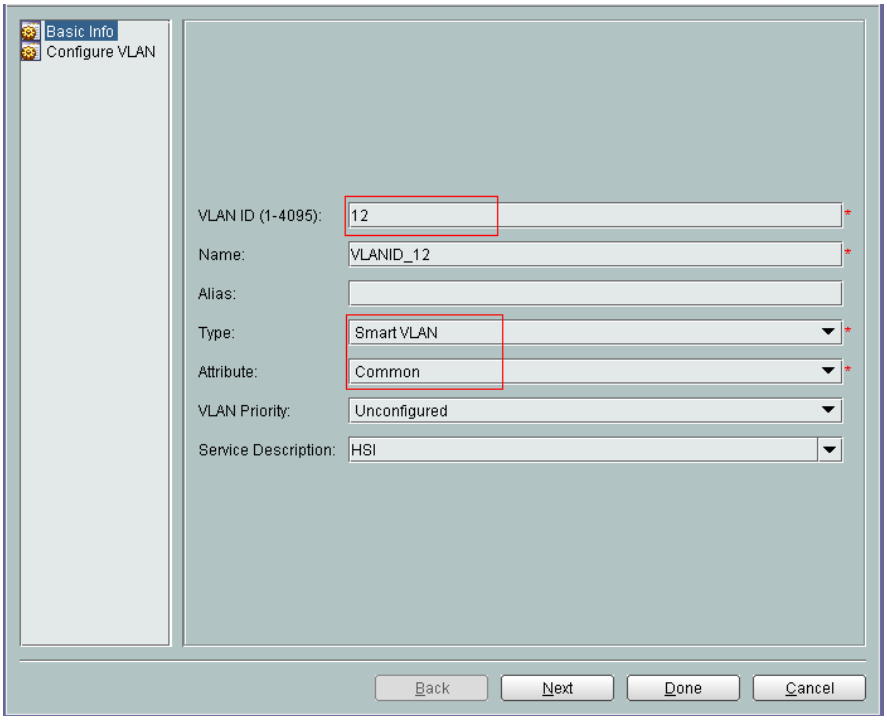
Downstream Traffic Profile: ip-traffic-table_2

6. Click **OK**.

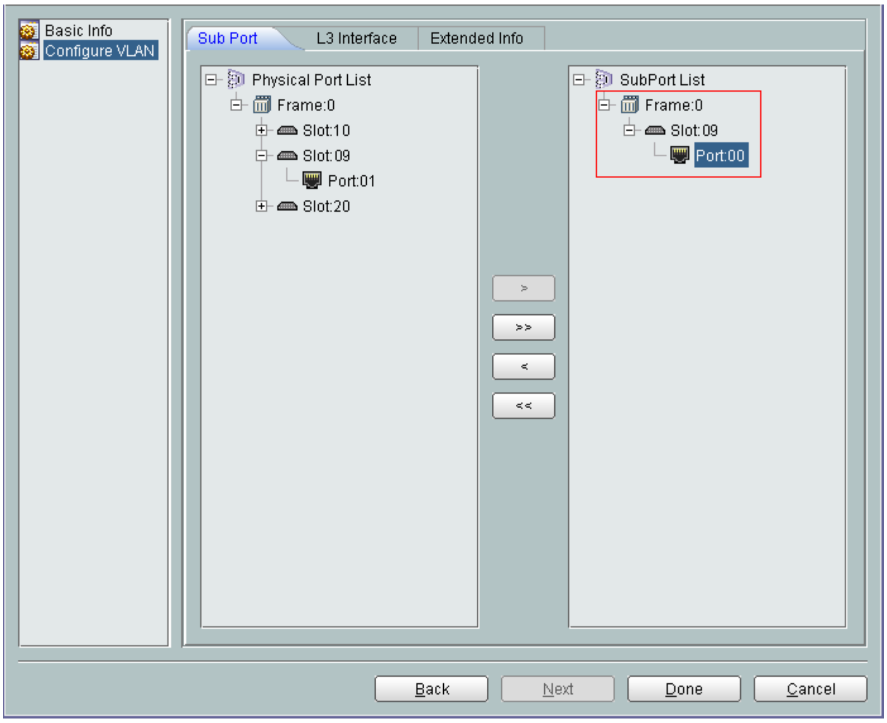
Step 5 Add an MPLS VLAN.

Before provisioning services to NEs, add an MPLS VLAN. The local peer communicates with the remote peer through the uplink port of the MPLS VLAN. Configure OLT as follows:

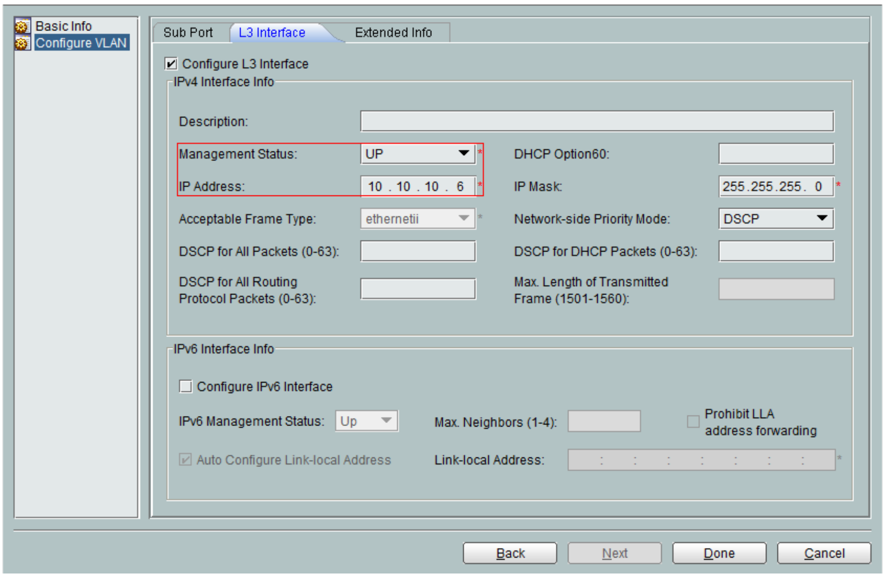
1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. On the **VLAN** tab page, set the filter criteria or click to display the VLANs.
4. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12 *
Name: VLANID_12 *
Alias:
Type: Smart VLAN *
Attribute: Common *
VLAN Priority: Unconfigured
Service Description: HSI



6. Click **Next**.
7. Click the **L3 Interface** tab.
8. In the dialog box that is displayed, set the parameters.



☑ Configure L3 Interface

IPv4 Interface Info

Description:

Management Status: UP

IP Address: 10 . 10 . 10 . 6

Acceptable Frame Type: ethernetii

DSCP for All Packets (0-63):

DSCP for All Routing Protocol Packets (0-63):

DHCP Option60:

IP Mask: 255 .255 .255 . 0

Network-side Priority Mode: DSCP

DSCP for DHCP Packets (0-63):

Max. Length of Transmitted Frame (1501-1560):

IPv6 Interface Info

☐ Configure IPv6 Interface

IPv6 Management Status: Up

Max. Neighbors (1-4):

☐ Prohibit LLA address forwarding

☑ Auto Configure Link-local Address

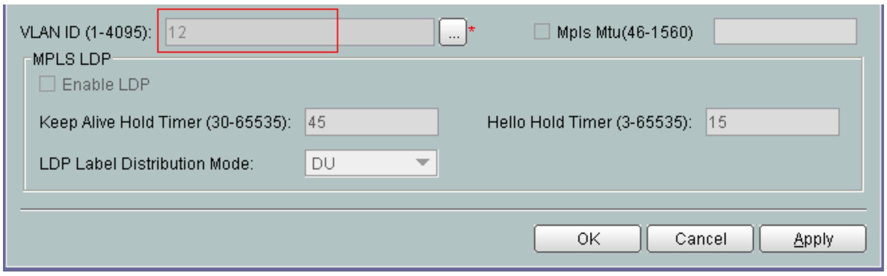
Link-local Address:

9. Click **Finish**.

Step 6 Add an MPLS interface.

The MPLS interface is a Layer 3 interface bound to the MPLS VLAN. The local peer can communicate with the remote peer using LSP after an MPLS interface is added and MPLS LDP is enabled. Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **MPLS Interface** tab.
4. Right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12

☐ Mpls Mtu(46-1560)

MPLS LDP

☐ Enable LDP

Keep Alive Hold Timer (30-65535): 45

Hello Hold Timer (3-65535): 15

LDP Label Distribution Mode: DU

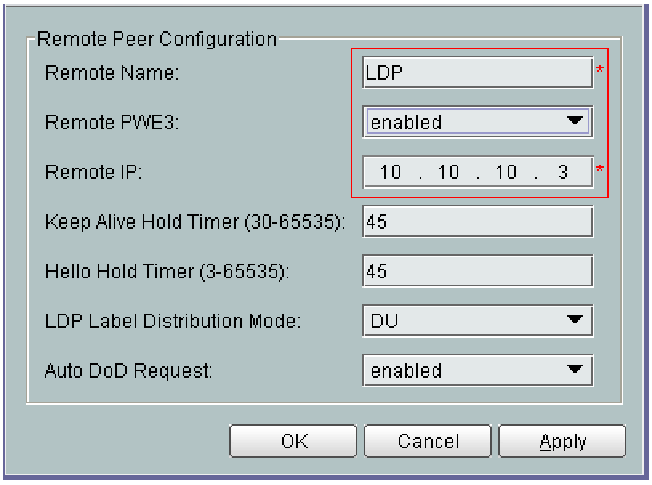
6. Click **OK**.

Step 7 Add a remote peer.

The remote peer is a remote label switching router (LSR) which establishes a session with the local LSR. The MPLS discovers the remote peer through LDP extension mechanism. The local peer periodically sends messages in UDP packets to the specified remote peer. In this case, the peers are routers connected to MA5600T as shown in **Figure 13-4**. Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **LDP Remote Peer** tab.

4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



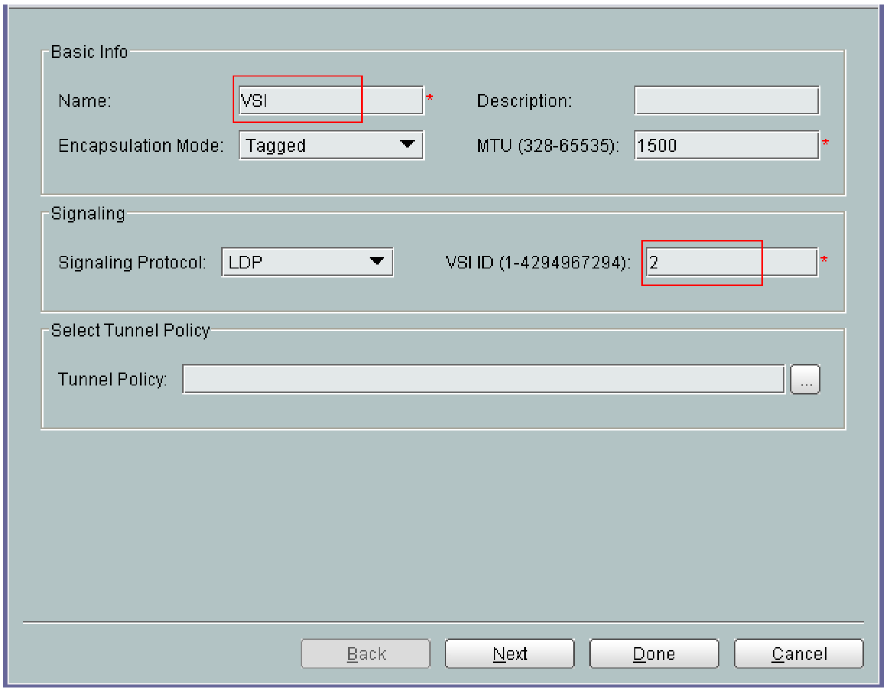
Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: enabled
Remote IP: 10 . 10 . 10 . 3 *
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled

6. Click **OK**.

Step 8 Add a VSI.

Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPLS Management** from the navigation tree.
3. On the **VSI** tab page, set the filter criteria or click ⩡ to display the VSIs.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



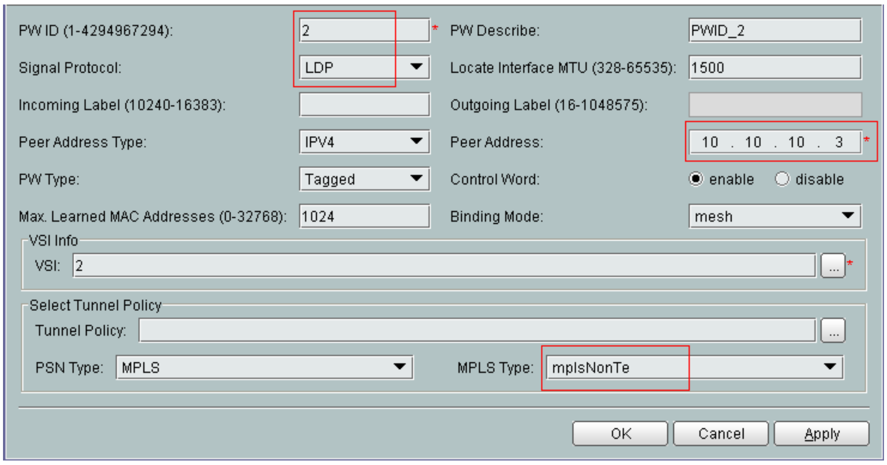
Basic Info
Name: VSI *
Description:
Encapsulation Mode: Tagged
MTU (328-65535): 1500 *
Signaling
Signaling Protocol: LDP
VSI ID (1-4294967294): 2 *
Select Tunnel Policy
Tunnel Policy:

6. Click **OK**.

Step 9 Bind the VSI to a PW.

Packet forwarding is limited to a scope after the VSI is bound to a PW. Therefore, packets are transmitted only on the PW to which the VSI is bound. Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPLS Management** from the navigation tree.
3. Click the **PW** tab, set the filter criteria or click ⌄ to display the PWs.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



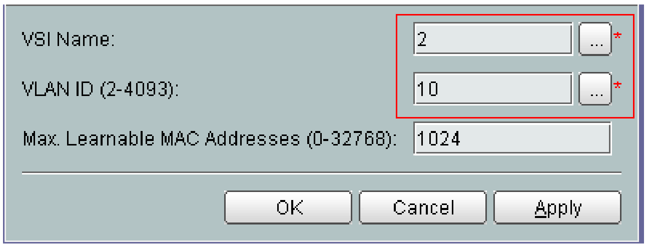
PW ID (1-4294967294): 2 *
PW Describe: PWID_2
Signal Protocol: LDP
Locate Interface MTU (328-65535): 1500
Incoming Label (10240-16383):
Outgoing Label (16-1048575):
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 3 *
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh
VSI Info
VSI: 2 *
Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe

6. Click **OK**.

Step 10 Bind the VSI to an AC.

Packet forwarding is limited to a scope after the VSI is bound to an AC. Therefore, only AC packets that are bound to the VSI can be transmitted on PWs. Configure OLT as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPLS Management** from the navigation tree.
3. On the **AC** tab page, set the filter criteria or click ⌄ to display the ACs.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VSI Name: 2 *
VLAN ID (2-4093): 10 *
Max. Learnable MAC Addresses (0-32768): 1024

6. Click **OK**.

----End

Result

After the preceding configuration is completed, the CE can communicate with the upper layer network of the OLT if the upper layer network configurations are correct.

13.15.2 Full-Mesh Network Configuration Case

This case describes how to configure VPLS services on a Full-Mesh network. VPLS is short for virtual private LAN service.

Prerequisites

- The networking shown in **Figure 13-5** has been completed.
- The network devices and lines are functioning properly.
- Service boards are online.

Scenario

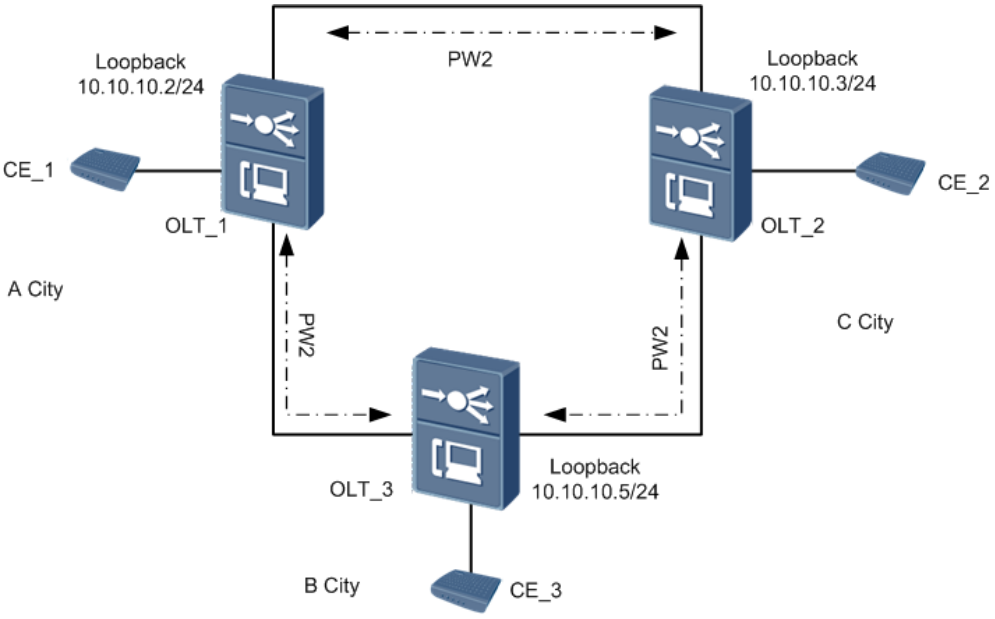
An enterprise has its own branches in cities A, B, and C. An MPLS backbone network with the VPLS technology can be used to interconnect enterprise networks of branches in cities A, B, and C.

Networking Description

Figure 13-5 shows the networking of a Full-Mesh service. On actual networks, there are multiple routers among three OLTs. The following figure does not show the routers because this case does not require router configuration. On a full-mesh network, every two OLTs are configured with a PW to enable OLTs to communicate with each other.

CE_1, CE_2, and CE_3 are Layer 2 devices (such as modems) on the lower layer of OLTs. They are accessed to OLT_1, OLT_2, and OLT_3 respectively through service ports on ADLF boards. The three OLTs are interconnected through GE uplink ports on the SCC board.

Figure 13-5 Full-Mesh networking



Data Plan

Table 13-4 Data plan for Full-Mesh service configuration

Configuration Item	Data	Remarks
Loopback interface and IP address	OLT_1: ● Interface Number: 3 ● IP Address: 10.10.10.2 ● Ip Mask Length: 24 ● The other parameters use the default values. OLT_2: ● Interface Number: 3 ● IP Address: 10.10.10.3 ● Ip Mask Length: 24 ● The other parameters use the default values. OLT_3:: ● Interface Number: 3 ● IP Address: 10.10.10.5 ● Ip Mask Length: 24 ● The other parameters use the default values.	-

Configuration Item	Data	Remarks
Configuring the MPLS Parameters	OLT_1: ● MPLS Switch: Enable ● Specify LSR(Label Switched Router) identifier: 10.10.10.2 ● Label Distribution Protocol(LDP): Enable ● Operate on MPLS L2VPN: Enable ● The other parameters use the default values. OLT_2: ● MPLS Switch: Enable ● Specify LSR(Label Switched Router) identifier: 10.10.10.3 ● Label Distribution Protocol(LDP): Enable ● Operate on MPLS L2VPN: Enable ● The other parameters use the default values. OLT_3: ● MPLS Switch: Enable ● Specify LSR(Label Switched Router) identifier: 10.10.10.5 ● Label Distribution Protocol(LDP): Enable ● Operate on MPLS L2VPN: Enable ● The other parameters use the default values.	**Specify LSR(Label Switched Router) identifier** must be the same as **Ip Address**.
Service VLAN	OLT_1, OLT_2, or OLT_3: ● VLAN ID: 10 ● Type: Smart VLAN ● Attribute: QinQ ● Sub Port: 0/9/0; 0/9/4 ● The other parameters use the default values.	-

Configuration Item	Data	Remarks
Service-port	OLT_1, OLT_2, or OLT_3: - Connection Type: LAN-ADSL - Interface Selection: 0/16/0 - VLAN Choice: Smart VLAN - VLAN ID: 10 - Auto-sensing: selected **Auto-sensing** check box - Service Type: Single - Upstream Traffic Profile/ Downstream Traffic Profile: ip-traffic-table_2 - The other parameters use the default values.	**VLAN ID** must be the same as the **VLAN ID** of the service VLAN.

Configuration Item	Data	Remarks
MPLS VLAN	OLT_1: ● VLAN ID: 12 ● Type: Smart VLAN ● Attribute: Common ● Sub Port: 0/9/0 or 0/9/4 ● Management Status: UP ● IP addresses: 10.10.10.6 ● The other parameters use the default values. OLT_2: ● VLAN ID: 12 ● Type: Smart VLAN ● Attribute: Common ● Sub Port: 0/9/0 or 0/9/4 ● Management Status: UP ● IP addresses: 10.10.10.7 ● The other parameters use the default values. OLT_3: ● VLAN ID: 12 ● Type: Smart VLAN ● Attribute: Common ● Sub Port: 0/9/0 or 0/9/4 ● Management Status: UP ● IP Address: 10.10.10.8 ● The other parameters use the default values.	-
MPLS interface	OLT_1, OLT_2, or OLT_3: ● VLAN ID: 12 ● Mpls Mtu: 60 ● Enable LDP: selected **Enable LDP** check box ● The other parameters use the default values.	**VLAN ID** must be the same as the **VLAN ID** of the MPLS VLAN.

Configuration Item	Data	Remarks
Remote Peer Configuration	OLT_1: ● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.3 or 10.10.10.5 ● The other parameters use the default values. OLT_2: ● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.2 or 10.10.10.5 ● The other parameters use the default values. OLT_3: ● Remote Name: LDP ● Remote PWE3: enabled ● Remote IP: 10.10.10.2 or 10.10.10.3 ● The other parameters use the default values.	-

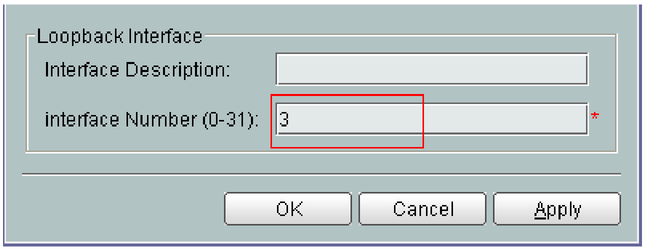
Configuration Item	Data	Remarks
PW	OLT_1: - PW ID: 2 - Signal Protocol: LDP - Peer Address: 10.10.10.3 or 10.10.10.5 - VLAN ID: 10 - MPLS Type: mplsNonTe - The other parameters use the default values. OLT_2: - PW ID: 2 - Signal Protocol: LDP - Peer Address: 10.10.10.2 or 10.10.10.5 - VLAN ID: 10 - MPLS Type: mplsNonTe - The other parameters use the default values. OLT_3: - PW ID: 2 - Signal Protocol: LDP - Peer Address: 10.10.10.2 or 10.10.10.3 - VLAN ID: 10 - The other parameters use the default values.	**Virtual local area network (VLAN)** must be the same as the **VLAN ID** of the service VLAN.

Procedure

Step 1 Configure an IP address for the interface.

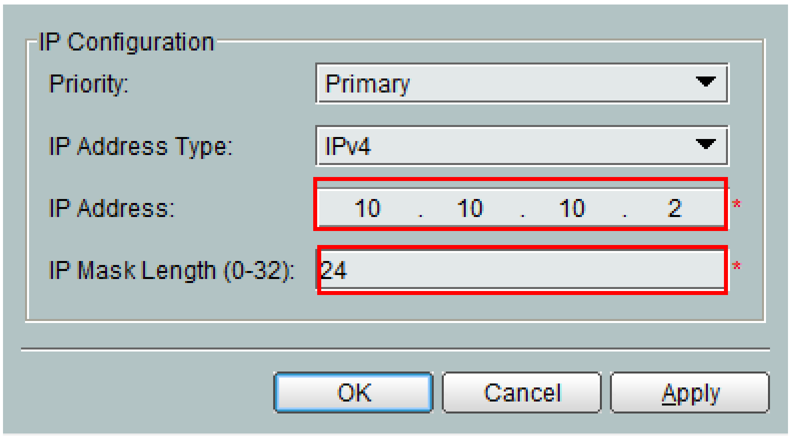
As the source interface of MPLS packets, the loopback interface retains Up after it was created. The IP address of the loopback interface is planned by carriers and must be the same as the value of **Specify LSR(Label Switched Router) identifier**. Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **LookBack Interface** from the navigation tree.
3. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters.

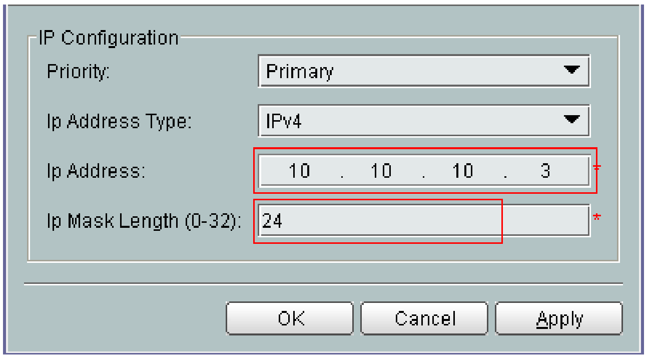

Loopback Interface
Interface Description:
interface Number (0-31): 3 *

5. Click **OK**.
6. Select the loopback and click the **IP Address** tab in the lower pane.
7. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
8. In the dialog box that is displayed, set the parameters.

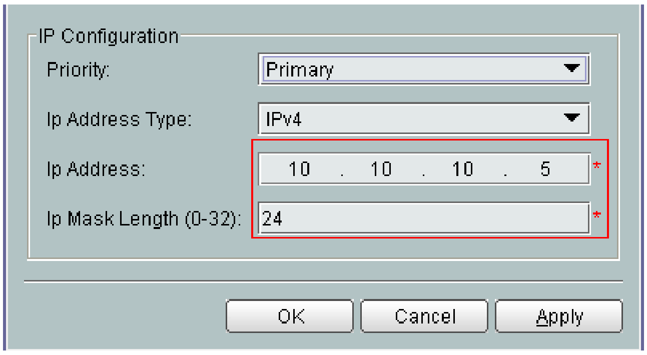
Configuring parameters for OLT_1


IP Configuration
Priority: Primary
IP Address Type: IPv4
IP Address: 10 . 10 . 10 . 2 *
IP Mask Length (0-32): 24 *

Configuring parameters for OLT_2


IP Configuration
Priority: Primary
Ip Address Type: IPv4
Ip Address: 10 . 10 . 10 . 3 *
Ip Mask Length (0-32): 24 *

Configuring parameters for OLT_3



Priority: Primary

Ip Address Type: IPv4

Ip Address: 10 . 10 . 10 . 5 *

Ip Mask Length (0-32): 24 *

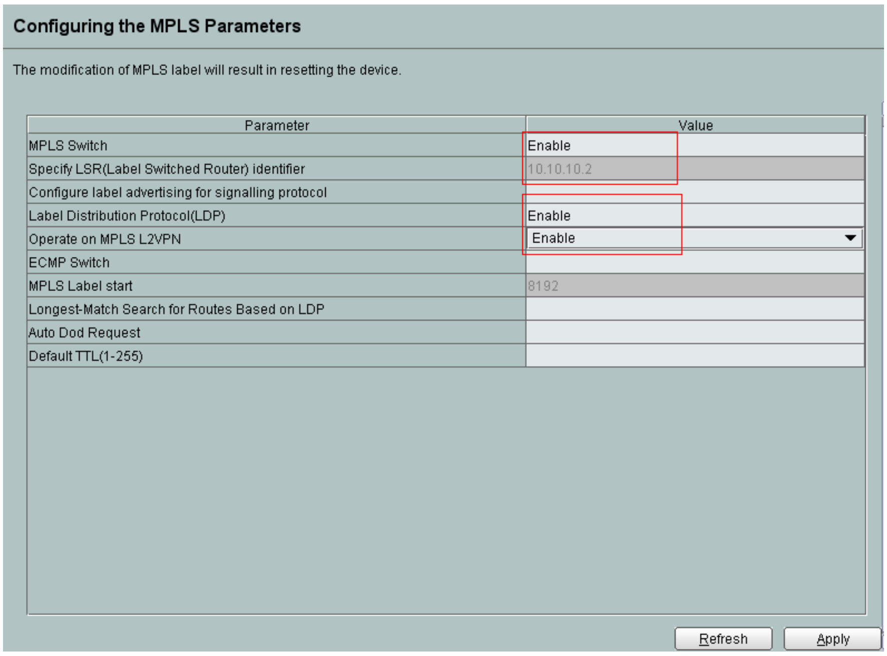
9. Click **OK**.

Step 2 Configure the global MPLS parameters.

Enable MPLS functions on network-wide NEs by setting global parameters, such as MPLS capability, LDP capability, and specify LSR identifier. Other VPWS configurations take effect only after global MPLS parameters are set. Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **NE Properties** > **Protocol** > **MPLS** from the navigation tree.
3. Configure global MPLS parameters in the **Value** column.

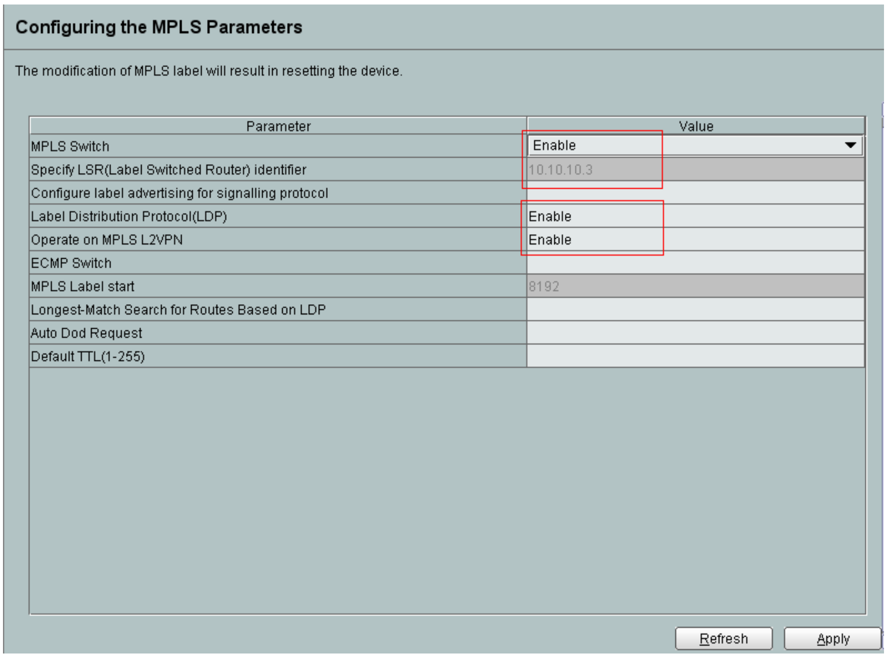
Configuring parameters for OLT_1



The modification of MPLS label will result in resetting the device.

Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.2
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

Configuring parameters for OLT_2

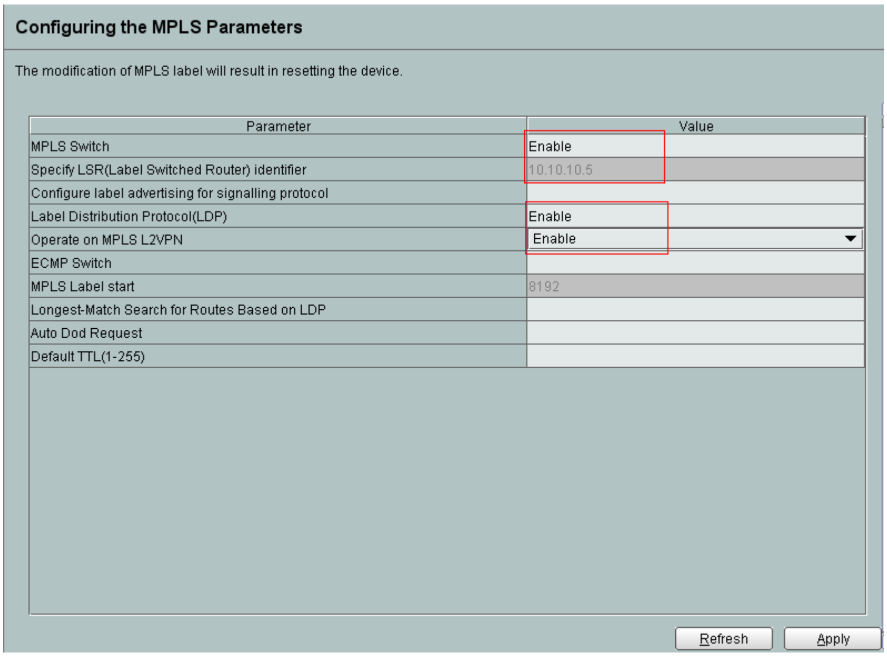


Configuring the MPLS Parameters

The modification of MPLS label will result in resetting the device.

Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.3
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

Configuring parameters for OLT_3



Configuring the MPLS Parameters

The modification of MPLS label will result in resetting the device.

Parameter	Value
MPLS Switch	Enable
Specify LSR(Label Switched Router) identifier	10.10.10.5
Configure label advertising for signalling protocol	
Label Distribution Protocol(LDP)	Enable
Operate on MPLS L2VPN	Enable
ECMP Switch	
MPLS Label start	8192
Longest-Match Search for Routes Based on LDP	
Auto Dod Request	
Default TTL(1-255)	

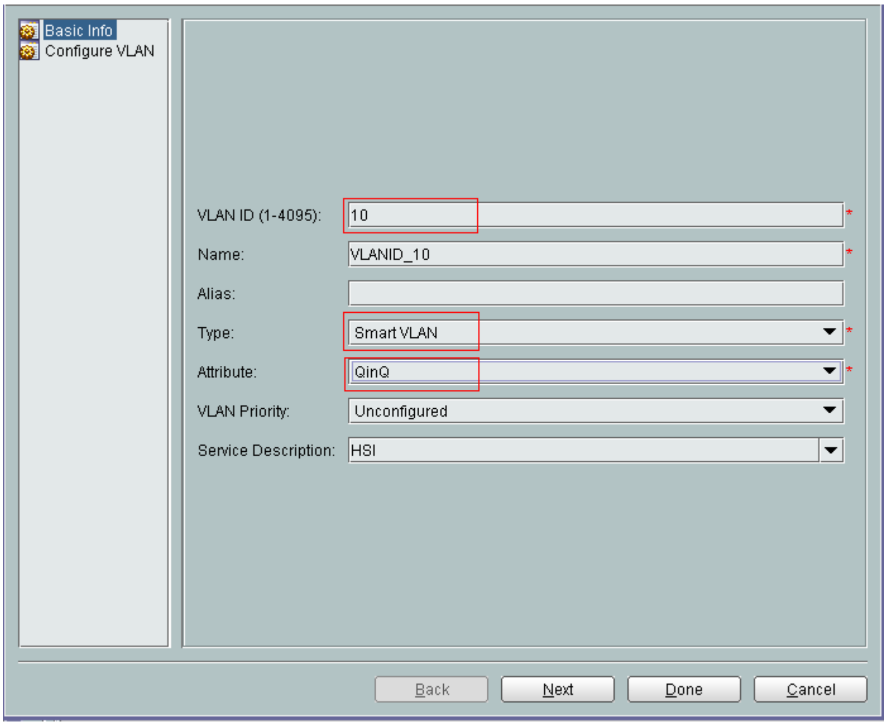
4. Click **Apply**.

Step 3 Add a service VLAN.

