EchoLife ONT Configuration Guide

Issue 02

Date 2019-07-05

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Contents

1 Configuring the Bridging-Type ONT

About This Chapter

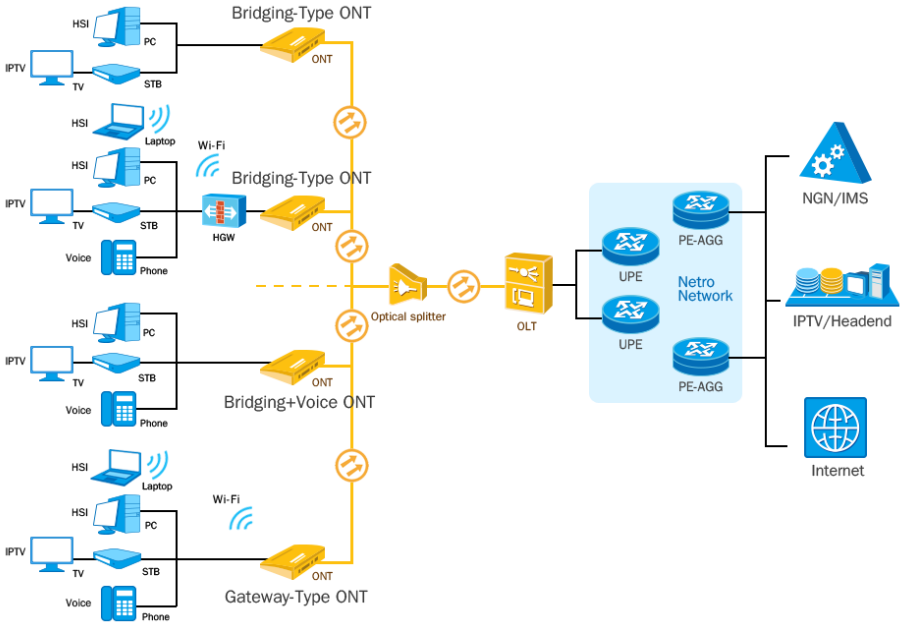
This topic describes the configuration of bridging-type ONTs and their web pages. Bridging-type ONTs only support Layer 2 features.

1.1 FTTH Networking and Configuration Scenarios

Typical FTTH Networking

Figure 1-1 shows the typical FTTH networking.

Figure 1-1 Typical FTTH networking diagram



Networking Scenario	Description
Bridging ONT + HGW Network Scenario	The HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users. Services are implemented on the HGW, and the bridging ONT works with the OLT to provide Layer 2 channels.
Bridging +Voice ONT Network Scenario	The ONT integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users. The bridging+voice ONT provides Layer 2 data and voice services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking. ● For data services, a PC directly performs dial-up. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address. ● The ONT with a built-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).
Gateway ONT Network Scenario	The ONT integrating an IAD provides Internet, VoIP, and IPTV services to users. The HGW ONT facilitates interconnection of home devices by providing Layer 3 services, such as Point-to-Point Protocol over Ethernet (PPPoE)/ DHCP dial-up, network address translation (NAT), and Internet Group Management Protocol (IGMP) snooping. This scenario provides fine-grained management channels and service control, and applies to Layer 3 networking.

FTTH Deployment Schemes

FTTH service application includes the deployment process and service provisioning process. The FTTH deployment process includes OLT deployment (configuration) and configuration of basic data. No deployment, however, is required on the ONT and the ONT is plug and play once services are provisioned.

Table 1-1 lists the FTTH deployment schemes and service provisioning methods.

Table 1-1 FTTH deployment schemes

-	Scheme	Parameter
Pre-configuration	● **On the NMS**: Profiles can be issued in batches. ● **Using commands on the OLT**: Configuration scripts containing commands can be imported to the OLT.	● DBA profile ● Line profile ● Service profile ● IP traffic profile ● Service level profile ● Global OLT configurations (rather than FTTH user configurations) such as multicast VLAN, multicast mode, and policy of forwarding unknown packets ● FTTH user service VLAN configurations including adding VLANs, setting the attributes of VLANs, and adding upstream ports for VLANs

-	Scheme	Parameter
Service Provisioning	● **Using the OSS**: This method is recommended and it can implement automatic service provisioning, and eliminate problems caused by manual service provisioning, such as large workload, low efficiency, and difficult management. ● **Using OSS+ITMS**: This method is recommended if the multiple private nodes are customized for carriers. Using a TR069 server, new gateways and value-added voice services can be simply added. – Layer 2 configuration data is issued on the NMS or OLT. – Other configuration data such as voice, Layer 3, and Wi-Fi data is issued using the ITMS. ● **On the NMS**: It applies to the scenario when no OSS is available and services need to be provisioned manually on the NMS. ● **On the ONT web page**: When it is not feasible to provision services on the OSS or NMS, you can log in to the ONT web page and configure or modify parameters to provision services.	See **Table 1-2**. ONT service provisioning parameters are classified into common parameters and customized parameters: ● Customized parameters are usually issued by the upper-layer system during service provisioning. ● Common parameters are usually configured at delivery or during data pre-configuration

Table 1-2 Parameters required for ONT service provisioning

Parameter Type	Layer 2	Voice	Above Layer 2 (Layer 3, Wi-Fi, and User Security)
Customized parameters	Parameters for adding ONTs, adding service flows, activating ports, configuring port rate limitation, and adding multicast users	• **Registration information**: IP address and port number of the local end and the proxy • **User data**: SIP user name and H.248 TID	Login user name and password

Parameter Type	Layer 2	Voice	Above Layer 2 (Layer 3, Wi-Fi, and User Security)
Common parameters	Various pre-configured profile data	● **Digitmap**: includes the digitmap timer and digitmap character strings. ● **Time configuration**: includes registration heartbeat and protocol timers. ● **Encoding and decoding**: includes voice encoding and decoding priorities and packetization period, G.711/G.729/G.722. ● Fax/Modem. ● Service permission and service data. ● **VAG**: implements multiple virtual AG devices on one physical device. ● Configurations for the interconnection between IMSs of softswitches of different specifications.	● WAN port configurations (routes, bridge WANs, and VLANs) ● LAN/WAN binding ● IGMP mode ● URL for the ITMS ● NTP server ● Default Wi-Fi configurations ● Local login IP address
ONT type	● Bridging ONTs (SFUs) ● Bridging+voice ONTs ● Gateway-type ONTs (HGUs)	● Bridging+voice ONTs. ● Gateway-type ONTs.	Gateway-type ONTs

The following describes the involved configuration scenarios:

- Service configuration on the NMS: Pre-configurations and service provisioning are implemented on the NMS. The ONT software version V300R018C00 is used as an example to describe how to provision the services on the NMS.
- Service configuration using commands: Pre-configurations are implemented using commands, and service provisioning is implemented on the ONT web pages.
- Service provisioning on the ITMS: Pre-configurations are implemented on the NMS or using commands, and Layer 3 and voice services are provisioned on the ITMS. Huawei U2560 is used as an example to describe how to provision the services on the ITMS.

Recommended tool: FTTx Script Generation Tool

This tool can generate configuration scripts through the configuration wizard for you efficiently or instantly transform any configuration page into a command script, making your configuration easy and improving your configuration efficiency.

Click to experience (for Carrier) : **FTTx Script Generation Tool**.

Click to experience (for Enterprise) : **FTTx Script Generation Tool**.

1.2 Principle of FTTH Data Plan

1.2.1 Data Plan Principles for IP Addresses

This section describes how to obtain an IP address in various scenarios.

Terminal Type	Service	Recommended Solution
Bridging +Voice ONT	Internet access	A PC obtains an IP address through PPPoE dialup. The ONT transparently transmits the packets.
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The set top box (STB) obtains an IP address from the DHCP server for ordering programs. The ONT transparently transmits the packets.
Bridging ONT+HGW	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. At the same time, the HGW functions as a DHCP server and allocates IP addresses to PCs through the network cable and wireless fidelity (Wi-Fi) access. The ONT transparently transmits the packets.

Terminal Type	Service	Recommended Solution
	VoIP	The HGW functions as a DHCP client and obtains an IP address from the DHCP server, or the application control server (ACS) issues a static IP address to the HGW using TR069. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port. The ONT transparently transmits the packets.
	IPTV	The HGW is configured with a bridging WAN port. The STB obtains an IP address from the DHCP server. The HGW transparently transmits packets. The ONT also transparently transmits the packets.
Gateway ONT	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. The ONT functions as a DHCP server and allocates IP addresses to PCs through the network cable.
	Wi-Fi access	● Layer 3 bridge Wi-Fi access service: A mobile equipment (ME) searches the SSID. After the ME is authenticated, the DHCP server assigns this ME the IP address by IPoE. ● Layer 3 route Wi-Fi access service: An ME searches the SSID. After the ME is authenticated, the DHCP address pool of an ONT assigns this ME the IP address and then PPPoE dialup is automatically performed on the ONT.
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The ONT functions as a DHCP client and obtains an IP address from the DHCP server. At the same time, the ONT functions as a DHCP server and allocates IP addresses to STBs.

1.2.2 Principle of QoS Planning

The QoS planning is an E2E planning, and it can be divided into following policies: traffic classification, marking, and scheduling policy; and traffic monitoring and DBA policy.

Traffic Classification, Marking, and Scheduling Policy

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONT Queue.ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Wi-Fi access service	1	PQ	1	1	1
Internet access service	0	PQ	0	0	0

NOTE

The greater the priority value, the higher the priority. The service priorities in this table are the recommended values. The service priorities are arranged according to the operators's actual plan.

Traffic Monitoring and DBA Policy

Items	Management service	Internet access service	Wi-Fi access service	VoIP service	IPTV service
GEM port	11 [Remark 1]	14	15	12	13
TCONT	Select a DBA type based on service types. For example, select Type1 for the management service, Type4 for the Internet access service, and Type2 for the VoIP and IPTV services.				
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)				
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is larger than or equal to the maximum bandwidth that users apply.				

Items	Management service	Internet access service	Wi-Fi access service	VoIP service	IPTV service
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit
Rate limit on ONU upstream port	No rate restriction				
Rate limit on ONU downstream port	No rate restriction				

Remark 1: GEM port value depends on the planning of the service provider, but in principle, use different GEM ports for different services.

Remark 2: **Table 1-3** shows the reference service bandwidth of each service for each user.

Table 1-3 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service/ Wi—Fi access service	Determined based on the service tariff package.	Determined based on the service tariff package.	Available bandwidth of Internet access service or Wi—Fi access service = Committed bandwidth of the service tariff package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 kbit/s	200 kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth is related to the coding format. This bandwidth is calculated for two POTS ports.

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
IPTV service (standard definition program)	N/A	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture information, 10% bandwidth burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires little bandwidth. Therefore, the bandwidth occupied by IGMP packets can be neglected.
IPTV service (high definition program)	N/A	9.7 Mbit/s per channel	

NOTE

- The rate restriction on the BRAS or SR is recommended. OLTs and ONTs do not restrict the rate for service streams.
- If BRAS does not support rate restriction, OLTs can restrict the rate for service streams through the traffic profile.
- Different service packets on the ONT are distinguished by different VLAN IDs. The service packets are mapped to GEM ports based on VLAN IDs so that different service packets are transmitted to different GEM ports. Each GEM port (each service) corresponds to a T-CONT or all GEM ports share a T-CONT.
- The sum of the assured bandwidth of all ONTs connected to a PON port and the fixed bandwidth of OMCI management channel is less than the GPON upstream bandwidth. Some bandwidth must be reserved for the future service expansion.

1.2.3 Principles of Internet and Wi-Fi Access Services Data Planning

This topic describes the principles of data planning for Internet and Wi-Fi access services and will focus on the VLAN planning and VLAN translation policy planning in different network scenarios.

Table 1-4 Planning of VLANs and VLAN translation policies for Internet access service

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+Voice ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.
Bridging ONT + HGW	Double-tagged VLAN	ONT: The upstream packets sent from the HGW carry user-VLANs and the ONT transparently transmits them. OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.
Gateway ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Table 1-5 Planning of VLANs and VLAN translation policies for Wi-Fi access service

Application Scenario	VLAN Plan	VLAN Translation Policy
Gateway ONT	Single-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S.

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.

- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- To ensure traceability of users and finer-grained QoS control and management of users and services, plan per user per service per VLAN (PUPSPV) for the Internet access service. Considering OLT capacity and VLAN scalability, use dual VLANs (S-VLAN+C-VLAN) on the OLT to differentiate users for the Internet access service.
- The outer VLAN (S-VLAN), which identifies services and physical location, can be allocated based on the OLT, PON board, or PON port. The inner VLAN (C-VLAN) identifies users. C-VLANs must be unique in one S-VLAN.
- It is recommended that you use stacking VLANs as S-VLANs so that security features, such as PPPoE+/option82, and anti-MAC attacks and anti-MAC spoofing, can be easily deployed.
- The 802.1q in 802.1q (QinQ) VLAN is used in the enterprise private line scenario, such as transparent LAN service (TLS), in which the device transparently transmits packets. It is not recommended that you use QinQ VLANs as S-VLANs for the triple play services of residential users.

1.2.4 Principle of Voice Service Data Plan

The voice service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios, and the plan of voice protocol.

VLAN and VLAN Translation Policy

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+voice ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have different C-VLANs. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT +HGW	Single-tagged VLAN (recommended)	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> S-VLAN). All the ONTs connected to the same OLT have the same voice service S-VLAN; ONTs connected to different OLTs may have different voice service S-VLANs. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> C-VLAN). The C-VLAN is an inner VLAN tag that differentiates users. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
Gateway ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN+C-VLAN').

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- The voice service is a closed service operated by carriers. The single-tagged S-VLAN is the mainstream application and is recommended.
- When the planned VLAN is single-tagged VLAN, the S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-VLANs identify services and physical locations. It is recommended that you set different voice VLANs for the OLTs connected to one voice SR to avoid an excessively large broadcast domain of the SR and convergence switch.
- When the planned VLAN is S-VLAN+C-VLAN (that is, double-tagged VLAN), the outer S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-+VLANs identify services and physical locations. It is recommended to allocate S-VLANs based on PON board or PON port. The inner C-VLAN is used to identify services (a fixed value) or users.

Voice Data Plan Based on H.248 or SIP

Item			Description
MG interface/SIP interface data **NOTE** must be consistent with the data on the MGC/IMS core network devices.	Media and signaling parameters	Media and signaling upstream VLANs	Upstream VLANs of the voice service
		Media and signaling upstream port	Upstream ports of the voice service
		Media IP addresses and signaling IP addresses	Supports separating media from signaling.
		Default gateway IP address.	The next hop IP address from an ONU/HGW to an MGC/IMS.
	MG interface/SIP interface ID		N/A
	Signaling port ID		Choose the transmission mode according to the requirement of the MGC/IMS side.

Item		Description
	IP address of active MGC (H.248)/IP address of active IMS device (SIP)	If the dual homing is not configured, only one MGC parameter needs to be configured. If the dual homing is configured, the IP address and port ID of the standby MGC need to be configured.
	Port ID of active MGC (H248)/port ID of active IMS device (SIP)	
	Coding	Choose the coding method according to the requirement on the MGC/IMS side. Generally, the text coding method is adopted.
	Transmission mode	Choose the transmission mode according to the requirement on the MGC/IMS side. Generally, the UDP transmission mode is adopted.
	Home domain (SIP)	N/A
	Profile index	N/A
	The version of H248 protocol that MG starts to negotiate	V1, V2 or V3 (by default). The interface may fail to be registered because some softswitches do not support V3.
Voice user configuration data	Phone number	For H248 protocol: The phone numbers allocated by the MGC need to be determined, and the paging numbers for users' emergency standalone need to be planned if the emergency standalone function is provided. For SIP protocol: The phone number that the IMS core network device allocates to the user must be configured.
	Terminal ID (H248)	If the TID template with which the POTS user is bound does not support terminal layering, this parameter needs to be configured.
	User priority	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)

Item		Description
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
Common parameter	system parameter	The system parameters including the overseas version flag and message waiting indication (MWI) mode need to be configured according to the local standard to ensure that the response of the user terminal complies with the local standard.
	Overseas parameters	The attributes such as the upper and lower thresholds of the flash-hooking duration need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	POTS port attributes	If the POTS port needs to support the polarity reversal accounting, the POTS port needs to be configured to support the polarity reversal pulse. Other attributes need not be modified if there is no special requirement.
	Ringing current attributes	When the attributes of ring current are changed, ring volume is changed accordingly. Generally, no adjustment is required for the ringing tone volume. You need to modify the parameters of the ringing current attributes according to the local standard only when the default ringing current attributes do not comply with the local standard.

1.2.5 Principle of IPTV Service Data Plan

The IPTV service data plan mainly include the plan of VLAN and VLAN translation policy in different network scenario, and the plan of IPTV service.

IPTV services include multicast service and video on demand (VoD) service. These two services are relevant but independent in VLAN planning.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
Bridging +Voice ONT	Multicast service	Single-tagged VLAN	ONTs replicate multicast packets based on user ports and multicast VLANs (M-VLANs) are removed downstream. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs add S-VLAN tags to iTV service packets. The OLT transparently transmits packets with S-VLANs.
		Double-tagged VLAN	All ONTs add the same C-VLAN tag to packets. The OLT implements VLAN translation: C->S+C'.
Bridging ONT + HGW	Multicast service	Single-tagged VLAN	ONTs transparently transmit upstream packets with M-VLANs sent from HGW. Multicast packets are replicated downstream with M-VLAN unchanged. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
		Single-tagged VLAN	ONTs translate the upstream VLANs sent from HGW to M-VLANs. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S.
		Double-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S+C.
Gateway ONT	Multicast service	Single-tagged VLAN	ONTs replicate packets based on user ports and M-VLANs are removed in downstream direction. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs add C-VLAN tags to packets. Untagged VLANs are translated to C-VLANs. The OLT implements VLAN translation: C -> S.

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- IPTV service is a closed service self-operated by carriers, and single-tagged S-VLAN is recommended.
- The same S-VLAN or different S-VLANs can be used as the M-VLAN and VoD VLAN. It is recommended that you use different S-VLANs as M-VLAN and VoD VLAN so that the upper-level device easily differentiates between the BTV service and VoD service.
- S-VLANs of VoD service can identify services and physical locations based on an entire network or an OLT. It is recommended that you set different VoIP VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the VoIP SR and convergence switch.

1.2.6 Principle of Security Data Plan

The security plan involves system security plan, user security plan, and service security plan. Security policy ensures service security from different aspects.

NOTE

The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:

- The security measures can be used on the live network.
- The security measures are easy to deploy.
- The security measures are effective.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.

Security Vulnerability	Solution	Description and Usage Suggestion
IP attack	Enable the anti-IP-attack function for OLT.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT.	After anti-MAC-duplicate is enabled, the system records the first MAC address learned from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
MAC attack	Enable the anti-MAC spoofing function for OLT.	After anti-MAC spoofing is enabled, the system can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
IP spoofing	Enable the anti-IP spoofing function for OLT.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

Service Security

Security Vulnerability	Solution	Description and Usage Suggestion
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on OLT, and the BRAS implements user authentication based on the RAIO information.	In the DHCP option 82 mode, user's physical location is added to the option 82 field carried in the DHCP request packet initiated by a user. The physical location, used for user authentication on the upper-layer authentication server, can help implement the following functions: ● The DHCP relay forwards DHCP response packets to devices with specified CID and RID. ● Prevents DHCP address exhaustion. ● Achieves static allocation of DHCP addresses. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the DHCP Internet access service.
Broadband access of residential users (PPPoE), user account theft/ borrowing	PPPoE+ (PITP) is enabled on OLT, and the BRAS implements user authentication based on binding of the RAIO information to the user account.	The BRAS responds to request packets of users with specified CID and RID. In this way, the following functions are implemented: ● Prevents IP address exhaustion. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the PPPoE Internet access service.

1.3 Configuring the Service by Using the NMS

This topic describes how to configure Internet access service, VoIP service and IPTV service by using the NMS.

1.3.1 Configuring FTTH Services (GPON Access)

This topic describes how to configure the Internet service, voice service, and multicast service in GPON access mode in the FTTH network scenario using the U2000.

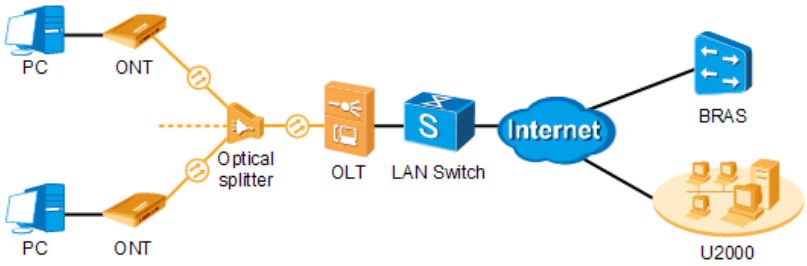
1.3.1.1 Configuring the GPON FTTH Layer 2 Internet Access Service on the NMS

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Networking

- The PC gains access to the Internet in PPPoE dialup mode.
- The ONT is connected to the GPBC card of the OLT through an optical fiber.
- The broadband remote access server (BRAS) provides broadband user access and functions of authentication and accounting.

Figure 1-2 Configuring the GPON FTTH Internet service



Data Plan

Table 1-6 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA Type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1 ID of the port on the ONT that is connected to the PC: 1

Item	Data
VLAN plan	Double-tagged VLAN ● S-VLAN ID: 100 ● S-VLAN type: Smart ● S-VLAN attribute: Stacking ● C-VLAN ID: 1001 ● C'VLAN ID: 1010 **NOTE** VLAN translation policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

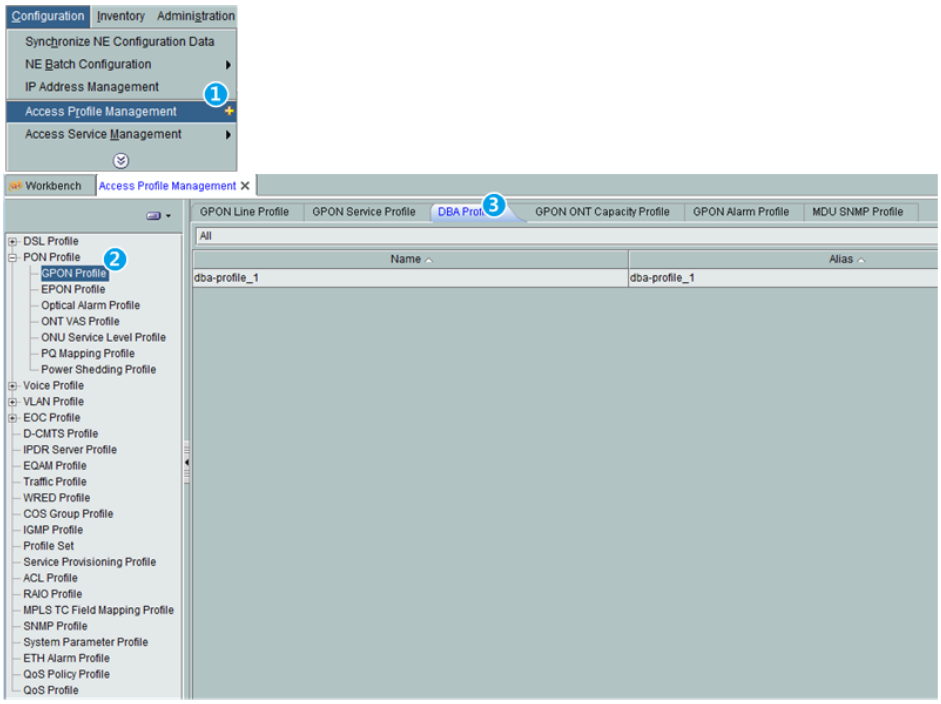
- **Implement pre-configurations.**

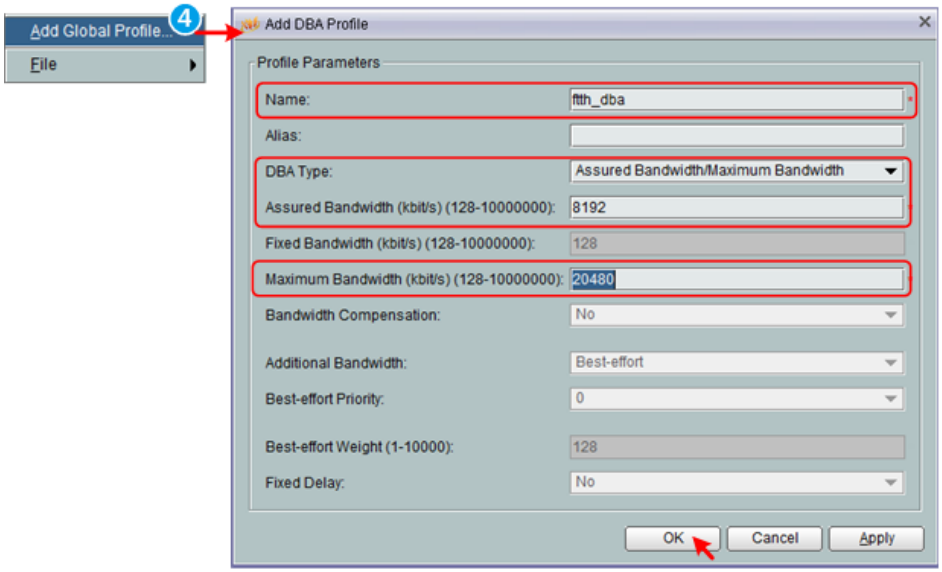
NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

1. **Configure a DBA profile.**

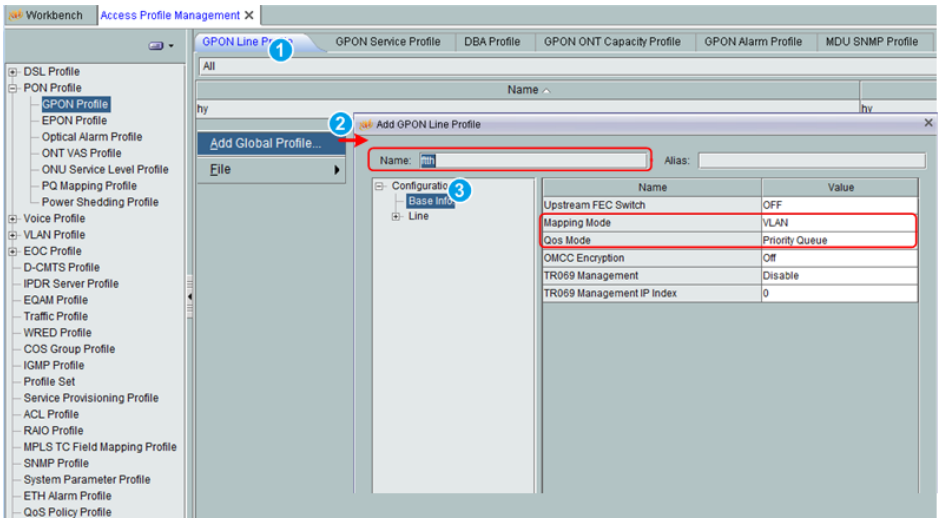


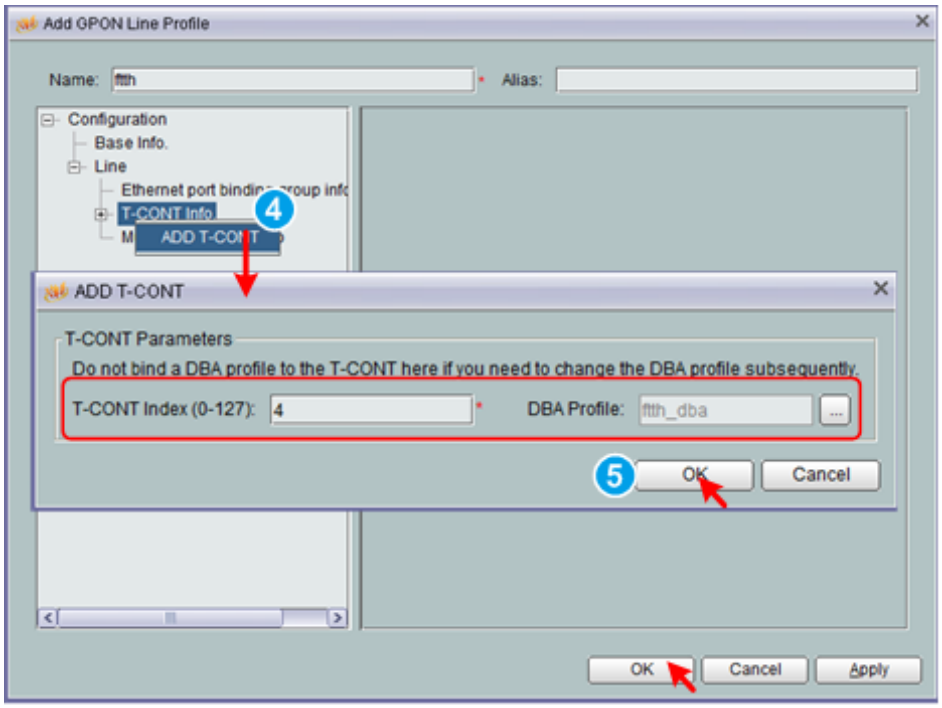


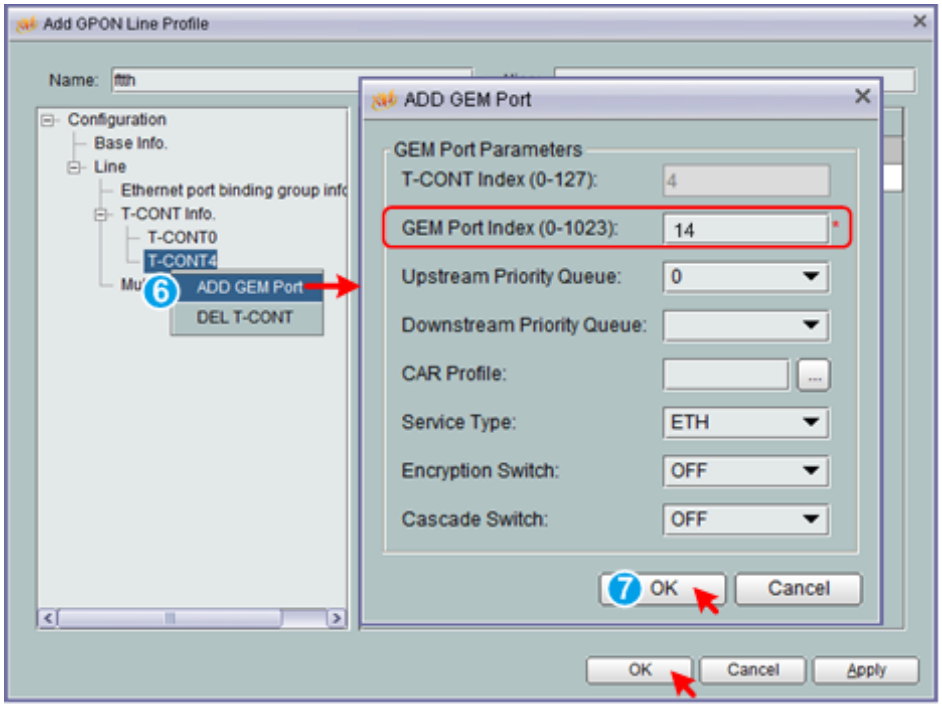
2. **Configure a line profile.**

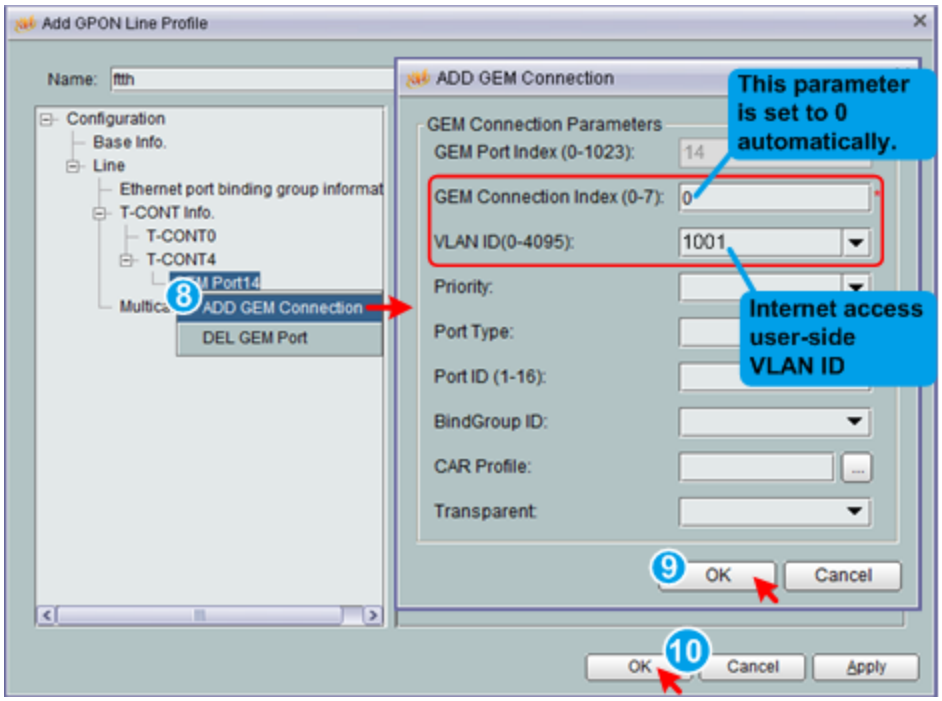
   In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

   In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 14. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.