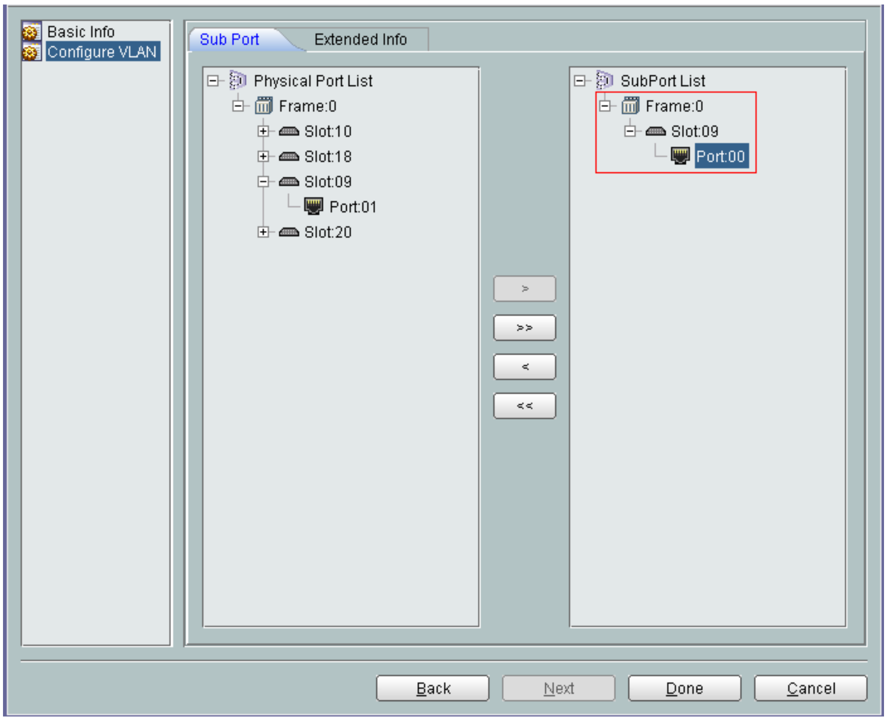
Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.
4. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.

5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 10 *
Name: VLANID_10 *
Alias:
Type: Smart VLAN *
Attribute: QinQ *
VLAN Priority: Unconfigured
Service Description: HSI



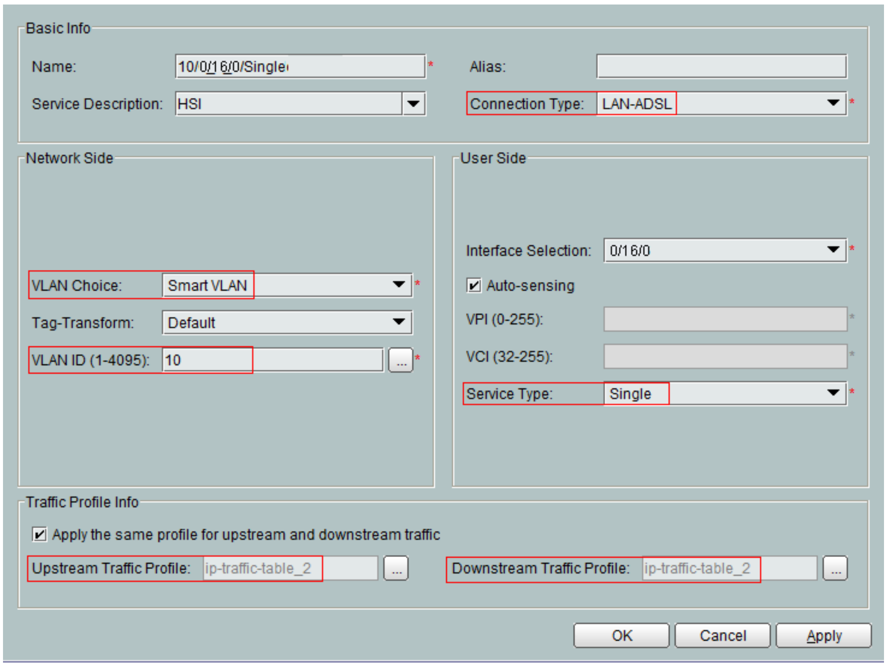
6. Click **Finish**.

Step 4 Add a service port.

The service port can carry various service flows after it is configured. Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

2. Choose **DSL** > **ADSL Port** from the navigation tree.
3. On the **ADSL** tab page, set the filter criteria or click ⌄ to display the ADSL ports.
4. In the information list, select an ADSL port record and click the **Service Port Info** tab. On the tab, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



Basic Info

Name: 10/0/16/0/Single

Alias:

Service Description: HSI

Connection Type: LAN-ADSL

Network Side

VLAN Choice: Smart VLAN

Tag-Transform: Default

VLAN ID (1-4095): 10

User Side

Interface Selection: 0/16/0

☑ Auto-sensing

VPI (0-255):

VCI (32-255):

Service Type: Single

Traffic Profile Info

☑ Apply the same profile for upstream and downstream traffic

Upstream Traffic Profile: ip-traffic-table_2

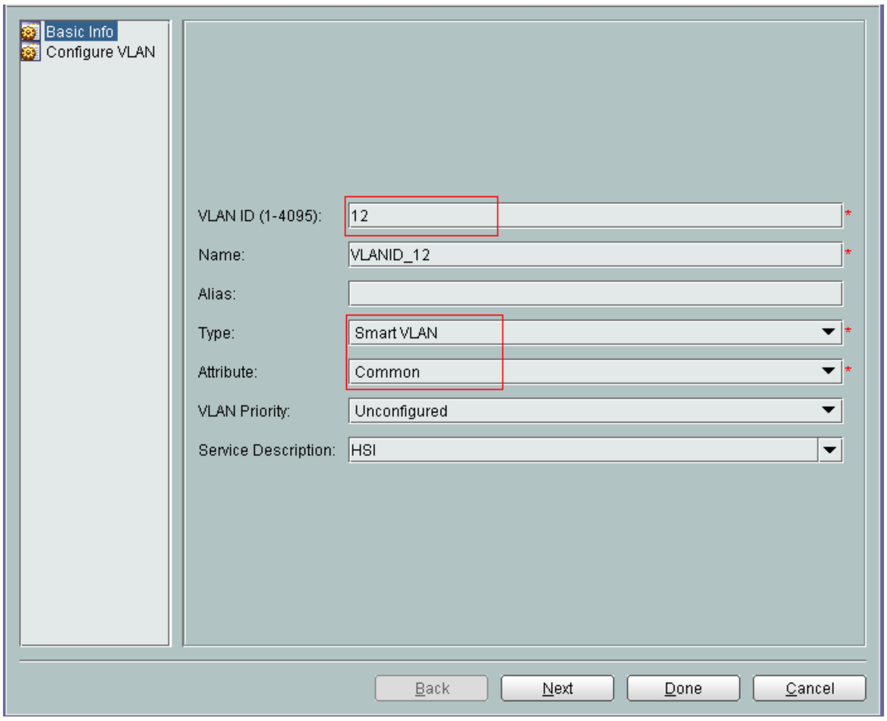
Downstream Traffic Profile: ip-traffic-table_2

6. Click **OK**.

Step 5 Add an MPLS VLAN.

Before provisioning services to NEs, add an MPLS VLAN. The local peer communicates with the remote peer through the uplink port of the MPLS VLAN. Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. On the **VLAN** tab page, set the filter criteria or click ⌄ to display the VLANs.
4. In the information list, right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VLAN ID (1-4095): 12

Name: VLANID_12

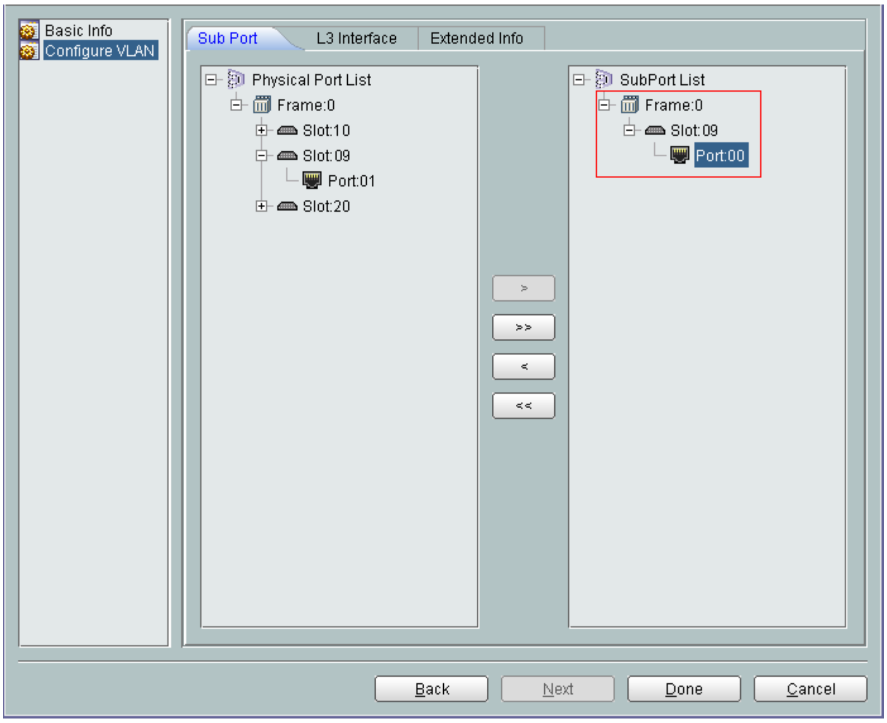
Alias:

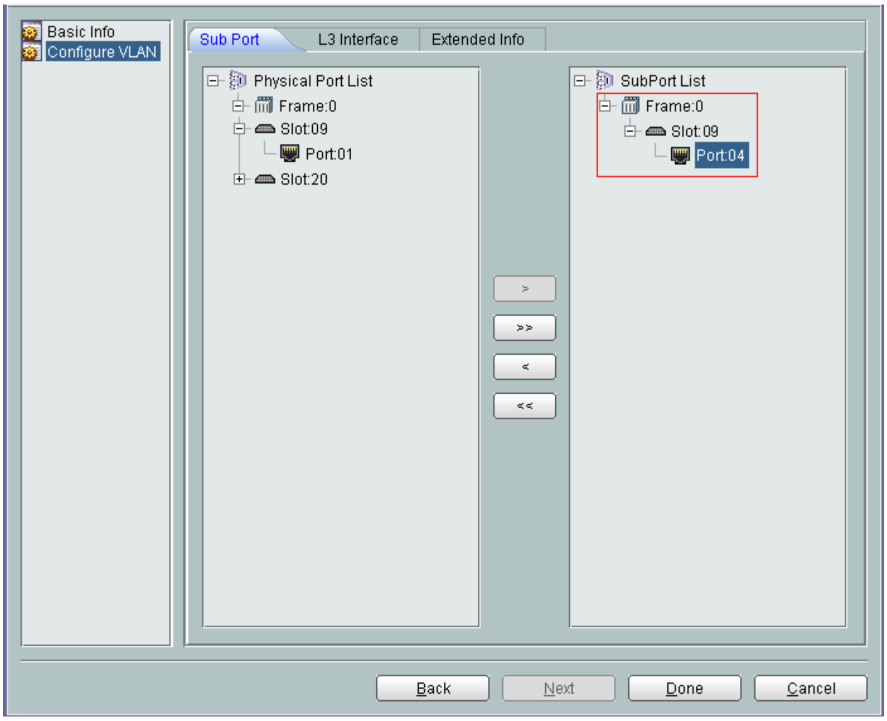
Type: Smart VLAN

Attribute: Common

VLAN Priority: Unconfigured

Service Description: HSI



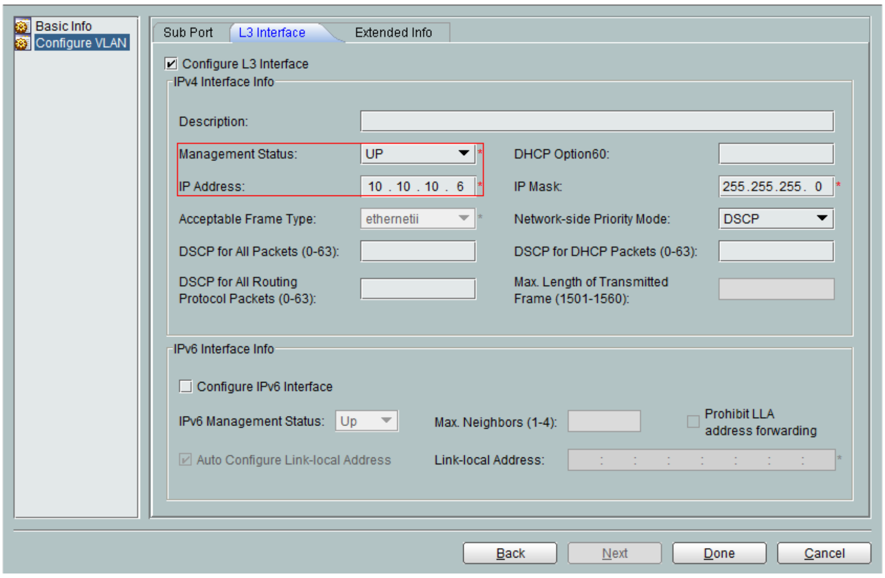


Physical Port List
Frame:0
Slot:09
Port:01
Slot:20

SubPort List
Frame:0
Slot:09
Port:04

6. Click **Next**.
7. Click the **L3 Interface** tab.
8. In the dialog box that is displayed, set the parameters.

Configuring parameters for OLT_1



☑ Configure L3 Interface

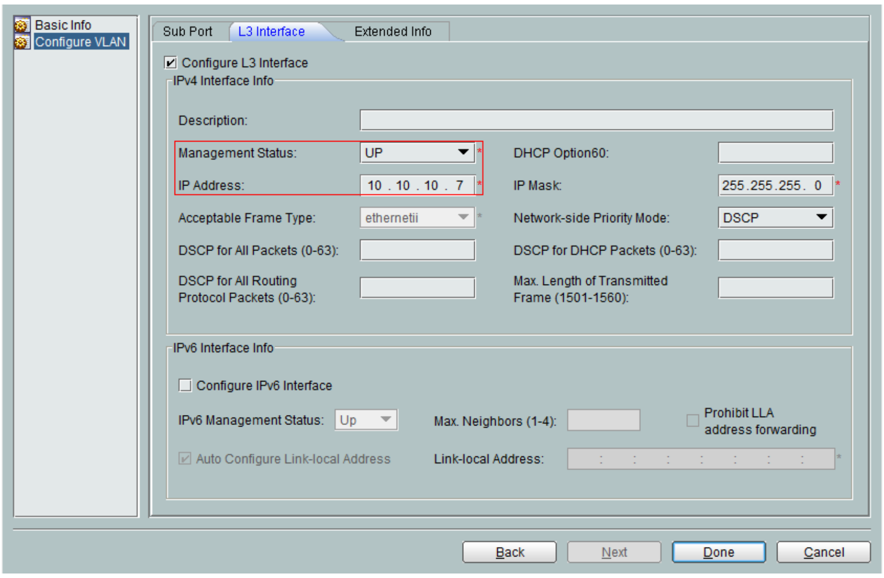
IPv4 Interface Info

Description:
Management Status: UP
IP Address: 10 . 10 . 10 . 6
Acceptable Frame Type: ethernetii
DSCP for All Packets (0-63):
DSCP for All Routing Protocol Packets (0-63):
DHCP Option60:
IP Mask: 255 .255 .255 . 0
Network-side Priority Mode: DSCP
DSCP for DHCP Packets (0-63):
Max. Length of Transmitted Frame (1501-1560):

IPv6 Interface Info

☐ Configure IPv6 Interface
IPv6 Management Status: Up
Max. Neighbors (1-4):
☐ Prohibit LLA address forwarding
☑ Auto Configure Link-local Address
Link-local Address:

Configuring parameters for OLT_2



☑ Configure L3 Interface

Management Status: UP

IP Address: 10 . 10 . 10 . 7

IP Mask: 255 .255 .255 . 0

Acceptable Frame Type: ethernetii

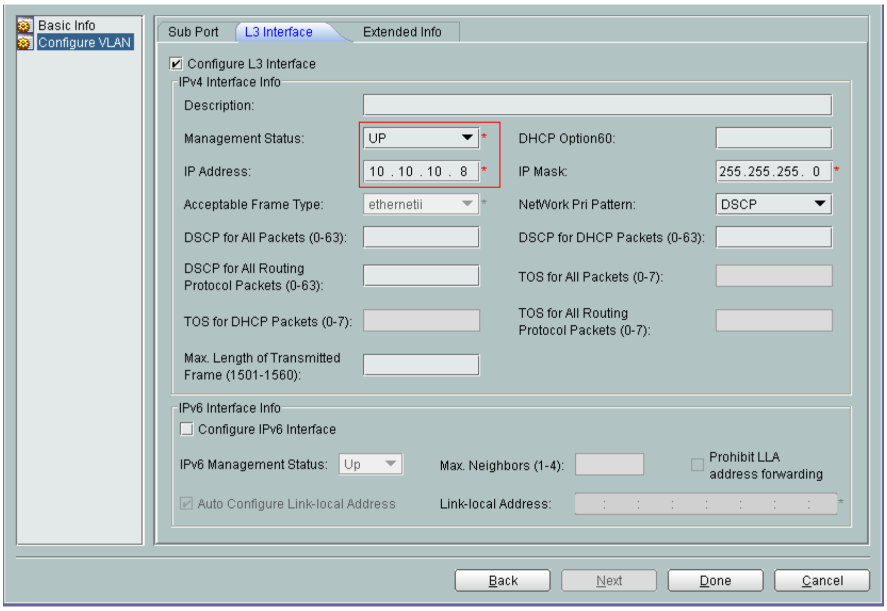
Network-side Priority Mode: DSCP

☐ Configure IPv6 Interface

IPv6 Management Status: Up

☑ Auto Configure Link-local Address

Configuring parameters for OLT_3


Basic Info
Configure VLAN
Sub Port
L3 Interface
Extended Info
IPv4 Interface Info
Description:
DHCP Option60:
DSCP for All Packets (0-63):
DSCP for DHCP Packets (0-63):
DSCP for All Routing Protocol Packets (0-63):
TOS for All Packets (0-7):
TOS for DHCP Packets (0-7):
TOS for All Routing Protocol Packets (0-7):
Max. Length of Transmitted Frame (1501-1560):
IPv6 Interface Info
Max. Neighbors (1-4):
Prohibit LLA address forwarding
Link-local Address:
Back
Next
Done
Cancel

☑ Configure L3 Interface

Management Status: UP

IP Address: 10 . 10 . 10 . 8

IP Mask: 255 .255 .255 . 0

Acceptable Frame Type: ethernetii

NetWork Pri Pattern: DSCP

☐ Configure IPv6 Interface

IPv6 Management Status: Up

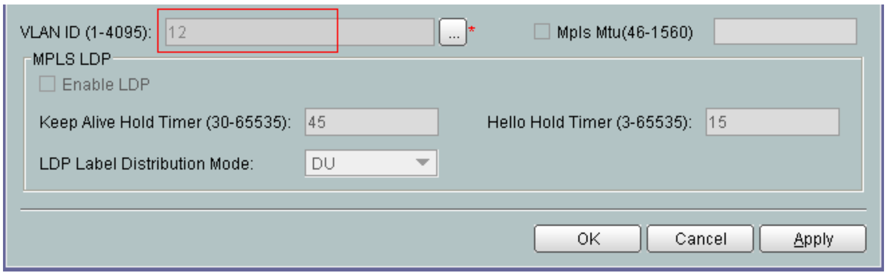
☑ Auto Configure Link-local Address

9. Click **Finish**.

Step 6 Add an MPLS interface.

The MPLS interface is a Layer 3 interface bound to the MPLS VLAN. The local peer can communicate with the remote peer using LSP after an MPLS interface is added and MPLS LDP is enabled. Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **MPLS Interface** tab.
4. Right-click in a blank area and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.


VLAN ID (1-4095): 12 *
☐ Mpls Mtu(46-1560):
MPLS LDP
☐ Enable LDP
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 15
LDP Label Distribution Mode: DU

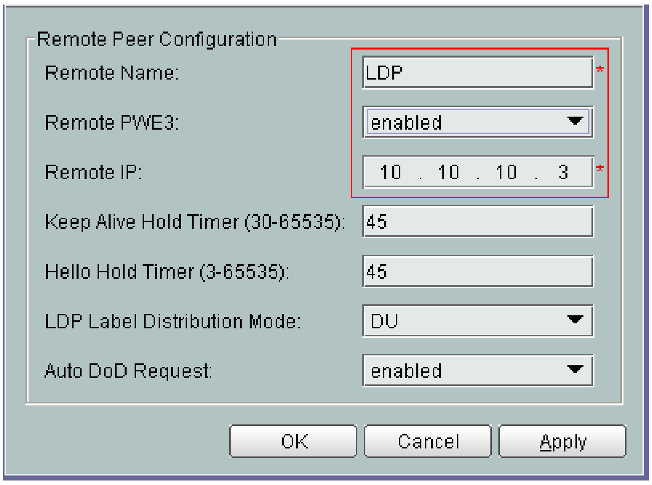
6. Click **OK**.

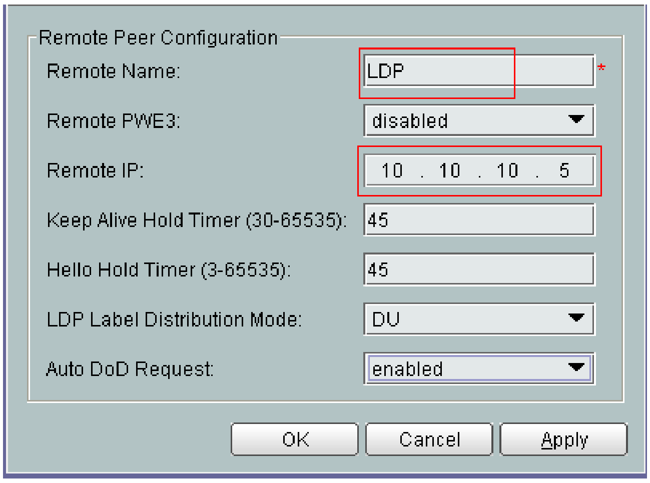
Step 7 Add a remote peer.

The remote peer is a remote label switching router (LSR) which establishes a session with the local LSR. The MPLS discovers the remote peer through LDP extension mechanism. The local peer periodically sends messages in UDP packets to the specified remote peer. In **Figure 13-5**, for each MA5600T, the other two are remote peers for it. Configure OLT_1, OLT_2 and OLT_3 as follows:

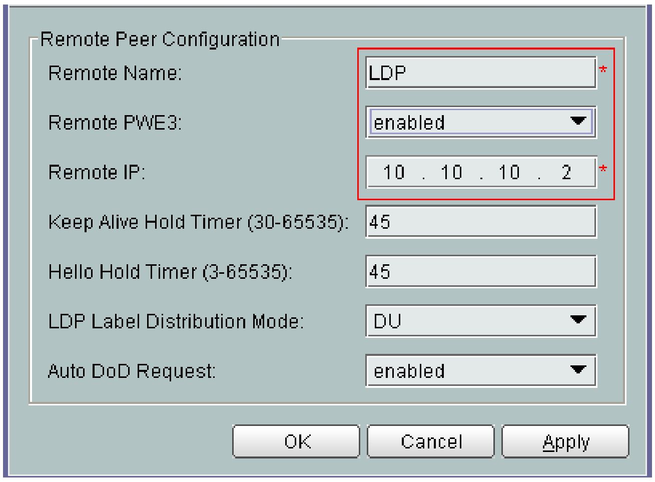
1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **MPLS Management** from the navigation tree.
3. Click the **LDP Remote Peer** tab.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.

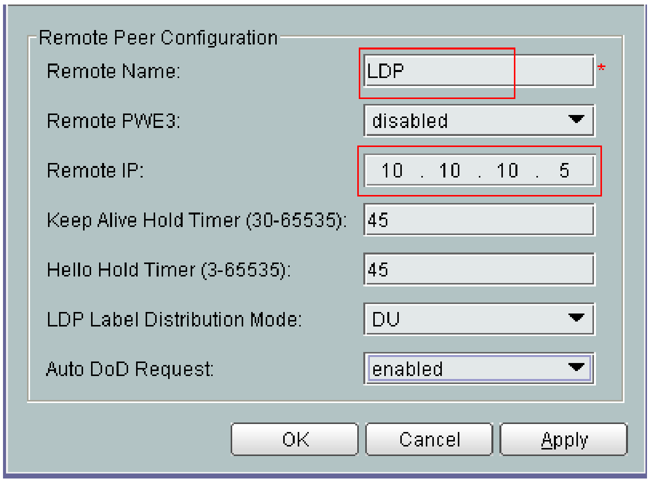
Configuring parameters for OLT_1


Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: enabled
Remote IP: 10 . 10 . 10 . 3 *
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled

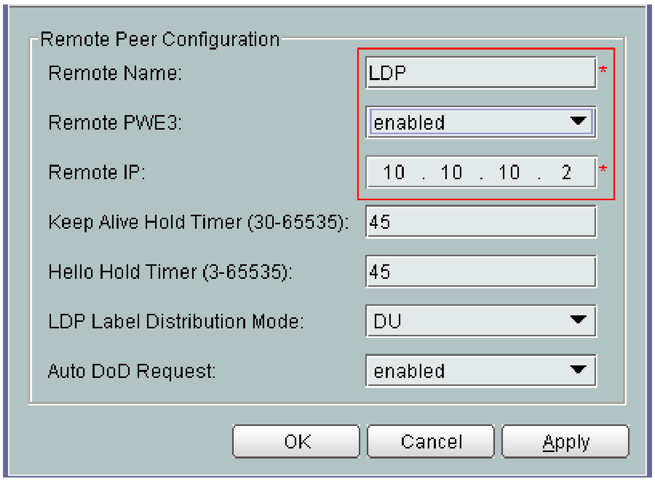

Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: disabled
Remote IP: 10 . 10 . 10 . 5
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled

Configuring parameters for OLT_2


Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: enabled
Remote IP: 10 . 10 . 10 . 2 *
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled


Remote Peer Configuration
Remote Name: LDP *
Remote PWE3: disabled
Remote IP: 10 . 10 . 10 . 5
Keep Alive Hold Timer (30-65535): 45
Hello Hold Timer (3-65535): 45
LDP Label Distribution Mode: DU
Auto DoD Request: enabled

Configuring parameters for OLT_3



Remote Peer Configuration

Remote Name: LDP *

Remote PWE3: enabled

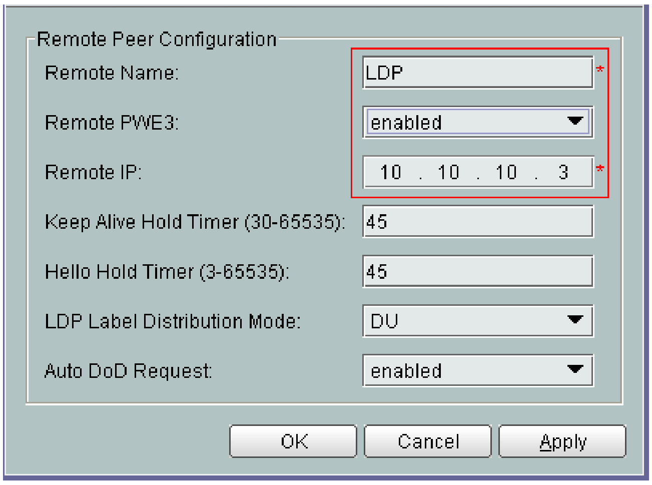
Remote IP: 10 . 10 . 10 . 2 *

Keep Alive Hold Timer (30-65535): 45

Hello Hold Timer (3-65535): 45

LDP Label Distribution Mode: DU

Auto DoD Request: enabled



Remote Peer Configuration

Remote Name: LDP *

Remote PWE3: enabled

Remote IP: 10 . 10 . 10 . 3 *

Keep Alive Hold Timer (30-65535): 45

Hello Hold Timer (3-65535): 45

LDP Label Distribution Mode: DU

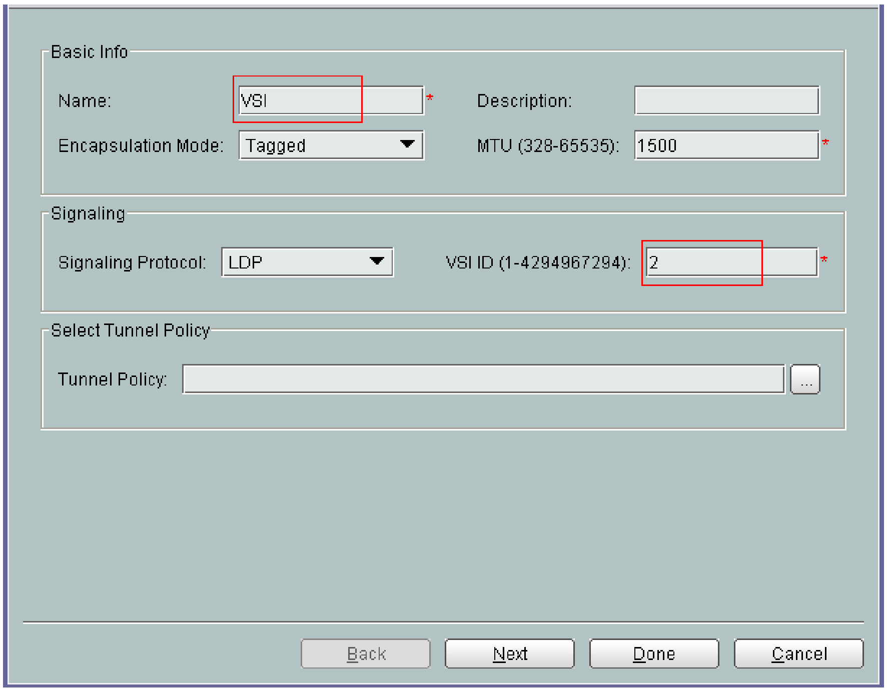
Auto DoD Request: enabled

6. Click **OK**.

Step 8 Add a VSI.

Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPLS Management** from the navigation tree.
3. On the **VSI** tab page, set the filter criteria or click ⌄ to display the VSIs.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



Basic Info
Name: VSI *
Description:
Encapsulation Mode: Tagged
MTU (328-65535): 1500 *

Signaling
Signaling Protocol: LDP
VSI ID (1-4294967294): 2 *

Select Tunnel Policy
Tunnel Policy:

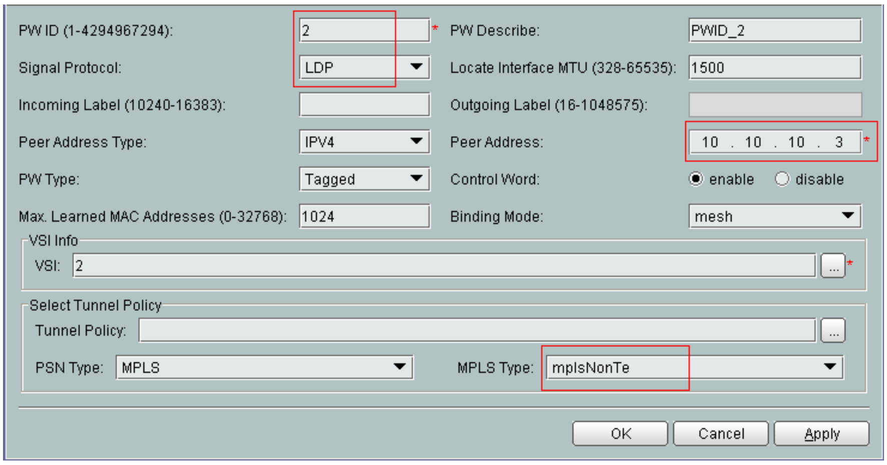
6. Click **OK**.

Step 9 Bind the VSI to a PW.

Packet forwarding is limited to a scope after the VSI is bound to a PW. Therefore, packets are transmitted only on the PW to which the VSI is bound. Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPLS Management** from the navigation tree.
3. Click the **PW** tab, set the filter criteria or click ⌄ to display the PWs.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.

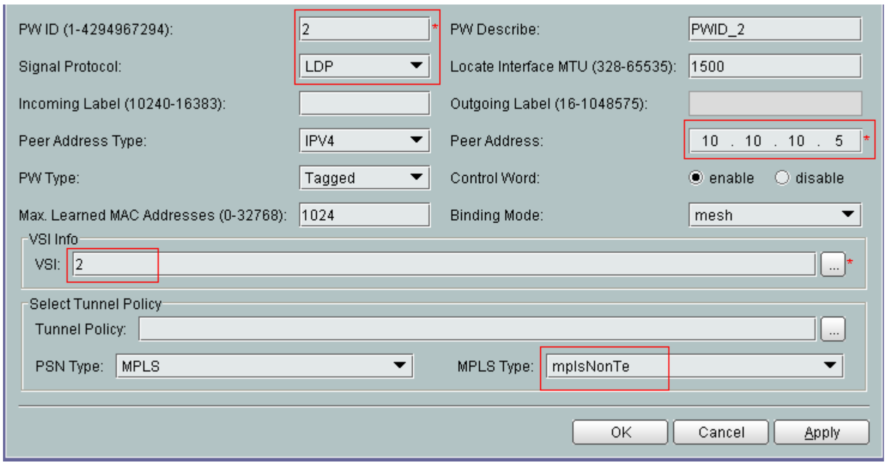
Configuring parameters for OLT_1



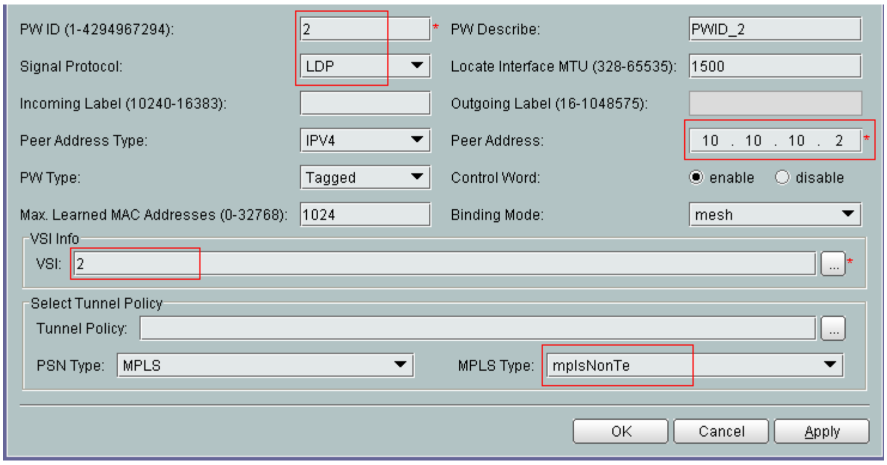
PW ID (1-4294967294): 2 *
PW Describe: PWID_2
Signal Protocol: LDP
Locate Interface MTU (328-65535): 1500
Incoming Label (10240-16383):
Outgoing Label (16-1048575):
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 3 *
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh

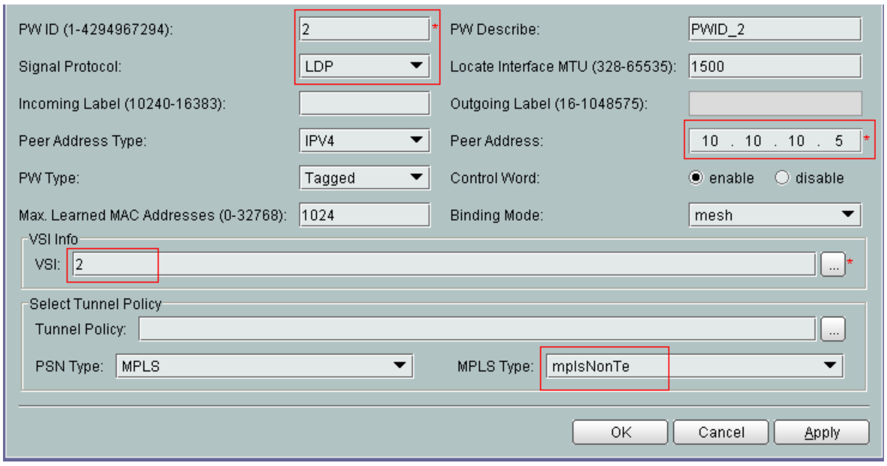
VSI Info
VSI: 2 *

Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe

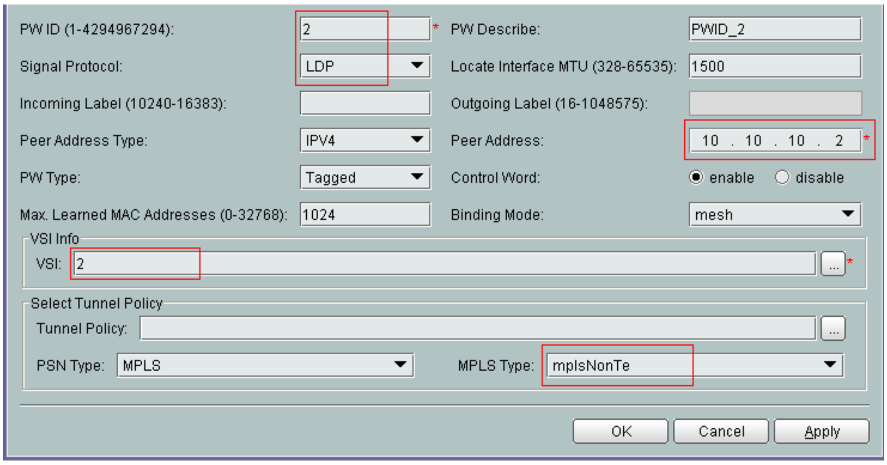

PW ID (1-4294967294): 2
PW Describe: PWID_2
Signal Protocol: LDP
Locate Interface MTU (328-65535): 1500
Incoming Label (10240-16383):
Outgoing Label (16-1048575):
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 5
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh
VSI Info
VSI: 2
Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe

Configuring parameters for OLT_2

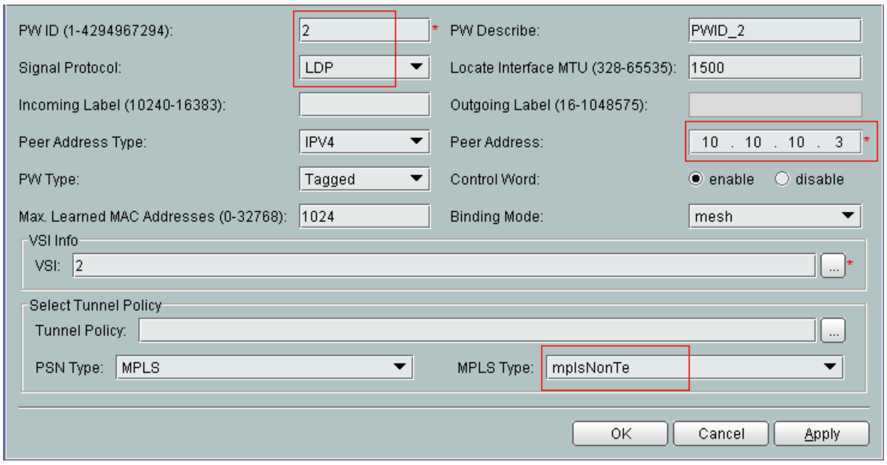

PW ID (1-4294967294): 2
PW Describe: PWID_2
Signal Protocol: LDP
Locate Interface MTU (328-65535): 1500
Incoming Label (10240-16383):
Outgoing Label (16-1048575):
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 2
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh
VSI Info
VSI: 2
Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe


PW ID (1-4294967294): 2
PW Describe: PWID_2
Signal Protocol: LDP
Locate Interface MTU (328-65535): 1500
Incoming Label (10240-16383):
Outgoing Label (16-1048575):
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 5
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh
VSI Info
VSI: 2
Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe

Configuring parameters for OLT_3



PW ID (1-4294967294): 2 *
PW Describe: PWID_2
Signal Protocol: LDP
Locate Interface MTU (328-65535): 1500
Incoming Label (10240-16383):
Outgoing Label (16-1048575):
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 2 *
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh
VSI Info
VSI: 2 *
Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe



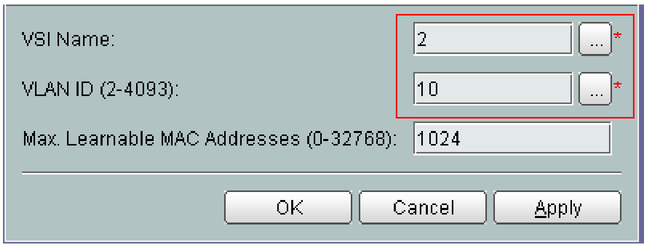
PW ID (1-4294967294): 2 *
PW Describe: PWID_2
Signal Protocol: LDP
Locate Interface MTU (328-65535): 1500
Incoming Label (10240-16383):
Outgoing Label (16-1048575):
Peer Address Type: IPV4
Peer Address: 10 . 10 . 10 . 3 *
PW Type: Tagged
Control Word: ● enable ○ disable
Max. Learned MAC Addresses (0-32768): 1024
Binding Mode: mesh
VSI Info
VSI: 2 *
Select Tunnel Policy
Tunnel Policy:
PSN Type: MPLS
MPLS Type: mplsNonTe

6. Click **OK**.

Step 10 Bind the VSI to an AC.

Packet forwarding is limited to a scope after the VSI is bound to an AC. Therefore, AC packets are transmitted on PWs after they are bound to the VSI. Configure OLT_1, OLT_2 and OLT_3 as follows:

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VPN** > **VPLS Management** from the navigation tree.
3. On the **AC** tab page, set the filter criteria or click ⌄ to display the ACs.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters.



VSI Name: 2 *
VLAN ID (2-4093): 10 *
Max. Learnable MAC Addresses (0-32768): 1024

6. Click **OK**.

----End

Result

After the preceding configuration is completed, the Layer 2 networks respectively connected to the three OLTs can communicate with each other if the Layer 2 network configurations are correct.

14 Configuring the Voice Service

About This Chapter

The OLT supports user access through copper cables to provide the voice service.

14.1 Configuring the VoIP PSTN Service
This topic describes the principles and features of the VoIP PSTN technology. In addition, this topic describes how to implement the voice service on the MA5600T and how to configure and manage the PSTN ports.

14.2 Configuring the R2 Signaling Service on the AG
This topic describes how to configure the R2 signaling service on the MA5600T to achieve PBX-NGN connection and PSTN-to-NGN migration.

14.3 Configuring the VoIP ISDN Service
This topic describes how to configure the VoIP ISDN service and how the voice service is implemented on the MA5600T.

14.1 Configuring the VoIP PSTN Service

This topic describes the principles and features of the VoIP PSTN technology. In addition, this topic describes how to implement the voice service on the MA5600T and how to configure and manage the PSTN ports.

Context

In the VoIP PSTN service, also called the VoIP service, traditional analog voice signals are specially processed, such as compressed and packetized, and then are transmitted over the IP packet switching network. This reduces the cost of the voice service.

14.1.1 Configuring the VoIP Media Gateway

In the NGN, the media gateway (MG) and the media gateway controller (MGC) are separated completely. That is, the functions of the user plane are separately from the functions of the control plane. The MA5600T functions as the MG and completes the message interconnection of the user plane, which performs the communication between the MA5600T and the upper layer MGC through the MG interface. The MGC completes the message interconnection of the control plane. An MG converts the media format of a type of networks into the media format of another type of networks. Hence, the messages of the user plane can interconnect with each other. In addition, the MG is also called the access gateway (AG).

14.1.1.1 Configuring the UAS Profile

The user agent server (UAS) profile is used to set the parameters of the SIP interface. When configuring the SIP interface, bind this profile to the SIP interface to specify the interface that communicates with the call control. After you configure the UAS profile and bind the profile to the SIP interface, the settings of the SIP interface are complete.

Procedure

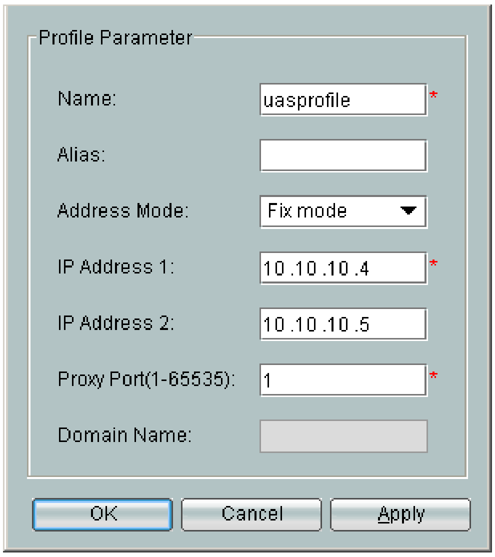
Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **Voice Profile** > **UAS Profile** from the navigation tree.

Step 3 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the parameters as follows:

Set the **Name**, **Alias**, **IP Address 1**, **IP Address 2**, **Proxy Port**, **Domain Name**, and **Address Mode** parameters.



Name: uasprofile *
Alias:
Address Mode: Fix mode
IP Address 1: 10 .10 .10 .4 *
IP Address 2: 10 .10 .10 .5
Proxy Port(1-65535): 1 *
Domain Name:

Step 5 Click **OK**.

----End

14.1.1.2 Configuring an MGC Profile

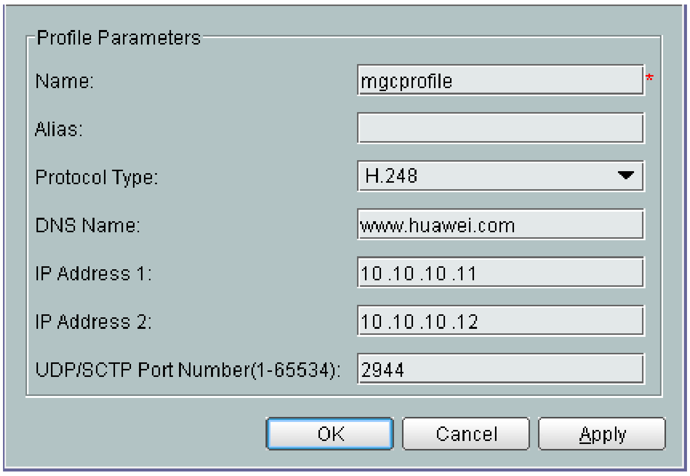
The media gateway controller (MGC) integrates multiple logical function entities, provides the call control and connection of integrated services, and implements integrated services. The MGC profile defines the parameters required for an MGC interface. The U2000 manages the parameters through the profile.

Procedure

Step 1 In the dialog box that is displayed, choose **Voice Profile** > **MGC Profile** from the navigation tree.

Step 2 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 3 In the dialog box that is displayed, set the parameters.



Name: mgcprofile *
Alias:
Protocol Type: H.248
DNS Name: www.huawei.com
IP Address 1: 10 .10 .10 .11
IP Address 2: 10 .10 .10 .12
UDP/SCTP Port Number(1-65534): 2944

Step 4 Click **OK**.

----End

14.1.1.3 Configuring a VLAN L3 Interface

The functions of a L3 interface that is based on the VLAN are similar to a L3 switch. Through L3 forwarding, the L3 interface forwards data between different VLANs.

Context

You can configure the L3 interfaces of common VLANs and stacking VLANs.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **VLAN** from the navigation tree.

Step 3 On the **VLAN** tab page, set the filter criteria or click ︾ to display the VLANs.

Step 4 Select a VLAN record, right-click, and then choose **Configure**.

Step 5 In the dialog box that is displayed, click the **L3 Interface** tab, select **Configure L3 Interface**, and then set the IP address and the subnet mask of the L3 interface.

Step 6 Click **OK**.

----End

14.1.1.4 Adding an MG (H.248/MGCP)

Before you provision services for network elements, you can add an MG according to the global data plan to provide the MG interface for communication with the upper layer MGC.

Prerequisites

The signaling IP address and the media IP address must exist in the corresponding IP address pool.

Context

- An MG ID must be unique on a device.
- Ensure that the MG parameter values are the same as the corresponding parameter values on the MGC.
- You can configure up to eight MGs on a device.
- After the MG is added, you must perform the cold starting or recovering operation so that the MG can work in the normal state.
- After the MG is added successfully, the system adds three MGCs concurrently. This MG can provide services to the user when the MG communicates with only one MGC.
- The H.248 protocol separates the signaling stream and the media stream and uses different QoS policies for the two types of streams.

NOTE

The procedure for adding an MG supporting the MGCP protocol is the same as the procedure for adding an MG supporting the H.248 protocol. The preset parameters, however, are different. The following procedure uses adding the MG supporting the H.248 protocol as an example.

Procedure

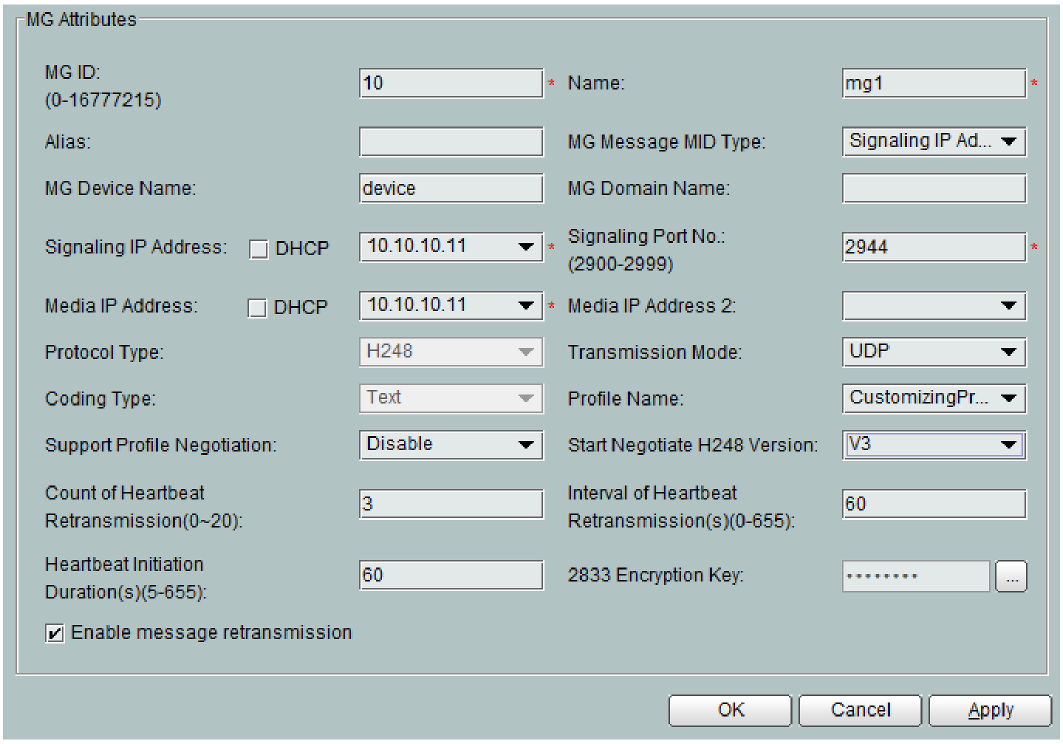
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 In the information list, right-click and choose **Add** > **H.248** from shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters as follows.



MG Attributes

MG ID: (0-16777215)	10 *	Name:	mg1 *
Alias:		MG Message MID Type:	Signaling IP Ad...
MG Device Name:	device	MG Domain Name:	
Signaling IP Address: ☐ DHCP	10.10.10.11 *	Signaling Port No.: (2900-2999)	2944 *
Media IP Address: ☐ DHCP	10.10.10.11 *	Media IP Address 2:	
Protocol Type:	H248	Transmission Mode:	UDP
Coding Type:	Text	Profile Name:	CustomizingPr...
Support Profile Negotiation:	Disable	Start Negotiate H248 Version:	V3
Count of Heartbeat Retransmission(0~20):	3	Interval of Heartbeat Retransmission(s)(0-655):	60
Heartbeat Initiation Duration(s)(5-655):	60	2833 Encryption Key:	••••••••

☑ Enable message retransmission

Step 6 Click **OK**.

----End

14.1.1.5 Adding an MG (SIP)

Before you provision services for network elements, you can add an MG according to the global data plan to provide the MG interface for communication with the upper layer device.

Prerequisites

The signaling IP address and the media IP address must exist in the corresponding IP address pool.

Context

- An MG ID must be unique on a device.
- You can configure up to eight MGs on a device.

- After the MG is added, you must perform the resetting operation so that the MG can work in the normal state.

Procedure

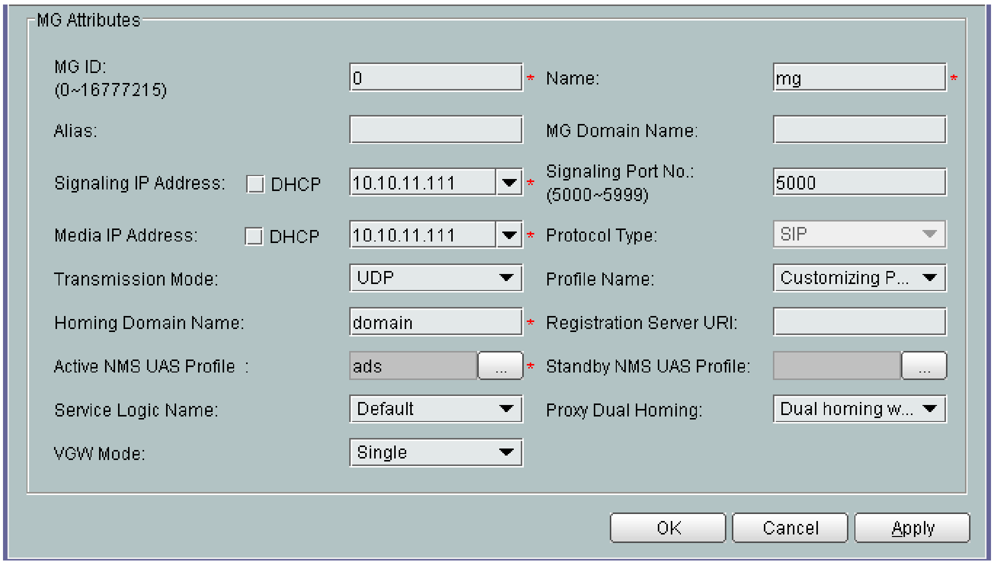
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 In the information list, right-click and choose **Add** > **SIP** from shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters as follows.



MG Attributes

MG ID: (0~16777215) 0 *
Name: mg *
Alias:
MG Domain Name:
Signaling IP Address: ☐ DHCP 10.10.11.111 *
Signaling Port No.: (5000~5999) 5000
Media IP Address: ☐ DHCP 10.10.11.111 *
Protocol Type: SIP
Transmission Mode: UDP
Profile Name: Customizing P...
Homing Domain Name: domain *
Registration Server URI:
Active NMS UAS Profile : ads *
Standby NMS UAS Profile:
Service Logic Name: Default
Proxy Dual Homing: Dual homing w...
VGW Mode: Single

Step 6 Click **OK**.

----End

14.1.1.6 Configuring an MGC (H.248/MGCP)

The MGC controls the status of calls that are inside the MG and are related to the control of media channel connections. An MGC integrates multiple logical function entities, provides the call control and connection of integrated services, and implements integrated services and interconnection and conversion of various signaling protocols.

Prerequisites

The corresponding MGC profile must exist. For details about how to add an MGC profile, see **14.1.1.2 Configuring an MGC Profile**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record, click the **MGC Information** tab.

Step 5 Right-click a record and choose **Modify** from the shortcut menu.

Step 6 In the dialog box that is displayed, select the MGC profile whose **Configured Name** is **mgcprofile**.

Step 7 Click **OK**.

----End

14.1.1.7 Starting Up an MG Interface

Cold starting the MG interface so that the MG interface can negotiate with the MGC through the specified MGC protocol. In this case, the MG interface can register with the MGC so that the configured data can take effect.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select the MG record to be configured, right-click, and then choose **Reset** > **Cold Start** (H.248) or **Reset** (MGCP or SIP).

Step 5 In the dialog box that is displayed, click **Yes**.

----End

14.1.1.8 Configuring Ringing Mapping

When the MGC interacts with the MA5600T, they negotiate the ringing mode. The purpose of ringing mapping is to match the peer parameters that the MGC applies to the MA5600T to a specified ringing mode. After the ringing mapping is added successfully, the MG initiates the ringing based on the ringing mode corresponding to the peer-end parameter sent by the MGC.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Context

- You can set the break duration of the ringing mode according to the local standard and up to 16 ringing modes can be set.
- In an MG, a peer parameter matches only one ringing mapping record.

- When the ringing mapping is not configured on the MG, the common ringing (NULL) is adopted for all users.
- Only 50 ringing mapping records can be configured on a device.

Procedure

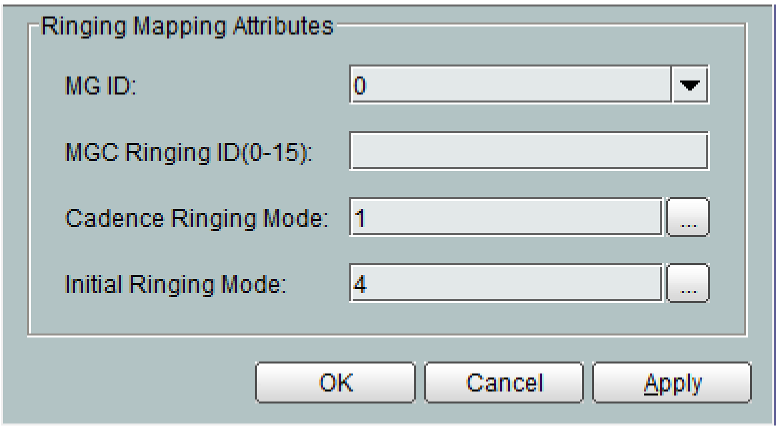
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Ringing Mapping** tab page, set the filter criteria to display the required ringing mapping records.

Step 4 In the information list, right-click and choose **Add** > **H.248** from shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Ringing Mapping Attributes

MG ID: 0

MGC Ringing ID(0-15):

Cadence Ringing Mode: 1

Initial Ringing Mode: 4

Step 6 Click **OK**.

----End

14.1.1.9 Setting the MGC Overload Parameters

An MGC needs to handle the calls reported by multiple AGs that the MGC controls. If the call traffic reported by the AGs increases, the MGC may overload. The MA5600T controls calls in the case of MGC overload and guarantees the priorities of the calls of high-priority users and emergency users. This enhances the reliability and availability of the system.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Context

NOTE

- You cannot set the MGC overload parameters if the system uses the MGCP protocol.
- The default value of **Highest Priority Channel Occupancy** is 50%.
- The relationship between the values of three types of channel occupancy is as follows: **Highest Priority Channel Occupancy** ≥ **Second Highest Priority Channel Occupancy** ≥ **Normal Priority Channel Occupancy**

Procedure

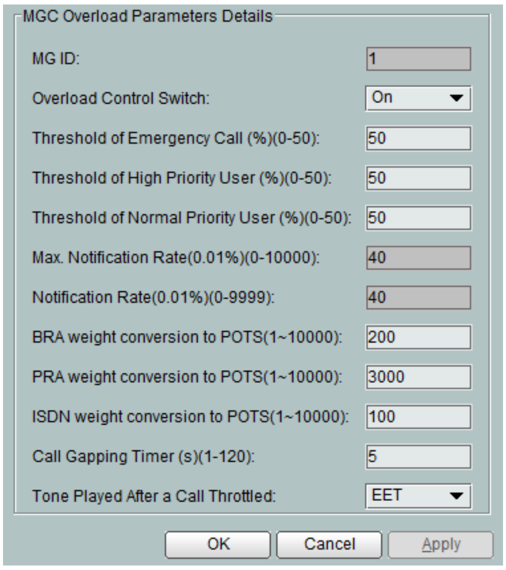
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MGC list, right-click, and then choose **Configure MGC Overload Parameters**.

Step 5 In the dialog box that is displayed, set the parameters.



MGC Overload Parameters Details

MG ID: 1
Overload Control Switch: On
Threshold of Emergency Call (%)(0-50): 50
Threshold of High Priority User (%)(0-50): 50
Threshold of Normal Priority User (%)(0-50): 50
Max. Notification Rate(0.01%)(0-10000): 40
Notification Rate(0.01%)(0-9999): 40
BRA weight conversion to POTS(1~10000): 200
PRA weight conversion to POTS(1~10000): 3000
ISDN weight conversion to POTS(1~10000): 100
Call Gapping Timer (s)(1-120): 5
Tone Played After a Call Throttled: EET

Step 6 Click **OK**.

----End

14.1.1.10 Setting Digitmap Parameters

A digitmap is a set of digit collection descriptors and it refers to the dialing policies on the MG. The digitmap is used to detect and report dialing events received by terminals.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Context

NOTE

If the MG communicates with the MGC in the normal state, the MGC sends the digitmap. If the MG loses communication with the MGC and the standalone function is enabled on the MG, the MG sends the digitmap.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

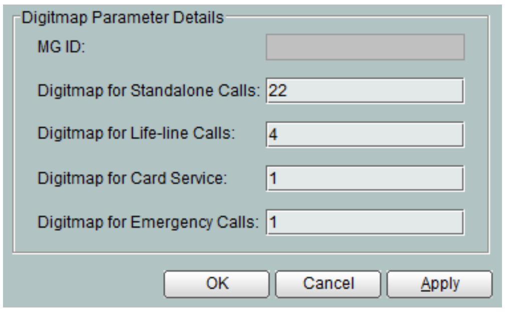
Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MG list, right-click, and then choose **Configure Digitmap Parameters**.

Step 5 In the dialog box that is displayed, set the digitmap parameters.

Setting digitmap parameters (H.248)



Digitmap Parameter Details

MG ID:

Digitmap for Standalone Calls: 22

Digitmap for Life-line Calls: 4

Digitmap for Card Service: 1

Digitmap for Emergency Calls: 1

Step 6 Click **OK**.

----End

14.1.1.11 Setting the TID Prefix Parameters

If the TID profile that is bound to the user in an MG interface does not support the layered configuration, you must set the TID field when configuring a user. If the TID profile that is bound to the user in an MG interface supports the layered configuration, you need not set the TID field because the TID field value is automatically generated according to rules. The TID prefix is the prefix of the automatic generation rule.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Context

NOTE

The terminal prefix cannot be empty.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

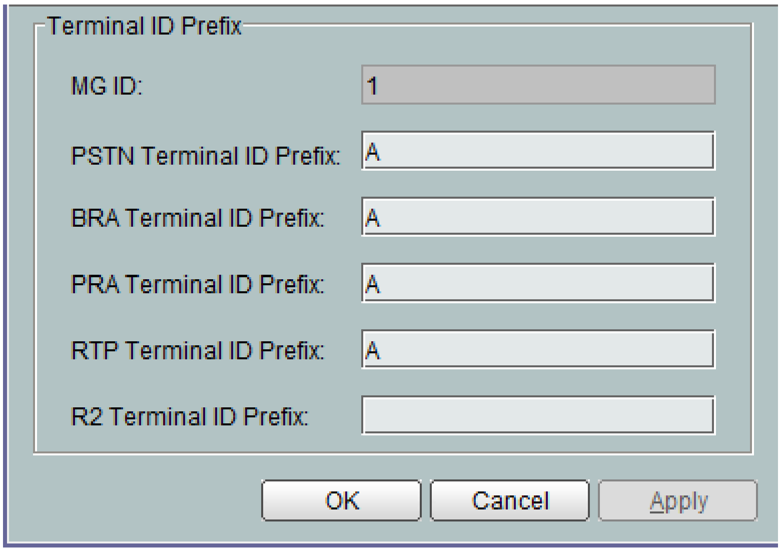
Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MG list, right-click, and then choose **Configure Terminal ID Prefix Parameters**.

Step 5 In the dialog box that is displayed, set the parameters of a TID prefix.

Setting the parameters of a TID prefix (H.248)



Terminal ID Prefix

MG ID: 1

PSTN Terminal ID Prefix: A

BRA Terminal ID Prefix: A

PRA Terminal ID Prefix: A

RTP Terminal ID Prefix: A

R2 Terminal ID Prefix:

Step 6 Click **OK**.

----End

14.1.1.12 Configuring the TID Profile Reference

Terminal ID stands for the target identifier and is also called TID. The TID is a prefix that a terminal carries when the terminal registers with the MG. The system automatically generates the TID string according to the TID profile. The MGC can identify the line that a user occupies by using the TID string.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

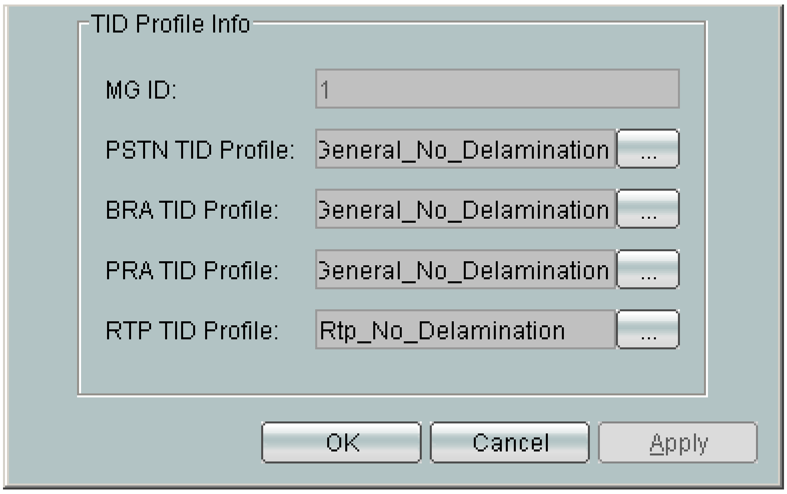
Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MG list, right-click, and then choose **Configure TID Profile References**.

Step 5 In the dialog box that is displayed, configure the reference of the TID profiles for terminals.

Configuring the reference of the TID profile (H.248)



MG ID: 1
PSTN TID Profile: General_No_Delamination
BRA TID Profile: General_No_Delamination
PRA TID Profile: General_No_Delamination
RTP TID Profile: Rtp_No_Delamination

Step 6 Click **OK**.

----End

14.1.1.13 Setting DMM Parameters

A country or region has particular requirements on the duration of various digitmap timers (DMMs). To meet different requirements, you can modify the DMM parameters to set the duration of a DMM.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Context

NOTE

- The start time of timers varies with the match policy and mode of a specific digitmap.
- When a user dials a telephone number, the MG starts the long timer if the MG confirms that the telephone number requires at least another digit to match any dialing policy in the digitmap.
- When a user dials a telephone number, the MG starts the short timer if the telephone number has matched a certain dialing policy in the digitmap but the MG confirms that more digits are required to match the other dialing policies in the digitmap.
- The start timer is used before any dialed number, that is, the duration from when the user picks up the phone to when the MG receives the first digit. If the start timer is set to 0, it indicates that the MG waits for dialing endlessly.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

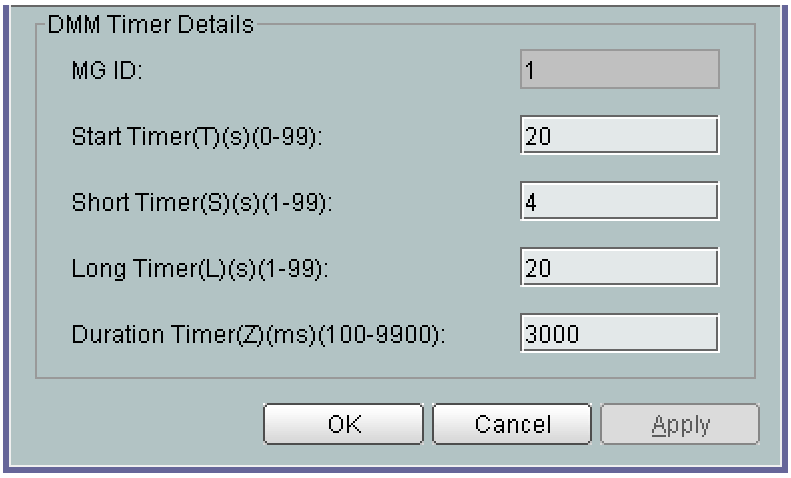
Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MG list, right-click, and then choose **Configure DMM Timer**.

Step 5 In the dialog box that is displayed, set the related DMM parameters.

Set the DMM parameters (H.248) such as **Start Timer**, **Short Timer**, and **Long Timer**, and **Duration Timer**.



DMM Timer Details

MG ID: 1

Start Timer(T)(s)(0-99): 20

Short Timer(S)(s)(1-99): 4

Long Timer(L)(s)(1-99): 20

Duration Timer(Z)(ms)(100-9900): 3000

Step 6 Click **OK**.

----End

14.1.1.14 Setting Authentication Parameters

The purpose of authentication is to verify the validity of users and networks. You can use the same authentication algorithm on the MG and MGC sides separately. Then, compare the calculation results on the MG and MGC sides separately. If the calculation results are the same, it indicates that the authentication is successful. If the calculation results are different, it indicates that the authentication fails.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Context

NOTE

- The device authentication configuration is optional but it must be the same as the device authentication configured on the MGC.
- If you use Huawei products such as the SoftX3000 as the MGC, the authentication gateway ID must be a character string that is more than eight digits.
- If the system uses the H.248 protocol, you can set the authentication parameters of the H.248 protocol. When the system uses the MGCP protocol, you can set the authentication parameters of the MGCP protocol.
- You need to enable the MG interface in cold mode for it to take effect after the authentication configuration. You need to reset the MG interface for it to take effect after the authentication configuration of the MGCP protocol.

Procedure

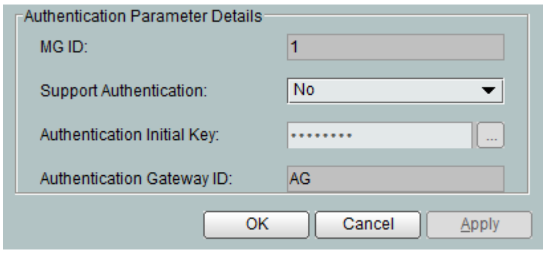
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MG list, right-click, and then choose **Configure Authentication Parameters**.

Step 5 In the dialog box that is displayed, set the related authentication parameters.



Authentication Parameter Details
MG ID: 1
Support Authentication: No
Authentication Initial Key: ••••••••
Authentication Gateway ID: AG

Step 6 Click **OK**.

----End

14.1.1.15 Setting Standalone Parameters

When the MG loses communication with the MGC, the standalone function ensures that internal calls are normal under the same MG.

Prerequisites

The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.

Context

NOTE

- You can set the standalone parameters only on the devices that support the H.248 protocol.
- The standalone function enables the users on the same MG interface to place calls to each other. In other words, the users on different MG interfaces cannot place calls to each other.
- To maintain the same user phone number in the standalone state as the one used in normal condition, configure the phone number on the MG to be the same as that on the MGC.

Procedure

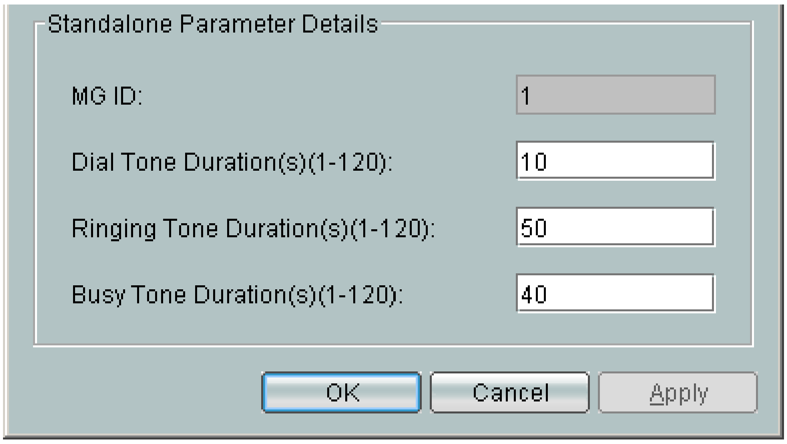
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MG list, right-click, and then choose **Configure Standalone Parameters**.