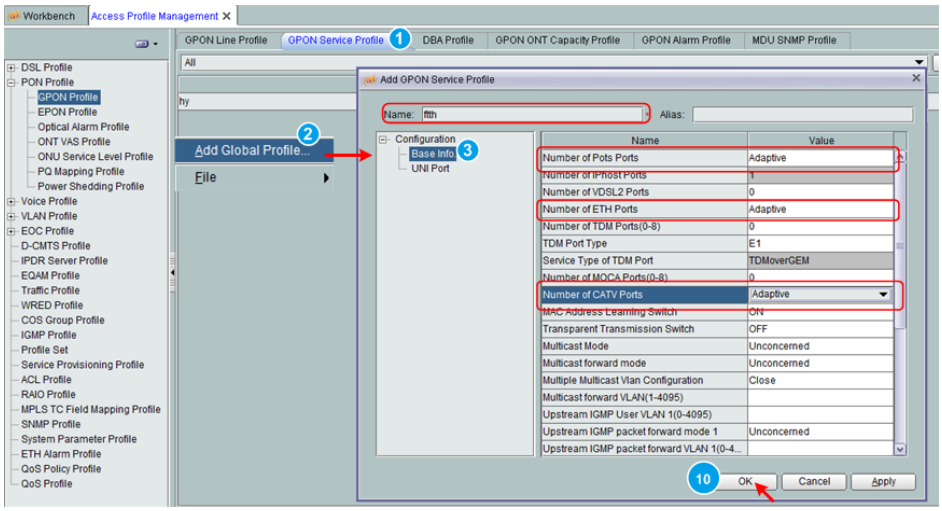

Add GPON Line Profile
Name: ftth
Alias:
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info.
4
ADD T-CONT
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127): 4
DBA Profile: ftth_dba
5
OK
Cancel
OK
Cancel
Apply

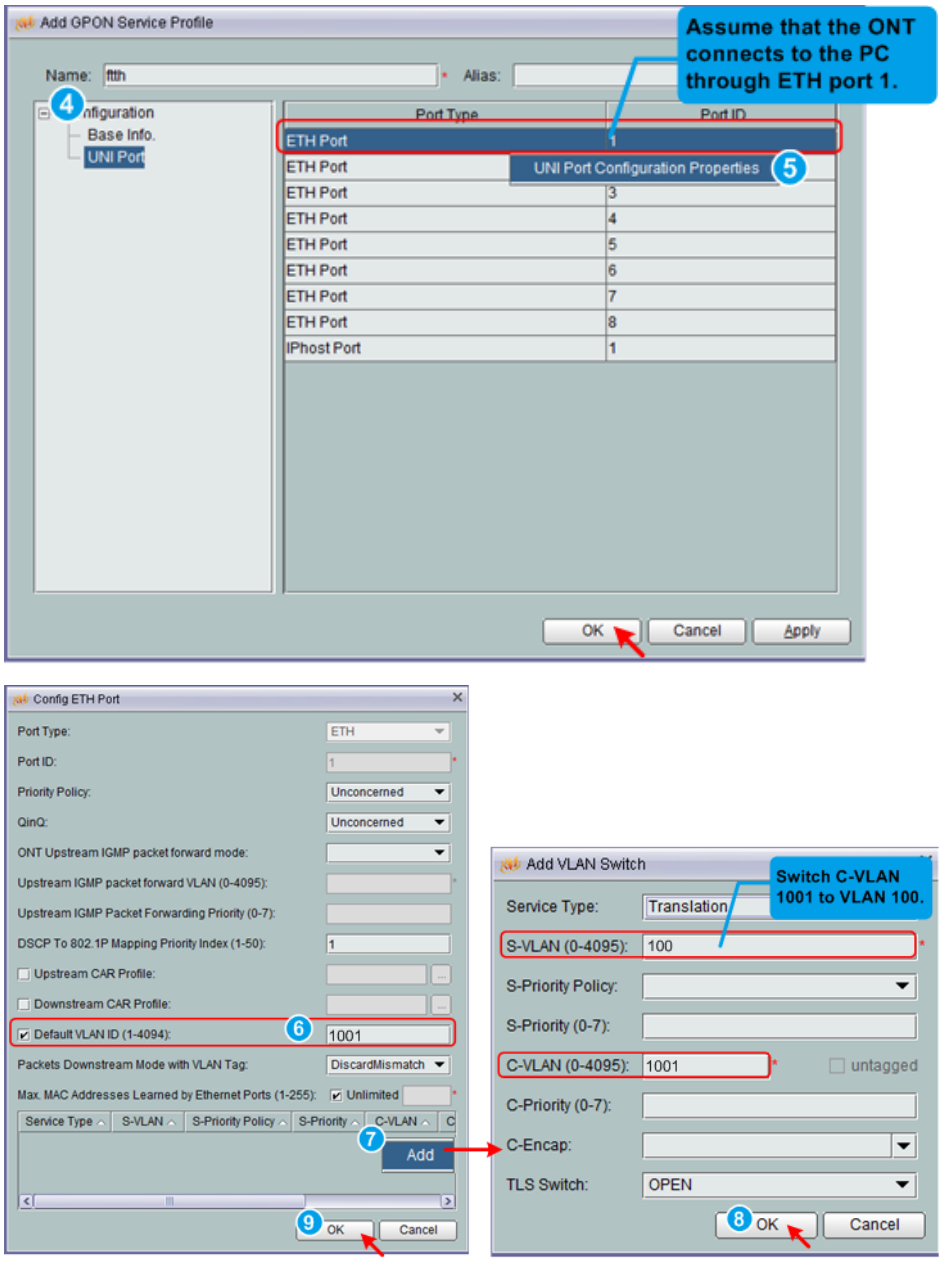

Add GPON Line Profile
Name: ftth
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info.
T-CONT0
T-CONT4
6
ADD GEM Port
DEL T-CONT
ADD GEM Port
GEM Port Parameters
T-CONT Index (0-127): 4
GEM Port Index (0-1023): 14
Upstream Priority Queue: 0
Downstream Priority Queue:
CAR Profile:
Service Type: ETH
Encryption Switch: OFF
Cascade Switch: OFF
7
OK
Cancel
OK
Cancel
Apply



3. **Configure a service profile.**

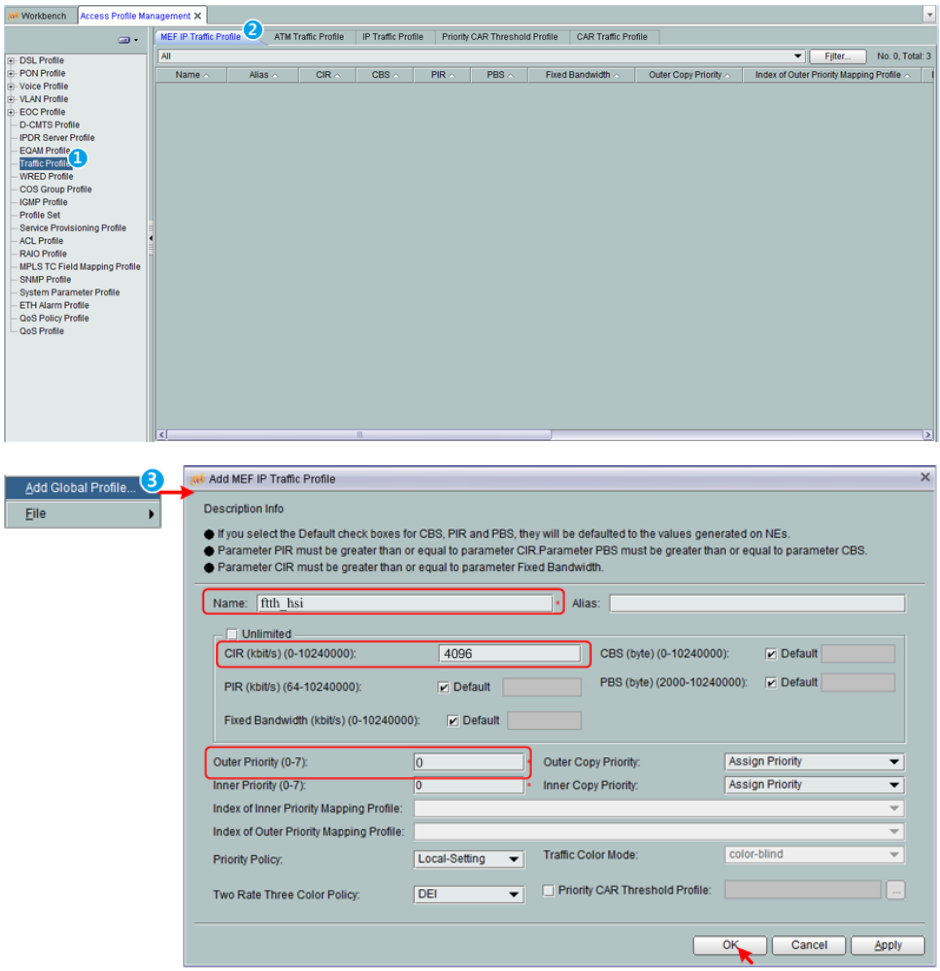
   Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability. Then, in the ONT service profile, configure a VLAN translation policy to translate C-VLAN 1001 to VLAN 100.





4. **Configure an MEF IP traffic profile.**

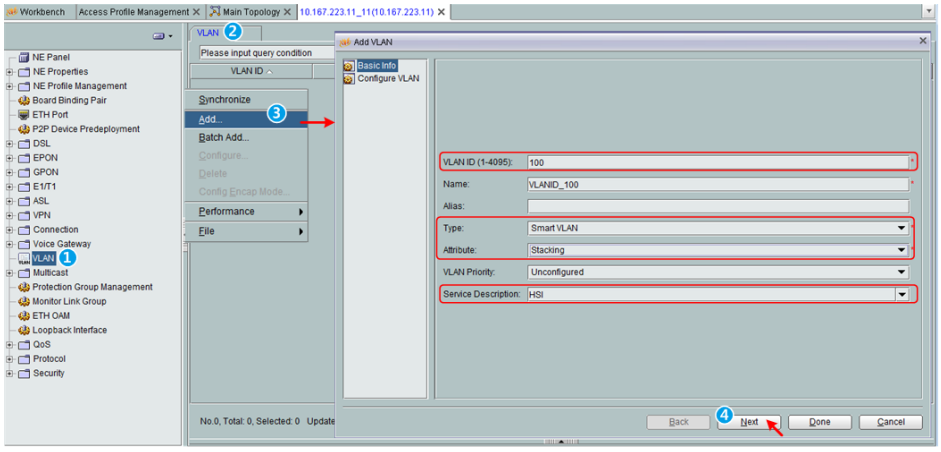
   The profile name is ftth_hsi, CIR is 4 Mbit/s, and the priority is 0. Traffic is scheduled based on the priority specified in the profile.

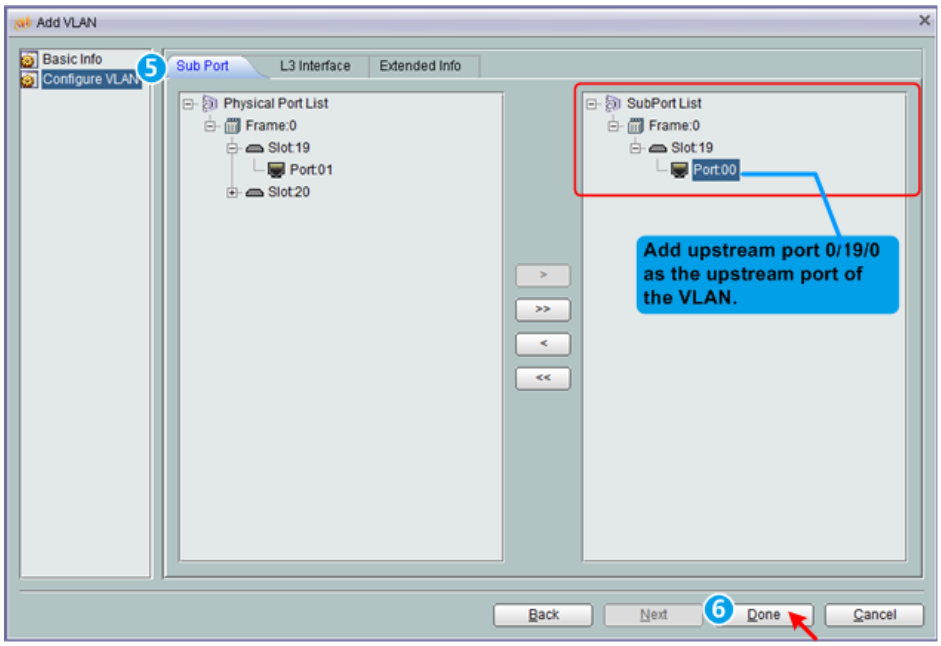


5. **Configure a service VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   A service VLAN is the VLAN used for the Internet service.