Step 5 In the dialog box that is displayed, set the parameters such as **Dial Tone Duration(s)**, **Ringing Tone Duration(s)**, and **Busy Tone Duration(s)**.



Standalone Parameter Details

MG ID: 1

Dial Tone Duration(s)(1-120): 10

Ringing Tone Duration(s)(1-120): 50

Busy Tone Duration(s)(1-120): 40

Step 6 Click **OK**.

----End

14.1.1.16 Configuring Dual Homing

Configuring the dual homing means registering one MA5600T with two MGCs. When one MGC is faulty and cannot support the communication, the MA5600T automatically switches to the other MGC.

Prerequisites

- The corresponding MG must exist. To add an MG, see **14.1.1.4 Adding an MG (H.248/MGCP)** or **14.1.1.5 Adding an MG (SIP)**.
- You can configure only a deactivated MG.
- The system uses the MGCP or H.248 protocol.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

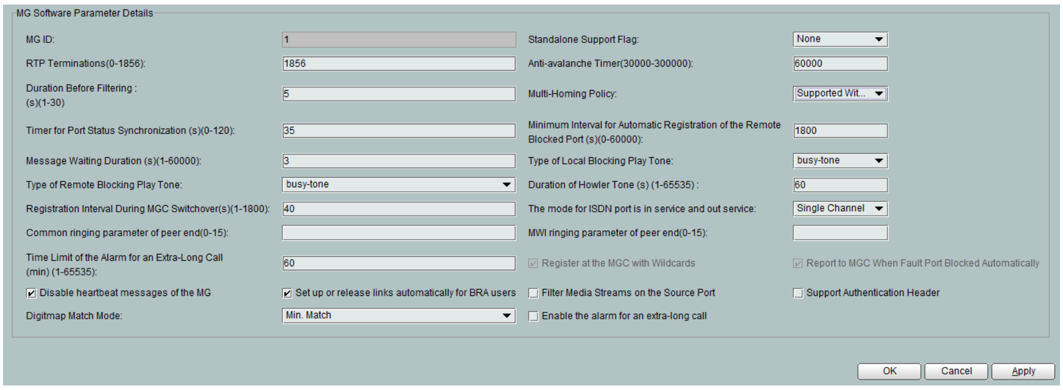
Step 2 Choose **Voice Gateway** > **Media Gateway** from the navigation tree.

Step 3 On the **Media Gateway** tab page, set the filter criteria to display the required MGs.

Step 4 Select a record from the MG list, right-click, and then choose **Configure MG Software Parameters**.

- If the MGCP protocol is used, in the dialog box that is displayed, set parameters to specify whether the device supports the dual-homing policy. If the dual-homing policy is supported, two options are available, that is, the active MGC automatically switches back and the active MGC does not automatically switch back.
- If the H.248 protocol is used, in the dialog box that is displayed, set **Multi-Homing Policy** to **Supported without switching back** or **Supported with switching back**.

This step uses the H.248 protocol as an example.



MG Software Parameter Details

MG ID: 1
RTP Terminations(0-1856): 1856
Duration Before Filtering : (s)(1-30) 5
Timer for Port Status Synchronization (s)(0-120): 35
Message Waiting Duration (s)(1-60000): 3
Type of Remote Blocking Play Tone: busy-tone
Registration Interval During MGC Switchover(s)(1-1800): 40
Common ringing parameter of peer end(0-15):
Time Limit of the Alarm for an Extra-Long Call (min) (1-65535): 60
☑ Disable heartbeat messages of the MG
☑ Set up or release links automatically for BRA users
Digitmap Match Mode: Min. Match
Standalone Support Flag: None
Anti-avalanche Timer(30000-300000): 60000
Multi-Homing Policy: Supported Wit...
Minimum Interval for Automatic Registration of the Remote Blocked Port (s)(0-60000): 1800
Type of Local Blocking Play Tone: busy-tone
Duration of Howler Tone (s) (1-65535) : 60
The mode for ISDN port is in service and out service: Single Channel
MWI ringing parameter of peer end(0-15):
☑ Register at the MGC with Wildcards
☑ Report to MGC When Fault Port Blocked Automatically
☐ Filter Media Streams on the Source Port
☐ Support Authentication Header
☐ Enable the alarm for an extra-long call

Step 5 Click **OK**.

----End

14.1.2 Configuring the VoIP Signaling Gateway

The signaling gateway (SG) is used to convert and transmit the signaling, and it converts the signaling system number 7 (SS7) of the ISDN network into the signaling protocol corresponding to the IP network. In this case, the signaling can be exchanged between the IP network and the ISDN network. The SG communicates with the softswitch through SCTP. If the upstream transmission is performed, the SG transmits the signaling that is converted through SCTP to the softswitch. If the downstream transmission is performed, the SG first receives the signaling of the IP network from the softswitch, converts the signaling into SS7 signaling, and then transmits the SS7 signaling to the ISDN network through the PSTN signaling interface.

14.1.2.1 Adding an SG

The SG is used to convert and transmit the signaling, and it converts the signaling system number 7 (SS7) of the ISDN network into the signaling protocol corresponding to the IP network. This topic describes how to add an SG so that the signaling can be exchanged between the IP network and the ISDN network.

Copyright © Huawei Technologies Co., Ltd.

Procedure

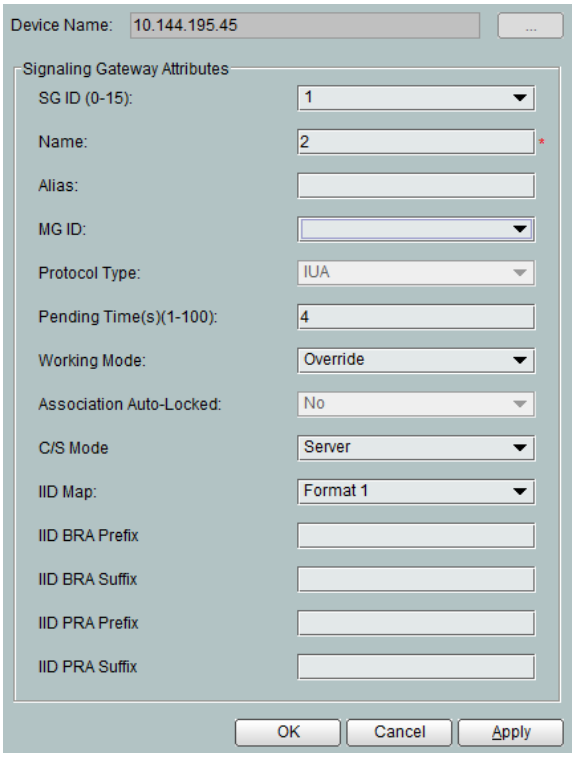
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Signaling Gateway** from the navigation tree.

Step 3 On the **Signaling Gateway** tab page, set the filter criteria to display the required SGs.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Device Name: 10.144.195.45

Signaling Gateway Attributes

SG ID (0-15): 1
Name: 2 *
Alias:
MG ID:
Protocol Type: IUA
Pending Time(s)(1-100): 4
Working Mode: Override
Association Auto-Locked: No
C/S Mode: Server
IID Map: Format 1
IID BRA Prefix
IID BRA Suffix
IID PRA Prefix
IID PRA Suffix

Step 6 Click **OK**.

----End

14.1.3 Configuring the VoIP PSTN Service

This topic describes how to access and configure the VoIP PSTN service.

Prerequisites

- Network devices and lines must be in the normal state.
- The VLAN L3 interface must be configured. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- A proper MGC profile (H.248 or MGCP) or UAS (SIP) profile must be configured. For details, see **14.1.1.2 Configuring an MGC Profile** or **14.1.1.1 Configuring the UAS Profile**.
- The MG interface (H.248 or MGCP) or SIP interface (SIP) must be configured. For details, see **14.1.1.4 Adding an MG (H.248/MGCP)**.

- The

  MA5600T

  must be able to communicate with the MGC or IMS (SIP).

Context

The MA5600T accesses the VoIP PSTN service stream through the voice service card and transmits the service stream upstream to the IP network through the control card, thus implementing the VoIP PSTN service.

14.1.3.1 Configuring a VoIP PSTN Port

This topic describes how to configure the service attributes and the physical attributes of a VoIP PSTN port to provide the required services.

Procedure

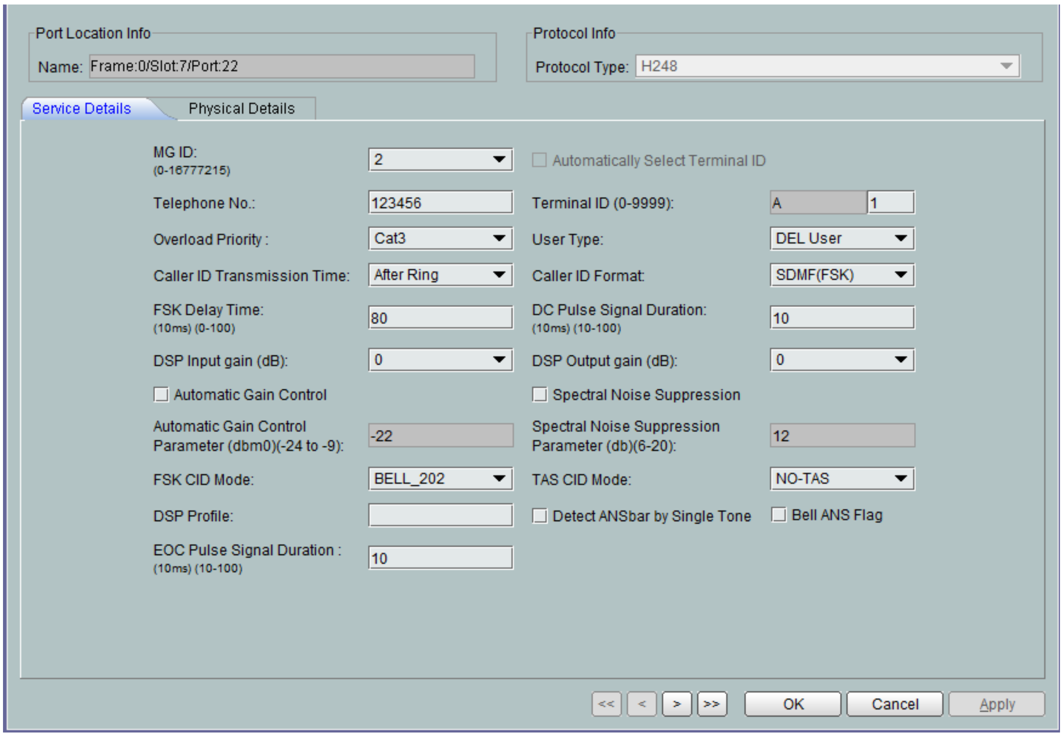
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ASL** > **POTS Port** from the navigation tree.

Step 3 Click the **VoIP PSTN Port** tab, and set the filter criteria to display the required VoIP PSTN ports.

Step 4 Select a record from the VoIP PSTN port list, right-click, and then choose **Configure Attribute**.

Step 5 In the dialog box that is displayed, click the **Service Details** tab. Configure the attributes of the VoIP PSTN port, including **MG ID**, **Terminal ID**, and **Telephone No.**.



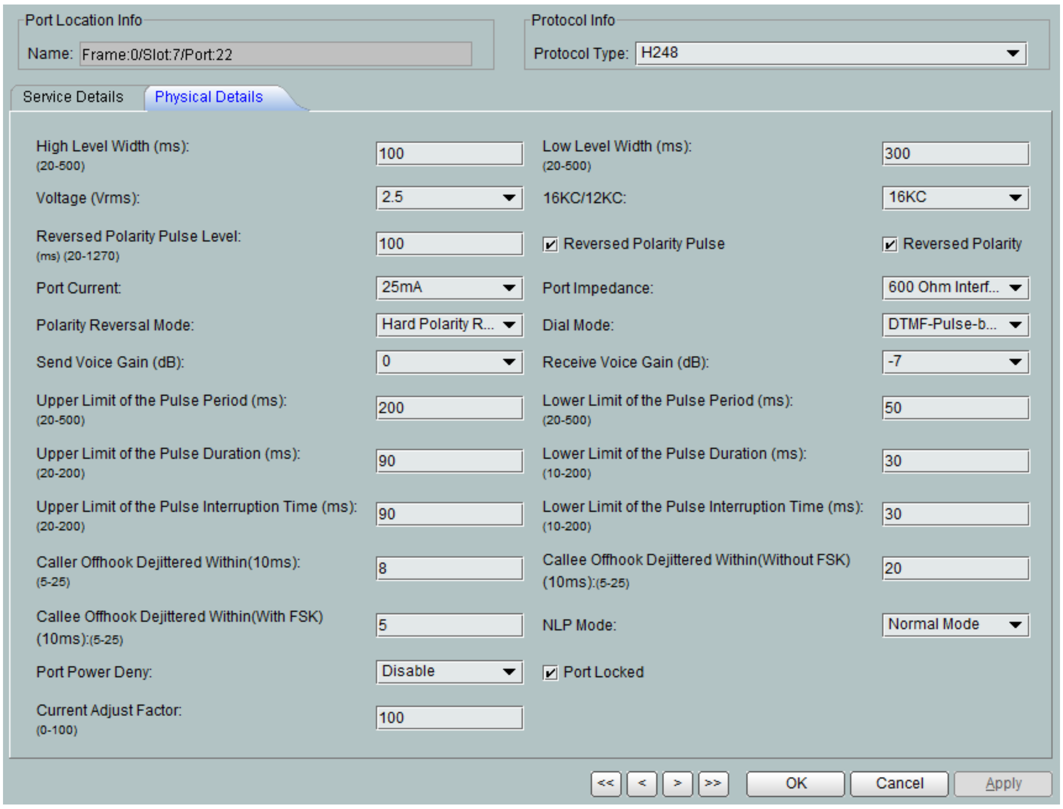
Port Location Info
Name: Frame:0/Slot:7/Port:22

Protocol Info
Protocol Type: H248

Service Details | Physical Details

MG ID: (0-16777215) 2
☐ Automatically Select Terminal ID
Telephone No.: 123456
Terminal ID (0-9999): A 1
Overload Priority : Cat3
User Type: DEL User
Caller ID Transmission Time: After Ring
Caller ID Format: SDMF(FSK)
FSK Delay Time: (10ms) (0-100) 80
DC Pulse Signal Duration: (10ms) (10-100) 10
DSP Input gain (dB): 0
DSP Output gain (dB): 0
☐ Automatic Gain Control
☐ Spectral Noise Suppression
Automatic Gain Control Parameter (dbm0)(-24 to -9): -22
Spectral Noise Suppression Parameter (db)(6-20): 12
FSK CID Mode: BELL_202
TAS CID Mode: NO-TAS
DSP Profile:
☐ Detect ANSbar by Single Tone
☐ Bell ANS Flag
EOC Pulse Signal Duration : (10ms) (10-100) 10

Step 6 Click the **Physical Details** tab. Configure the physical attributes of the VoIP PSTN port, including **High Level Width**, **Low Level Width**, **Reversed Polarity**, and **Dial Mode**.



Port Location Info
Name: Frame:0/Slot:7/Port:22
Protocol Info
Protocol Type: H248

High Level Width (ms): (20-500) 100
Low Level Width (ms): (20-500) 300
Voltage (Vrms): 2.5
16KC/12KC: 16KC
Reversed Polarity Pulse Level: (ms) (20-1270) 100
☑ Reversed Polarity Pulse
☑ Reversed Polarity
Port Current: 25mA
Port Impedance: 600 Ohm Interf...
Polarity Reversal Mode: Hard Polarity R...
Dial Mode: DTMF-Pulse-b...
Send Voice Gain (dB): 0
Receive Voice Gain (dB): -7
Upper Limit of the Pulse Period (ms): (20-500) 200
Lower Limit of the Pulse Period (ms): (20-500) 50
Upper Limit of the Pulse Duration (ms): (20-200) 90
Lower Limit of the Pulse Duration (ms): (10-200) 30
Upper Limit of the Pulse Interruption Time (ms): (20-200) 90
Lower Limit of the Pulse Interruption Time (ms): (10-200) 30
Caller Offhook Dejittered Within(10ms): (5-25) 8
Callee Offhook Dejittered Within(Without FSK) (10ms):(5-25) 20
Callee Offhook Dejittered Within(With FSK) (10ms):(5-25) 5
NLP Mode: Normal Mode
Port Power Deny: Disable
☑ Port Locked
Current Adjust Factor: (0-100) 100

Step 7 Click **OK**.

----End

14.1.3.2 Enabling a VoIP PSTN Port

After you configure the attributes of a VoIP PSTN port, you need to enable the port to start services.

Context

NOTE

You can start services only on the VoIP PSTN port whose **User Port Configuration** is set to **VoIP Configured and Authorized**.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ASL** > **POTS Port** from the navigation tree.

Step 3 Click the **VoIP PSTN Port** tab, and set the filter criteria to display the required VoIP PSTN ports.

Step 4 Select a record from the VoIP PSTN port list, right-click, and then choose **Enable Service**.

Step 5 Click **YES**.

----End

14.1.4 Configuration Example of the VoIP PSTN Service(H.248/ MGCP)

This topic provides an example for configuring the VoIP PSTN service in an example network. After the configuration, PSTN users will be able to make calls.

Prerequisites

- The example network as shown in **Figure 14-1** must be complete.
- Network devices and lines must be in the normal state.
- The OLT must use the H.248 or MGCP protocol.

NOTE

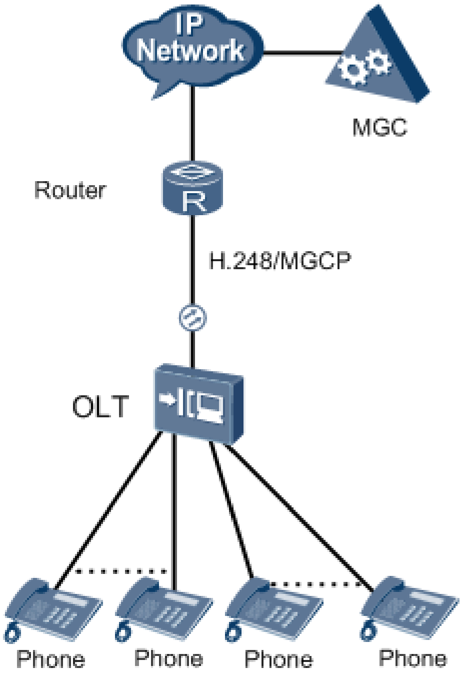
In the NE Explorer, choose **NE Properties** > **Voice** > **System protocol** to view or configure the system protocol of an NE.

- The OLT must be able to communicate with the MGC.

Example Network

Phones are connected to the PSTN ports of the OLT. The voice service travels upstream to the upper layer network through the upstream ports of the OLT.

Figure 14-1 Example network of the VoIP PSTN service



Data Plan

Table 14-1 provides the data plan for the VoIP PSTN service.

Table 14-1 Data plan for the VoIP PSTN service

Item		Data	Remarks
MGC profile		Name: mgcprofile1 Protocol type: H.248 IP Address 1: 10.13.4.120 UDP/STCP Port Number: 2944	-
MG interface	Upstream port	Subport: 0/9/0	-
	MG interface parameters	MG ID: 1 Name: ag1 MG Message MID Type: Signaling IP Address Signaling IP Address: 10.10.10.7 Media IP Address: 10.10.10.7 Signaling Port No.: 2944	Configure the MG interface to enable the standalone function. Use default values for the other parameters. **NOTE** The MG interface parameters must be the same as the corresponding parameters preset on the MGC.
	Ringing mapping	MG ID: 1 MGC Ringing ID: 1 Cadence Ringing Mode: 2 Initial Ringing Mode: 2	-
PSTN user data	Physical location	0/2/0-0/3/31	Use default values for the other attributes.
	MG ID	1	
	Terminal ID	1-64	
	Telephone No.	Phone numbers of users in ports 0/2/0-0/3/31: 5500-5563	

Procedure

Step 1 **Configure the MGC profile.**

- Name: mgcprofile1
- Protocol type: H.248

- IP Address 1: 10.13.4.120
- UDP/STCP Port Number: 2944

Step 2 Configure VLANs.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. Right-click the device list, and then choose **Add**.
4. In the dialog box that is displayed, set the parameters.
   - VLAN ID: 10
   - VLAN Type: Smart VLAN
5. Click **Done**.

Step 3 Configure the upstream port of a VLAN and the L3 interface.

1. Select the VLAN whose **VLAN ID** is 10, right-click, and then choose **Configure**.
2. In the dialog box that is displayed, select **Configure VLAN**. On the right pane, click the **Sub Port** tab, and then configure the upstream port of the VLAN to port 0/9/0.
3. On the right pane, click the **L3 Interface** tab, and then configure the L3 interface.
   - Management Status: UP
   - IP Address: 10.10.10.7
   - IP Mask: 255.255.0.0
4. Click **Done**.

Step 4 Configure the IP interface.

- IP Address: 10.10.10.7
- IP Type: Media/Signaling
- Gateway: 10.10.10.1

Step 5 Add an MG interface.

1. Choose **Voice Gateway** > **Media Gateway** from the navigation tree.
2. On the **Media Gateway** tab page, set the filter criteria to display the required MGs.
3. In the information list, right-click and choose **Add** from the shortcut menu. Right-click the MG list, and then choose **Add** > **H.248**.
4. In the dialog box that is displayed, set the parameters.
   - MG ID: 1
   - Name: ag1
   - MG Message MID Type: Signaling IP Address
   - Signaling IP Address: 10.10.10.7
   - Media IP Address: 10.10.10.7
   - Signaling Port No.: 2944
5. Click **OK**.

Step 6 Configure the MGC.

1. In the information list, select a record with **MG ID** as **1** and click the **MGC Attribute Info** tab in the lower pane. In the list, select a record with **MGC Index** as **0** and choose **Modify...** from the shortcut menu.
2. In the dialog box that is displayed, select an MGC template with **NMS MGC Profile** as **mgcprofile1**.
3. Click **OK**.

Step 7 (Optional) Configure MG Software Parameters.

1. In the information list, select a record with **MG ID** as **1**, right-click and choose **Configure MG Software Parameters** from the shortcut menu. In the dialog box that is displayed, set **Standalone Support Flag** to **All**.
2. Click **OK**.

Step 8 (Optional) Configure the ringing mapping.

1. On the **Ringing Mapping** tab page, set the filter criteria to display the required ringing mapping records.
2. In the information list, right-click and choose **Add** from the shortcut menu.
3. In the dialog box that is displayed, set the parameters.
   - MG ID: 1
   - MGC Ringing ID: 1
   - Cadence Ringing Mode: 2
   - Initial Ringing Mode: 2
4. Click **OK**.

Step 9 Start the MG interface.

1. In the information list, select a record with **MG ID** as **1**, right-click and choose **Reset** > **Cold Start** from the shortcut menu.
2. In the dialog box that is displayed, click **Yes**.

Step 10 Configure the attributes of the VoIP PSTN port, including the user data and the physical attributes.

1. Choose **ASL** > **POTS Port** from the navigation tree.
2. Click the **VoIP PSTN Port** tab, and set the filter criteria to display the required VoIP PSTN ports.
3. Select ports 0/2/0-0/3/31 in batches from the PSTN port list, right-click, and then choose **Configure Attribute**.
4. In the dialog box that is displayed, click the **Field Name** drop-down list and configure the VoIP PSTN service.
   - MG ID: 1
   - Telephone No.: 5500-5563
   - Terminal ID: 1-64
5. (Optional) Select the VoIP PSTN ports one by one and click the **service details** and **physical details** tabs to configure customized services and physical attributes. In this situation, retain default values for the physical attributes.
6. Click **OK**.

Step 11 Save the data.

1. On the tab page that is displayed, click above the navigation tree. Choose **Save data Immediately**.
2. Click **OK**.

NOTE

- The U2000 displays the progress of saving the data in the prompt area.
- Do not power off or reset the device before the data saving is complete. Otherwise, the data saved in the flash memory is damaged.

----End

Result

- The caller is able to hear the dialing tone.
- When a user calls another user, the callee is able to hear the ringing tone successfully and the caller is able to hear the ring-back tone.
- The caller and the callee are able to talk to each other successfully.
- The caller is able to hear the busy tone after the callee places the phone on the hook.
- If the OLT loses communication with the MGC, the users connected to the OLT are able to call each other.

14.1.5 Configuration Example of the VoIP PSTN Service (SIP)

This topic provides an example for configuring the VoIP PSTN service based on SIP protocol in an example network. After the configuration, PSTN users should be able to make calls.

Prerequisites

- The example network as shown in **Figure 14-2** must be complete.
- Network devices and lines must be in the normal state.
- The OLT must use the SIP protocol.

  NOTE

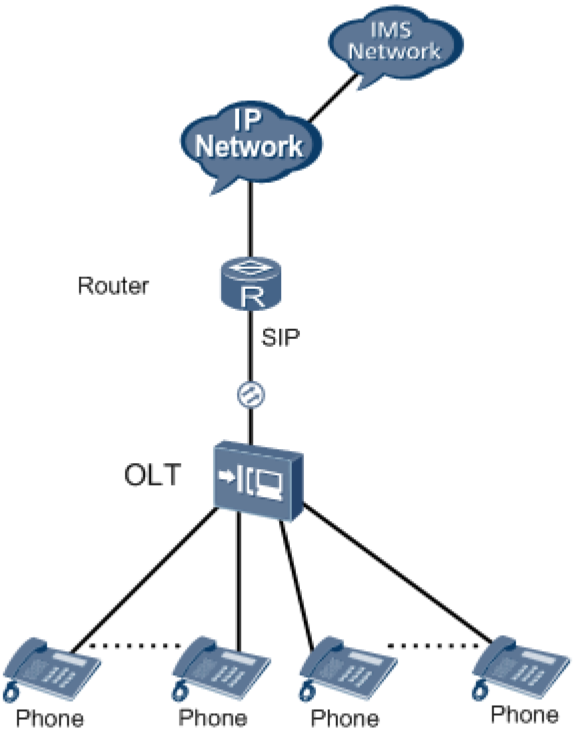
  In the NE Explorer, choose **NE Properties** > **Voice** > **System protocol** to view or configure the system protocol of an NE.
- The OLT must be able to communicate with the IMS.
- The PSTN user data corresponding to the SIP interface must be configured on the IMS.

Example Network

In this example, the device runs in China. The default configurations of system parameters and the overseas feature parameters meet the standard and the application requirements. Therefore, you need not configure these parameters.

Phones are connected to the PSTN ports of the OLT. The voice service travels upstream to the upper layer network through the upstream ports of the OLT.

Figure 14-2 Example network of the VoIP PSTN service



Data Plan

Table 14-2 provides the data plan for the VoIP PSTN service.

Table 14-2 Data plan for the VoIP PSTN service (SIP)

Item	Data	Remarks
Parameters of the media and the signaling	The upstream interface of the media stream and the signaling flow: 0/19/0 IP address and mask of the VLAN port: 10.13.4.116/16 Upstream VLAN of the media and the signaling: 200 Media IP address and IP address for the signaling flow: 10.13.4.116	-

Item	Data	Remarks
Basic attribute parameters of the SIP interface	The SIP interface ID: 0 Name: gw1 Media IP address and signaling IP address: 10.13.4.116 Signaling port ID: 5555 Transmission protocol: UDP Homing domain name: OLT	Use default values for the other attributes. **NOTE** The SIP interface parameters must be the same as the corresponding parameters preset on the IMS.
UAS Profile	Name: uasprofile1 IP address of the main proxy server: 10.13.4.110 IP address of the standby proxy server: 10.13.4.120 Proxy port: 5555 Address Mode: Fix mode	-
Voice service card	Slot of the card: 0/2 Service port: 0/2/0-0/2/63	Use default values for the other attributes.
SIP gateway ID	ID: 0	
Telephone No.	User phone numbers: 5500-5563	

Procedure

Step 1 Configure VLANs.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. Right-click the device list, and then choose **Add**.
4. In the dialog box that is displayed, set the parameters.
   - VLAN ID: 200
   - VLAN Type: Smart VLAN
5. Click **Done**.

Step 2 Configure the upstream port of the VLAN and the L3 interface.

1. Choose **VLAN** from the navigation tree.
2. Right-click the VLAN whose **VLAN ID** is **200** and choose **Configure** from shortcut menu.
3. In the dialog box that is displayed, select **Configure VLAN**. On the right pane, click the **Sub Port** tab, and then configure the upstream port of the VLAN to port 0/19/0.
4. On the right pane, click the **L3 Interface** tab, and then configure the L3 interface.
   - Management Status: UP

   - IP Address: 10.13.4.116
   - IP Mask: 255.255.0.0
5. Click **Done**.

Step 3 Configure the IP interface.

- IP Address: 10.13.4.116
- IP Type: Media/Signaling
- Gateway: 10.13.4.1

Step 4 **Configure the UAS profile.**

- Name: uasprofile1
- IP Address 1: 10.13.4.110
- IP Address 2: 10.13.4.120
- Proxy Port: 5555
- Address Mode: Fix mode

Step 5 Add a SIP interface.

1. Choose **Voice Gateway** > **Media Gateway** from the navigation tree.
2. On the **Media Gateway** tab page, set the filter criteria to display the required MGs.
3. Right-click in the list and choose **Add** > **SIP** from shortcut menu.
4. In the dialog box that is displayed, set the parameters.
   - MG ID: 0
   - Name: gw1
   - Media/Signaling IP Address: 10.13.4.116
   - Signaling Port No.: 5555
   - Transmission Mode: UDP
   - Homing Domain Name: OLT
   - Active NMS UAS Profile: uasprofile1
5. Click **OK**.

Step 6 Configure the attributes of the VoIP PSTN port (user data and physical attributes of the port).

1. Choose **ASL** > **POTS Port** from the navigation tree.
2. Click the **VoIP PSTN Port** tab, and set the filter criteria to display the required VoIP PSTN ports.
3. Select ports 0/2/0-0/2/63 from the list one by one, right-click, and choose **Configure Attribute** from shortcut menu.
4. In the dialog box that is displayed, click the **Service Details** tab, and then configure the VoIP PSTN service.
   - MG ID: 0
   - Telephone No.: 5500-5563
5. Click the **Physical Details** tab and configure the physical attributes of the VoIP PSTN port. In this example, the default values are used.
6. Click **OK**.

Step 7 Save the data.

1. On the tab page that is displayed, click above the navigation tree. Choose **Save data Immediately**.
2. Click **OK**.

NOTE

- The U2000 displays the progress of saving the data in the prompt area.
- Do not power off or reset the device before the data saving is complete. Otherwise, the data saved in the flash memory is damaged.

----End

Result

After the configuration, users of Phone 0-Phone 63 can communicate with each other successfully.

- The calling party can hear the dialing tone after picking up the phone.
- When the calling party dials the phone number of the called party, the phone of the called party can ring normally, and the calling party can hear the ring-back tone.
- The calling party and the called party can communicate in the normal state.
- After the called party hooks on, the calling party can hear the busy tone.

14.1.6 Configuring the VoIP VAG Service

The virtual access gateway (VAG) simulates a physical access gateway (AG) device in the form of multiple virtual AG devices, thus reallocating the AG resources.

Prerequisites

- Network devices and lines must be in the normal state.
- The VLAN L3 interface must be configured. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- A proper MGC profile must be configured. For details, see **14.1.1.2 Configuring an MGC Profile**.
- The MG interface must be configured. For details, see **14.1.1.4 Adding an MG (H.248/MGCP)** or **14.1.1.5 Adding an MG (SIP)**.
- The MA5600T must be able to communicate with the MGC.

Context

The MA5600T supports the VAG function as an AG device. One MA5600T can support up to eight VAGs.

NOTE

- The MG interface parameter must be the same as the related parameters preset on the MGC.
- The cadence ringing mode and the initial ringing mode comply with local standards.

Procedure

Step 1 Configure the VoIP PSTN user in VAG1. For details, see **14.1.4 Configuration Example of the VoIP PSTN Service(H.248/MGCP)** or **14.1.5 Configuration Example of the VoIP PSTN Service (SIP)**.

NOTE

VAG1 does not support the standalone function. The telephone numbers range from 12345000 to 12345031.

Step 2 Configure the VoIP PSTN user in VAG2. For details, see **14.1.4 Configuration Example of the VoIP PSTN Service(H.248/MGCP)** or **14.1.5 Configuration Example of the VoIP PSTN Service (SIP)**.

NOTE

VAG2 supports the standalone function. The internal telephone digitmap (the standalone switching digitmap) is 12345xxx. The telephone numbers range from 12345032 to 12345063.

Step 3 Verify the configuration of the VoIP VAG service.

- Any two users in VAG1 are able to call each other.
  - The caller is able to hear the dialing tone.
  - When a user calls another user, the callee is able to hear the ringing tone and the caller is able to hear the ring-back tone.
  - The caller and the callee are able to talk to each other.
  - The caller is able to hear the busy tone after the callee places the phone on the hook.
- Any two users in VAG2 are able to call each other.
  - The caller is able to hear the dialing tone.
  - When a user calls another user, the callee is able to hear the ringing tone successfully and the caller is able to hear the ring-back tone.
  - The caller and the callee are able to talk to each other successfully.
  - The caller is able to hear the busy tone after the callee places the phone on the hook.
- Users in VAG1 and VAG2 are able to place calls to each other.
  - The caller is able to hear the dialing tone.
  - When a user calls another user, the callee is able to hear the ringing tone successfully and the caller is able to hear the ring-back tone.
  - The caller and the callee are able to talk to each other successfully.
  - The caller is able to hear the busy tone after the callee places the phone on the hook.
- If the MG loses communication with the MGC, the users whose telephone numbers range from 12345000 to 12345031, that is, users in VAG1, cannot place calls to each other.
- If the MG loses communication with the MGC, the users whose telephone numbers range from 12345032 to 12345063, that is, users in VAG2, can place calls to each other.

----End

14.1.7 Configuring the MoIP Service

The modem over IP (MoIP) is a modem service that is provided between IP networks or between the IP network and the traditional PSTN network. In the NGN network, traditional modems are connected to the voice service ports that the MG provides. Under the control of the MGC, the

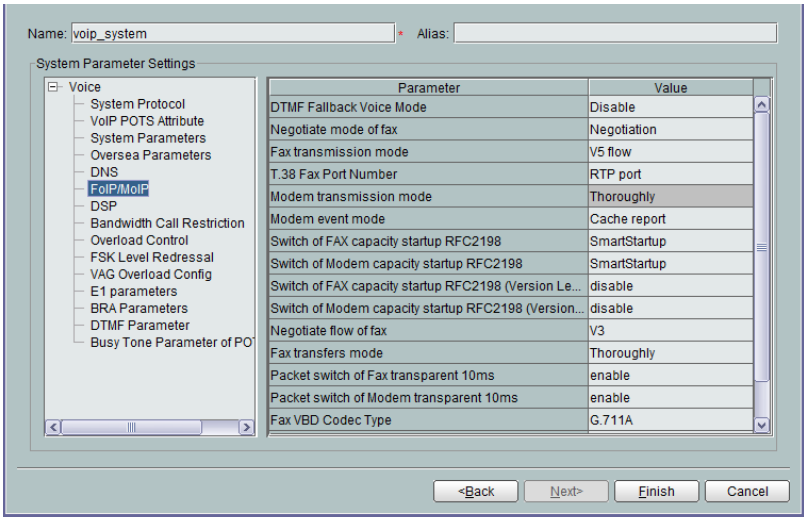
MG encodes the modem data service that is received, encapsulates the service into packets, and then transmits the packets over the IP network. This implements the modem service.

Prerequisites

- Network devices and lines must be in the normal state.
- The MG interface must be configured. For details, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.
- The VoIP user must be configured. For details, see**14.1.3.1 Configuring a VoIP PSTN Port**.
- The voice service port for the MoIP service must be in the normal state, and the voice service of this port must be normal.

Procedure

- Configuration flow of MoIP service under the MGCP/H.248:
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
  2. In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.
  3. On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.
  4. In the information list, right-click and choose **Add Global Profile** from the shortcut menu.
  5. In the dialog box that is displayed, enter the name of the system parameter profile. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters** navigation tree, and then click **Next**.
  6. Select **Voice** > **FoIP/MoIP** from the **System Parameter Settings** navigation tree, and then set the parameters, such as **Modem event mode**.