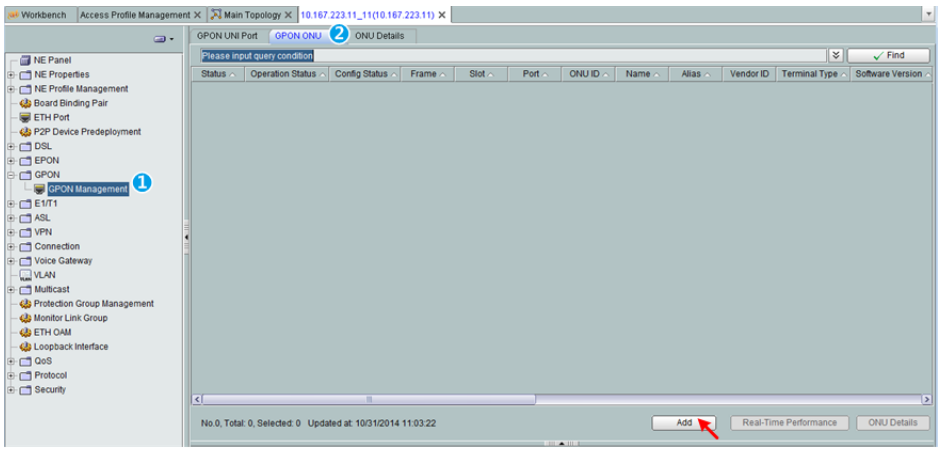


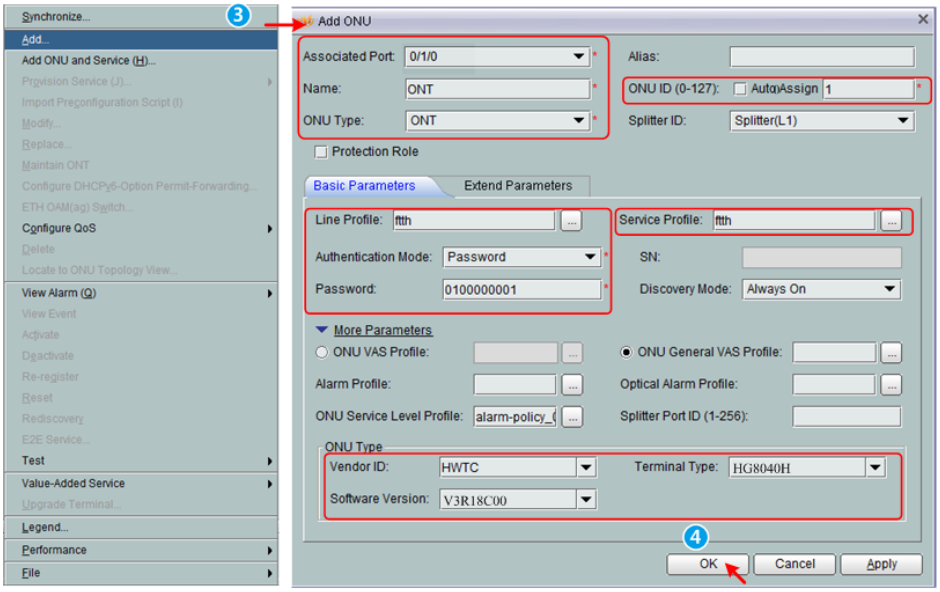
- **Provision services.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

  The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



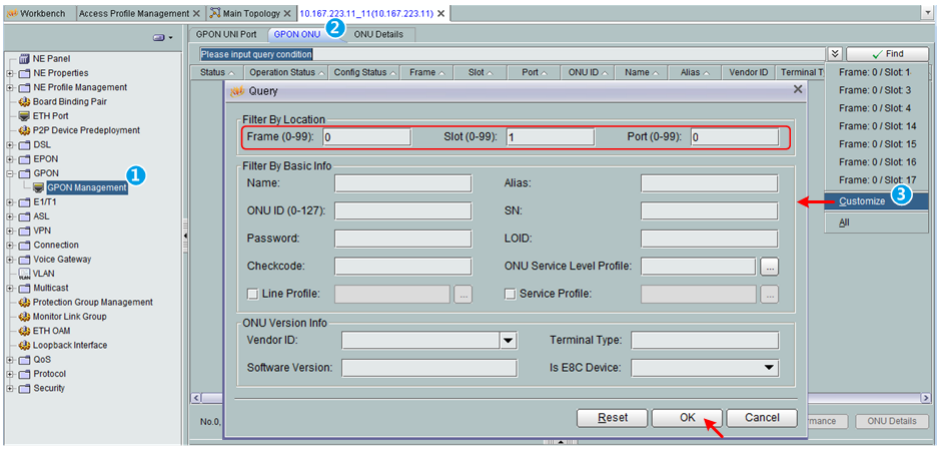


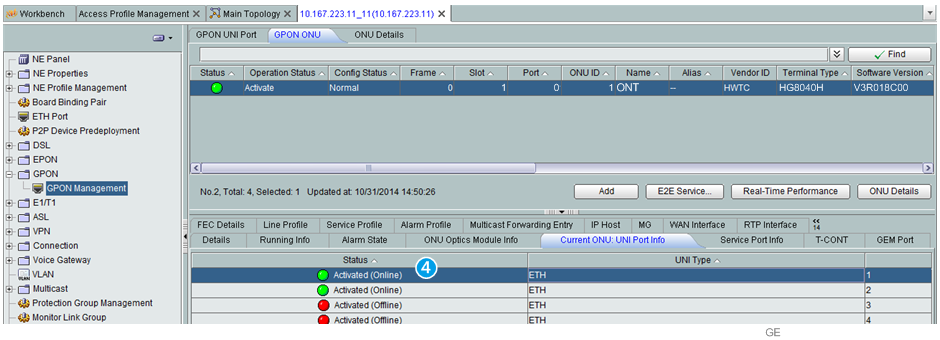
NOTE

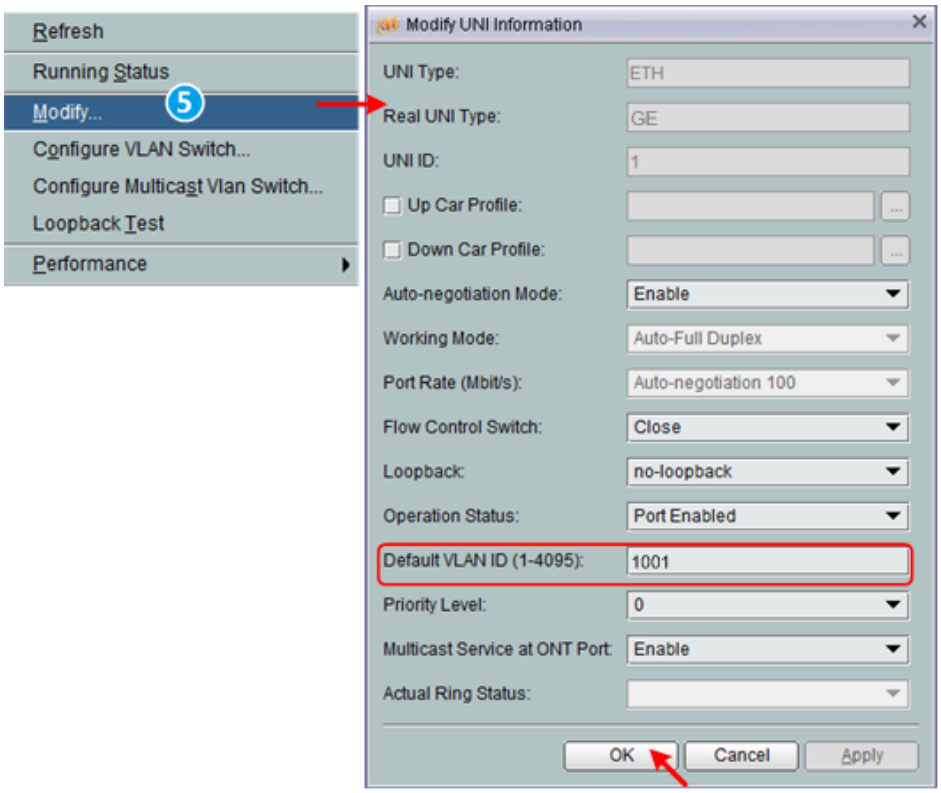
HG8010H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

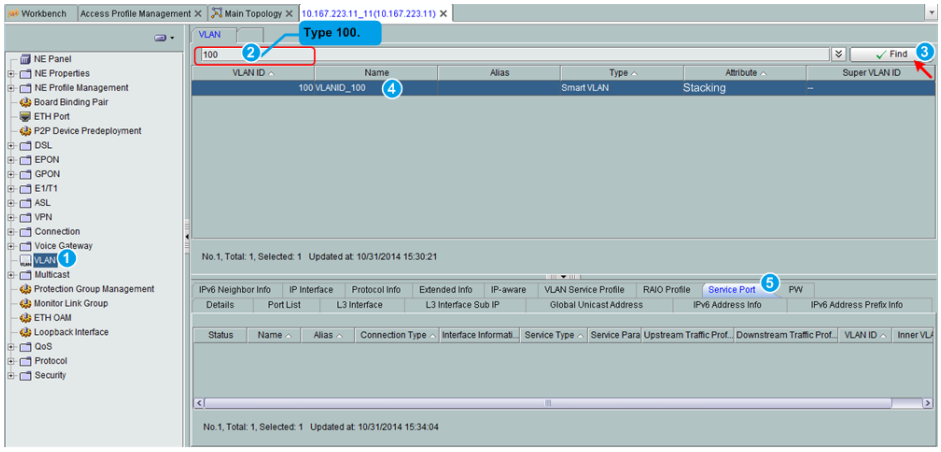
b. **Configure an ETH port of the GPON ONU.**

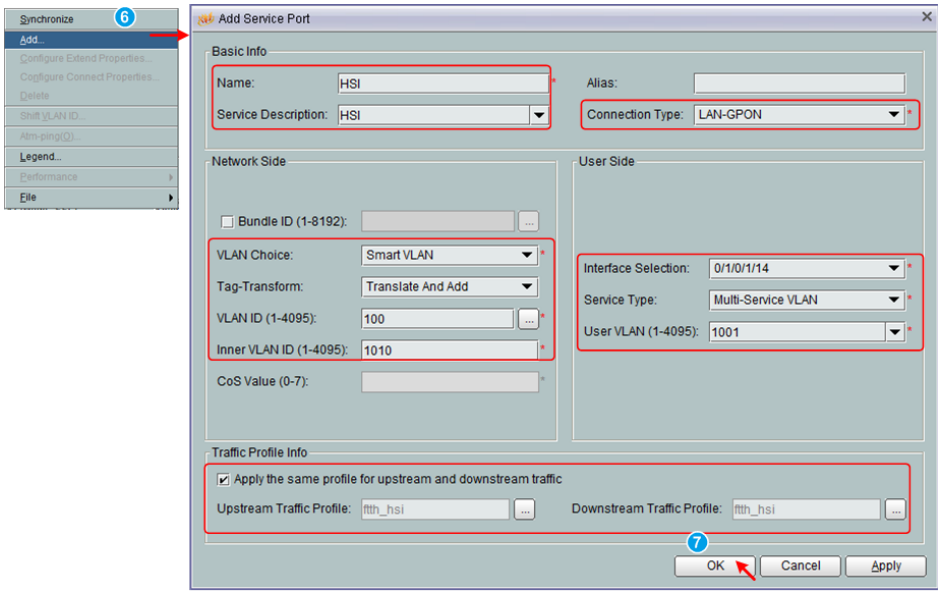






c. **Add a service virtual port on the OLT side.**





Result

Check whether the user successfully gains access to the Internet through dialup on the PC.

1. The LAN1 port of the ONT is connected to the Ethernet port of the PC properly.
2. Dial up on the PC using the PPPoE dialup software.
3. The user gains access to the Internet on the PC after the dialup is successful.

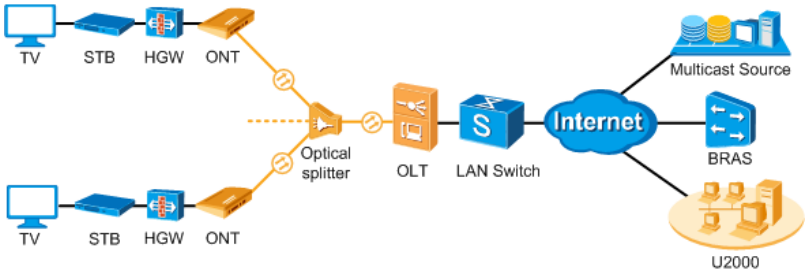
1.3.1.2 Configuring the GPON FTTH Layer 2 Multicast Service on the NMS

This topic describes how to configure the multicast service when an ONT is connected to an OLT through a GPON port.

Networking

- The ONT is connected to the OLT in Layer 2 mode.
- The OLT uses IGMP proxy, which is a Layer 2 multicast protocol.
- The IGMP version of the multicast VLAN is IGMPv2.
- The multicast programs are obtained in the dynamic mode.

Figure 1-3 Configuring the GPON FTTH multicast service



Data Plan

Table 1-7 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA Type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for video services: 13
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1 ID of the port on the ONT that is connected to the PC: 2
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode
VLAN Plan	● S-VLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: Smart ● VLAN attribute: Common **NOTE** VLAN translation policy: ● ONT: transparently transmits the MVLAN of the HGW. Multicast packets are duplicated downstream with MVLAN unchanged. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.