Name: voip_system *
Alias:

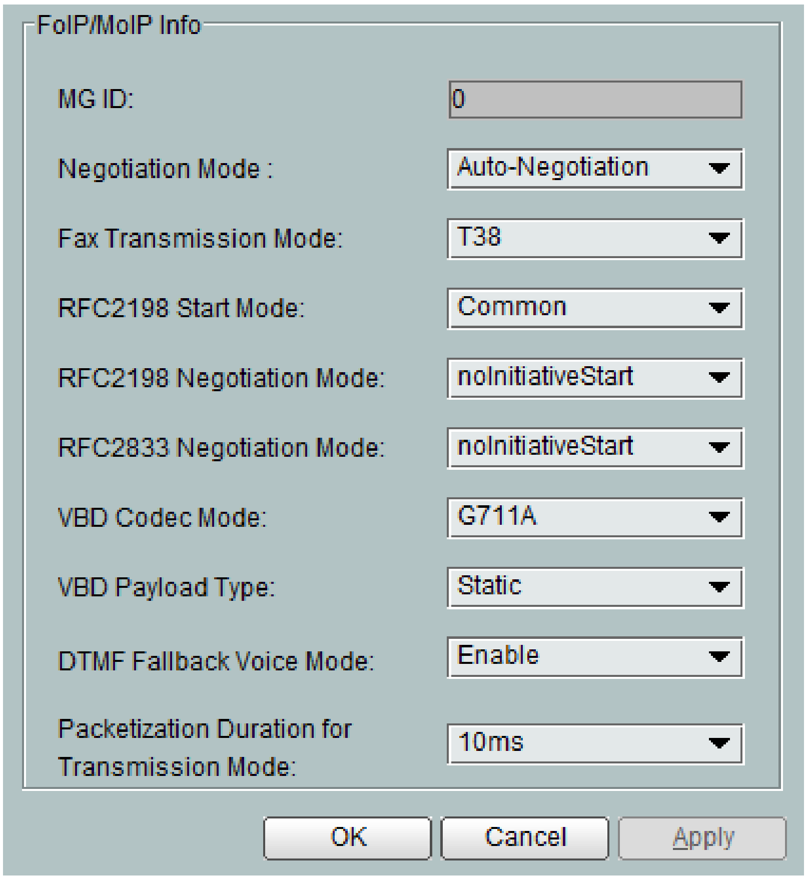
System Parameter Settings

Parameter	Value
DTMF Fallback Voice Mode	Disable
Negotiate mode of fax	Negotiation
Fax transmission mode	V5 flow
T.38 Fax Port Number	RTP port
Modem transmission mode	Thoroughly
Modem event mode	Cache report
Switch of FAX capacity startup RFC2198	SmartStartup
Switch of Modem capacity startup RFC2198	SmartStartup
Switch of FAX capacity startup RFC2198 (Version Le...	disable
Switch of Modem capacity startup RFC2198 (Version...	disable
Negotiate flow of fax	V3
Fax transfers mode	Thoroughly
Packet switch of Fax transparent 10ms	enable
Packet switch of Modem transparent 10ms	enable
Fax VBD Codec Type	G.711A

  7. Click **Finish**.

8. In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
9. In the dialog box that is displayed, select the required NE(s), and click **OK**.

- Configuration flow of MoIP service under the SIP:
  1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
  2. Choose **Voice Gateway** > **Media Gateway** from the navigation tree.
  3. On the **Media Gateway** tab page, set the filter criteria to display the required MGs.
  4. Select a record from the MG list, right-click, and then choose **Configure FoIP/MoIP Parameters**.
  5. In the dialog box that is displayed, set the parameters.



FoIP/MoIP Info

MG ID: 0

Negotiation Mode : Auto-Negotiation

Fax Transmission Mode: T38

RFC2198 Start Mode: Common

RFC2198 Negotiation Mode: noInitiativeStart

RFC2833 Negotiation Mode: noInitiativeStart

VBD Codec Mode: G711A

VBD Payload Type: Static

DTMF Fallback Voice Mode: Enable

Packetization Duration for Transmission Mode: 10ms

  6. Click **OK**.

----End

14.1.8 Configuring the FoIP Service

The fax over IP (MoIP) is a fax service that is provided between IP networks or between the IP network and the traditional PSTN network. In the NGN network, traditional faxes are connected to the voice service ports that the MG provides. Under the control of the MGC, the MG encodes the fax data service that is received, encapsulates the service into packets, and then transmits the packets over the IP network. This implements the fax service.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- Network devices and lines must be in the normal state.
- The MG interface must be configured. For details, see **14.1.1.4 Adding an MG (H.248/ MGCP)** or **14.1.1.5 Adding an MG (SIP)**.
- The VoIP user must be configured. For details, see**14.1.3.1 Configuring a VoIP PSTN Port**.
- The voice service port for the FoIP service must be in the normal state, and the voice service of this port must be normal.

Context

Table 14-3 and **Table 14-4** describe the items involved in the FoIP service that the OLT supports.

Table 14-3 Items involved in the FoIP service based on the H.248 or MGCP protocol

Fax Mode	Description
V2 T38	If the fax service is implemented under the same gateway, you can configure the T.38 fax port at random. If the fax service is implemented across gateways, you need to increase the number of the T.38 fax port by two. Ensure that the numbers of the T.38 fax ports in two gateways are the same. That is, you need to increase the numbers of the two T.38 fax ports by two for each or you do not increase the numbers of the two T. 38 fax ports at the same time.
	When the T.38 mode is used, the training modes must be the same at the two ends of the gateway. That is, configure the remote training mode or the local training mode at the two ends of the gateway. In this case, the fax service in the T.38 mode is successful. It is recommended that you use the remote training mode at the two ends.
V3 flow	All the fax processes of MGs are controlled by the MGC. The MGC applies the training mode, coding mode, and port number to the MG.
	All the fax processes of MGs are controlled by the MGC. The MGC applies the training mode, coding mode, and port number to MGs. If the MGC uses the T.38 mode, the fax port number can be negotiated. For example, the fax port number can be voice port number at one end, and the fax port number can be the sum of the voice port number plus two at the other end.
Selfswitch thoroughly	You need to configure the fax mode only on the MG.

Fax Mode	Description
	The training modes must be the same at the two ends of the gateway. That is, configure the remote training mode or the local training mode at the two ends of the gateway. It is recommended that you use the remote training mode at the two ends.
V5 flow	All the fax processes of MGs are controlled by the MGC. The MGC applies the training mode, coding mode, and port number to MGs. The V5 flow mode is compatible with the thoroughly mode and the V3 flow mode. For example, the thoroughly or V3 flow mode is configured on the peer end, and the V5 flow mode is configured on the local end. When the fax service is implemented, the two ends can communicate.
Selfswitch T38	When the MGC communicates with the MG in the normal state, the MG uses the self-negotiation T.38 mode to implement the FoIP service. When the MGC breaks down, the MG implements the FoIP service in the selfswitch thoroughly mode.
V2 Thoroughly	When the V2 thoroughly mode is used, the MG uses the voice service port as the fax port to access the T30 fax packets, encodes the fax packets in the G.711 mode, bears the fax packets in the G.711 codes, and then transmits the fax packets transparently to the peer end.

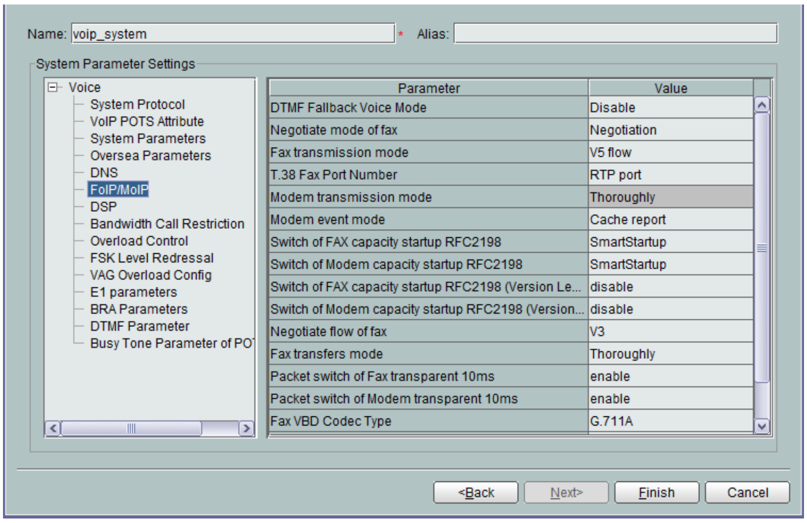
Table 14-4 Items involved in the FoIP service based on the SIP protocol

Fax Mode		Description
Thoroughly	Negotiation	According to whether the SIP signaling is involved, the fax mode can be negotiation or selfswitch. According to the coding scheme, the fax mode can be transparent fax (G.711 coding) or T.38 fax (T.38 coding).
	Selfswitch	
T.38 fax	Negotiation T.38	
	Selfswitch T.38	

Procedure

- Configuration flow of FoIP service under the MGCP/H.248:
  1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

2. In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.
3. On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.
4. In the information list, right-click and choose **Add** from the shortcut menu.
5. In the dialog box that is displayed, enter the name of the system parameter profile. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters** navigation tree, and then click **Next**.
6. Select **Voice** > **FoIP/MoIP** from the **System Parameter Settings** navigation tree, and then set the parameters, such as **Fax transmission mode**, **T.38 fax port**, **Negotiate mode of fax**, **Negotiate flow of fax**.

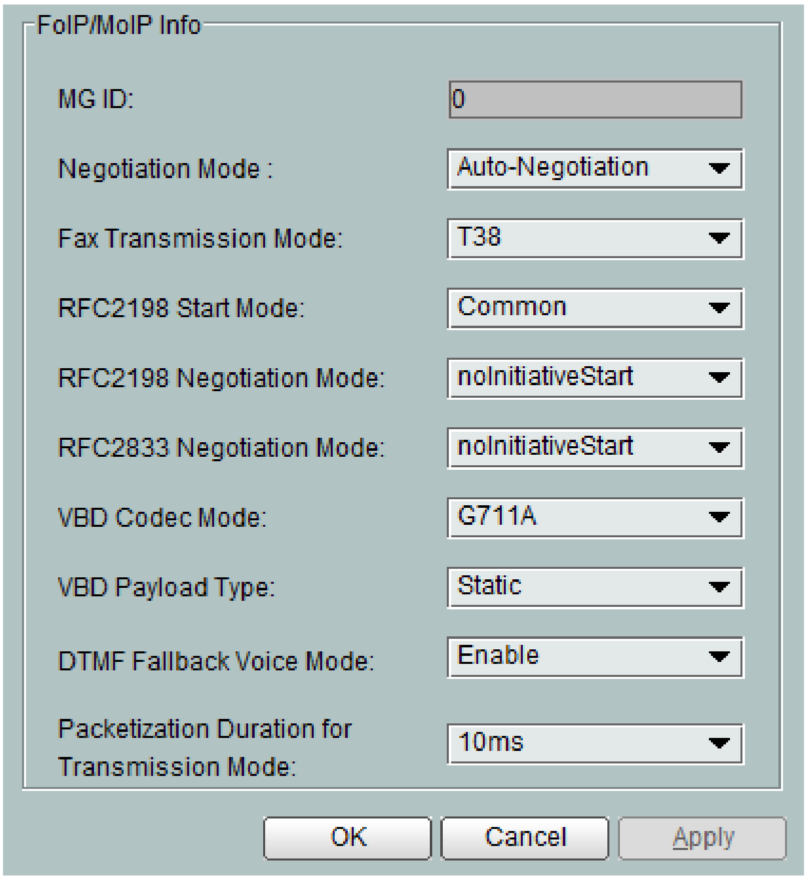


Name: voip_system *
Alias:

Parameter	Value
DTMF Fallback Voice Mode	Disable
Negotiate mode of fax	Negotiation
Fax transmission mode	V5 flow
T.38 Fax Port Number	RTP port
Modem transmission mode	Thoroughly
Modem event mode	Cache report
Switch of FAX capacity startup RFC2198	SmartStartup
Switch of Modem capacity startup RFC2198	SmartStartup
Switch of FAX capacity startup RFC2198 (Version Le...	disable
Switch of Modem capacity startup RFC2198 (Version...	disable
Negotiate flow of fax	V3
Fax transfers mode	Thoroughly
Packet switch of Fax transparent 10ms	enable
Packet switch of Modem transparent 10ms	enable
Fax VBD Codec Type	G.711A

7. Click **Finish**.
8. In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
9. In the dialog box that is displayed, select the required NE(s), and click **OK**.

- Configuration flow of FoIP service under the SIP:
  1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
  2. Choose **Voice Gateway** > **Media Gateway** from the navigation tree.
  3. On the **Media Gateway** tab page, set the filter criteria to display the required MGs.
  4. Select a record from the MG list, right-click, and then choose **Config FoIP/MoIP Parameters**.
  5. In the dialog box that is displayed, set the parameters.



FoIP/MoIP Info

MG ID: 0

Negotiation Mode : Auto-Negotiation

Fax Transmission Mode: T38

RFC2198 Start Mode: Common

RFC2198 Negotiation Mode: noInitiativeStart

RFC2833 Negotiation Mode: noInitiativeStart

VBD Codec Mode: G711A

VBD Payload Type: Static

DTMF Fallback Voice Mode: Enable

Packetization Duration for Transmission Mode: 10ms

6. Click **OK**.

----End

14.2 Configuring the R2 Signaling Service on the AG

This topic describes how to configure the R2 signaling service on the MA5600T to achieve PBX-NGN connection and PSTN-to-NGN migration.

14.2.1 R2 Signaling Service

R2 signaling is channel-associated signaling using the international R2 protocol. Based on E1 digital networks, R2 signaling applies to international and national networks.

Service Description

Channel-associated signaling indicates that signaling and voice information is transmitted over the same channel. Channel-associated interoffice signaling includes line signaling for monitoring and register signaling for control.

- **Line signaling**

  Line signaling monitors the transmission channels between or inside switches. It is used to establish, maintain, release, and monitor the routes during a call.

Line signaling has two types: analog signaling and digital signaling. Currently, the U2000 supports digital R2 line signaling only. Digital line signaling uses timeslot 16 in the PCM 30/32 system.

- **Register signaling**

  Register signaling consists of selective signaling and service signaling. It is transmitted over a data channel that has been occupied by line signaling. Register signaling carries control signals such as routing signals, calling numbers, and called numbers for connecting calls. Register signaling occupies channel resources and functions only during the call establishment phase.

Service Specifications

The R2 signaling service is implemented on EDTB boards. An EDTB board has sixteen R2 ports.

14.2.2 Configuring the R2 Signaling Service

In the R2 signaling service, the MA5600T connects to the PBX by transmitting R2 signaling over twisted-pair cables. In this way, the private branch exchange (PBX) connects to the next generation network (NGN) to achieve migration from the public switched telephone network (PSTN) to the NGN.

Prerequisites

- MG-1 supports R2 signaling and PBX users have been configured on MG-1.
- The user of phone D has been configured on MG-2.
- The PBX supports R2 signaling and is configured correctly. Phones A, B, and C connected to the PBX can communicate with each other.

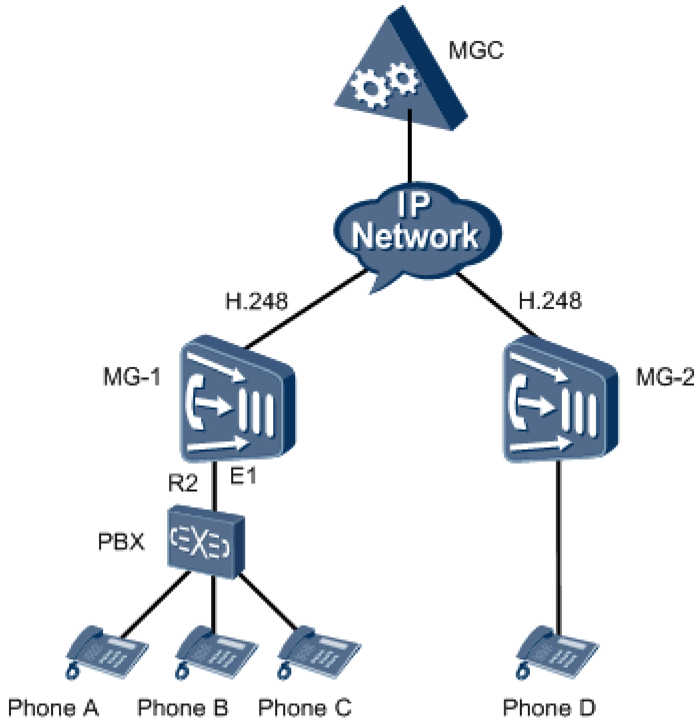
Context

- ITU-T Q.400-Q.490 specifies the basic R2 signaling standard. This standard takes different forms in different countries and areas.
- The U2000 provides country-specific R2 scripts to facilitate R2 signaling service configuration. This topic describes a simplified procedure for configuring the R2 signaling service.

Network Diagram

The PBX uses R2 signaling to access the NGN. The interfaces connecting the media gateways (MGs) and media gateway controller (MGC) use the H.248 protocol and the interfaces connecting MG-1 and the PBX use the R2 protocol.

Figure 14-3 PBX-NGN connection using R2 signaling



NOTE

To implement PBX-NGN connection using R2 signaling, MG-1 needs to make conversion between R2 signaling and H.248 signaling.

- In the upstream direction, the MA5600T terminates R2 signaling from the PBX, converts the R2 signaling to H.248 signaling, and forwards the H.248 signaling to the MGC.
- In the downstream direction, the MA5600T terminates H.248 signaling from the MGC, converts the H.248 signaling to R2 signaling, and forwards the R2 signaling to the PBX.

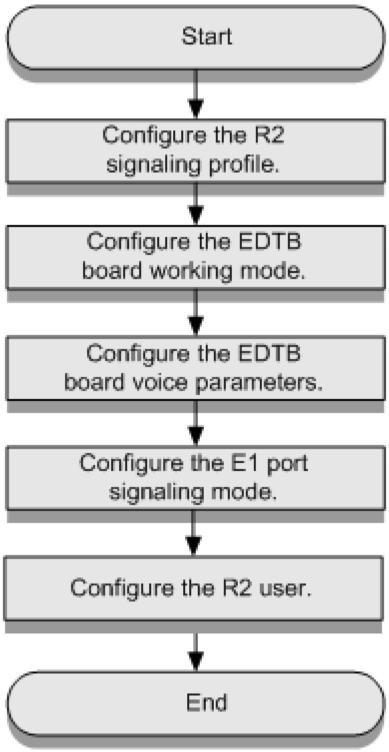
Data Plan

Item	Data	Remarks
Service board	R2 port: 0/12/0	The EDTB board supports the R2 signaling service.
	Board working mode: VOICE	The EDTB board supports 16 channels of SHDSL services and 16 channels of E1 services. After the board working mode is set to **VOICE**, the board works in voice mode.
	Port running mode: Service	Only the EDTB board in service mode (a sub-mode of voice) can process the R2 signaling service.

Item	Data	Remarks
	Port signaling mode: CAS	Because R2 signaling is channel-associated signaling, the port signaling mode must be CAS.
R2 signaling profile	Name: r2profile	-
	Incoming signaling type: MFC Outgoing signaling type: MFC	Currently, the U2000 supports MFC and DTMF for signaling types of incoming and outgoing calls.

Configuration Procedure

Figure 14-4 Configuration procedure of R2 signaling service


Start
Configure the R2 signaling profile.
Configure the EDTB board working mode.
Configure the EDTB board voice parameters.
Configure the E1 port signaling mode.
Configure the R2 user.
End

Procedure

1. Add an R2 signaling profile and apply the profile to an MG.

   NOTE

   To implement R2 signaling multiple countries adaptation, the MG integrates the commands of R2 register signaling, line signaling, and address signaling to scripts based on country-specific R2 signaling standards, and loads the scripts for R2 signaling service configuration.

   a. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in

Application Center and choose **Access Service** > **Access Profile Management** from the main menu (application style).

b. In the dialog box that is displayed, choose **Voice Profile** > **R2 Signalling Profile** from the navigation tree.

c. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.

   Set parameters as follows:

   - **Name**: r2profile
   - **Signaling Type of Incoming Call** and **Signaling Type of Outgoing Call**: MFC
   - Use the default values for other parameters.

d. Click **OK**.

e. In the R2 signaling profile list, right-click the configured **r2profile** and choose **Download to NE** from the shortcut menu.

f. In the dialog box that is displayed, select the NE configured with the target R2 user and click **OK**.

2. Set the working mode of the EDTB board.
   a. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
   b. In the NE Explorer, choose **NE Panel** from the navigation tree.
   c. Right-click the desired EDTB board and choose **Config Board Work Mode** from the shortcut menu.
   d. In the dialog box that is displayed, set **Board Work Mode** to **VOICE**.
   e. Click **OK**.
3. Set voice parameters for the EDTB board.
   a. Right-click the EDTB board and choose **Configure Board Voice Params** from the shortcut menu.
   b. In the dialog box that is displayed, set **Running Mode** to **Service**.
   c. Click **OK**.
4. Set the signaling mode for E1 ports.
   a. Choose **E1/T1** > **PRI E1/T1 Port** from the navigation tree.
   b. In the E1 port list, right-click 0/12/0 and choose **Modify** from the shortcut menu.
   c. In the dialog box that is displayed, set **Signaling Mode** to **CAS** and **Working Mode for digital access** to **Digital section access**.
5. Configure the R2 user.
   a. Click the **AG R2 Port** tab, and set the filter criteria to display the required AG R2 ports.
   b. In the E1 port list, right-click 0/12/0 and choose **Config** from the shortcut menu.
   c. In the dialog box that is displayed, set **MG ID** and select the R2 signaling profile.
   d. Click **OK**.

Result

Phones A, B, and C can communicate with phone D.

14.3 Configuring the VoIP ISDN Service

This topic describes how to configure the VoIP ISDN service and how the voice service is implemented on the MA5600T.

Context

The integrated services digital network (ISDN) is a CCITT standard and is developed from the integrated digital network (IDN). The ISDN network can support the end to end digital connection to implement various telecom services, such as the voice service and non-voice service.

The VoIP ISDN service implements the ISDN access function under the control of the H.248 protocol or the MGCP protocol. In this case, the VoIP ISDN service provides the integrated voice, video and the data service for users.

14.3.1 Configuring the VoIP ISDN BRA Service

The VoIP ISDN BRA service indicates that the ISDN BRA user on the MG side uses the ISDN basic rate interface to implement the access under the control of the H.248 protocol, the SIP protocol or the MGCP protocol. In addition, the ISDN service is transmitted to the next generation network (NGN) to implement the point-to-point (P2P) or point-to-multipoint (P2MP) multimedia communication of the voice, image, and data over the IP networking.

Prerequisites

- The corresponding MG must be configured. For details about how to configure the MG, see **14.1.1 Configuring the VoIP Media Gateway**.
- The corresponding SG must be configured. For details about how to configure the SG, see **14.1.2 Configuring the VoIP Signaling Gateway**.

Context

The basic rate access (BRA) provides two B-channels with the rate of 64 kbit/s and one D-channel with the rate of 16 kbit/s. The B-channel is mainly used to carry the service, and the D-channel is mainly used to transmit the call control signaling and the maintenance and management signaling.

14.3.1.1 Adding an Association

An association is a stream control transmission protocol (SCTP) association, which indicates that a logical relationship (channel) for data transmission which is set up by two SCTP endpoints through the four-way startup handshake mechanism of SCTP. An association provides the reliable transmission for the signaling.

Prerequisites

- The corresponding SG must exist. For details about how to add an SG, see **14.1.2.1 Adding an SG**.

- The corresponding MGC profile must exist. For details about how to add an MGC profile, see **14.1.1.2 Configuring an MGC Profile**.
- The local IP address used for the association must exist in the IP address pool.

Context

The endpoint of the association can have multiple IP addresses. The SCTP port number of the association endpoint, however, must be unique.

Procedure

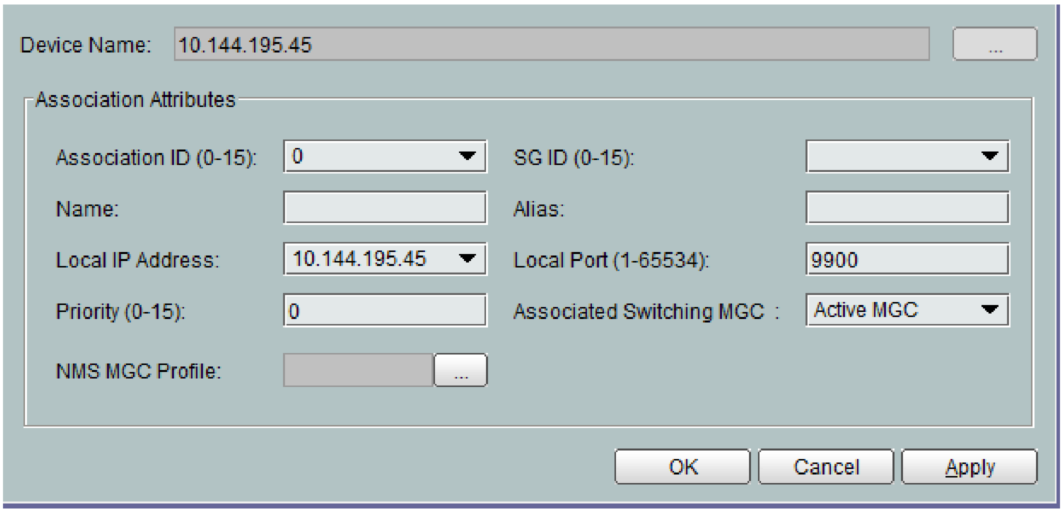
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Voice Gateway** > **Signaling Gateway** from the navigation tree.

Step 3 On the **Association** tab page, set the filter criteria to display the required associations.

Step 4 In the information list, right-click and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set the parameters.



Device Name: 10.144.195.45

Association Attributes

Association ID (0-15): 0

SG ID (0-15):

Name:

Alias:

Local IP Address: 10.144.195.45

Local Port (1-65534): 9900

Priority (0-15): 0

Associated Switching MGC : Active MGC

NMS MGC Profile:

Step 6 Click **OK**.

----End

14.3.1.2 Configuring the Attributes of a VoIP ISDN BRA Port

To configure the attributes of a VoIP ISDN BRA port and make the port meet the requirements, perform this operation.

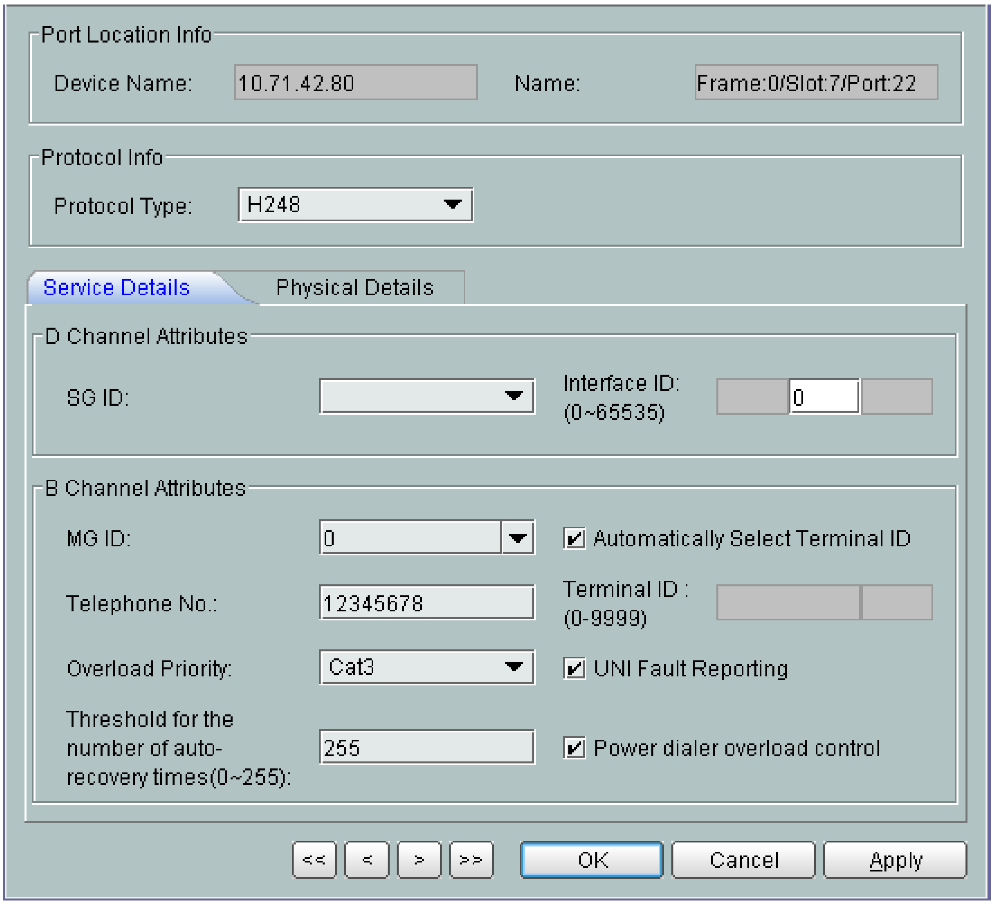
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **ISDN(BRA) Port** from the navigation tree.

Step 3 Click the **VoIP BRA Port** tab, and set the filter criteria to display the required VoIP ISDN BRA ports. Select a record to be configured from the list, right-click, and then choose **Configure Attribute**.

Step 4 In the dialog box that is displayed, select the device, and then set the attributes of the port as follows. (This step uses the H.248 protocol as an example.)



Port Location Info

Device Name: 10.71.42.80

Name: Frame:0/Slot:7/Port:22

Protocol Info

Protocol Type: H248

D Channel Attributes

SG ID:

Interface ID: (0~65535) 0

B Channel Attributes

MG ID: 0

☑ Automatically Select Terminal ID

Telephone No.: 12345678

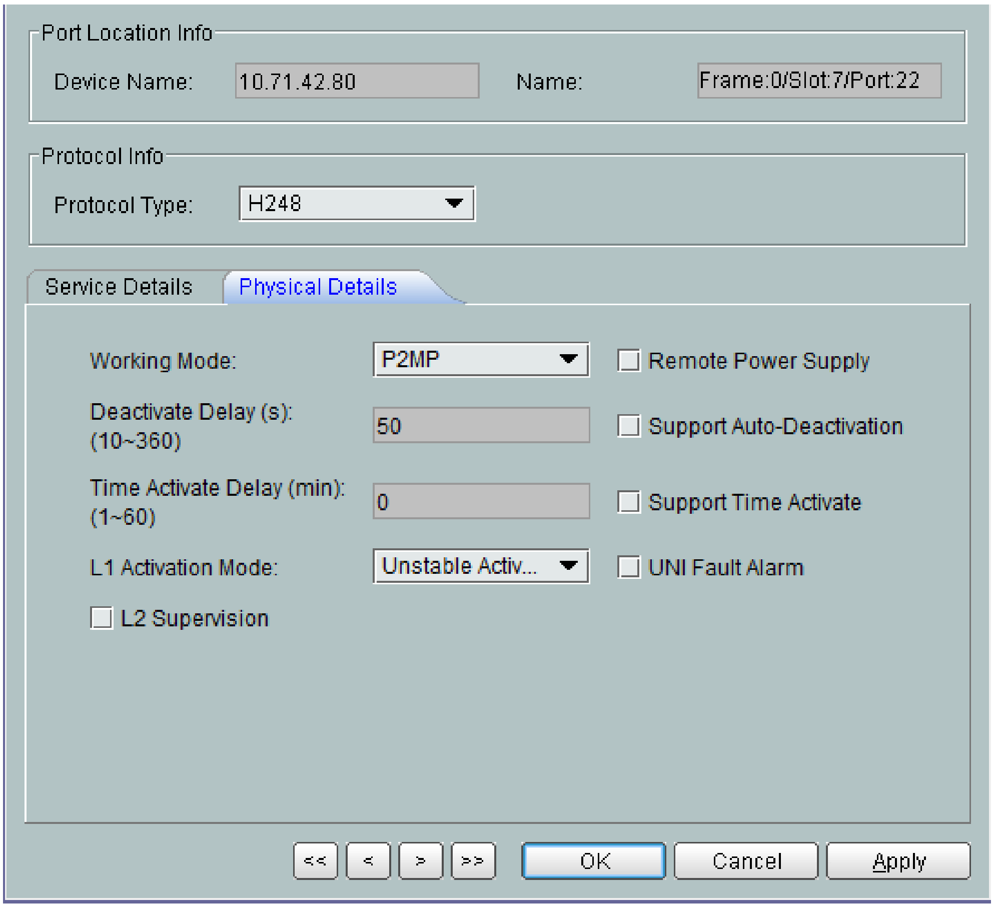
Terminal ID : (0-9999)

Overload Priority: Cat3

☑ UNI Fault Reporting

Threshold for the number of auto-recovery times(0~255): 255

☑ Power dialer overload control


Port Location Info

Device Name: 10.71.42.80 Name: Frame:0/Slot:7/Port:22

Protocol Info

Protocol Type: H248

Service Details | Physical Details

Working Mode: P2MP

Deactivate Delay (s): (10~360) 50

Time Activate Delay (min): (1~60) 0

L1 Activation Mode: Unstable Activ...

☐ L2 Supervision

☐ Remote Power Supply

☐ Support Auto-Deactivation

☐ Support Time Activate

☐ UNI Fault Alarm

NOTE

The BRA works in the P2MP or P2P mode.

- In the P2P working mode, one network terminal (NT) can connect to only one terminal, and the L2 link is always in the setup state to ensure that the service can be carried at any time.
- In the P2MP working mode, one NT can connect to multiple terminals, two L2 links can be set up concurrently, and a maximum of two users can call concurrently. If no call service is processed, the terminals can be deactivated automatically to save the power.

Step 5 Click **OK**.

----End

14.3.2 Configuring the VoIP ISDN PRA Service

The VoIP ISDN PRA service indicates that the ISDN PRA user on the MG side uses the ISDN basic rate interface to implement the access under the control of the H.248 protocol, SIP protocol or the MGCP protocol. In addition, the ISDN service is transmitted the next generation network (NGN) to implement the multimedia communication of the voice, image, and data over the IP networking.

Prerequisites

- The corresponding MG must be configured. For details about how to configure the MG, see **14.1.1 Configuring the VoIP Media Gateway**.

- The corresponding SG must be configured. For details about how to configure the SG, see **14.1.2 Configuring the VoIP Signaling Gateway**.

Context

The primary rate access (PRA) provides one D-channel and 23 (T1) or 30 (E1) B-channels. Each channel is with the rate of 64 kbit/s. The B-channel is mainly used to carry the service, and the D-channel is mainly used to transmit the call control signaling and the maintenance and management signaling.

14.3.2.1 Configuring the CRC4

To configure the CRC4 for the E1 port, perform this operation. The method for CRC4 must be the same with that for the LE.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **E1/T1** > **PRI E1/T1 Port** from the navigation tree.

Step 3 Click the **TDM E1 Port** tab and enter the filter criteria to display the required TDM E1 ports.

Step 4 In the port list, right-click a record and choose **Modify** from the shortcut menu.

Step 5 In the dialog box that is displayed, set **CRC4** to **Enable**.

Step 6 Click **OK**.

----End

14.3.2.2 Configuring the Working Mode of the EDTB Card

To configure an EDTB card to work in the independent mode, perform this operation. After the working mode of the card is configured, you can configure services to the card.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **NE Panel** from the navigation tree.

Step 3 Right-click the required EDTB card and choose **Config Work Mode** from the shortcut menu.

Step 4 In the dialog box that is displayed, set **Board Work Mode**.

Step 5 Click **OK**.

----End

14.3.2.3 Configuring the Attributes of a VoIP ISDN PRA Port

To configure the attributes of a VoIP ISDN PRA port and make the port meet the requirements, perform this operation.