Procedure

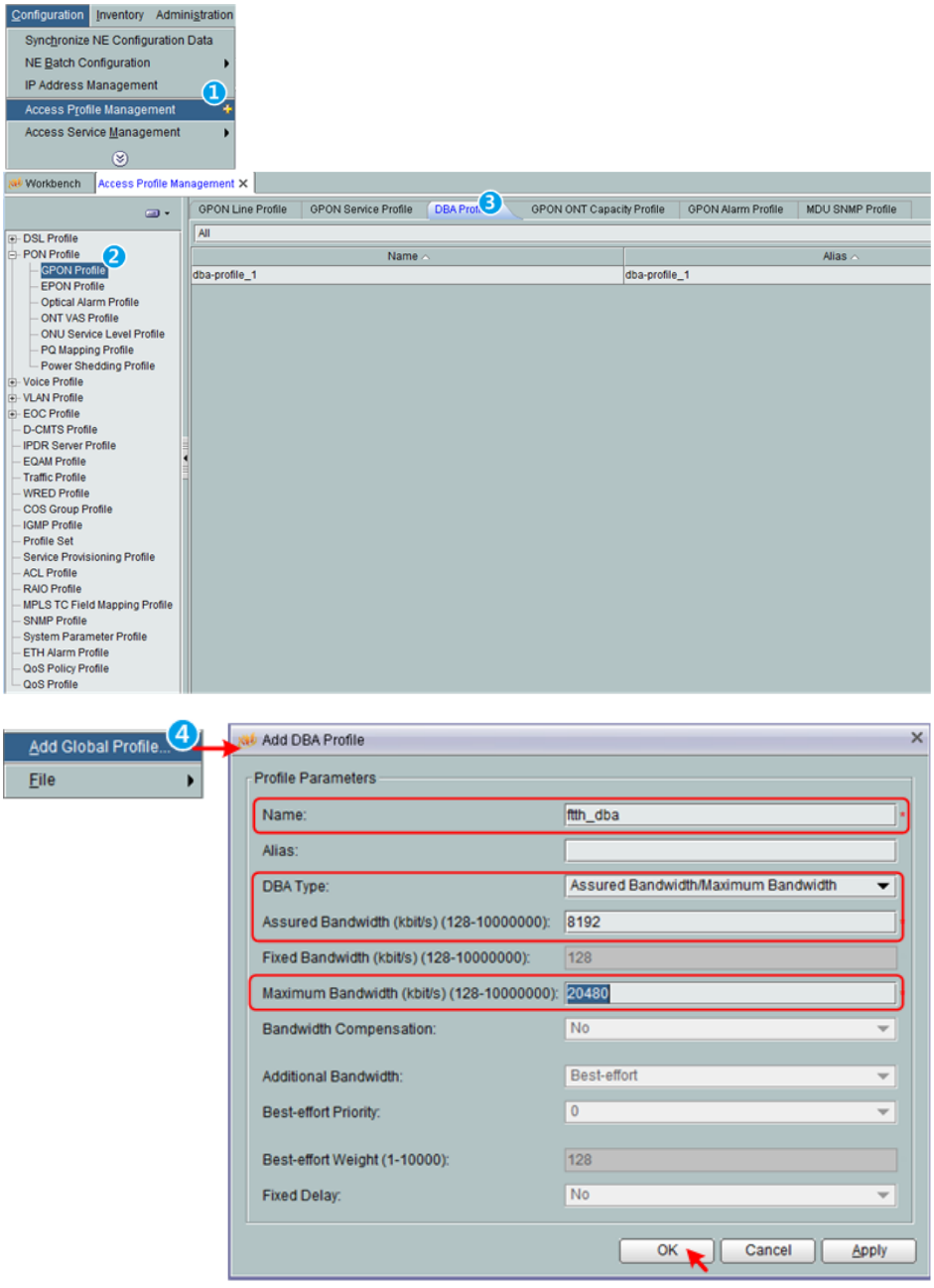
- **Implement pre-configurations.**

NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

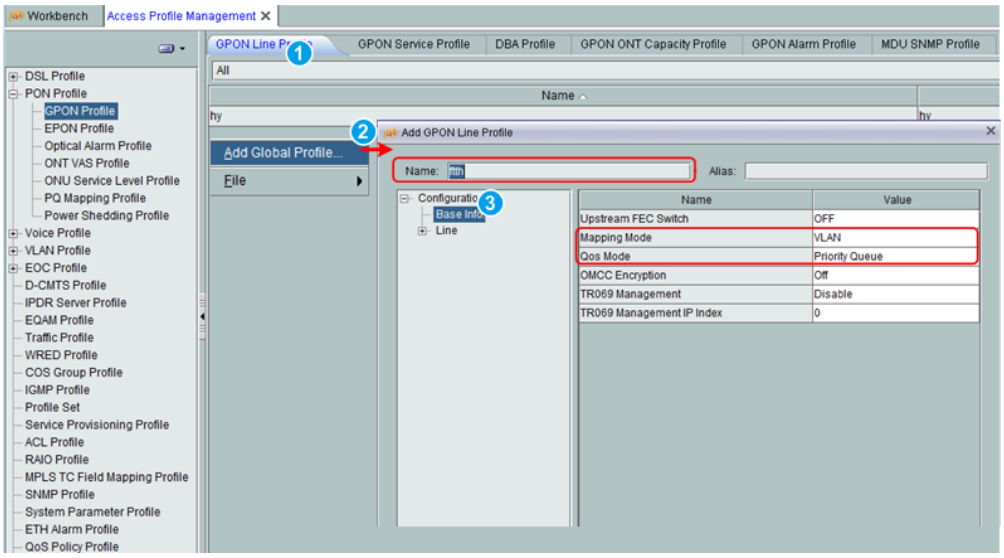
1. **Configure a DBA profile.**

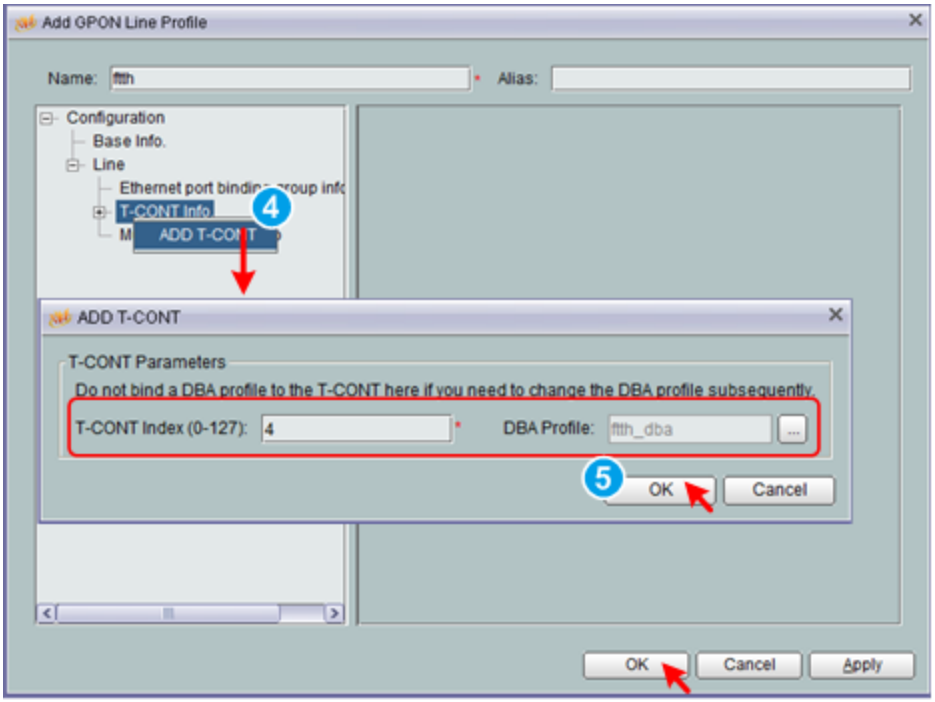


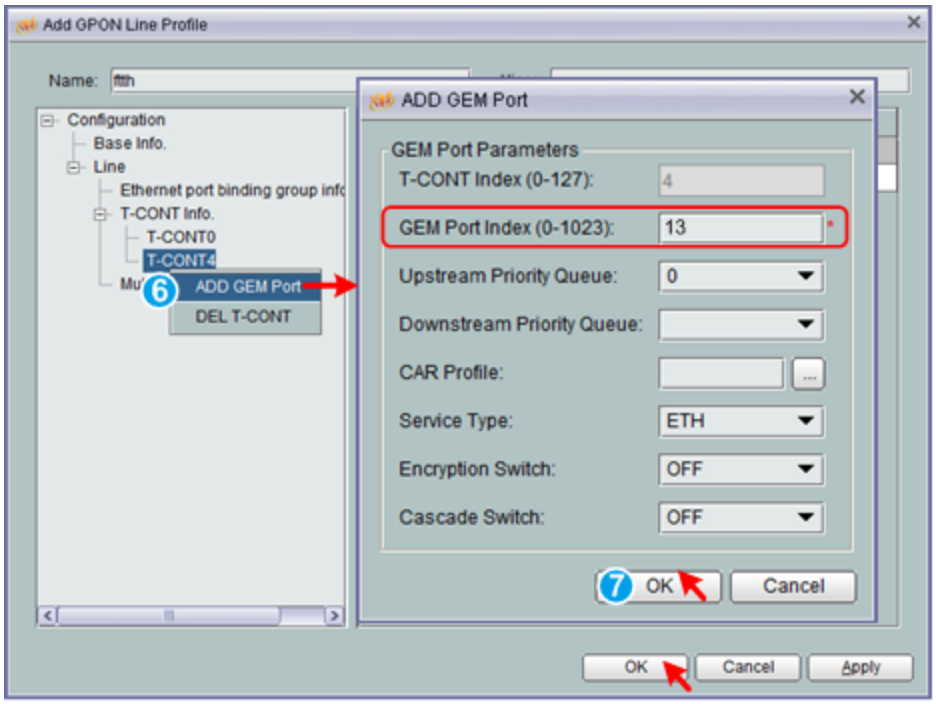
2. **Configure a line profile.**

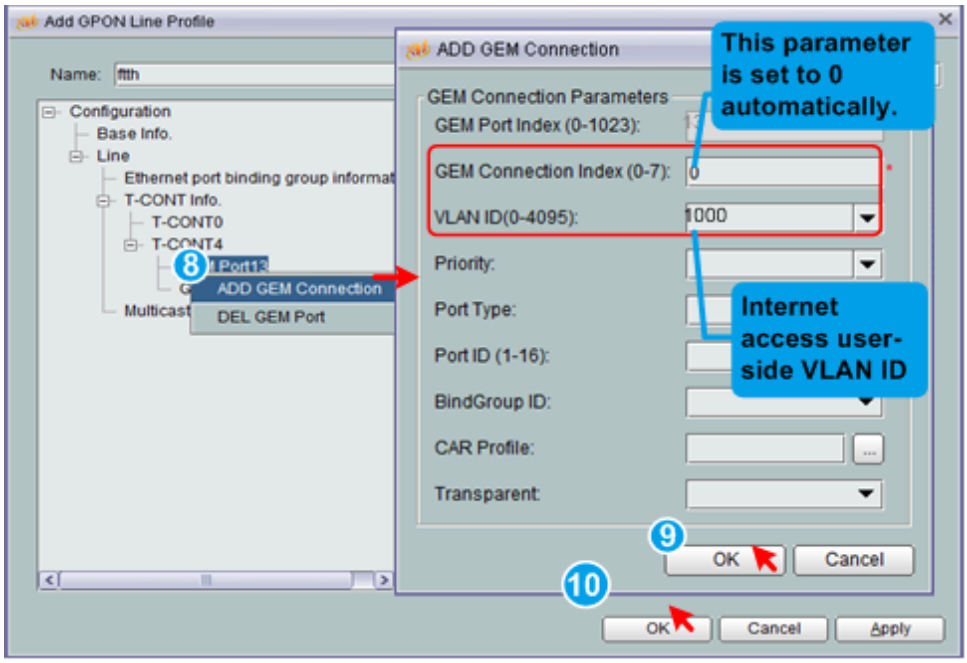
   In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

   In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 13. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.


Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
Add Global Profile...
File
Add GPON Line Profile
Name: ftth
Alias:
Configuration
Base Info.
Line
Name
Value
Upstream FEC Switch
OFF
Mapping Mode
VLAN
Qos Mode
Priority Queue
OMCC Encryption
Off
TR069 Management
Disable
TR069 Management IP Index
0
1
2
3

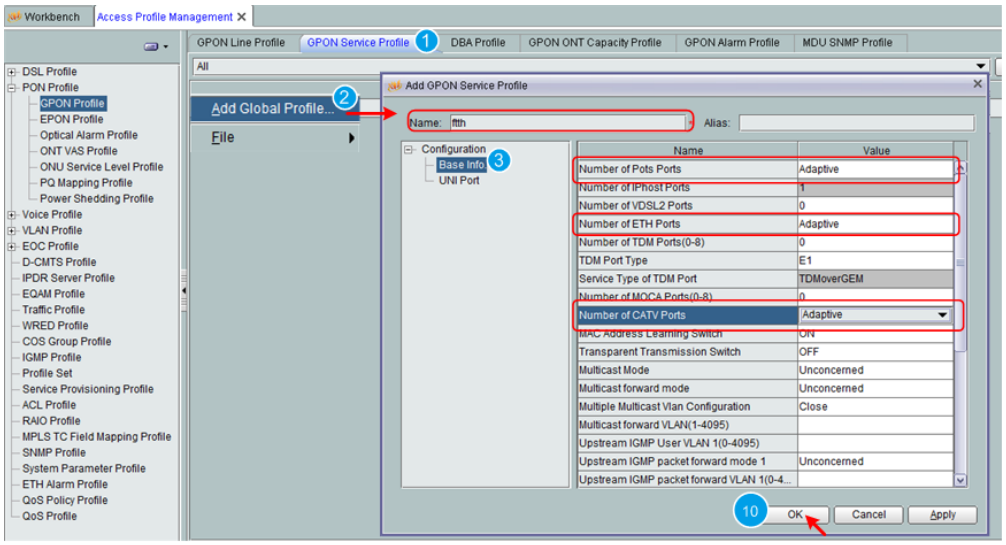

Add GPON Line Profile
Name: ftth
Alias:
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info
ADD T-CONT
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127): 4
DBA Profile: ftth_dba
5
OK
Cancel
OK
Cancel
Apply

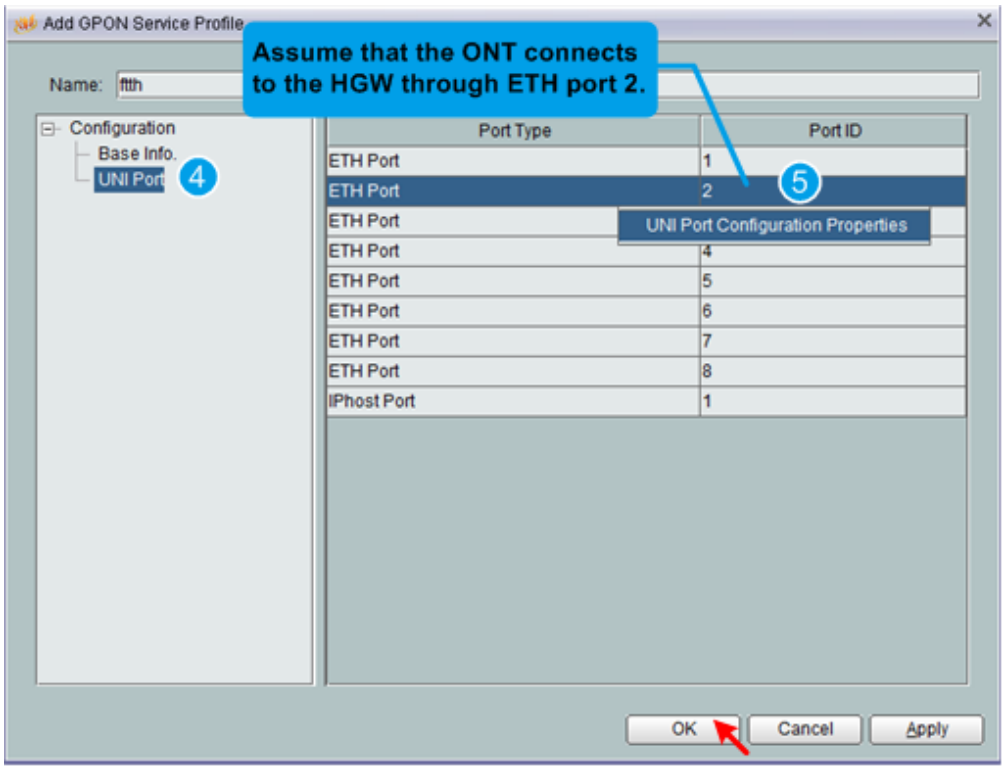


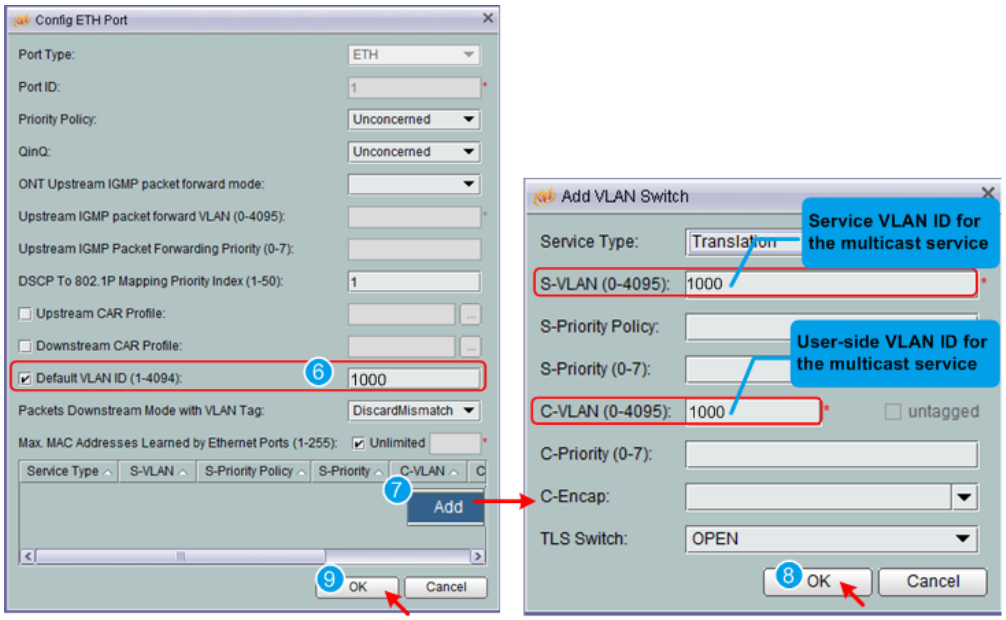


3. **Configure a service profile.**

   Configure a VLAN translation policy for the ONT ETH port. Assume that the ONT connects to the HGW through ETH port 2. Configure a VLAN translation policy to make the ONT transparently transmit the MVLAN of the HGW in the upstream direction, and replicate multicast packets with the MVLAN unchanged in the downstream direction.