Procedure

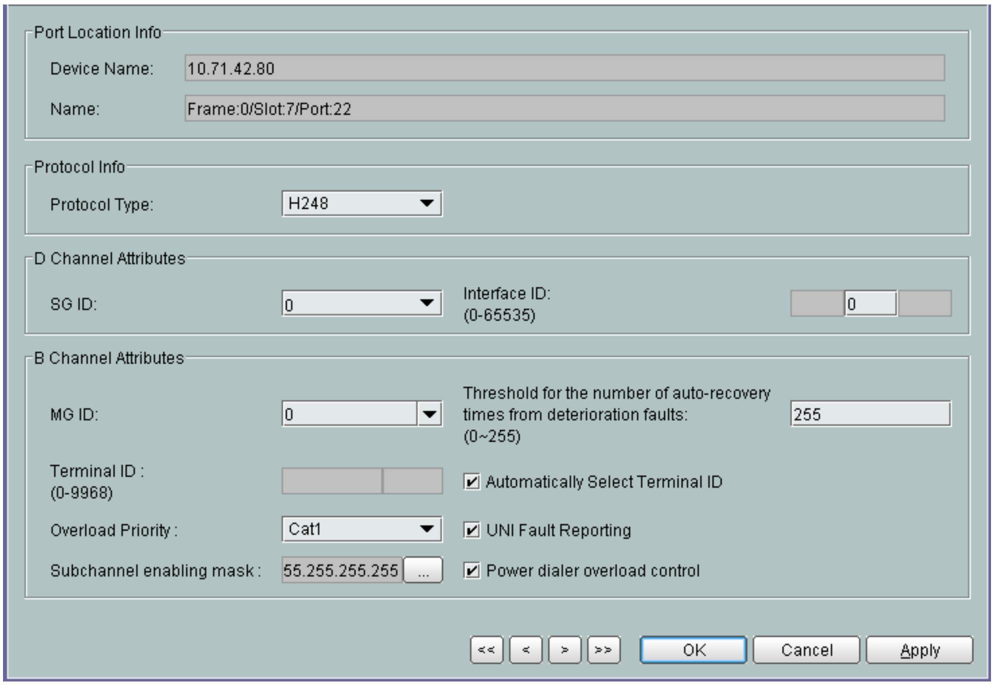
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **E1/T1** > **PRI E1/T1 Port** from the navigation tree.

Step 3 Click the **VoIP ISDN PRA Port** tab, and set the filter criteria to display the required VoIP ISDN PRA ports.

Step 4 In the port list, right-click a record to be configured and choose **Configure Attribute** from the shortcut menu.

Step 5 In the dialog box that is displayed, select the device, and then set the attributes of the D-channel and B-channel of the port as follows. (This step uses the H.248 protocol as an example.)



Port Location Info
Device Name: 10.71.42.80
Name: Frame:0/Slot:7/Port:22

Protocol Info
Protocol Type: H248

D Channel Attributes
SG ID: 0
Interface ID: (0-65535) 0

B Channel Attributes
MG ID: 0
Threshold for the number of auto-recovery times from deterioration faults: (0~255) 255
Terminal ID : (0-9968)
☑ Automatically Select Terminal ID
Overload Priority : Cat1
☑ UNI Fault Reporting
Subchannel enabling mask : 55.255.255.255
☑ Power dialer overload control

Step 6 Click **OK**.

----End

14.3.3 Configuration Example of the VoIP ISDN BRA Service

This topic provides an example for configuring the VoIP ISDN BRA service in an example network. After the configuration, ISDN BRA users should be able to make calls.

Prerequisites

The OLT must be able to communicate with the MGC.

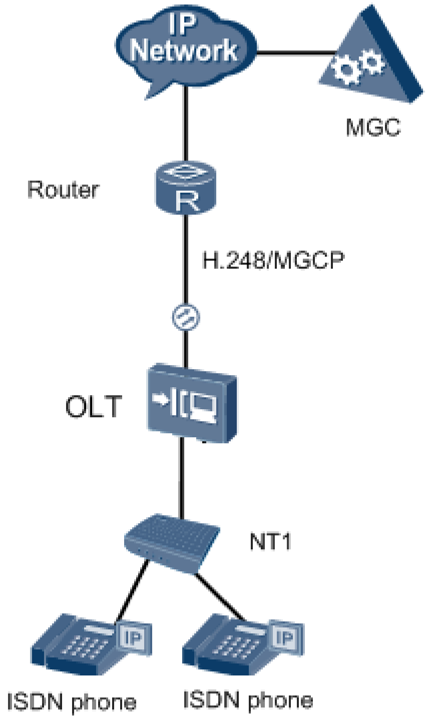
The ISDN digital telephone must support the P2P function.

Context

Example Network

Figure 14-5 shows an example network for configuring the VoIP ISDN BRA service.

Figure 14-5 Example network for configuring the VoIP ISDN BRA service



Data Plan

Table 14-5 lists the data plan for the VoIP ISDN BRA service.

Table 14-5 Data plan for the VoIP ISDN BRA service

Item		Data	Remarks
MGC profile		Name: mgcprofile Protocol type: H.248 IP Address 1: 10.10.10.10 UDP/STCP Port Number: 2944	-
Media Gateway	Upstream port	Subport: 0/9/0	-

Item		Data	Remarks
	MG interface parameters	MG ID: 1 Name: ag1 MG Message MID Type: Signaling IP Address Signaling IP Address: 10.10.10.7 Media IP Address 1: 10.10.10.7 Signaling Port Number: 2944	Use default values for the other attributes.
Signaling Gateway	SG interface parameters	SG ID: 1 Association ID: 0 MGC profile ● Name: xuaprofile ● Protocol type: xUA ● IP Address: 10.10.10.7 ● Port ID: 2944 Local Port: 9900	-
ISDN BRA ports	Physical location	0/7/0-0/7/1	Use default values for the other attributes.
	Working mode	P2P	
	Telephone No.	12345000 and 12345001	

Procedure

Step 1 Configure the MGC profile.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **Voice Profile** > **MGC Profile** from the navigation tree.
3. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.

   Set the parameters as follows:

   - Name: mgcprofile

- Protocol type: H.248
- IP Address 1: 10.10.10.10
- UDP/STCP Port Number: 2944

NOTE

Repeat this step to add an MGC profile by setting **Name** to **xuaprofile**, **Protocol type** to **xUA**, and **IP Address** to **10.10.10.7**.

4. Click **OK**.

Step 2 Configure VLANs.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. Right-click the device list, and then choose **Add**.
4. In the dialog box that is displayed, set the parameters.
   - VLAN ID: 10
   - VLAN Type: Smart VLAN
5. Click **Done**.

Step 3 Configure the upstream port of a VLAN and the L3 interface.

1. Select the VLAN whose **VLAN ID** is 10, right-click, and then choose **Configure**.
2. In the dialog box that is displayed, select **Configure VLAN**. On the right pane, click the **Sub Port** tab, and then configure the upstream port of the VLAN to port 0/9/0.
3. On the right pane, click the **L3 Interface** tab, and then configure the L3 interface.
   - Management Status: UP
   - IP Address: 10.10.10.7
   - IP Mask: 255.255.0.0
4. Click **Done**.

Step 4 Configure the IP interface.

- IP Address: 10.10.10.7
- IP Type: Media/Signaling
- Gateway: 10.10.10.1

Step 5 Add an MG interface.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **Voice Gateway** > **Media Gateway** from the navigation tree.
3. On the **Media Gateway** tab page, set the filter criteria to display the required MGs. Right-click in the MG list, and choose **Add** > **H.248** from the shortcut menu.
4. In the dialog box that is displayed, set the parameters.
   - MG ID: 1
   - Name: ag1
   - MG Message MID Type: Signaling IP Address

- Signaling IP Address: 10.10.10.7
- Media IP Address 1: 10.10.10.7
- Signaling Port No.: 2944

5. Click **OK**.

Step 6 Configure the MGC.

1. Click **MGC Attribute Info** tab in the lower pane,Right-click a record and choose **Modify** from the shortcut menu.
2. In the dialog box that is displayed, click the button of **NMS MGC Profile**, and then select the profile whose **Name** is **mgcprofile**.
3. Click **OK**.

Step 7 Start the MG interface.

1. On the **Media Gateway** tab page, set the filter criteria to display the required MGs. Click **Filter** to display the MG whose **MG ID** is 1. Right-click a record to be started in the list and choose **Reset** > **Cold Start** from the shortcut menu.
2. Click **OK**.

Step 8 Add the SG.

1. On the **Signaling Gateway** tab page, set the filter criteria to display the required SGs.
2. Click **Signal Gateway** tab in the pane, In the information list, right-click and choose **Add** from the shortcut menu.
3. In the dialog box that is displayed, set the parameters.

   Set the parameters as follows:

   - Name: sg1
   - SG ID: 1
   - Penging Time: 4
   - Work mode: Override
   - MG ID: 1

4. Click **OK**.

Step 9 Add the association.

1. Click **Association** tab in the pane, In the information list, right-click and choose **Add** from the shortcut menu.
2. In the dialog box that is displayed, set the parameters.

   Parameter settings:

   - Association ID: 0
   - SG ID: 1
   - Local IP: 10.10.10.7
   - Local Port: 9900
   - Profile Name: xuaprofile

3. Click **OK**.

Step 10 Configure the attributes of the VoIP ISDN BRA port.

1. Choose **DSL** > **ISDN(BRA) Port** from the navigation tree.
2. Click the **VoIP BRA Port** tab, and set the filter criteria to display the required VoIP ISDN BRA ports. Select ports 0/7/0 and 0/7/1 from the list, right-click, and then choose **Configure Attribute** from the shortcut menu.
3. In the dialog box that is displayed, set the parameters.

   Set the parameters as follows:
   - Protocol Type: *H.248*
   - MG ID: *1*
   - SG ID: *1*
   - Association ID: *0*
   - Interface ID: *1 with the step of 1*
   - Telephone No.: *12345000 with the step of 1*
   - Working Mode: *P2P*
4. Click **OK**.

Step 11 Save the data.

1. In the Main Topology, choose **MA5600T** from the navigation tree, right-click, and then choose **Save Data Immediately** from the shortcut menu.
2. Click **OK**.

NOTE

- When saving the data, the U2000 displays the progress of saving the data in the prompt area.
- Do not power off or reset the device before the data is saved completely. Otherwise, the data saved in the flash memory is lost.

Step 12 Verify the configuration of the VoIP ISDN BRA service.

After the configuration, the ISDN BRA user connected to port 0/7/0 and the ISDN BRA user connected to port 0/7/1 should be able to communicate successfully. In addition, these two ports are always in the activated state.

----End

14.3.4 Configuration Example of the VoIP ISDN PRA Service

This topic provides an example for configuring the VoIP ISDN PRA service in an example network. After the configuration, ISDN PRA users should be able to make calls.

Prerequisites

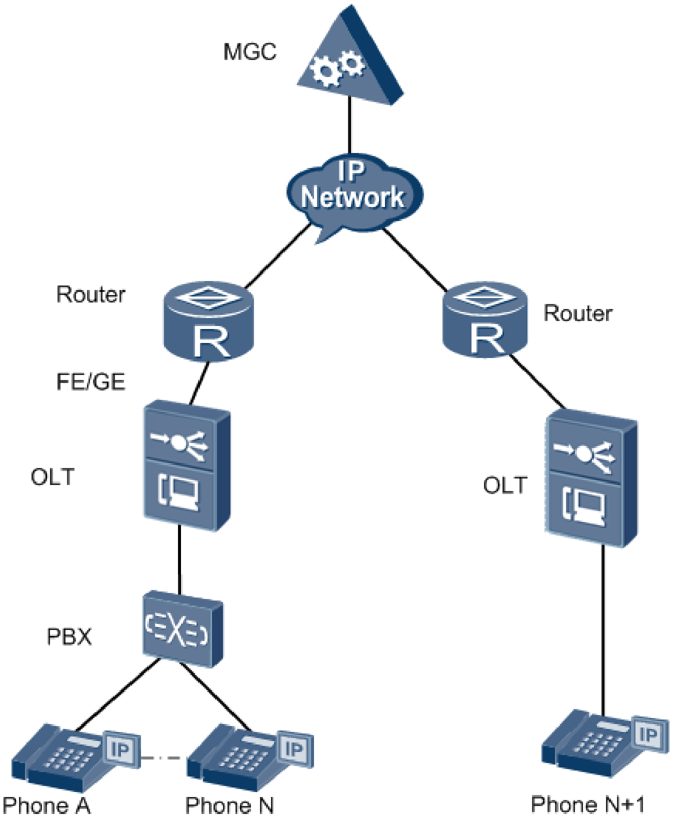
The OLT must be able to communicate with the MGC.

Context

Example Network

Figure 14-6 shows an example network for configuring the VoIP ISDN PRA service.

Figure 14-6 Example network for configuring the VoIP ISDN PRA service



Data Plan

Table 14-6 lists the data plan for the VoIP ISDN PRA service.

Table 14-6 Data plan for the VoIP ISDN PRA service

Item		Data	Remarks
MGC profile		Name: mgcprofile Protocol type: H.248 IP Address 1: 10.10.10.10 UDP/STCP Port Number: 2944	-
Media Gateway	Upstream port	Subport: 0/9/0	-

Item		Data	Remarks
	MG interface parameters	MG ID: 1 Name: ag1 MG Message MID Type: Signaling IP Address Signaling IP Address: 10.10.10.7 Media IP Address 1: 10.10.10.7 Signaling Port Number: 2944	Use default values for the other attributes.
Signaling Gateway	SG interface parameters	SG ID: 1 Association ID: 0 MGC profile ● Name: xuaprofile ● Protocol type: xUA ● IP Address: 10.10.10.7 ● Port number: 2944 Local Port: 9900	-
ISDN PRA ports	Physical location	0/7/0-0/7/1	Use default values for the other attributes.
	Terminal ID	Terminal ID Auto Selected	-
	Overload Priority	Cat1	-

Procedure

Step 1 Configure the MGC profile.

1. Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).
2. In the dialog box that is displayed, choose **Voice Profile** > **MGC Profile** from the navigation tree.
3. In the information list, right-click and choose **Add Global Profile** from the shortcut menu. In the dialog box that is displayed, set the parameters.

   Set the parameters as follows:

   - Name: mgcprofile
   - Protocol type: H.248

- IP: 10.10.10.10
- UDP/STCP Port Number: 2944

NOTE

Repeat this step to add an MGC profile by setting **Name** to **xuaprofile**, **Protocol type** to **xUA**, and **IP Address 1** to **10.10.10.7**.

4. Click **OK**.

Step 2 Configure VLANs.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. Right-click the device list, and then choose **Add**.
4. In the dialog box that is displayed, set the parameters.
   - VLAN ID: 10
   - VLAN Type: Smart VLAN
5. Click **Done**.

Step 3 Configure the upstream port of a VLAN and the L3 interface.

1. Select the VLAN whose **VLAN ID** is 10, right-click, and then choose **Configure**.
2. In the dialog box that is displayed, select **Configure VLAN**. On the right pane, click the **Sub Port** tab, and then configure the upstream port of the VLAN to port 0/9/0.
3. On the right pane, click the **L3 Interface** tab, and then configure the L3 interface.
   - Management Status: UP
   - IP Address: 10.10.10.7
   - IP Mask: 255.255.0.0
4. Click **Done**.

Step 4 Configure the IP interface.

- IP Address: 10.10.10.7
- IP Type: Media/Signaling
- Gateway: 10.10.10.1

Step 5 Add an MG interface.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **Voice Gateway** > **Media Gateway** from the navigation tree.
3. Click **Media Gateway** tab in the pane, right-click in the list and choose **Add** > **SIP** from shortcut menu. In the dialog box that is displayed, set the parameters.

   Set the parameters as follows:
   - MG ID: 1
   - Name: ag1
   - MG Message MID Type: Signaling IP Address
   - Signaling IP Address: 10.10.10.7

- Media IP Address 1: 10.10.10.7
- Signaling Port Number: 2944

4. Click **OK**.

Step 6 Configure the MGC.

1. Click **MGC Attribute Info** tab in the lower pane,Right-click a record and choose **Modify** from the shortcut menu.
2. In the dialog box that is displayed, click the button of **NMS MGC Profile**, and then select the profile whose **Name** is **mgcprofile**.
3. Click **OK**.

Step 7 Start the MG interface.

1. On the **Media Gateway** tab page, set the filter criteria to display the required MGs. Click **Filter** to display the MG whose **MG ID** is 1. Right-click a record to be started and choose **Reset** > **Cold Start** from the shortcut menu.
2. Click **OK**.

Step 8 Add the SG.

1. On the **Signaling Gateway** tab page, set the filter criteria to display the required SGs.
2. Click **Signal Gateway** tab in the pane, In the information list, right-click and choose **Add** from the shortcut menu. In the dialog box that is displayed, set the parameters.

   Set the parameters as follows:

   - Name: sg1
   - SG ID: 1
   - Penging Time: 4
   - Work mode: Override
   - MG ID: 1

3. Click **OK**.

Step 9 Add the association.

1. Click **Association** tab in the pane, In the information list, right-click and choose **Add** from the shortcut menu.
2. In the dialog box that is displayed, set the parameters.

   Parameter settings:

   - Association ID: 0
   - SG ID: 1
   - Local IP: 10.10.10.7
   - Local Port: 9900
   - Profile Name: xuaprofile

3. Click **OK**.

Step 10 Configure the attributes of the VoIP ISDN PRA port.

1. Choose **E1/T1** > **PRI E1/T1 Port** from the navigation tree.

2. Click the **VoIP ISDN PRA Port** tab, and set the filter criteria to display the required VoIP ISDN PRA ports. Select ports 0/7/0 and 0/7/1 from the list, right-click, and then choose **Configure Attribute** from the shortcut menu.
3. In the dialog box that is displayed, set the parameters.

   Set the parameters as follows:

   - Protocol Type: *H.248*
   - MG ID: *1*
   - SG ID: *1*
   - Interface ID: *1 with the step of 1*
   - Terminal ID: *Terminal ID Auto Selected*
4. Click **OK**.

Step 11 Save the data.

1. In Main Topology, choose **MA5600T** from the navigation tree, right-click, and choose **Save Data Immediately** from the shortcut menu.
2. Click **OK**.

NOTE

- When saving the data, the U2000 displays the progress of saving the data in the prompt area.
- Do not power off or reset the device before the data is saved completely. Otherwise, the data saved in the flash memory is lost.

Step 12 Verify the configuration of the VoIP ISDN PRA service.

After the configuration, the ISDN PRA user connected to port 0/7/0 and the ISDN PRA user connected to port 0/7/1 should be able to communicate successfully. In addition, these two ports are always in the activated state.

----End

15 Maintaining the TDM G.SHDSL Terminal

About This Chapter

This topic describes how to query information about the TDM G.SHDSL terminal, reset the terminal, and configure a loopback for the terminal.

15.1 Querying the Information About a TDM G.SHDSL Terminal
This topic describes how to query the information about a TDM G.SHDSL terminal on the U2000, such as the basic information, SHDSL Port information, E1 Port and DTE port information.

15.2 Restarting a TDM G.SHDSL Terminal
This topic describes how to restart a TDM G.SHDSL terminal to make the configurations on the terminal take effect, or to prevent some unpredictable problems occurring on the terminal.

15.1 Querying the Information About a TDM G.SHDSL Terminal

This topic describes how to query the information about a TDM G.SHDSL terminal on the U2000, such as the basic information, SHDSL Port information, E1 Port and DTE port information.

Prerequisites

- The TDM G.SHDSL terminal must be managed remotely by the U2000.
- The TDM G.SHDSL terminal must be activated.

Procedure

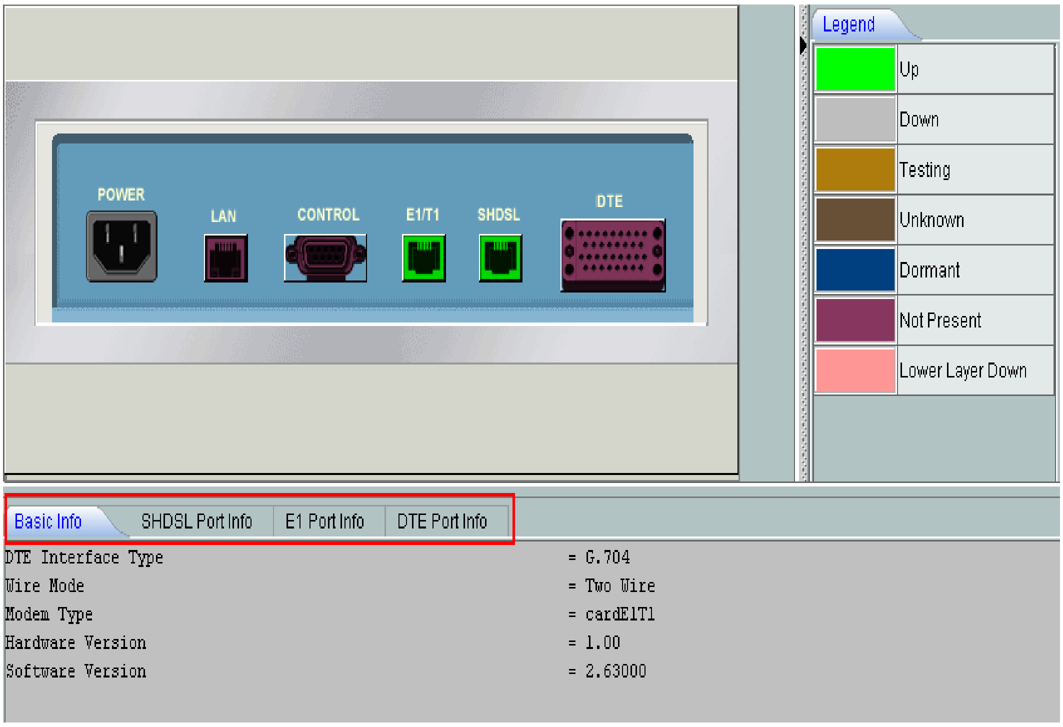
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **(TDM) G.SHDSL Port** from the navigation tree.

Step 3 On the **(TDM) G.SHDSL Port** tab page, set the filter criteria or click ⌄ to display the TDM G.SHDSL ports.

Step 4 In the TDM G.SHDSL terminal list, right-click a record and choose **Terminal Manage** from the shortcut menu.

Step 5 In the dialog box that is displayed, click the **Terminal Panel** tab. Click the **Basic Info** tab in the lower pane to view the details of the TDM G.SHDSL terminal.



```
DTE Interface Type                                     = G.704
Wire Mode                                              = Two Wire
Modem Type                                             = cardE1T1
Hardware Version                                       = 1.00
Software Version                                       = 2.63000
```

Step 6 On the **Terminal Panel** tab page, click the **SHDSL Port info** , **E1 Port info** and **DTE port info** to view the details.

----End

15.2 Restarting a TDM G.SHDSL Terminal

This topic describes how to restart a TDM G.SHDSL terminal to make the configurations on the terminal take effect, or to prevent some unpredictable problems occurring on the terminal.

Prerequisites

- The TDM G.SHDSL terminal must be managed remotely by the U2000.
- The TDM G.SHDSL terminal must be activated.

Context

⚠ **NOTICE**

Resetting the terminal will affect the ongoing service. Therefore, exercise caution when performing this operation.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **DSL** > **(ATM) G.SHDSL Port** from the navigation tree.

Step 3 On the **(ATM) G.SHDSL Port** tab page, set the filter criteria or click ︾ to display the G.SHDSL ports.

Step 4 In the TDM G.SHDSL terminal list, right-click a record and choose **Terminal Manage** from the shortcut menu.

Step 5 On the **Reset Terminal** tab page, right-click a record and choose from the shortcut menu.

----End

16 Configuring the Link Detection

About This Chapter

The OLT provides the function of the layer 2 link detection.

16.1 Configuring the Ethernet OAM Diagnosis
This topic describes the principles, configuration procedure, and configuration example of the Ethernet OAM diagnosis.

16.2 Configuring the BFD Network Monitoring
The bidirectional forwarding detection (BFD) is used to test the link status between two devices quickly. When the main channel is faulty, the OLT can switch the service to the standby channel, and thus to increase the reliability of the service and the inband maintenance channel.

16.1 Configuring the Ethernet OAM Diagnosis

This topic describes the principles, configuration procedure, and configuration example of the Ethernet OAM diagnosis.

Prerequisites

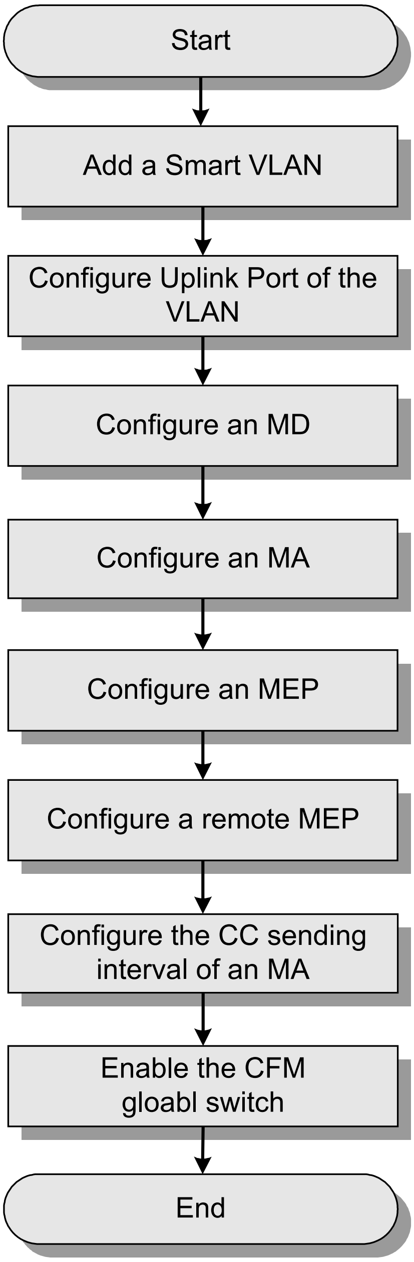
- The corresponding VLAN must exist. For details, see **4.1.2.2 Adding a VLAN**.
- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.

Context

With the extension of the Ethernet technology from the carrier network to MAN and WAN, carriers are more concerned about the maintainability of devices. Therefore, the maintenance of Ethernet devices becomes more and more important. The operations, administration and maintenance (OAM) issue of the transmission network is pressing. The 802.1ag connectivity fault management (CFM) provides an end-to-end method for detecting faults. The Ethernet OAM mechanism supported by the 802.1ag CFM covers connectivity check (CC), loopback (LB), link trace (LT), and forward AIS alarms.

Figure 16-1 shows the flowchart for configuring the Ethernet OAM diagnosis on the OLT.

Figure 16-1 Flowchart for configuring the Ethernet OAM diagnosis


Start
Add a Smart VLAN
Configure Uplink Port of the VLAN
Configure an MD
Configure an MA
Configure an MEP
Configure a remote MEP
Configure the CC sending interval of an MA
Enable the CFM gloabl switch
End

16.1.1 Introduction to the Ethernet OAM

This topic describes the basic concepts and principles of the Ethernet connectivity fault management (CFM) and the example network of the Ethernet OAM. The Ethernet OAM mechanism supported by the 802.1ag covers the connectivity check (CC), link trace (LT), and loopback (LB).

Context

The basic concepts and principles of the Ethernet CFM are described as follows:

1. Basic concepts:
   - Maintenance domain (MD): The Ethernet CFM divides a network into a maximum of eight layers. A bridge can have different layers to manage different MDs. A CFM MD consists of bridges, and is a combination of bridges and maintenance levels. MDs come under three layers: user domain (levels 7-5), service provider domain (levels 4-3), and carrier domain (levels 2-0). Different MDs are maintained by different management entities.
   - Maintenance association (MA): An MD can be divided into multiple MAs. Each MA maps with a service instance (SI) identified by a VLAN in the MD. That is, the MA can be understood as a combination of an MD and a VLAN. (According to the standard, multiple VLANs can map with one SI, and one SI maps with one MA.)
   - Maintenance point (MP): An MA consists of maintenance points (MPs) that are defined on the ports of bridges. That is, an MP is a combination of a bridge port, a VLAN, and a maintenance level. MPs are classified into two types: maintenance association end point (MEP) and maintenance association intermediate point (MIP). An MEP initiates and responds to CFM messages. An MIP does not initiate CFM messages. It only transparently transmits or responds to CFM messages.
2. Principles of fault detection:
   - Continuity check messages (CCMs) are used to detect Ethernet faults. Each MEP actively sends CCM packets at regular intervals. The CCM packets are copied to the multicast addresses. All the MIPs and MEPs in the MD can receive the CCM packets but need not respond. When an MEP receives CCM packets from other MEPs, it sets up and maintains an MEP CCM database. The database records the MEP IDs, MAC addresses of the MEPs, and the mappings between the MEPs and the receiving ports. The database also records the information about other MEPs in the MA. If the MEP does not receive CCM packets from another MEP for three successive times, the MEP reports a fault.
   - Loss of CCM packets may be caused by a link fault, a switched network fault, or wrong configurations between two MEPs. The NMS can use other methods, such as loss of physical layer signals, instead of CCM packets, to detect the link faults. But in this case, the NMS cannot detect the non-link faults, such as switched network faults or wrong configurations. After a fault is discovered through CCM packets, you can use LB or LT to locate the fault (for example, in the switched network).
   - CCM packets can detect not only the link faults and switched network faults, but also the service configuration errors (such as unmatched MA names), repeated MEP configurations (such as repeated MEP names), undesired MEPs, loopback (repeated serial numbers), data loss, and data corruption (such as wrong checksum).
3. Alarm mechanism: There are four types of alarms.
   - Cross-connection alarm: After an MEP on a bridge receives a CCM packet, the MEP checks whether certain configuration (including the type and length of the MD name; the MD name; the type and length of the MA name; and the MA name) of the peer MEP as carried by the CCM packet is completely the same as the local configuration. If the configurations are different, the MEP reports a cross-connection alarm.
   - Loss-of-CCM alarm: If an MEP on a bridge does not receive a CCM packet from a remote MEP in a specific period (3.5 times the sending interval), the MEP reports a loss-of-CCM alarm.
   - Error alarm: After an MEP on a bridge receives a CCM packet, the MEP compares the MEP information in the received CCM packet with the configuration information about

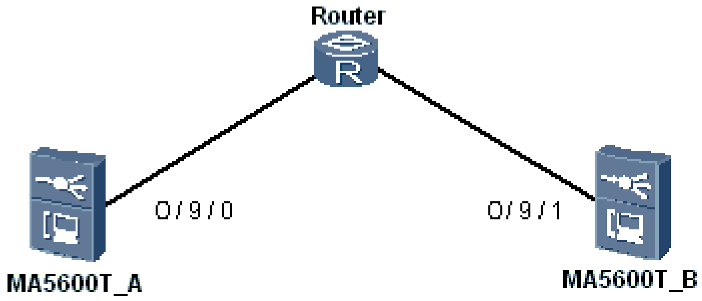
the remote MEP, including the interval for sending CCM packets. If the information does not match, the MEP reports an error alarm.

- RDI alarm: If a local MEP does not receive CCM packets from its remote MEP, the local MEP sends a CCM packet with an RDI bit. When another MEP receives the CCM packet with the RDI bit, the MEP reports an RDI alarm.

4. LT principle:
   - The LT helps to check the MIP path between two MEPs. A link trace message (LTM) contains a known multicast address, but is not multicasted. The LTM contains additional information indicating the MAC address of the destination MEP. When the LTM is forwarded by MIPs to the destination MEP in unicast mode, each MIP sends a link trace reply (LTR) to the source MEP. In this way, the source MEP learns the MIPs along the path to the destination MEP and records their MAC addresses.
5. LB principle:
   - LB helps an MEP to locate faults in an MA. LB uses the unicast MAC address of an MEP or MIP that is discovered by the CC or LT. The source MEP creates a loopback message (LBM) containing the index of the destination MEP, sends the LBM, and starts the timer. After receiving the LBM, the destination MEP sends an LBR to the source MEP. The loopback test succeeds. If the timer of the source MEP expires, the loopback test fails.

Figure 16-2 shows the example network of the Ethernet OAM on the OLT. The link between OLT_A and OLT_B uses the Ethernet OAM mechanism to detect link faults. Both OLT_A and OLT_B are configured with a local MEP and a remote MEP. The local MEP ID of OLT_B is the same as the remote MEP ID of OLT_A. The remote MEP ID of OLT_B is the same as the local MEP ID of OLT_A.

Figure 16-2 Example network of the Ethernet OAM



16.1.2 Configuring an MD

This topic describes how to configure an MD. Different MDs are maintained by different management entities.

Prerequisites

- The corresponding VLAN must exist. For details, see **4.1.2.2 Adding a VLAN**.
- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.

- You can perform this operation only after the CFM function is enabled globally.

Context

- The system supports three MDs.
- MDs with the same name format and the same name cannot be created on the same device, but can be created on different devices.
- MDs of the same level cannot be created on the same device, but can be created on different devices.
- The total length of the names of an MA and the corresponding MD must be less than or equal to 43 characters.

Procedure

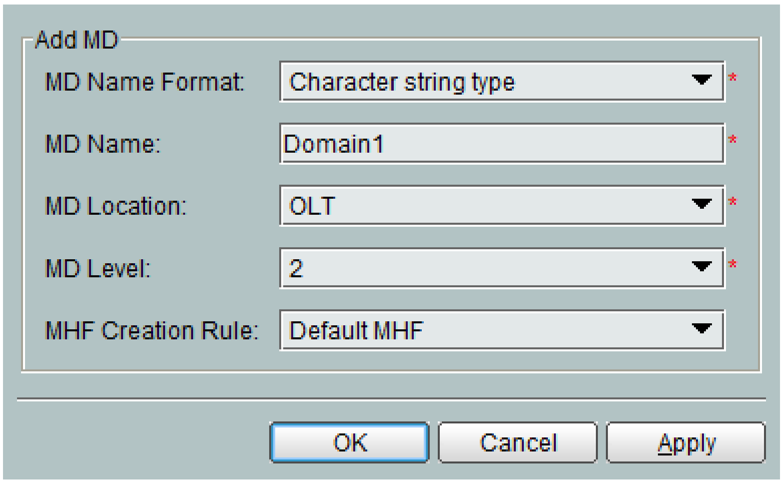
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ETH OAM** from the navigation tree.

Step 3 Click the **Maintenance Domain** tab, and set the filter criteria to display the required MDs.

Step 4 Right-click in the list and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set **MD Name Format**, **MD Name**, **Level** and **MHF Creation Rule** as follows.



Add MD

MD Name Format: Character string type *

MD Name: Domain1 *

MD Location: OLT *

MD Level: 2 *

MHF Creation Rule: Default MHF

Step 6 Click **OK**.

----End

16.1.3 Configuring an MA

This topic describes how to add an MA, add devices to the MA, configure the interval for sending CCM packets and the function of checking remote MEPs, check the remote MEPs configured in the MA, and report alarms of detected faults.

Prerequisites

- The corresponding VLAN must exist. For details, see **4.1.2.2 Adding a VLAN**.

- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MD must be configured. For details, see **16.1.2 Configuring an MD**.

Context

- You can perform this operation only after the CFM function is enabled globally.
- Each MD can be configured with up to 48 MAs and the system supports up to 48 MAs. That is, if you configure 48 MAs in an MD, no more MAs can be configured in other MDs.
- The MA must belong to an MD. Do not create an MA that is the same as an existing one.
- The MAs in the same MD cannot be associated with the same VLAN.
- The total length of the names of an MA and the corresponding MD must be less than or equal to 43 characters.