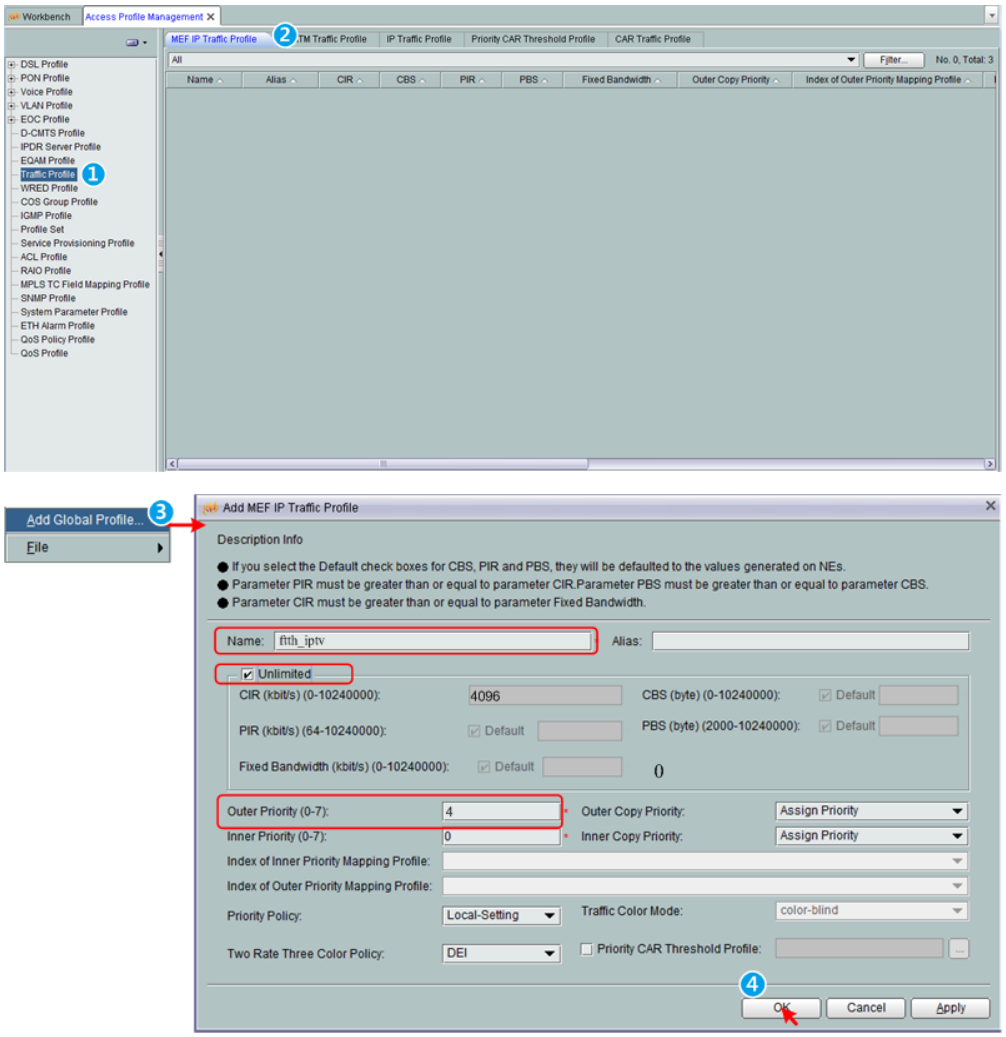

Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
QoS Profile
Add Global Profile...
File
Add GPON Service Profile
Name: ftth
Alias:
Configuration
Base Info
UNI Port
Name
Value
Number of Pots Ports
Adaptive
Number of IPhost Ports
1
Number of VDSL2 Ports
0
Number of ETH Ports
Adaptive
Number of TDM Ports(0-8)
0
TDM Port Type
E1
Service Type of TDM Port
TDMoverGEM
Number of MOCA Ports(0-8)
0
Number of CATV Ports
Adaptive
MAC Address Learning Switch
ON
Transparent Transmission Switch
OFF
Multicast Mode
Unconcerned
Multicast forward mode
Unconcerned
Multiple Multicast Vlan Configuration
Close
Multicast forward VLAN(1-4095)
Upstream IGMP User VLAN 1(0-4095)
Upstream IGMP packet forward mode 1
Unconcerned
Upstream IGMP packet forward VLAN 1(0-4...
OK
Cancel
Apply
1
2
3
10


Add GPON Service Profile
Assume that the ONT connects to the HGW through ETH port 2.
Name: ftth
Configuration
Base Info.
UNI Port
Port Type
Port ID
ETH Port 1
ETH Port 2
ETH Port 3
ETH Port 4
ETH Port 5
ETH Port 6
ETH Port 7
ETH Port 8
IPhost Port 1
UNI Port Configuration Properties
OK
Cancel
Apply
4
5



4. **Configure an MEF IP traffic profile.**

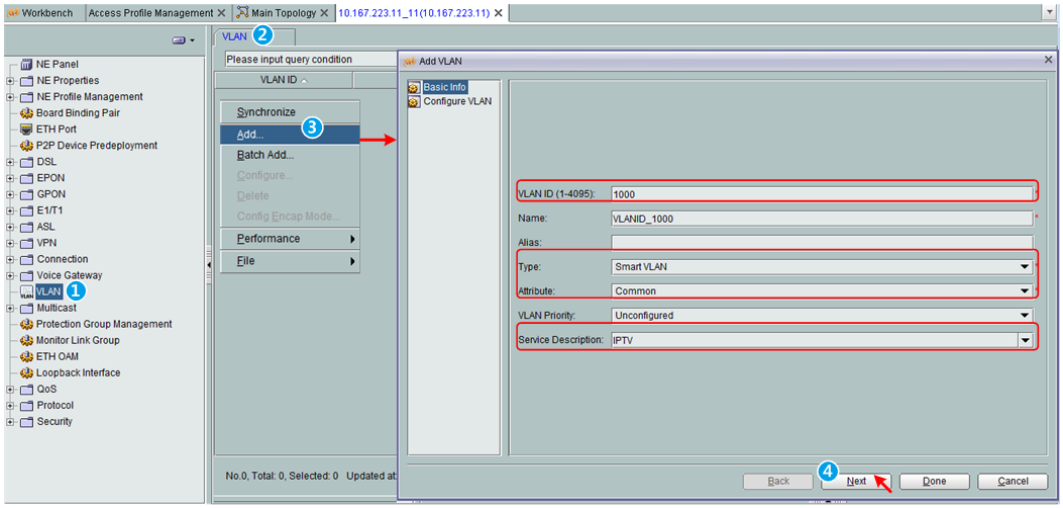
   The profile name is ftth_iptv, CIR is off, priority is 4, and priority-based scheduling policy is Local-Setting. Traffic is scheduled based on the priority specified in the profile.

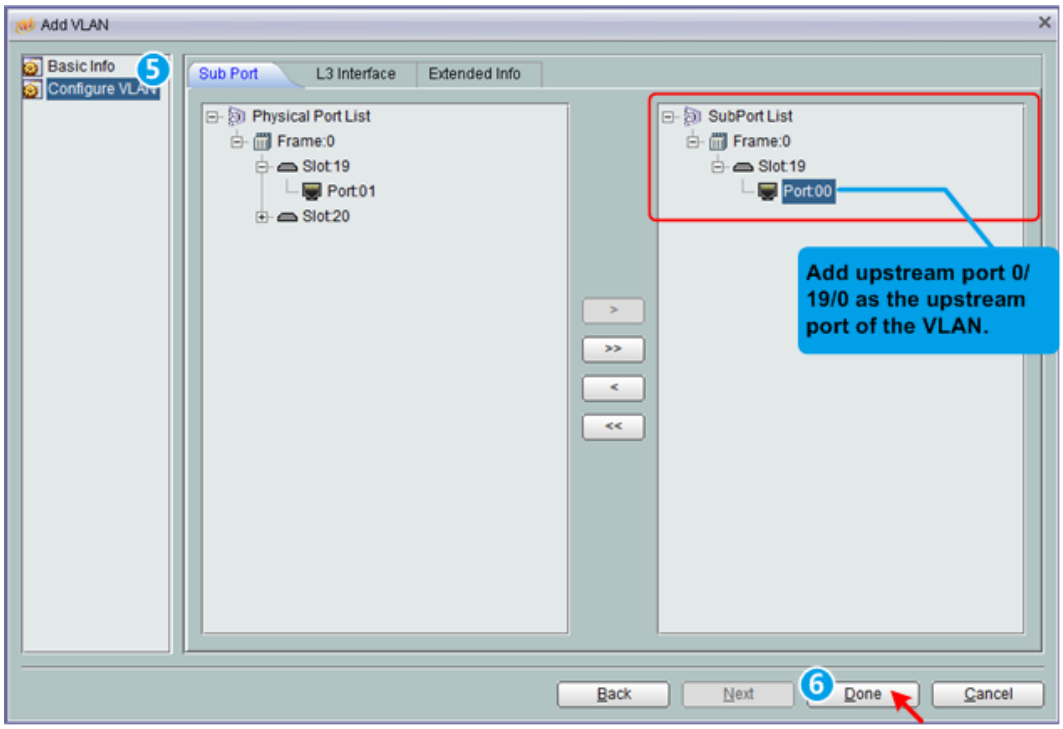


5. **Configure an S-VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   The S-VLAN is used for the multicast service.



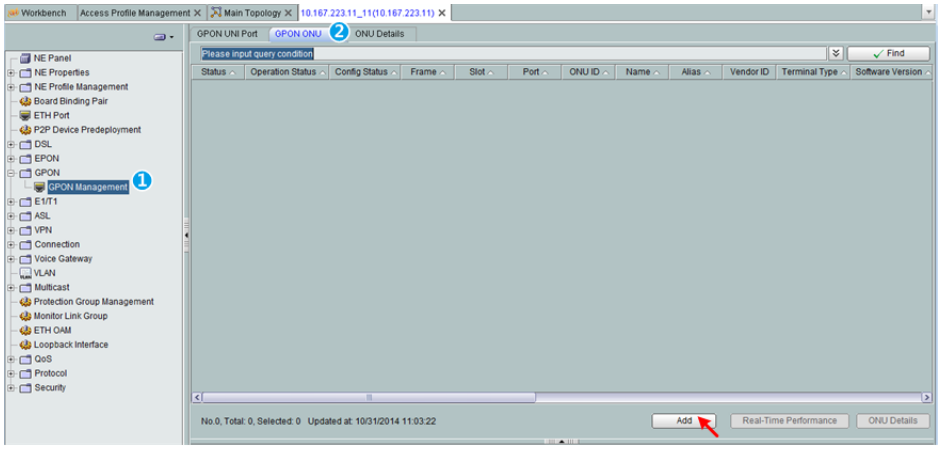


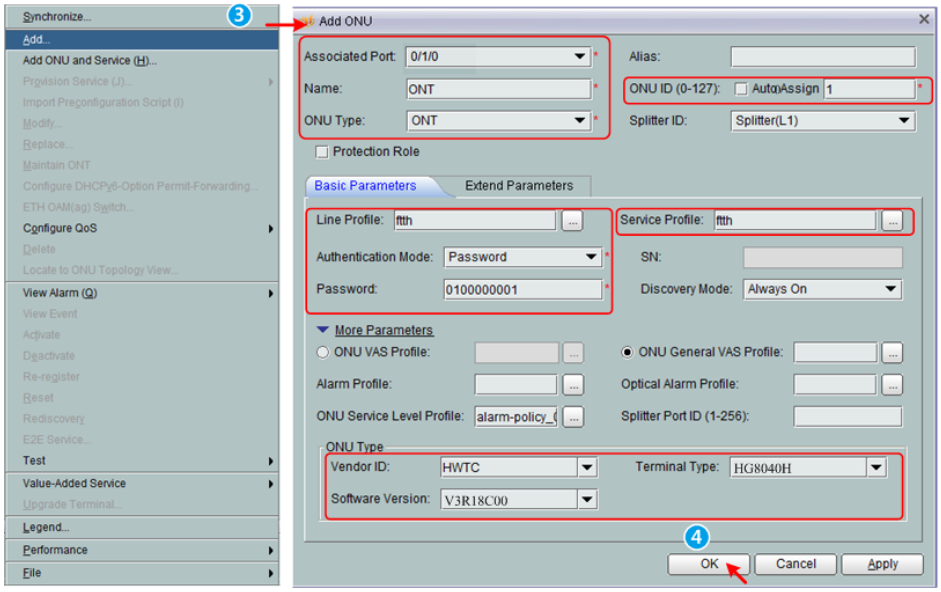
- **Provision services.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



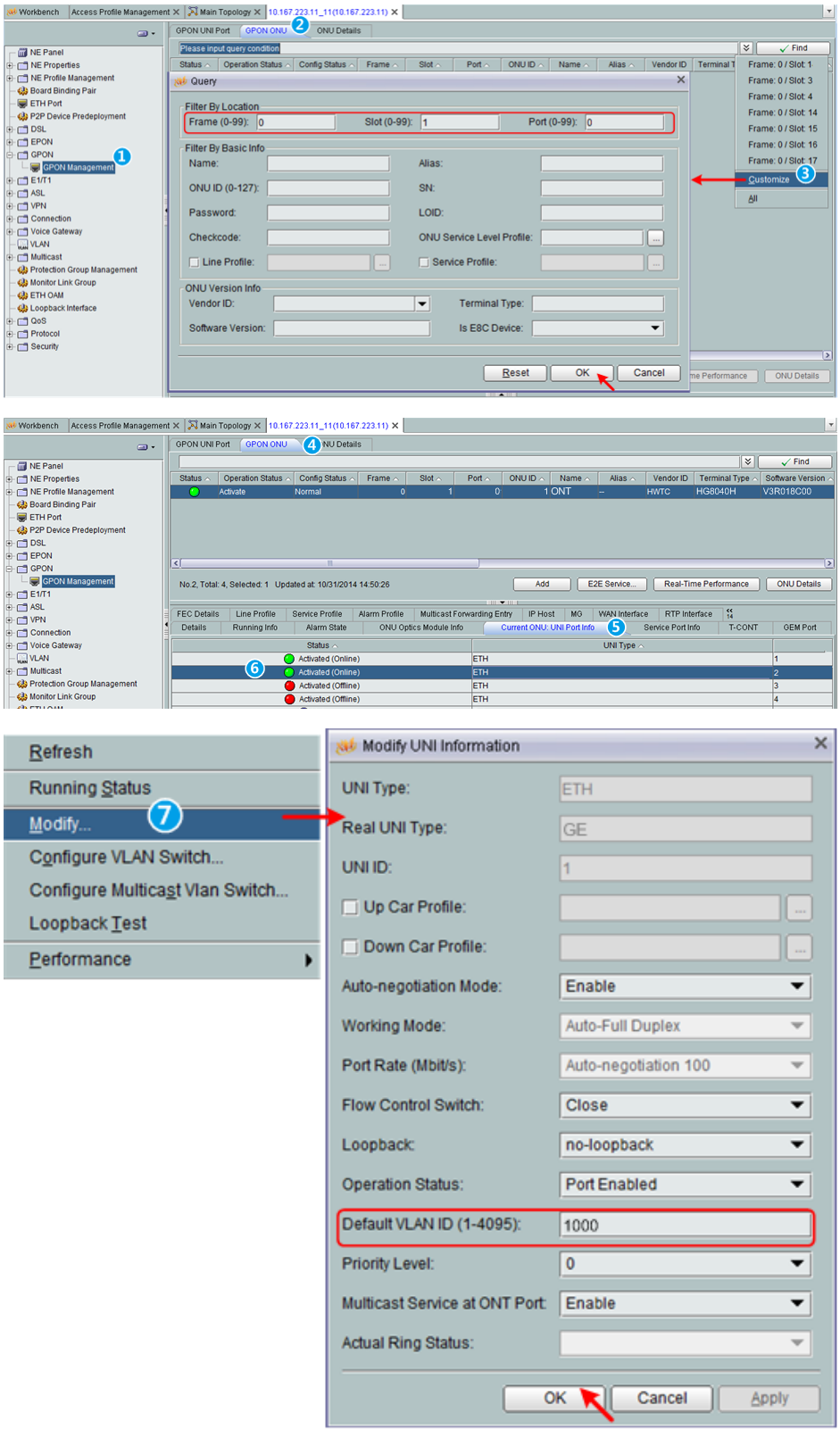


NOTE

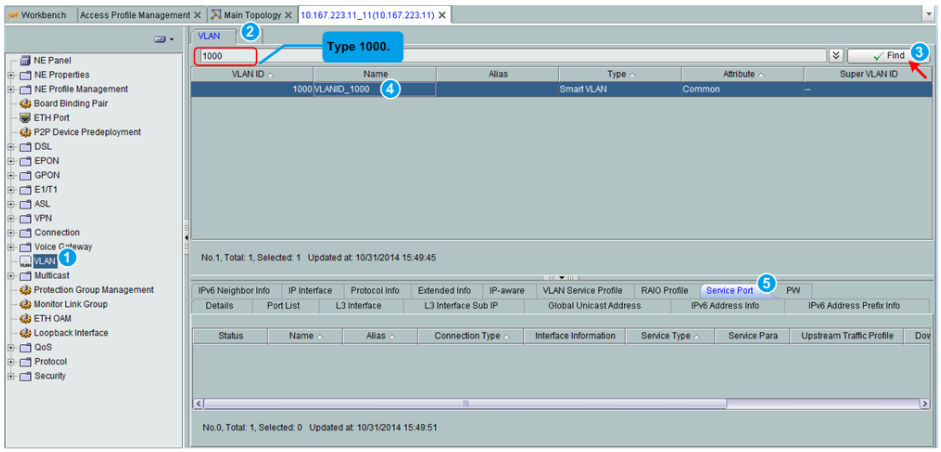
HG8010H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