Procedure

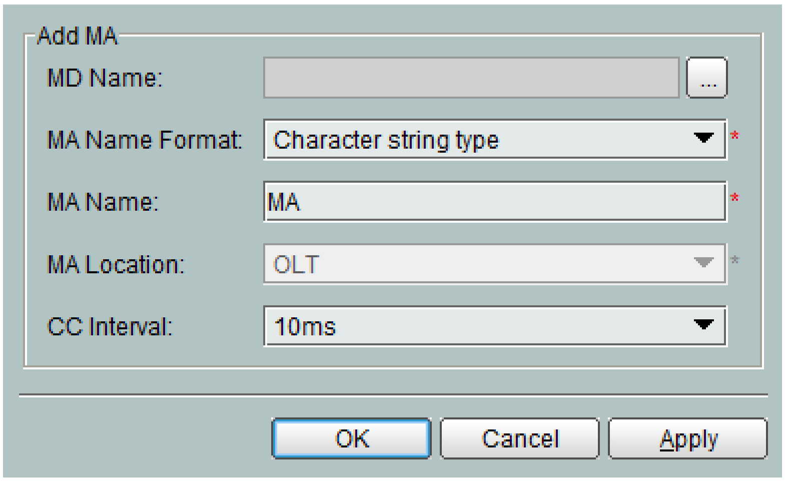
Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ETH OAM** from the navigation tree.

Step 3 Click the **Maintenance Association** tab, and set the filter criteria to display the required MAs.

Step 4 Right-click in the list and choose **Add** from the shortcut menu.

Step 5 In the dialog box that is displayed, set **MD Name**, **MA Name Format**, **MA Name**, and **CC Interval** as follows.



Add MA

MD Name:

MA Name Format: Character string type *

MA Name: MA *

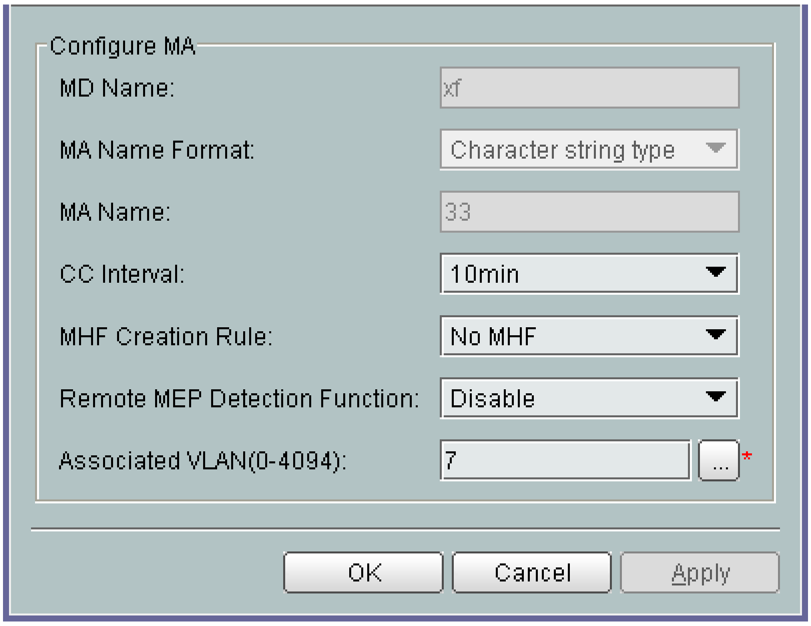
MA Location: OLT *

CC Interval: 10ms

Step 6 Click **OK**.

Step 7 Right-click MA1 and choose **Configure** from the shortcut menu.

Step 8 In the dialog box that is displayed, set **MHF Creation Rule**, **Remote MEP Detection Function** and **Associated VLAN** as follows.


Configure MA

MD Name: xf

MA Name Format: Character string type

MA Name: 33

CC Interval: 10min

MHF Creation Rule: No MHF

Remote MEP Detection Function: Disable

Associated VLAN(0-4094): 7

Step 9 Click **OK**.

----End

16.1.4 Configuring a Source MEP

This topic describes how to create a source MEP to detect the connectivity of a channel in an MA, and how to configure the administrative status, CCM and LTM priority, and CCM sending status for the MEP.

Prerequisites

- The corresponding VLAN must exist. For details, see **4.1.2.2 Adding a VLAN**.
- The VLAN must be configured with an upstream port. For details, see **5.3 Configuring the Upstream Port of a VLAN**.
- The MD must be configured. For details, see **16.1.2 Configuring an MD**.
- The MA must be configured. For details, see **16.1.3 Configuring an MA**.

Context

An MEP is the end point of a maintenance channel. Ethernet OAM depends on the MEPs at both ends of a channel to check the connectivity. Therefore, the MEPs must be created. After creating the MEPs, you can use them to check the connectivity of a channel in an MA.

- The MEP takes effect only after the administrative function is enabled.
- The MEP can send CCM packets at regular intervals to check the connectivity of a channel only after the CCM packet sending function is enabled successfully.
- After the CCM and LTM priority is successfully configured, the system discards the packets with lower priority in case of congestion.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **ETH OAM** from the navigation tree.

Step 3 Click the **Maintenance Association** tab, and set the filter criteria to display the required MAs.

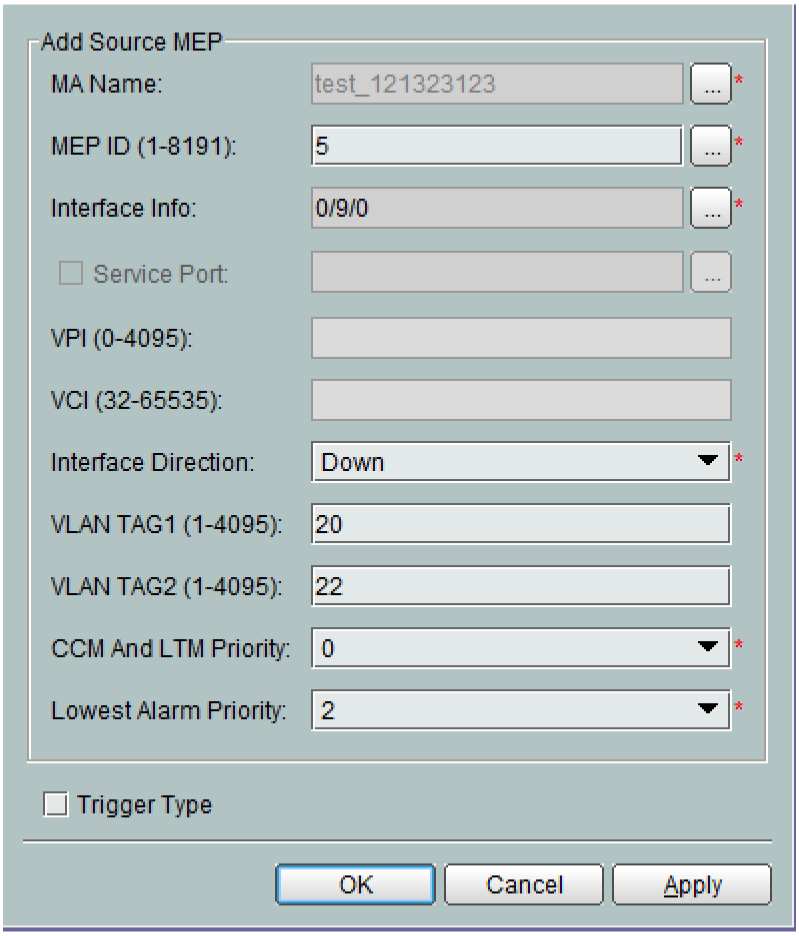
Step 4 Select an MA, and click the **Source MEP ID Info** tab in the lower pane.

NOTE

Step 3 and step 4 can be merged into one step: On the **Source MEP ID Info** tab page, set the filter criteria to display the required multicast source MEPs.

Step 5 Right-click in the list and choose **Add** from the shortcut menu.

Step 6 In the dialog box that is displayed, set **MEP ID**, **Interface Info**, **Interface Direction**, **VLAN TAG1**, **VLAN TAG2** and **CCM And LTM Priority** as follows.

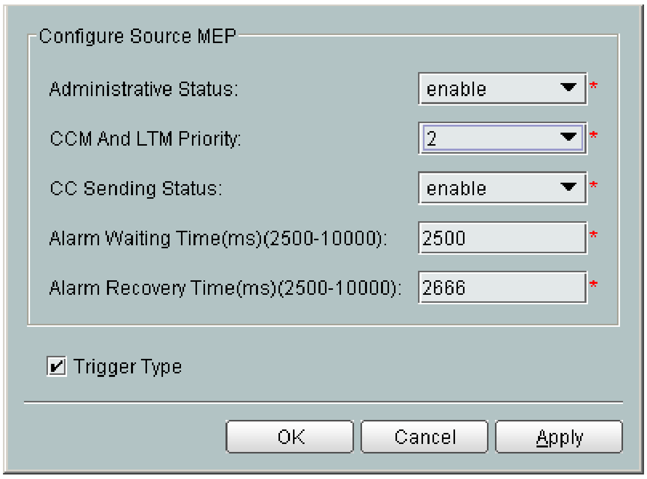


Add Source MEP
MA Name: test_121323123
MEP ID (1-8191): 5
Interface Info: 0/9/0
☐ Service Port:
VPI (0-4095):
VCI (32-65535):
Interface Direction: Down
VLAN TAG1 (1-4095): 20
VLAN TAG2 (1-4095): 22
CCM And LTM Priority: 0
Lowest Alarm Priority: 2
☐ Trigger Type

Step 7 Click **OK**.

Step 8 Right-click the added source MEP and choose **Configure** from the shortcut menu.

Step 9 In the dialog box that is displayed, enable the **Administrative Status** and **CC Sending Status** of the MEP and set **CCM And LTM Priority**, **Alarm Waiting Time** and **Alarm Recovery Time** as follows.



Configure Source MEP

Administrative Status: enable *

CCM And LTM Priority: 2 *

CC Sending Status: enable *

Alarm Waiting Time(ms)(2500-10000): 2500 *

Alarm Recovery Time(ms)(2500-10000): 2666 *

☑ Trigger Type

Step 10 Click **OK**.

----End

16.1.5 Enabling the Global CFM Function

This topic describes how to set the Ethernet OAM global parameters on the U2000 and apply the parameters to the specified devices. You can configure the Ethernet OAM global parameters in the **System Parameter Profile** of the U2000. Devices can detect and locate Ethernet faults through the bound **System Parameter Profile**.

Context

When the global CFM function is enabled, the CFM packets are captured, and the functions of CC, LB and LT are enabled. When the global CFM function is disabled, the CFM packets are not captured, and the functions of CC, LB, and LT are disabled.

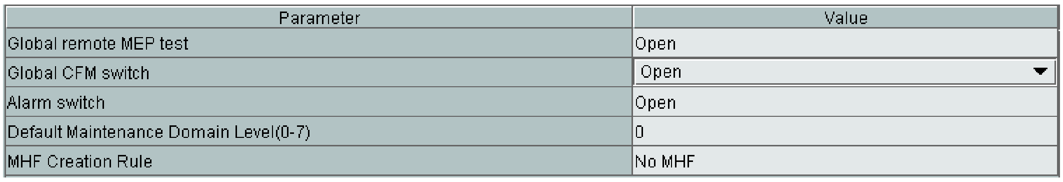
The system parameter profile is a collection of system parameters, such as ETH OAM parameters and other parameters. After a system parameter profile is applied to a device successfully, the parameters in the profile overwrite the original parameters on the device. This may affect the services of the device. Therefore, the system parameter profile must be applied to the device before service provisioning.

Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 On the tab page that is displayed, choose **NE Properties** > **Protocol** > **ETH OAM** from the navigation tree.

Step 3 In the parameter configuration area in the right pane, set the global parameters of the Ethernet OAM devices, including the multicast MAC base address that is used to send CC/LT packets, and then set **Global remote MEP test** and **Global CFM switch**.



Parameter	Value
Global remote MEP test	Open
Global CFM switch	Open
Alarm switch	Open
Default Maintenance Domain Level(0-7)	0
MHF Creation Rule	No MHF

Step 4 Click **Apply**.

----End

16.1.6 Configuration Example of the Ethernet OAM Diagnosis

This topic provides an example for configuring the Ethernet OAM on the OLT.

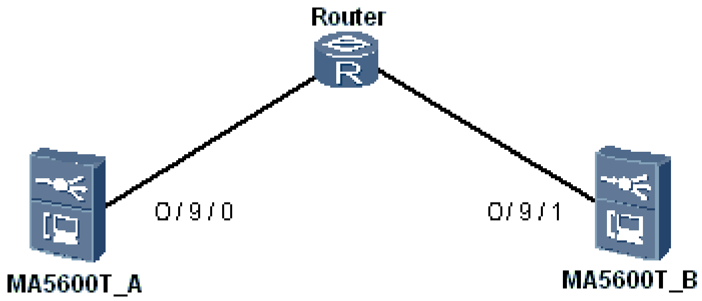
Prerequisites

- The example network as shown in **Figure 16-3** must be complete.
- The network devices and lines must be in the normal state.

Example Network

Figure 16-3 shows the example network of the Ethernet OAM on the OLT. The link between OLT_A and OLT_B uses the Ethernet OAM mechanism to detect link faults. Both OLT_A and OLT_B are configured with a local MEP and a remote MEP. The local MEP ID of OLT_B is the same as the remote MEP ID of OLT_A. The remote MEP ID of OLT_B is the same as the local MEP ID of OLT_A.

Figure 16-3 Example network of the Ethernet OAM



Data Plan

Table 16-1 provides the data plan for the Ethernet OAM on the OLT.

Table 16-1 Data plan for the Ethernet OAM

Item	Data
OLT_A	● Port: 0/9/0; ● Smart VLAN: 100 ● MD Name Format: character string type ● MD Name: MD1 ● Level: 3 ● MA Name Format: character string type ● MA Name: MA1 ● Remote MEP check: Enable ● Associated VLAN: 100 ● MEP ID: 2 ● Interface Direction: DOWN ● CCM and LTM Priority: 7 ● Administrative Status: enable ● CC Sending Status: enable ● Alarm Waiting Time: 2500 ● Alarm Recovery Time: 10000
OLT_B	● Port: 0/9/1; ● Smart VLAN: 100 ● MD Name Format: character string type ● MD Name: MD1 ● Level: 3 ● MA Name Format: character string type ● MA Name: MA1 ● Remote MEP check: Enable ● Associated VLAN: 100 ● MEP ID: 2 ● Interface Direction: UP ● CCM and LTM Priority: 7 ● Administrative Status: enable ● CC Sending Status: enable ● Alarm Waiting Time: 2500 ● Alarm Recovery Time: 10000

NOTE

- Configure the remote MEP of OLT_A on OLT_B in the same way as configuring the MEP of OLT_A.
- This topic considers the configuration on OLT_A as an example.

Procedure

Step 1 Add a VLAN and configure the upstream port of the VLAN.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. Choose **VLAN** from the navigation tree.
3. Right-click in the list and choose **Add** from the shortcut menu. In the dialog box that is displayed, set the related parameters as follows:
   - VLAN ID: 100
   - Type: Smart VLAN
   - Attribute: Common
4. Click **Next** and select port **0/9/0** as the upstream port. Click **Done**.

Step 2 Configure the MD.

1. Choose **ETH OAM** from the navigation tree.
2. Click the **Maintenance Domain** tab, and set the filter criteria to display the required MDs.
3. Right-click in the list and choose **Add** from the shortcut menu.
4. In the dialog box that is displayed, set the device name and the name format, name, and level of the MD as follows, and then click **OK**.
   - MD name format: character string type
   - MD name: MD1
   - Level: 3

Step 3 Configure the MA.

1. Click the **Maintenance Association** tab, and set the filter criteria to display the required MAs.
2. Right-click in the list and choose **Add** from the shortcut menu.
3. In the dialog box that is displayed, set the name format, name and associated VLAN of the MA as follows, and then click **OK**.
   - MD name: MD1
   - MA name format: character string type
   - MA name: MA1
4. Right-click the added MA1 and choose **Configure** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters as follows and click **OK**.
   - Remote MEP check: Enable
   - Associated VLAN: 100

Step 4 Configure the MEP ID.

1. Click the **Maintenance Association** tab, set the filter criteria to display the records.

2. Select the added MA1 and click the **MEP ID Info** tab in the lower pane. Right-click in the list and choose **Add** from the shortcut menu.
3. In the dialog box that is displayed, set **MEP ID** to **2**.

Step 5 Configure the MEP.

1. Click the **Maintenance End Point** tab, and select the required device type from the **Device Type** drop-down list.
2. Right-click in the list and choose **Add** from the shortcut menu.
3. In the dialog box that is displayed, set the name of the MA, the name and identifier of the MEP, the port information, and the port direction as follows, and then click **OK**.
   - MEP ID: 2
   - Interface Info: **0/9/0**
   - Interface Direction: UP
   - CCM and LTM Priority: 7
4. Right-click the added MEP1 and choose **Configure** from the shortcut menu.
5. In the dialog box that is displayed, set the parameters as follows and click **OK**.
   - Administrative Status: enable
   - CCM and LTM Priority: 7
   - CC Sending Status: enable
   - Alarm Waiting Time: 2500
   - Alarm Recovery Time: 10000

Step 6 Enable the global CFM function.

1. In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.
2. On the tab page that is displayed, choose **NE Properties** > **Protocol** > **ETH OAM** from the navigation tree.
3. Enable **Global remote MEP test** and **Global CFM switch**.
4. Click **Apply**.

----End

Result

After successful configuration, you can query the statistics of the packets on OLT_A or OLT_B. The number of the transmitted CCM packets and the number of the received CCM packets are not zero.

16.2 Configuring the BFD Network Monitoring

The bidirectional forwarding detection (BFD) is used to test the link status between two devices quickly. When the main channel is faulty, the OLT can switch the service to the standby channel, and thus to increase the reliability of the service and the inband maintenance channel.

16.2.1 Introduction to BFD

The bidirectional forwarding detection (BFD) is used to detect the link status between two devices quickly. When the main channel is faulty, the OLT switches the service to the standby channel, and thus to increase the reliability of the service and the inband maintenance channel.

Prerequisites

The VLAN is set up. For details, see **4.1.2.2 Adding a VLAN**.

Context

- Currently, BFD only supports the detection of the static route faults.
- Up to 32 BFD sessions are supported.
- When the route is bound to a BFD, select the link according to the status of the BFD and the priority of the route; when the route is not bound to a BFD, select the link only according to the priority of the route.
- To avoid the route switching to the route with higher priority but not bound to a BFD, if there is another route bound to the BFD going to the same destination, you must reduce the priority of the route that is not bound to the BFD before unbinding the route from the port.

16.2.2 Setting BFD Parameters

The device can handle the BFD protocols and you can configure the BFD functions only after the global BFD function is enabled.

Procedure

Step 1 Choose **Configuration** > **Access Profile Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Access Service** > **Access Profile Management** from the main menu (application style).

Step 2 In the dialog box that is displayed, choose **System Parameter Profile** from the navigation tree.

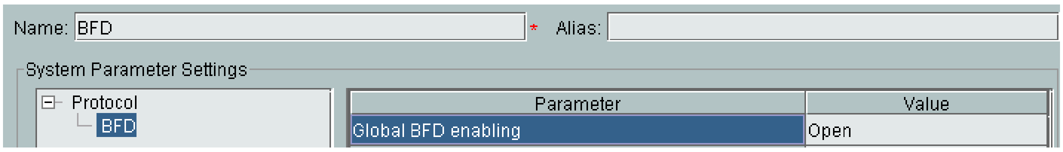
Step 3 On the **System Parameter Profile** tab page, select the required device type from the **Device Type** drop-down list.

Step 4 In the information list, right-click and choose **Add Global Profile** from the shortcut menu.

Step 5 In the dialog box that is displayed, enter the name of the system parameter profile. Choose needed parameters from the **Parameters for Selection** navigation tree, click > to add the parameters to the **Selected Parameters** navigation tree, and then click **Next**.

Step 6 In the dialog box that is displayed, set the name of the system parameter profile and choose **Protocol** > **BFD** from the **System Parameter Settings** navigation tree.

Step 7 In the right pane, set **Global BFD enabling** to **Open**.



Name: BFD *
Alias:

Parameter	Value
Global BFD enabling	Open

Step 8 Click **Finish**.

Step 9 Select the system parameter profile, right-click, and then choose **Download to NE**.

Step 10 In the dialog box that is displayed, select a device to which the profile is to be applied, and then click **OK**.

----End

16.2.3 Setting the BFD Session Parameters

Before the detection of the link fault, the BFD session between the two ends of the channel need to be set up and the peer IP address need to be bound to the local VLAN.

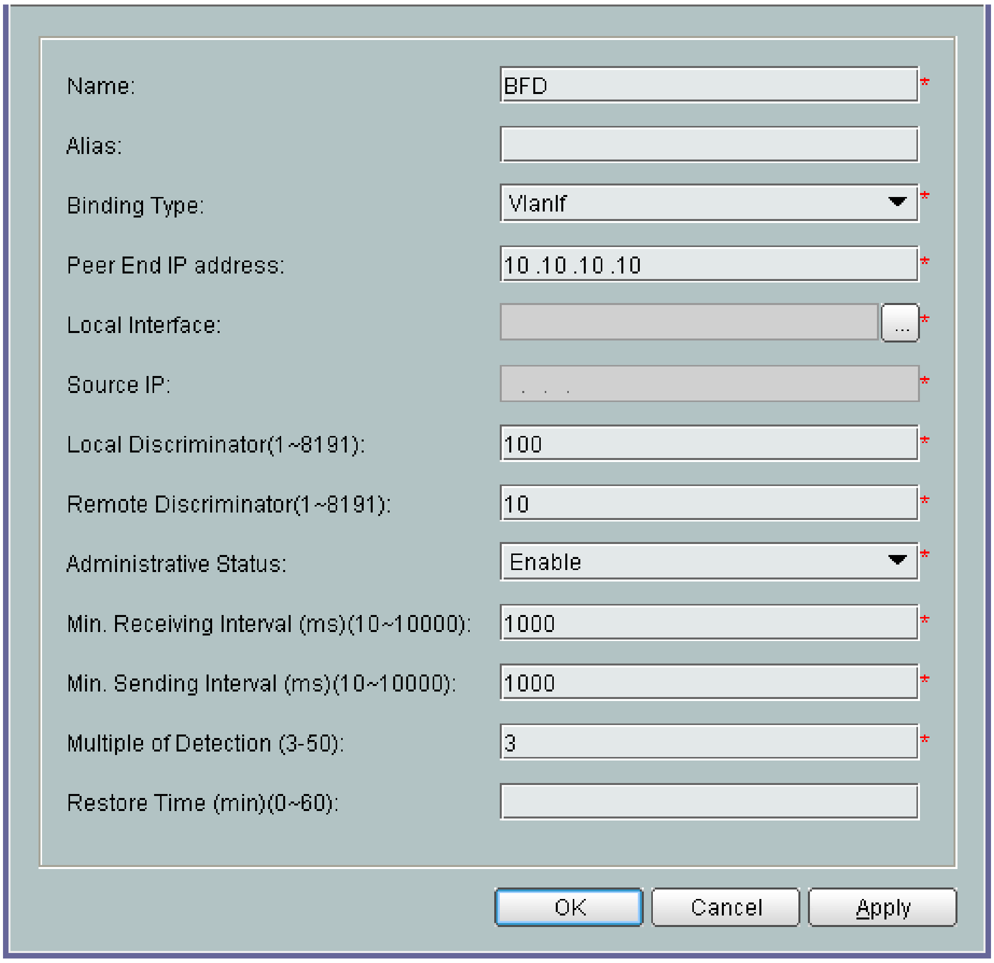
Procedure

Step 1 In the Main Topology, double-click the required NE and choose **NE Explorer** from the shortcut menu.

Step 2 Choose **Protocol** > **BFD** from the navigation tree.

Step 3 In the information list, right-click and choose **Add** from the shortcut menu.

Step 4 In the dialog box that is displayed, set the BFD session parameters.



Name: BFD *
Alias:
Binding Type: VlanIf *
Peer End IP address: 10 .10 .10 .10 *
Local Interface: *
Source IP: . . . *
Local Discriminator(1~8191): 100 *
Remote Discriminator(1~8191): 10 *
Administrative Status: Enable *
Min. Receiving Interval (ms)(10~10000): 1000 *
Min. Sending Interval (ms)(10~10000): 1000 *
Multiple of Detection (3-50): 3 *
Restore Time (min)(0~60):

Step 5 Click **OK**.

----End

17 Remote Maintenance Guide

About This Chapter

This topic describes the tasks of maintaining the OLT software through the U2000, and the reference standard, operation guide, exception handling, and command reference of the tasks.

17.1 Monitoring Critical and Major Alarms of NEs
It is recommended that you check whether unhandled critical and major alarms persist in the system every day. This operation helps timely detect and solve the problems that may occur when the NEs are running.

17.2 Measuring the CPU Usage of a Board
It is recommended that you measure the CPU usage rat of each board once ever week to rectify the fault of the board whose CPU usage is not in the normal range. This helps you to learn the running status of the boards in time, rectify the capacity fault, and prevent the potential security risks (such as the DoS attack) during the running of the boards.

17.3 Measuring the Performance of an Upstream Ethernet Port
It is recommended that you measure the performance of the upstream Ethernet port once every week. This operation ensures that the services on the upstream Ethernet port are normal and reliable.

17.4 Measuring the Usage of NE Resources
This topic describes how to measure the resource usage of the NE. You can query the NE information, such as the number, software version, type, MAC address, physical location, and running status.

17.5 Checking the NE User Level
It is recommended that you check whether the allocation of the level of the user who configures NEs is correct once every month. This operation ensures that the allocated user level can be the same as the user level that is planned and deployed, and that the user level meets the requirement of NE maintenance.

17.6 Changing the Password of an NE User
To ensure the security of an account, it is recommended that you change the password of an NE user periodically instead of using the same password for a long period during maintenance.

17.7 Saving, Backing Up, and Restoring NE Data
The topic describes how to save and back up NE data and restore NE data when an NE fails to be upgraded. NE data may be lost upon an NE malfunction, upgrade, or downgrade. To prevent

data loss, you need to back up NE data (or NE configuration) to the NE Software Management server or client. In this manner, you can restore NE data from the backup files if required.

17.1 Monitoring Critical and Major Alarms of NEs

It is recommended that you check whether unhandled critical and major alarms persist in the system every day. This operation helps timely detect and solve the problems that may occur when the NEs are running.

Prerequisites

The hardware for monitoring NE alarms must be configured, such as an environment monitoring unit (EMU) and sensors.

Context

- Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Browse Current Alarm** from the main menu (application style).Then, the required alarm information is displayed after setting the default profile. For information on how to set and change the default profile, see Setting the Default Profile.
- You can set the policies for defining alarms according to the extent that the alarms are concerned and the actual requirement, including setting alarm names, function classifications, and alarm severity. For details, see Configuring the Policy of Redefining Alarms and Events.
- A great number of alarms may be generated during the repair, test, and deployment of devices. In this case, you can mask the alarms that are irrelevant. In this manner, the alarms are not displayed or saved on the U2000. For details, see Configuring the Policy of Masking Alarms and Events.

Reference Standard

You can determine the alarm severity according to colors of the alarm legends. Generally, the critical and major alarms should not persist in the system. The following table lists the alarm legends and provides the meanings of the legends.

Legend	Color	Alarm Severity
Critical	Red	Critical
Major	Orange	Major
Minor	Yellow	Minor
Warning	Blue	Warning

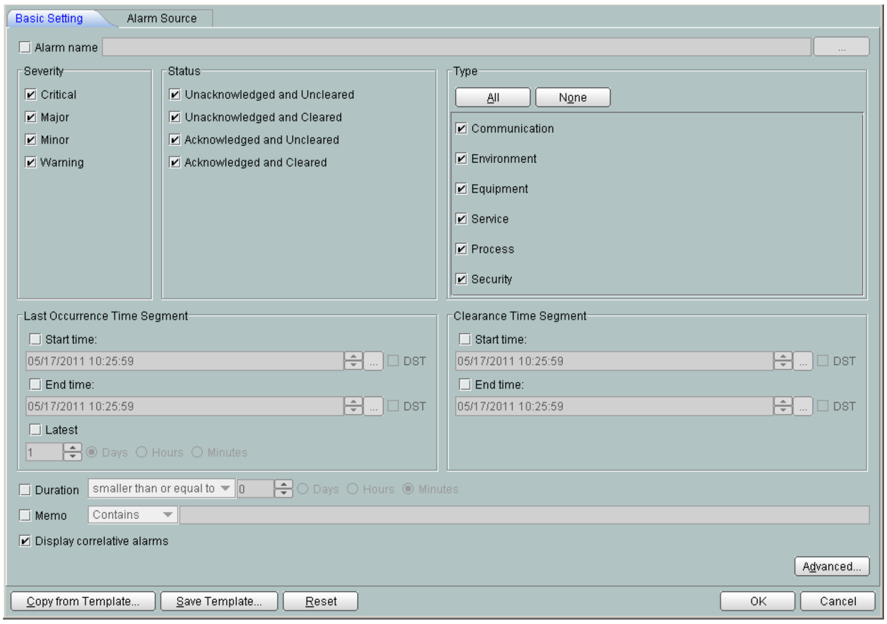
Procedure

Step 1 Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Browse Current Alarm** from the main menu (application style). Then, the **Filter** dialog box is displayed.

NOTE

- If you already set the default template for the current alarms, the alarms that meet the default template criteria are directly displayed, without the displaying of the **Filter** dialog box.
- You can choose **Template** > **New** in the lower pane to create an alarm profile and set the device alarm parameters. You can also choose **Template** > **Open** to query the device alarms by selecting the new alarm profile.

Step 2 On the **Basic Setting** tab, set the parameters required for querying alarms, such as the alarm name, severity, status, and type. These parameters are optional.



☐ Alarm name

Severity
☑ Critical
☑ Major
☑ Minor
☑ Warning

Status
☑ Unacknowledged and Uncleared
☑ Unacknowledged and Cleared
☑ Acknowledged and Uncleared
☑ Acknowledged and Cleared

Type
☑ Communication
☑ Environment
☑ Equipment
☑ Service
☑ Process
☑ Security

Last Occurrence Time Segment
☐ Start time: 05/17/2011 10:25:59 ☐ DST
☐ End time: 05/17/2011 10:25:59 ☐ DST
☐ Latest 1 ● Days ○ Hours ○ Minutes

Clearance Time Segment
☐ Start time: 05/17/2011 10:25:59 ☐ DST
☐ End time: 05/17/2011 10:25:59 ☐ DST

☐ Duration smaller than or equal to 0 ○ Days ○ Hours ● Minutes
☐ Memo Contains
☑ Display correlative alarms

Step 3 On the **Alarm Source** tab, set the alarm source information for querying alarms. In the **Select Mode** area, set the mode for filtering alarms.

- If **All objects** is selected, it indicates that alarms are not filtered and all alarms of the alarm source are queried.
- If **Custom** is selected, click **Add** to filter the concerned alarm source according to **Object below NE** and **Object Group**.

Step 4 Click **OK** to display the required critical and major alarms.

----End

Exception Handling

- Select a fault alarm that is not recovered. The alarm information is displayed in **Alarm Details** in the lower pane and the cause of the alarm and handling suggestions are displayed in **Handling Suggestion**. Handle the alarm according to the suggestions. Click **Click here to show detail Information** under **Handling Suggestion** to display the related alarm reference topic in the *U2000 Help*. You can learn the alarm impact, alarm cause, handling procedures through the topic.
- Record the critical alarms that occur frequently at recent time and their recovery information. Handle the alarms according to the cause and handling suggestions, and analyze potential risks that may exist in the system.

- If the fault persists, contact Huawei technical support engineers. For details, see How to Obtain Technical Support from Huawei.

NOTE

For an alarm that is handled successfully, it is recommended that you record the detailed handling measures, which helps locate and troubleshoot the similar faults that occur. To enter the maintenance experience, select the alarm, right-click, and then choose **Experience**.

Related Commands

To...	Run the Command...	In...
Query the alarm history	**display alarm history**	User mode
Query the basic information about alarms	**display alarm list**	User mode
Query the alarm configuration	**display alarm configuration**	User mode
Query the alarm statistics	**display alarm statistics**	User mode
Query the information about the existing alarms in the system	**display alarm active**	Privilege mode

17.2 Measuring the CPU Usage of a Board

It is recommended that you measure the CPU usage rat of each board once ever week to rectify the fault of the board whose CPU usage is not in the normal range. This helps you to learn the running status of the boards in time, rectify the capacity fault, and prevent the potential security risks (such as the DoS attack) during the running of the boards.

Prerequisites

- You must have Create a Performance Measurement Task.
- If the attributes of NE resources change, you need to perform synchronize to keep the data of the NE and performance management module the same and then perform query . Otherwise , the collection of performance data is abnormal. The procedure of synchronizing information is as follows:

1. On the **Main Topology** tab, select an NE from the **Physical Root** navigation tree, right-click, and then choose **Synchronize NE Data**.
2. Choose **Performance** > **Performance Monitoring Management** from the main menu (traditional style); alternatively, double-click **Fix-Network Performance** in **Application Center** and choose **Performance Monitoring** > **Performance Monitoring Management** from the main menu (application style). In the **Performance Monitoring Management** tab, right-click the monitoring instance, and select **Synchronization Resource**.

Context

Only the control boards and service boards support this operation.

Reference Standard

- The CPU usage ranges from 0% to 100%. The CPU usage of a board that runs normally does not exceed 70%.
- The high CPU usage of a board occurs only when the board data is being written to the flash memory of the control board or is being saved. The high CPU usage usually lasts less than 60s.

Procedure

Step 1 Choose **Performance** > **Browse Historical Performance Data** from the main menu (traditional style); alternatively, double-click **Fix-Network Performance** in **Application Center** and choose **Browse Performance Data** > from the main menu (application style).

Step 2 Click **Resource**. And then configure the **Query Type** to **Resource Name**.

NOTE

If the query profile is created, you can click **Template**.

Step 3 Enter the resource name in the **Resource Name** text box to query.

Step 4 Click **Advanced >>**, to perform advanced query of resources.

Click ... corresponding to the **Resource Type** field. Choose **Performance Management** > **NE** > **Access** > **Card** > **Board Health**.

Step 5 Click **Query** to query the resources.

Step 6 In the **Available Resources** area, click ↓, to move the resources to the **Selected Resources** area.

Step 7 Click **Settings** to select the times and the indexes of the **CPU Occupancy Profile** index group.

Step 8 Click **OK** to get the performance data based on the filter conditions set for one graph one resource.

Step 9 Select the display mode as line chart, bar chart, or table from the drop-down list.

Step 10 Click **Print** to print the graph results.

Step 11 Click **Save** to save the queried performance data.

----End

Copyright © Huawei Technologies Co., Ltd.

Exception Handling

- If the CPU usage of a board is temporarily over-high, there is no need to proceed.
- If the CPU usage of a board is frequently over-high, check the following items:
  - Whether the data configuration of the device is proper. If the data configuration is improper, it is recommended that you decrease the number of users or increase the capacity of the system.
  - Whether the networking is proper and whether a larger number of broadcast packets are generated due to the existing loop networks.
  - Whether the DoS attack exists, which may lead to the high CPU usage. The solution is to enable the anti-DoS attack function.
- If the fault persists, contact Huawei technical support engineers. For details, see How to Obtain Technical Support from Huawei.

Related Commands

To...	Run the Command...	In...
Query the CPU usage of a board	**display cpu**	Privilege mode

17.3 Measuring the Performance of an Upstream Ethernet Port

It is recommended that you measure the performance of the upstream Ethernet port once every week. This operation ensures that the services on the upstream Ethernet port are normal and reliable.

Prerequisites

- You must have Create a Performance Measurement Task.
- If the attributes of NE resources change, you need to perform synchronize to keep the data of the NE and performance management module the same and then perform query . Otherwise , the collection of performance data is abnormal. The procedure of synchronizing information is as follows:
  1. On the **Main Topology** tab, select an NE from the **Physical Root** navigation tree, right-click, and then choose **Synchronize NE Data**.
  2. Choose **Performance** > **Performance Monitoring Management** from the main menu (traditional style); alternatively, double-click **Fix-Network Performance** in **Application Center** and choose **Performance Monitoring** > **Performance Monitoring Management** from the main menu (application style). In the **Performance Monitoring Management** tab, right-click the monitoring instance, and select **Synchronization Resource**.

Reference Standard

In the statistics of the upstream Ethernet port, a small number of frames with cyclical redundancy check (CRC) errors and a few packet loss errors exist and the traffic transmission is stable.

Procedure

Step 1 Choose **Performance** > **Browse Historical Performance Data** from the main menu (traditional style); alternatively, double-click **Fix-Network Performance** in **Application Center** and choose **Browse Performance Data** > from the main menu (application style).

Step 2 Click **Query**. The dialog is displayed. The resources and the corresponding indicators associated with the selected resources is displayed.

NOTE

If the query profile is created, click **Template** > **Open**. In the dialog box that is displayed, select the required profile, and then import the profile to query the performance statistics.

Step 3 Enter the resource name in the **Resource Name** text box to query.

Step 4 Click **Advanced >>**, to perform advanced query of resources.

Click ... corresponding to the **Resource Type** field. Choose **Performance Management** > **NE** > **Access** > **Port** > **Ethernet Port**.

Step 5 Click **Query** to query the resources.

Step 6 In the **Available Resources** area, click ⬇, to move the resources to the **Selected Resources** area.

Step 7 Click **Settings** to select the times and the indicators.

Step 8 Click **OK** to get the performance data based on the filter conditions set for one graph one resource.

Step 9 Select the display mode as line chart, bar chart, or table from the drop-down list.

Step 10 Click **Print** to print the graph results.

Step 11 Click **Save** to save the queried performance data.

----End

Exception Handling

- If a large number of frames with CRC errors exist or the traffic on an Ethernet port is low in a certain period, check whether the line quality is poor or whether any Ethernet port of the device is faulty.
- If a large number of packets are lost, check whether the traffic suppression function is enabled.
- If the fault persists, replace the port to prevent the communication failure caused by the port fault.
- If the fault persists, contact Huawei technical support engineers. For details, see How to Obtain Technical Support from Huawei.

Related Commands

To...	Run the Command...	In...
Query the statistics of an Ethernet port	**display port statistics**	GIU mode, SCU mode, ETH mode, and OPF mode

17.4 Measuring the Usage of NE Resources

This topic describes how to measure the resource usage of the NE. You can query the NE information, such as the number, software version, type, MAC address, physical location, and running status.

Prerequisites

The NE must be added to the U2000 successfully.

Procedure

Step 1 Choose **Inventory** > **Physical Inventory** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Configuration** in **Application Center** and choose **Inventory** > **Physical Inventory** from the main menu (application style).

Step 2 Click the **By NE Statistics** or **By Subnet Statistics** tab. On the tab page, set the **Statistics Scope** and **Statistics Type** parameters as follows:

1. Click ... next to **Statistics Scope**. In the dialog box that is displayed, select the NE to be measured, and then click **OK**.
2. Select **NE Type**, **Software Version**, **NE Type+Software Version**, or **Customize** from the **Statistics Type** drop-down list.
    - Select **NE Type** from the **Statistics Type** drop-down list. The number of NEs of different types is displayed in the information list in the lower pane.
    - Select **Software Version** from the **Statistics Type** drop-down list. The number of NEs of different software versions is displayed in the information list in the lower pane.
    - Select **NE Type+Software Version** from the **Statistics Type** drop-down list. The number of NEs of different software versions corresponding to different NE types is displayed in the information list in the lower pane.
    - Select **Customize**. In the **Customize NE Statistics Type** dialog box, click **New**. In the **New Customize NE Statistics Type** dialog box, enter the name of the measurement item to be customized in the **Custom Name** text box in the **Customize NE Statistics Type** area. In the **Basic Item** area, select the measurement item to be customized, click > to add the selected measurement item to the **Combined Item** area. Then, click **OK**.

Step 3 Click the **Equivalent NE Statistics** tab. On this tab page, click **Count**. The actual number of NEs and the number of equivalent NEs will be displayed by NE type.

Step 4 Select the required record from the NE list, and then you can perform the following operations:

- Click **Count** to refresh the statistics.
- Choose **Print**. In the dialog box that is displayed, set **Start Row** and **End Row**, and then click **OK** to print the report.
- Choose **Save As**. In the dialog box that is displayed, set **Start Row** and **End Row**, and then click ... next to **File Name**. In the dialog box that is displayed, set **File Name**, **File Type** and **Encoding**, and then click **Save**. Click **OK** in the **Saving Options** dialog box to save the report to the specified path.

  NOTE

  The reports can be saved as .txt, .xls, .html or .xls files.

----End

Command Reference

To...	Run the Command...	In...
Query the details of a board (After performing an operation on a board, you can query the details of the board, such as the slot number, name, status, daughter board information, port information and online status.)	**display board**	User mode

17.5 Checking the NE User Level

It is recommended that you check whether the allocation of the level of the user who configures NEs is correct once every month. This operation ensures that the allocated user level can be the same as the user level that is planned and deployed, and that the user level meets the requirement of NE maintenance.

Context

- A common user can perform basic system operations and simple query operations.
- An operator can perform basic configurations for the device and services.
- An administrator can perform all configurations. The administrator is responsible for maintaining the device, user account, and rights to manage devices.

Reference Standard

The level of the user who configures NEs is the same as the level that is planned and deployed, and can meet the requirement of NE maintenance. The user rights are allocated properly.

Procedure

Step 1 Choose **Administration** > **NE Security Management** > **LCT User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **NE Security** > **Fix-Network NE** > **LCT User Management** from the main menu (application style).

Step 2 In the **LCT User Management** window, click the **NE User** tab.

Step 3 Select the required device type from the **Device Type** drop-down list. The information about all the users of the selected device type is displayed in the list. Then, click **Filter** to display the NE users that meet the filtering criteria.

Step 4 Query the level of the NE user in the **Level** column in the list.

----End

Exception Handling

- If the allocation of the NE user level is improper, right-click the record to be queried in the list on the **NE User** tab, and then select **Configure** to modify the NE user level.

  NOTE

  Only the user with the administrator or higher-level right can modify the NE user level.
- If the fault persists, contact Huawei technical support engineers. For details, see How to Obtain Technical Support from Huawei.

Related Commands

To...	Run the Command...	In...
Query the NE user level	**display terminal user**	User mode
Modify the NE user level	**terminal user level**	Privilege mode

17.6 Changing the Password of an NE User

To ensure the security of an account, it is recommended that you change the password of an NE user periodically instead of using the same password for a long period during maintenance.

Prerequisites

You must be an NMS user with the Security Manager User authority or higher.

Reference Standard

You can log in to an NE by using the new password.

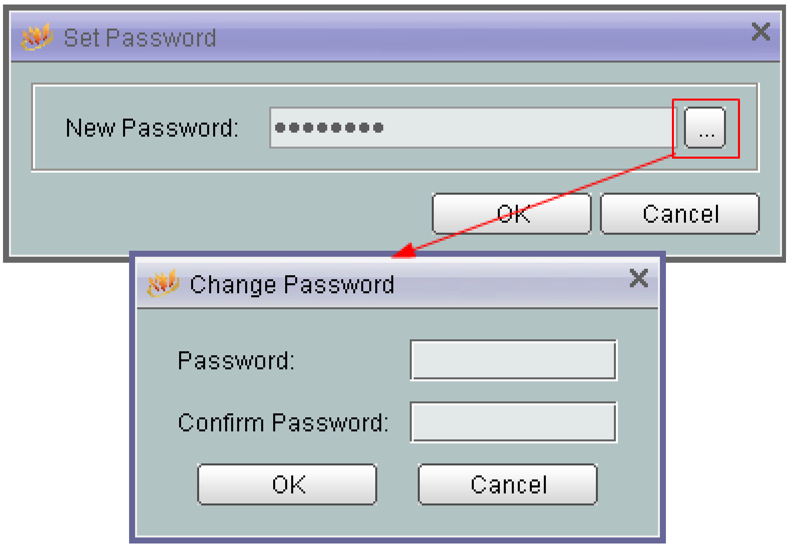
Procedure

Step 1 Choose **Administration** > **NE Security Management** > **LCT User Management** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **NE Security** > **Fix-Network NE** > **LCT User Management** from the main menu (application style).

Step 2 Click the **NE User** tab, and then select the required device type from the **Device Type** drop-down list. All the users on this type of devices are displayed in the user list. Click **Find** to display the required users.

Step 3 Select one or more records from the user list, right-click, and then choose **Set Password**.

Step 4 In the **Set Password** dialog box as shown in the following figure, set a new password.



NOTE

To ensure system security, password must be complex enough. For example, a password must contain eight or more characters of two types. The allowed characters are digits, letters, and special characters. Remember to change passwords regularly.

Step 5 Click **OK**.

----End

Exception Handling

- If the password fails to be changed, the U2000 displays a message indicating the failure. In this case, check whether the password is correct according to the message.
- If the problem persists, contact Huawei technical support engineers. For information on how to contact Huawei technical support engineers, see How to Obtain Technical Support from Huawei.

Related Commands

To...	Run the Command...	In...
Change the password of an NE user	**terminal user password**	Privilege mode

17.7 Saving, Backing Up, and Restoring NE Data

The topic describes how to save and back up NE data and restore NE data when an NE fails to be upgraded. NE data may be lost upon an NE malfunction, upgrade, or downgrade. To prevent data loss, you need to back up NE data (or NE configuration) to the NE Software Management server or client. In this manner, you can restore NE data from the backup files if required.

17.7.1 Saving and Backing Up the NE Data Periodically

The DC saves and backs up data periodically according to the default policy or user-defined policy and thus helps to restore and load the data in future.

17.7.1.1 Saving and Backing Up the NE Data by Using the Default Policy

This topic describes how to save and back up the NE data periodically by using the default policy. Hence, you can save and back up the NE data at a fixed time, which facilitates the restoring and loading of the NE data.

The backup has certain impact on the running rate of the NE. Therefore, it is recommended that you back up the NE data when the NE carries minimum traffic, for example, at 2:00 a.m.

- The **DCServer** process runs in the normal state.
- The communication between the NE and the U2000 must be in the normal state.
- Related xFTP settings have been configured. To obtain the configuration instructions, choose **Administration** > **NMS Commissioning Wizard** from the main menu and then select **NMS Communication with NEs** from the navigation tree.

The backup/save policy that runs on an NE by default is the default policy.

Procedure

Step 1 Choose **Administration** > **NE Software Management** > **NE Backup Policy Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Software Management** in **Application Center** and choose **NE Software Management** > **NE Backup Policy Management** from the main menu (application style).

Step 2 Click the **Auto Backup Policy** tab, and choose **All Policy** > **Default Policy** from the navigation tree.

Operation	Procedure
View Policy	Right-click a policy and choose **View Policy** from the shortcut menu. In the dialog box that is displayed, view the policy information.

Operation	Procedure
Modify Policy	Right-click a policy and choose **Modify Policy** from the navigation tree. In the dialog box that is displayed, modify the policy information. NOTE ● The information about the NEs involved in the default policy cannot be modified. ● The name of the default policy cannot be modified. ● For the descriptions and settings of the parameters on **Advanced Settings**, see Setting Backup Attributes.
Enable Backup/ Save Policy	After the backup/save policy is enabled, the DC will back up and save the NE data at the specified time. ● **Enable the backup/save policy of all involved NEs** Right-click a policy in the navigation tree and choose **Enable Backup Policy** or **Enable Save Policy** from the shortcut menu. ● **Enable the backup/save policy of certain involved NEs** – Select the required NE type from the **NE Type** drop-down list. – In the NE list, select one or more NEs, right-click, and then choose **Enable Backup Policy** or **Enable Save Policy** from the shortcut menu.
Disable Backup/ Save Policy	After you disable the backup/save policy, the DC does not back up or save NE data even if the policy period reaches the specified time. ● **Disable the backup/save policy of all involved NEs** Right-click a policy in the navigation tree and choose **Disable Backup Policy** or **Disable Save Policy** from the shortcut menu. ● **Disable the backup/save policy of certain involved NEs** – Select the required NE type from the **NE Type** drop-down list. – In the NE list, select one or more NEs, right-click, and then choose **Disable Backup Policy** or **Disable Save Policy** from the shortcut menu.

Operation	Procedure
Move to Other Policy	After an NE is moved from the original policy to the target policy, the policy of the NE is changed to the target policy. By doing so, the backup/ save policy of an NE can be changed quickly. ● **Move all NEs involved in a policy to another policy.** 1. Right-click a policy in the navigation tree and choose **Move to Other Policy** from the shortcut menu. 2. Select the target policy and click **OK**. NOTE The default policy of the NEs is not deleted after you perform this operation. ● **Move certain NEs involved in a policy to another policy** – Select the required NE type from the **NE Type** drop-down list. – In the NE list, select one or more NEs, right-click, and then choose **Move to Other Policy** from the shortcut menu. – Select the target policy and click **OK**.
Export Policy	You can save the policy to the local computer so that you can view the policy at any time. 1. Select the required NE type from the **NE Type** drop-down list. 2. In the NE list, select one or more NEs, right-click, and then choose **Export Policy** from the shortcut menu. 3. In the dialog box that is displayed, set the parameters for saving the policy. NOTE ● You can save a policy to a .TXT, an .HTML, or a .CSV file. ● The default path for storing the policy is **\client\report**.

----End

To...	Run the Command...	In...
Configure the conditional backup function of the automatic backup	**auto-backup condition**	Global config mode
Configure the periodical backup function of the automatic backup	**auto-backup period**	Global config mode

17.7.1.2 Saving and Backing Up the NE Data by Using the Customized Policy

This topic describes how to save and back up the NE data periodically by using the customized policy. Hence, you can save and back up the required NE data at a fixed time, which facilitates the restoring and loading of the NE data.

The backup has certain impact on the running rate of the NE, therefore, it is recommended that you back up the NE data when the NE carries minimum traffic, for example, at 2:00 a.m.

- The **DCServer** process runs in the normal state.
- The communication between the NE and the U2000 must be in the normal state.
- Related xFTP settings have been configured. To obtain the configuration instructions, choose **Administration** > **NMS Commissioning Wizard** from the main menu and then select **NMS Communication with NEs** from the navigation tree.

You can configure the save and backup policies for a single NE or for multiple NEs simultaneously.

Procedure

Step 1 Choose **Administration** > **NE Software Management** > **NE Backup Policy Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Software Management** in **Application Center** and choose **NE Software Management** > **NE Backup Policy Management** from the main menu (application style).

Step 2 Click the **Auto Backup Policy** tab, right-click in the policy navigation tree, and then choose **New Policy** from the shortcut menu.

Step 3 Select the NE type and NE version to be configured with the save and backup policies as required.

1. Select the required NE type from the **NE Type** drop-down list.
2. **Optional:** Select the required NE version from the **NE Version** drop-down list.
3. Choose one or more NEs to be configured with the save and backup policies from the navigation tree under the **NE Version** drop-down list.

Step 4 Click **Next** and the **Setting Policy[Create Policy]** dialog box is displayed.

Step 5 Set the policy parameters as required.

NOTE

- If you set **The Added NE's Policy Status** to **Run**, the DC backs up and saves the data of the new NE (that is moved from another policy) at the specified time.
- If you set **The Added NE's Policy Status** to **Stop**, the DC does not back up or save the data of the new NE even if the policy period reaches the specified time.
- For the descriptions and settings of the parameters on **Advanced Settings**, see Setting Backup Attributes.

Step 6 Click **OK** to complete the configurations of the save and backup policies.

Step 7 Choose a new policy from the policy navigation tree and perform other operations as required.

Operation	Procedures
View Policy	Right-click a policy and choose **View Policy** from the shortcut menu. In the dialog box that is displayed, view the policy information.

Operation	Procedures
Modify Policy	1. Right-click a policy and choose **Modify Policy** from the shortcut menu. 2. In the **Select NE[Create Policy]** dialog box, modify the NE information involved in the policy. a. Select the required NE type from the **NE Type** drop-down list. b. **Optional:** Select the required NE version from the **NE Version** drop-down list. c. Choose one or more NEs to be configured with the save and backup policies from the navigation tree under the **NE Version** drop-down list. 3. Click **Next**. In the **Setting Policy[Create Policy]** dialog box, set the policy parameters as required. NOTE ● If you set **The Added NE's Policy Status** to **Run**, the DC backs up and saves the data of the new NE (that is moved from another policy) at the specified time. ● If you set **The Added NE's Policy Status** to **Stop**, the DC does not back up or save the data of the new NE even if the policy period reaches the specified time. ● For the descriptions and settings of the parameters on **Advanced Settings**, see Setting Backup Attributes.
Enable Backup/ Save Policy	After the backup/save policy is enabled, the DC will back up and save the NE data at the specified time. ● **Enable the backup/save policy of all involved NEs** Right-click a policy in the navigation tree and choose **Enable Backup Policy** or **Enable Save Policy** from the shortcut menu. ● **Enable the backup/save policy of certain involved NEs** – Select the required NE type from the **NE Type** drop-down list. – In the NE list, select one or more NEs, right-click, and then choose **Enable Backup Policy** or **Enable Save Policy** from the shortcut menu.
Disable Backup/ Save Policy	After you disable the backup/save policy, the DC does not back up or save NE data even if the policy period reaches the specified time. ● **Disable the backup/save policy of all involved NEs** Right-click a policy in the navigation tree and choose **Disable Backup Policy** or **Disable Save Policy** from the shortcut menu. ● **Disable the backup/save policy of certain involved NEs** – Select the required NE type from the **NE Type** drop-down list. – In the NE list, select one or more NEs, right-click, and then choose **Disable Backup Policy** or **Disable Save Policy** from the shortcut menu.

Operation	**Procedures**
Move to Other Policy	After an NE is moved from the original policy to the target policy, the policy of the NE is changed to the target policy. By doing so, the backup/save policy of an NE can be changed quickly. ● **Move all NEs involved in a policy to another policy.** 1. Right-click a policy in the navigation tree and choose **Move to Other Policy** from the shortcut menu. 2. Select the target policy and click **OK**. NOTE The policy of the NEs is deleted after you perform this operation. ● **Move certain NEs involved in a policy to another policy** - Select the required NE type from the **NE Type** drop-down list. - In the NE list, select one or more NEs, right-click, and then choose **Move to Other Policy** from the shortcut menu. - Select the target policy and click **OK**.
Export Policy	You can save the policy to the local computer so that you can view the policy at any time. 1. Select the required NE type from the **NE Type** drop-down list. 2. In the NE list, select one or more NEs, right-click, and then choose **Export Policy** from the shortcut menu. 3. In the dialog box that is displayed, set the parameters for saving the policy. NOTE ● You can save a policy to a .TXT, an .HTML, and a .CSV file. ● The default path for storing the policy is **\client\report**.

----End

To.	**Run the Command...**	**In...**
Configure the conditional backup function of the automatic backup	**auto-backup condition**	Global config mode
Configure the periodical backup function of the automatic backup	**auto-backup period**	Global config mode

17.7.2 Saving and Backing Up NE Data Immediately

The DC can save and back up NE data periodically or immediately to meet the requirements in different scenarios.

17.7.2.1 Saving the NE Data Immediately

The process of saving NE data is to save the new NE data from the memory of the new NE to the flash memory. When the files in the flash memory need to be backed up, the operation of saving new NE data must be performed first.

Prerequisites

- The communication between the NE and the U2000 must be in the normal state.
- The **DCServer** process runs in the normal state.

Context

Do not perform this operation on different types of NEs at the same time.

The manual saving task cannot be interrupted after it is started.

Procedure

Step 1 Choose **Administration** > **NE Software Management** > **NE Data Backup/Restoration** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Software Management** in **Application Center** and choose **NE Software Management** > **NE Data Backup/Restoration** from the main menu (application style).

Step 2 Click ▭, and expand the OLT NE node from the NE navigation tree.

- If a certain NE type is selected, all the NEs of this type are displayed in the NE list in the **NE View** window in the right pane.
- If a NE version is selected in a certain NE type node, all the NEs of this version are displayed in the NE list in the **NE View** window in the right pane.

Step 3 **Optional:** To locate a specific NE, click **Find** in the **NE View** window in the right pane.

Step 4 Select one or multiple records from the NE list in the **NE View** window in the right pane, right-click, and then choose **Save**.

Step 5 In the dialog box that is displayed, select one or multiple records need to be saved, and then click **Start** to save the NE data.

Step 6 The saving process and the operation results are displayed in the **Operation Status** of the list.

----End

Related Commands

To...	Run the Command...	In...
Save the current database file and configuration file of the system	**save**	Privilege mode

Copyright © Huawei Technologies Co., Ltd.

To...	Run the Command...	In...
Save the current database file of the system	**save data**	Privilege mode
Save the current configuration file of the system	**save configuration**	Privilege mode

17.7.2.2 Backing Up the NE Data Immediately

This topic describes how to manually back up NE data. When maintaining, upgrading, or downgrading an NE, you need to back up the data of the NE to the U2000 server or client to prevent loss of or damage to the NE data due to upgrade or downgrade or exceptions.

Impact on the System

The backup has certain impact on the running rate of the NE. Therefore, it is recommended that you back up the NE data when the device carries minimum traffic, for example, at 2:00 a.m.

Prerequisites

- The **DCServer** process runs in the normal state.
- The communication between the device and the U2000 must be in the normal state.
- Related xFTP settings have been configured. To obtain the configuration instructions, choose **Administration** > **NMS Commissioning Wizard** from the main menu and then select **NMS Communication with NEs** from the navigation tree.
- When you back up NE data to the U2000 client, ensure that files can be transferred between the client and the server successfully by means of the FTP or SFTP protocol (by default, the SFTP protocol is used).

Context

If you back up NE data to the NE Software Management server, the **backup** directory is created automatically in the file transfer root directory. The backup NE data is transferred to the **backup** directory by means of the FTP/SFTP protocol.

The data of the NEs of different types can be backed up at the same time.

After a manual backup task is started, it cannot be stopped.

Procedure

Step 1 Choose **Administration** > **NE Software Management** > **NE Data Backup/Restoration** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Software Management** in **Application Center** and choose **NE Software Management** > **NE Data Backup/Restoration** from the main menu (application style).

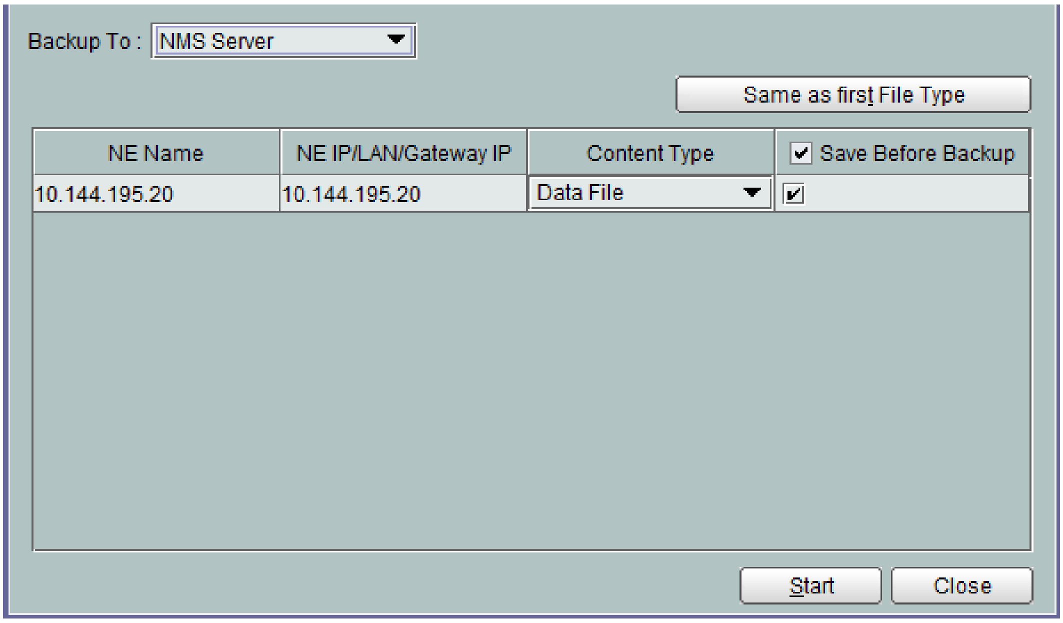
Step 2 Click ⌨, and expand the OLT NE node from the NE navigation tree.

- If a certain NE type is selected, all the NEs of this type are displayed in the NE list in the **NE View** window in the right pane.
- If a NE version is selected in a certain NE type node, all the NEs of this version are displayed in the NE list in the **NE View** window in the right pane.

Step 3 **Optional:** To locate a specific NE, click **Find** in the **NE View** window in the right pane.

Step 4 Select one or more records from the NE list in the **NE View** window in the right pane, right-click, and then choose **Backup** or click **Backup** in the lower pane.

Step 5 In the dialog box as shown in the following figure, set the parameters related to backing up the NE data immediately.



Backup To : NMS Server

NE Name	NE IP/LAN/Gateway IP	Content Type	☑ Save Before Backup
10.144.195.20	10.144.195.20	Data File	☑

NOTE

- **NMS Server**: Back up the NE data to the backup folder in the file transfer root directory on the NMS server.
- **NMS Client**: Click ... to select the path on the NMS client for saving the backup NE data.
- **Save Before Backup**: If you select the **Save Before Backup** check box, the running data in the memory of the NE is save to the flash memory to ensure that the backup NE data in the flash memory is the latest (that is, the same as the current running data of the NE).

Step 6 Click **Start** to back up the NE data.

Step 7 The backup process and the operation results are displayed in the **Operation Status** of the list. If the backup is successful, the information about the backup file is displayed on the **Backup Information** tab.

----End

Related Commands

To...	Run the Command...	In...
Back up the database file manually	**backup data**	Privilege mode
Back up the configuration file manually	**backup configuration**	Privilege mode
Back up the data to the backup server manually	**auto-backup manual**	Global config mode

17.7.3 Checking the Backup of the NE Configuration Data

It is recommended that you check whether the NE configuration data is backed up successfully once every week. This operation helps you to restore the recent system data in time in the case that an unexpected fault occurs in the system. Thus, the impact on users is minimized.

Prerequisites

The parameters for periodically backing up the NE data must be set.

NOTE

After the backup policy is configured successfully, you need not manually back up data every day and need only to check the backup once every week.

Context

- The OLT supports the saving and backing up of the database file. This ensures that the system can be restored in the case that an unexpected fault occurs in the system. For information on how to restore the NE data, see **Restoring the NE Data Immediately**.
- The U2000 supports the function of transferring the database file of the OLT in the FTP/SFTP mode. To back up the data, you can upload the file saved on the OLT to a specified file server. To restore the data, you can download the file saved on the specified file server to the OLT. Using SFTP is recommended because of its higher security than FTP.

Reference Standard

No backup failure is recorded in the log, and the backup database file exists in the specified path.

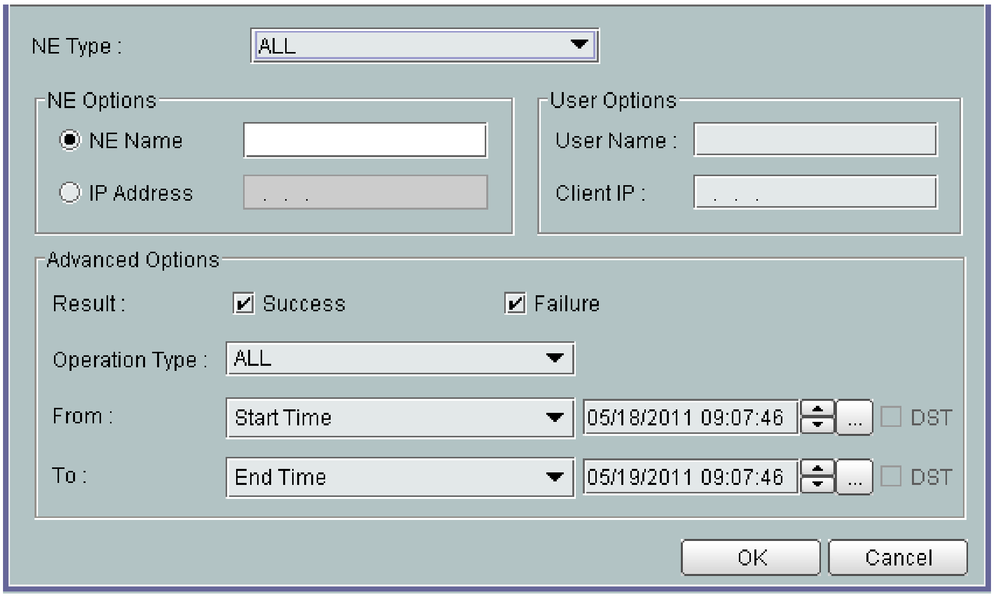
Procedure

Step 1 Choose **Administration** > **NE Software Management** > **NE Software Log Management** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Software**

Management in **Application Center** and choose **NE Software Management** > **NE Software Log Management** from the main menu (application style).

Step 2 In the **NE Software Log Management** window, click **Filter**. The **Filter Log** dialog box is displayed.

Step 3 In the **Filter Log** dialog box, select **Backup** from the **Operation Type** drop-down list, and then set other filtering criteria to display the required log that records backup operations (the filtering criteria items are optional), as shown in the following figure.



NE Type : ALL

NE Options
● NE Name
○ IP Address . . .

User Options
User Name :
Client IP : . . .

Advanced Options
Result : ☑ Success ☑ Failure
Operation Type : ALL
From : Start Time 05/18/2011 09:07:46 ☐ DST
To : End Time 05/19/2011 09:07:46 ☐ DST

Step 4 Click **OK**. The information about the backup operation logs is displayed in the information list. You can determine whether the database is backed up successfully by viewing the **Result** column in the information list. If **Success** is displayed in the **Result** column, view the directory for saving backup files in the **File Path** column.

----End

Exception Handling

- If **Failure** is displayed in the **Result** column, take measures according to the information displayed in the **Details** column. If the data is backed up in the FTP/SFTP mode, check the following items:
  - Whether you can ping through the IP address of the maintenance network port on the control board or the IP address of a layer 3 interface of a VLAN from the FTP/SFTP server. That is, check whether the communication between the OLT and the U2000 is normal.
  - Whether the entered IP address of the FTP/SFTP server is correct.
  - Whether the FTP/SFTP program is running on the backup server.
  - Whether the path in the FTP/SFTP program is set correctly.
- If the automatic backup fails, back up the data manually. In addition, locate the cause of the backup failure and modify the settings according to the cause.
- If the fault persists, contact Huawei technical support engineers. For details, see How to Obtain Technical Support from Huawei.

Copyright © Huawei Technologies Co., Ltd.

Related Commands

To...	Run the Command...	In...
Query user logs	**display log**	User mode
Query the file server	**display file-server**	Privilege mode
Configure the file server	**file-server**	Privilege mode

17.7.4 Restoring the NE Data Immediately

The DC can restore the history backup data after a NE is selected. This operation ensures that the NE data can be restored if the system upgrade fails or any problems occur. Thus, the system can be restored to the normal state.

Prerequisites

- The **DCServer** process runs in the normal state.
- The communication between the NE and the U2000 must be in the normal state, and there must be no packet loss in the network.
- Related xFTP settings have been configured. To obtain the configuration instructions, choose **Administration** > **NMS Commissioning Wizard** from the main menu and then select **NMS Communication with NEs** from the navigation tree.
- The NE data must be backed up to the NMS server.

  NOTE

  To copy the backup files that contain the NE data to another path, copy the directory where the backup files exist. If you copy only a certain backup file, the file is invalid when the NE data is recovered.
- When you recover NE data from the U2000 client, ensure that files can be transferred between the client and the server successfully by means of the FTP or SFTP protocol (by default, the SFTP protocol is used).

Context

The NE Software Management transfers the backup file to be recovered to the NE by using the FTP/SFTP protocol and then activates the backup file for the file to take effect on the NE. Finally, the NE data is recovered.

The data of the NEs of different types can be recovered at the same time.

After a manual restoring task is started, it cannot be stopped.

NOTICE

Before recovering the database file of an NE to the NE, ensure that the database file for data recovery is correct. Otherwise, services are interrupted.

NOTE

After a manual restoring task is started, it cannot be stopped.

Procedure

Step 1 Choose **Administration** > **NE Software Management** > **NE Data Backup/Restoration** from the main menu (traditional style); alternatively, double-click **Fix-Network NE Software Management** in **Application Center** and choose **NE Software Management** > **NE Data Backup/Restoration** from the main menu (application style).

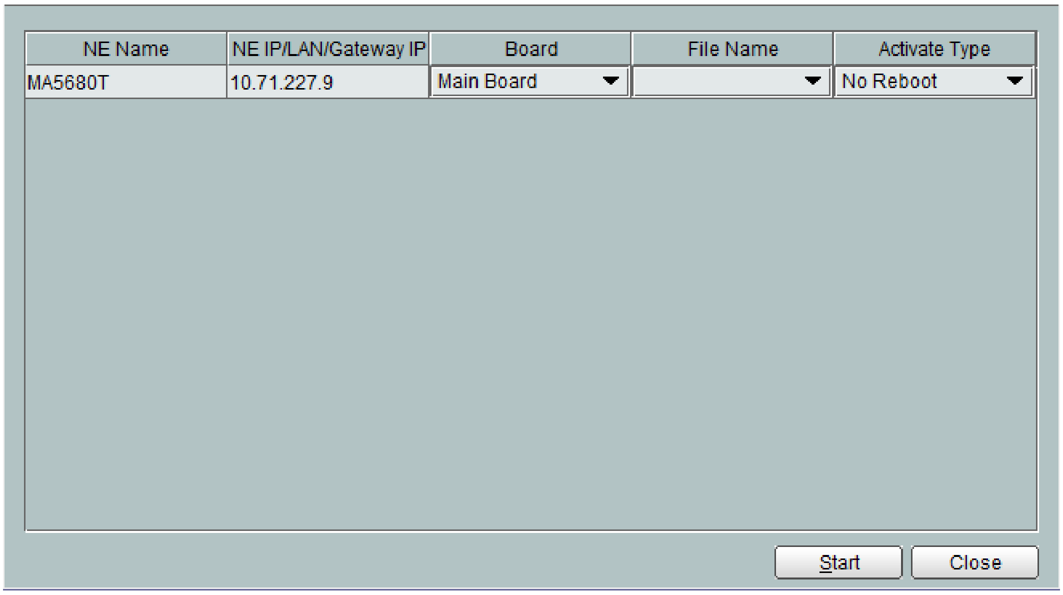
Step 2 Click ⌨, and expand the OLT NE node from the NE navigation tree.

- If a certain NE type is selected, all the NEs of this type are displayed in the NE list in the **NE View** window in the right pane.
- If a NE version is selected in a certain NE type node, all the NEs of this version are displayed in the NE list in the **NE View** window in the right pane.

Step 3 **Optional:** To locate a specific NE, click **Find** in the **NE View** window in the right pane.

Step 4 Select one or multiple records from the NE list in the **NE View** window in the right pane, right-click, and then choose **Recover** or click **Recover** in the lower pane.

Step 5 In the dialog box that is displayed, set the parameters related to restoring the NE data immediately.



NE Name	NE IP/LAN/Gateway IP	Board	File Name	Activate Type
MA5680T	10.71.227.9	Main Board		No Reboot

NOTE

- The activation types are **No Reboot** and **With Service Interruption**.
  - **No Reboot**: NE is not restarted automatically. The configuration file takes effect when the NE is restarted next time.
  - **With Service Interruption**: The NE is restarted in the process of activation, and the services on the NE are interrupted.
- To restore the data for multiple NEs of the same type, click **Same as first Board** or **Same as first Activate Type** in the upper right corner of the **Recover** dialog box. In this manner, you can configure multiple NEs with the same board type or activation type at a time rather than restore the NE data one by one.

Step 6 Click **Start** to restore the history backup data of the selected NE.

Step 7 In the **Operation Confirmation** dialog box, click **Yes**.

Step 8 In the **Operation Status** column of the NE list, the restoring process and result are displayed.

----End

Related Commands

To...	Run the Command...	In...
Load the configuration file	**load configuration**	Privilege mode
Load the database file	**load data**	Privilege mode

Copyright © Huawei Technologies Co., Ltd.