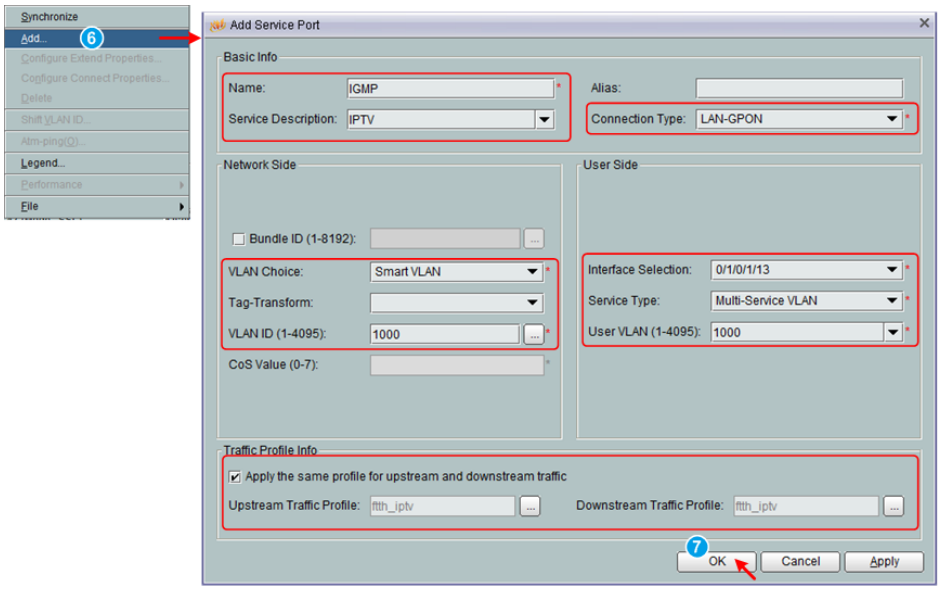
The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

b. **Configure Ethernet port attributes and service channels of a GPON ONU.**

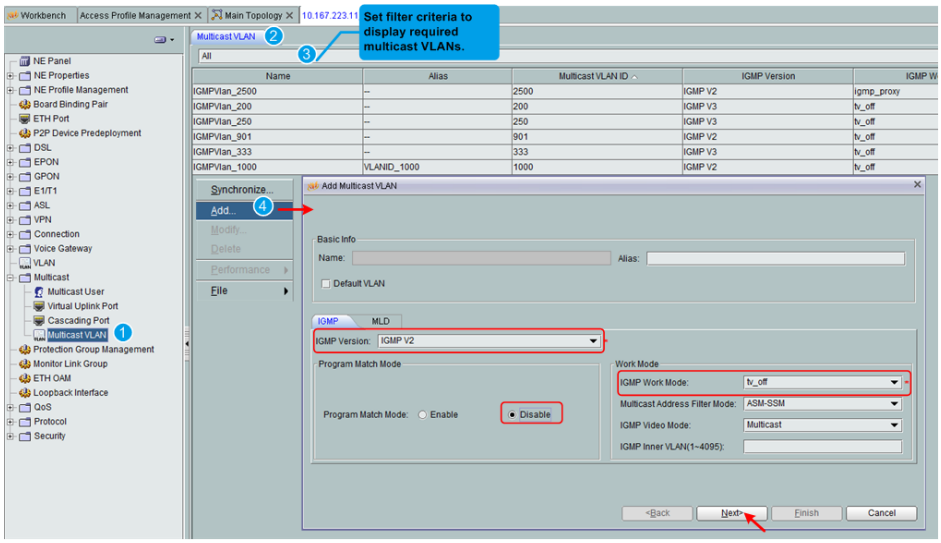


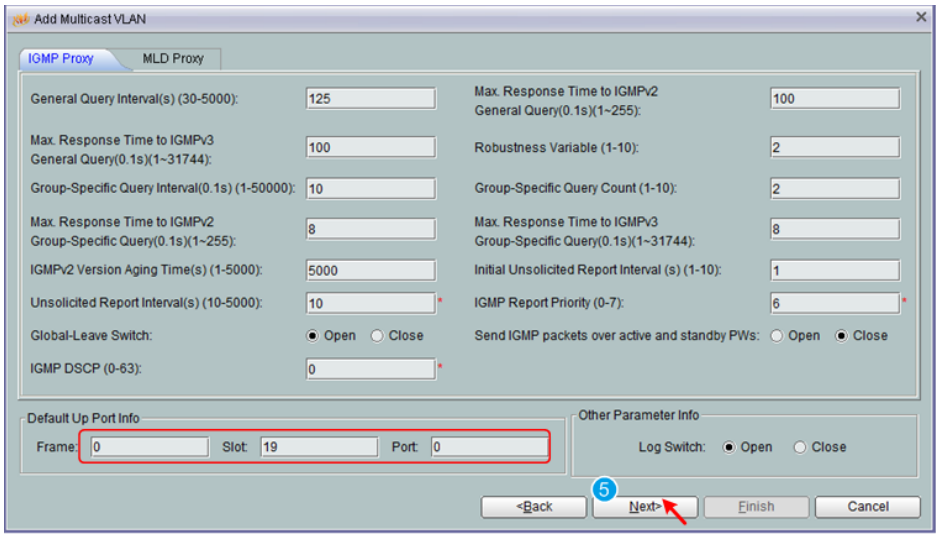
c. **Add a service virtual port on the OLT side.**

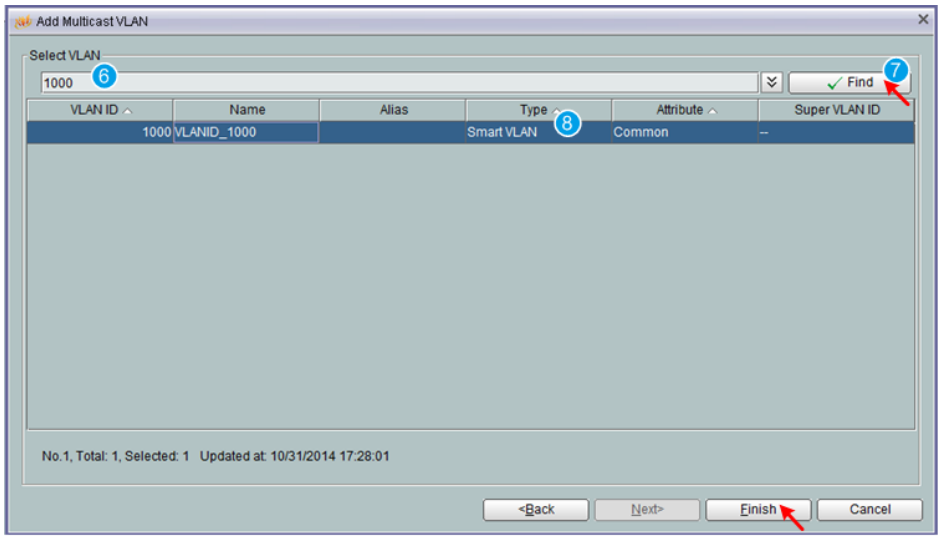




d. **Add a multicast VLAN on the OLT side.**







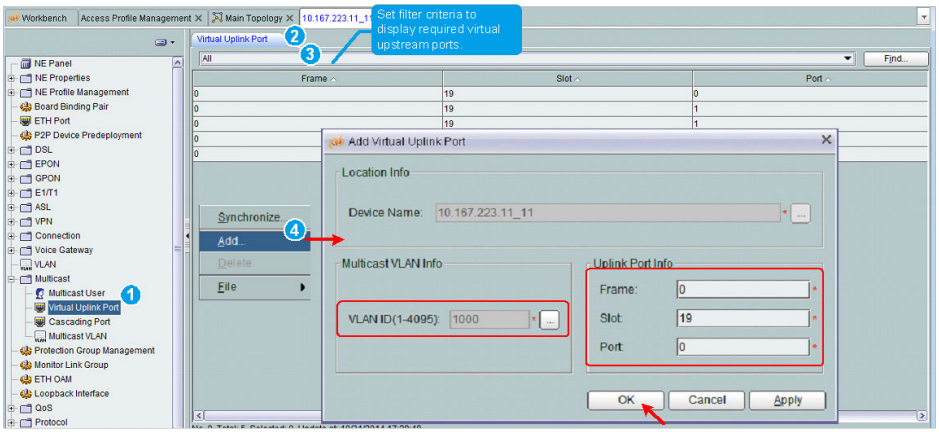
NOTE

Program match mode can be set when **IGMP Work Mode** is **tv_off**. The values of **Program match mode** are as follows:

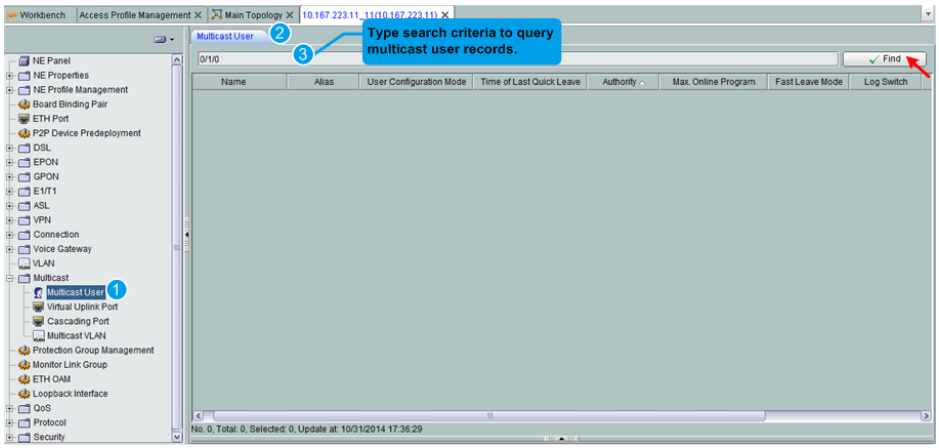
- Enable: Multicast programs are configured statically. Dynamic program generation is not supported.
- Disable: Multicast programs are dynamically generated. Static program configuration is not supported.

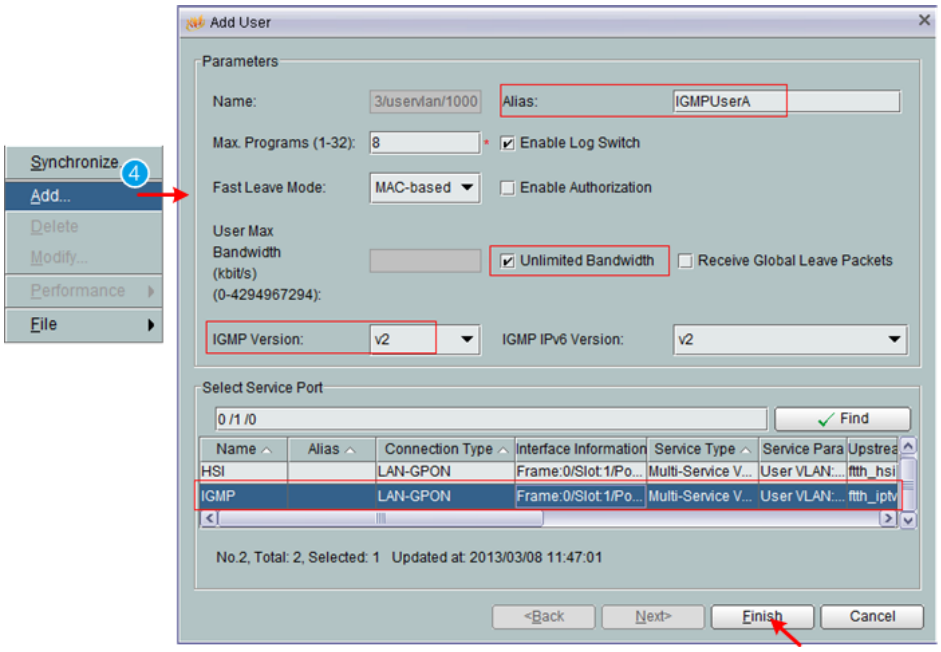
After Configuration, **IGMP Work Mode** should be set to **Proxy** again, otherwise IGMP work abnormally.

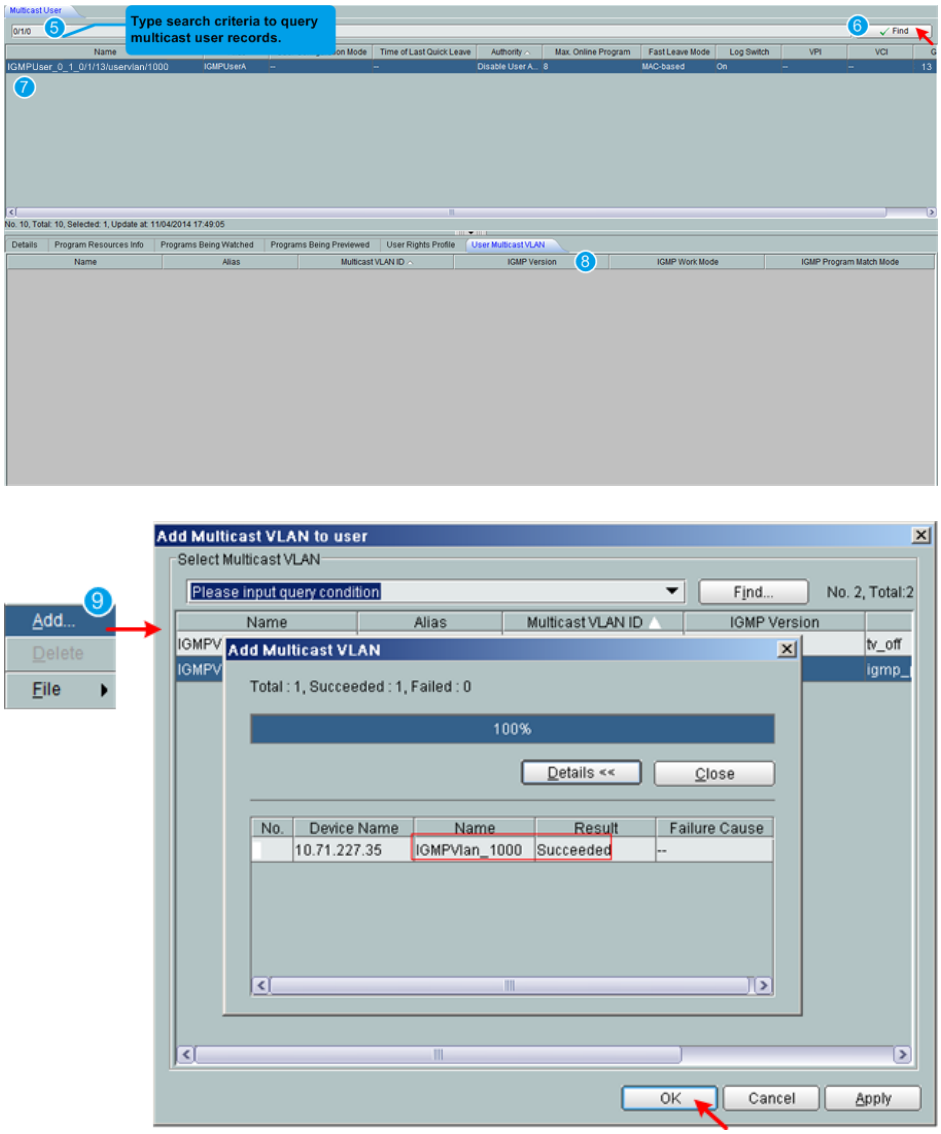
e. **Add a virtual multicast upstream port on the OLT side.**



f. **Configure a multicast user on the OLT side.**







Result

The user can watch programs on TV.

1.4 Configuration by Using OLT Commands

This topic describes how to configure the Internet access service, VoIP service and IPTV service by using OLT commands.

1.4.1 Bridging ONT + HGW Network Scenario (GPON and 10G GPON Access)

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when bridging ONTs + HGWs are used to build an FTTH network.

The FTTH GPON and 10G GPON access have the same configuration procedure. ONT web pages for configuring them have differences; however, they have the same configuration

parameters. The following uses GPON ONT configuration as an example. For differences on web pages, see the related ONT manuals.

1.4.1.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to user homes and triple play services are required. The following provides detailed service requirements:

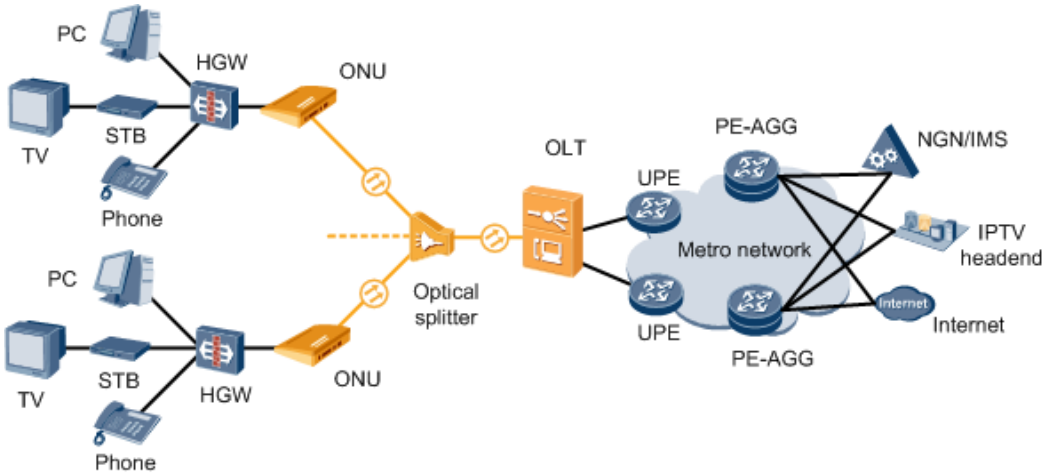
- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service extension is supported and different services do not affect each other.
- Proper service security is ensured.
  - Internet access services are protected against unauthorized access, user account theft or borrowing, MAC/IP spoofing, and malicious attacks.
  - Voice and IPTV services are protected against MAC/IP spoofing, malicious attack, and traffic flooding attacks.
- Service faults are easy to locate and services are easy to maintain.

Application Scenario

As shown in **Figure 1-4**, the HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users.

Services are mainly implemented on the HGW, and the bridging ONT works with the OLT to provide Layer 2 channels.

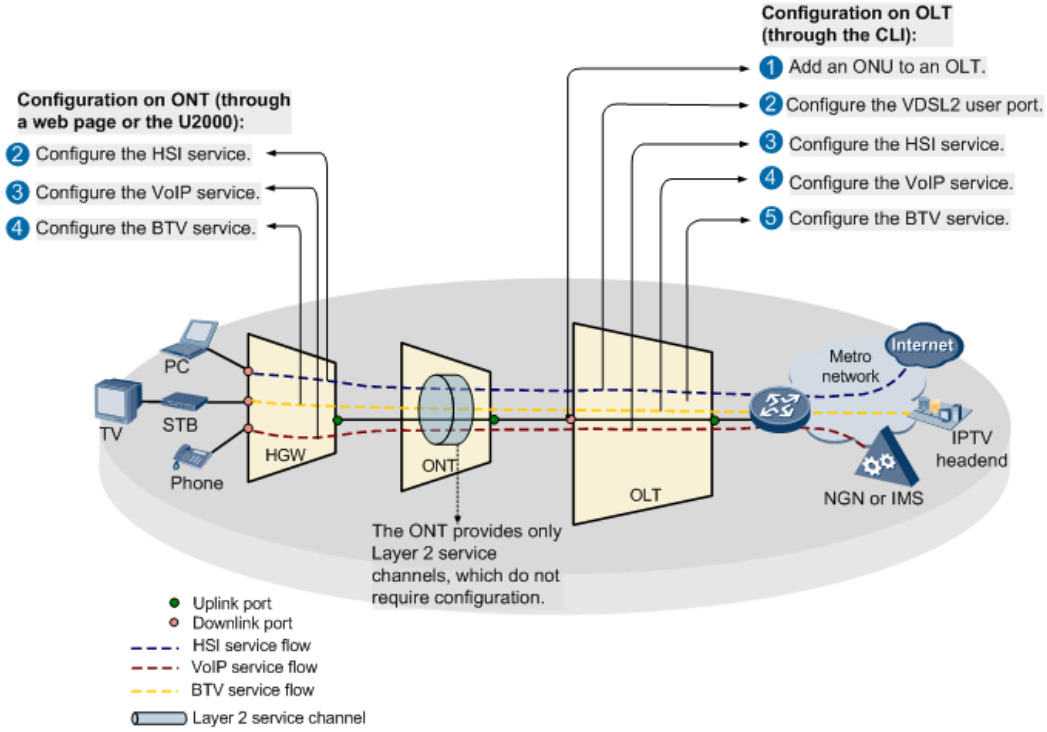
Figure 1-4 Bridging ONT + HGW



1.4.1.2 Configuration Process

Figure 1-5 shows the configuration roadmap in fiber to the home (FTTH) networking using a bridging optical network terminal (ONT)+home gateway (HGW).

Figure 1-5 Configuration roadmap in FTTH networking using a bridging ONT+HGW



The following table describes the configuration steps.

Item	Step		Description
Optical line terminal (OLT)	Adding an ONT to an OLT		Services can be configured for an ONT only after the ONT is successfully added to an OLT.
OLT HGW	Configuring the Internet Access Service		• An ONT provides only Layer 2 service channels, which do not require configuration. An HGW is equipped with an integrated access device (IAD) provides the Internet access, VoIP, and IPTV services for users. • IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.
	Configuring the Voice Service		
	Configure the IPTV service.	Configuring the BTV Service	
		Configuring the VoD Service	
OLT	Configuring Link Aggregation, Congestion Control, and Security Policies		The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Item	Step	Description
OLT	Verifying Services	The OLT provides remote verification methods including ONT PPPoE/DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

1.4.1.3 Adding an ONT to an OLT

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Data Plan

Item	Data
DBA profile	Profile name: ftth_dba_mngt ● Profile type: Type1 ● Fixed bandwidth: 1 Mbit/s Profile name: ftth_dba_hsi ● Profile type: Type4 ● Maximum bandwidth: 32 Mbit/s Profile name: ftth_dba_voip ● Profile type: Type2 ● Assured bandwidth: 1 Mbit/s Profile name: ftth_dba_iptv ● Profile type: Type2 ● Assured bandwidth: 1 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID for management services: 4 T-CONT ID for voice services: 5 T-CONT ID for video services: 6 T-CONT ID for Internet access services: 7 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: adaptive

Item	Data
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2

Procedure

Step 1 Configure GPON ONT profiles.

GPON ONT profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONT-side service.
- Service profile: A service profile provides the service configuration channel for the ONT that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONT lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query the existing DBA profiles in the system. If the existing DBA profiles in the system cannot meet the requirements, run the **dba-profile add** command to add a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name ftth_dba_mngt type1 fix 1024
   huawei(config)#dba-profile add profile-name ftth_dba_voip type2 assure 1024
   huawei(config)#dba-profile add profile-name ftth_dba_iptv type2 assure 1024
   huawei(config)#dba-profile add profile-name ftth_dba_hsi type4 max 32768
   ```

   NOTE

   Select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONT. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba_mngt
   huawei(config-gpon-lineprofile-1)#tcont 5 dba-profile-name ftth_dba_voip
   huawei(config-gpon-lineprofile-1)#tcont 6 dba-profile-name ftth_dba_iptv
   huawei(config-gpon-lineprofile-1)#tcont 7 dba-profile-name ftth_dba_hsi
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.


```
huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 5
huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 6
huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 7
```

NOTE

1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

After the configurations are complete, run the **commit** command to apply the parameters settings.

```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure an ONT service profile.

   Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   ```

   After the configurations are complete, run the **commit** command to apply the parameters setting.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.
   - The default GPON alarm profile 1 is used. The alarm thresholds for the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONT line.

Step 2 Add an ONT.

The procedures for configuring GPON, XG-PON, and XGS-PON services are the same. The difference lies in this step. Here, the GPON service is used as an example. When configuring XG-PON and XGS-PON services, you need to configure the ONT network-side interface type parameter (ont-type) in the **ont add** and **ont confirm** commands. Select a value based on the actual ONT capability or service data plan, for example, 10g/2.5g.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **3230313126595540** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-
  aging omci ont-lineprofile-name
  ```

```
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-
aging omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

- Confirm automatically discovered ONTs.

  If the password or SN of an ONT is unknown, run the **port *portid* ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONTs connected
to the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 3230313126595540
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

  NOTE

  If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-
name ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of
the ONT is normal.
  Match state          : match     //Indicates that the capability profile bound
to the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactivated**, run the **ont activate** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the

diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.

----End

1.4.1.4 Configuring the Internet Access Service

The OLT is connected to the remote ONT through a GPON port to provide users with high-speed Internet access services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONT has been added to the OLT. For details, see **1.4.1.3 Adding an ONT to an OLT**.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.
- Residential users generally access the Internet in Point-to-Point Protocol over Ethernet (PPPoE) dial-up mode. PPPoE dial-up can be performed on personal computers (PCs) or HGWs.
- The configuration processes on HGWs of different models or in different appearances are similar. This topic describes how to configure the Internet access service on an HG239 that is connected to an ONT upstream through a LAN.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID for Internet access service: 14
Network topology data	Upstream port: 0/9/0 PON port: 0/1/0 ONT IDs: 1 and 2 ID of the port on the HGW that is connected to the PC: 1

Item	Data
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-VLAN ID: 1001-1002 ● U-VLAN ID: 45 VLAN translation policy: ● ONT: The upstream packets sent from the HGW carry user-VLANs and the ONT transparently transmits them. ● OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the profile ID to ftth_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

     ```
     huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0
     priority-policy local-setting
     ```

  b. Configure the mapping between a GEM port and a VLAN.

     The service flow of user-side VLAN 45 is mapped to GEM port 14 in the ONT line profile.

     NOTE

     Here, the user-side VLAN is the VLAN carried by packets sent from HGW to ONT, namely, U-VLAN.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 45
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  c. Configure the VLAN of the Ethernet port on the ONT.

     Add Ethernet port 1 to VLAN 45 in the ONT service profile.

     ```
     huawei(config)#ont-srvprofile gpon profile-name ftth
     huawei(config-gpon-srvprofile-1)#port vlan eth 1 45
     huawei(config-gpon-srvprofile-1)#commit
     ```

  d. Create an Internet access service VLAN and add an upstream port to it.

     Add upstream port 0/9/0 to VLAN 100.


```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/9 0
```

e. Create Internet access service flows.

Set S-VLAN ID to 100 and GEM port ID to 14. Use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service user-vlan 45 tag-transform translate-and-add
inner-vlan 1001 inbound traffic-table name ftth_hsi outbound traffic-
table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-
service user-vlan 45 tag-transform translate-and-add
inner-vlan 1002 inbound traffic-table name ftth_hsi outbound traffic-
table name ftth_hsi
```

f. Save the data.

```
huawei(config)#save
```

- Configure the HGW.

a. Log in to the web configuration window.

i. Enter the default IP address in the address bar of the browser, and then press **Enter**.

ii. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

b. Set parameters for the Internet access service.

i. Choose Internet access service configuration from the navigation tree.

ii. Set parameters for the Internet access service.

Parameter	Value
Bearing service	Internet
VLAN enabling (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	Enabled: VLAN tags are added to upstream packets. **NOTE** When Internet access service flows are created on the OLT, if the value of **uservlan** is **untagged**, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID[1-4094] (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	The internet VLAN ID on the HGW. In this example, set this parameter to **45**.

Parameter	Value
VPI/VCI (Set this parameter when the HGW uses ADSL2+ for upstream transmission)	Set the VPI/VCI to be the same as that configured on the devices at the central office. In this example, set this parameter to **0/35**.
Mode	PPPoE

iii. Submit the configuration.

----End

1.4.1.5 Configuring the Voice Service

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see **1.4.1.3 Adding an ONT to an OLT**.
- HGWs have different models and appearance and therefore, their configuration processes are not the same. This topic describes how to configure the voice service on an HGW. The actual configuration varies depending on different HGWs.
- The built-in integrated access device (IAD) of the HGW uses SIP as the voice protocol.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● UVLAN ID: 47 VLAN translation policy: ● ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. ● OLT: translates the VLAN tag (user VLAN <-> S-VLAN).
Voice parameter	IP address of the SIP server: 10.10.100.10/24 Port ID of the SIP server: 5060 User phone number: 77730010

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     ```
     huawei(config)#traffic table ip name ftth_voip cir off priority 5
     priority-policy
      local-setting
     ```

  b. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 47 is mapped to GEM port 12 in the ONT line profile.

     NOTE

     The user VLAN is the VLAN in the packets sent from the HGW to the ONT, that is, the UVLAN.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 47
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  c. Configure the VLAN of the Ethernet port on the ONT.

     If the ONT is connected to the HGW through Ethernet port 1, add Ethernet port 1 to VLAN 47 in the ONT service profile.

     ```
     huawei(config)#ont-srvprofile gpon profile-name ftth
     huawei(config-gpon-srvprofile-1)#port vlan eth 1 47
     ```



```
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

d. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/9 0
```

e. Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 47, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 47 inbound traffic-table name ftth_voip outbound traffic-table
name ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 47 inbound traffic-table name ftth_voip outbound traffic-table
name ftth_voip
```

f. Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

g. Save the data.

```
huawei(config)#save
```

- Configure the HGW.

a. Log in to the web configuration window.

i. Enter the default IP address in the address bar of the browser, and then press **Enter**.

ii. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

b. Set parameters of the voice service.

i. Choose the voice service configuration from the navigation tree.

ii. Set parameters of the voice service.

Parameter	Value
Bearing service	VoIP
Enabling status	Enabled

Parameter	Value
VLAN enabling (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	Enabled: VLAN tags are added to upstream packets. **NOTE** When voice service flows are created on the OLT, if the value of **uservlan** is **untagged**, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID[1-4094] (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	The voice VLAN ID on the HGW. In this example, set this parameter to **47**.
VPI/VCI (Set this parameter when the HGW uses ADSL2+ for upstream transmission)	Set the VPI/VCI to be the same as that configured on the devices at the central office. In this example, set this parameter to **0/35**.
802.1p	Enabled
Mode	Route: Route mode
DHCP	Enabled

iii. Choose the voice telephone number configuration from the navigation tree. Set the parameters as follows:

Parameter	Value
Address	Preferred IP address of the proxy server: 10.10.100.10
Port ID	Preferred signaling port ID of the proxy server: 5060
Enabled	Enabled
User number	To use the VoIP account, you can set the account to the user telephone number. In this example, set the user telephone number to **77730010**.

Parameter	Value
User password	-

iv. Submit the configuration.

----End

1.4.1.6 Configuring the BTV Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the multicast service.

Prerequisites

- The OLT is connected to the BRAS and the multicast source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **1.4.1.3 Adding an ONT to an OLT**.
- HGWs have different models and appearance and therefore, their configuration processes are not the same. This topic describes how to configure the Internet access service on an HGW generally. The actual configuration varies depending on different HGWs.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting

Item	Data
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● HGW VLAN: 43 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONT: translates the upstream VLAN of the HGW to an MVLAN. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Set the profile name to ftth_iptv. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip name ftth_iptv cir off priority 4
     priority-policy local-setting
     ```

  b. Configure the mapping relationship between a GEM port and a VLAN.

     If the ONT is connected to the HGW through Ethernet port 2, map the service flow of Ethernet port 2 to GEM port 13 in the ONT line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 13 2 vlan 1000
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  c. Configure a VLAN translation policy for the Ethernet port on the ONT.

     If the ONT is connected to the HGW through Ethernet port 2, VLAN 43 of the HGW is translated to VLAN 1000 and the MVLAN of the ONT is translated to VLAN 1000.

     ```
     huawei(config)#ont-srvprofile gpon profile-name ftth
     huawei(config-gpon-srvprofile-1)#port vlan eth 2 translation 1000 user-
     vlan 43
     huawei(config-gpon-srvprofile-1)#multicast-forward tag translation 43
     ```



```
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

d. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/9 0
```

e. Create service flows.

Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile ftth_iptv.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13
multi-service
user-vlan 1000 inbound traffic-table name ftth_iptv outbound traffic-
table name ftth_iptv
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13
multi-service
user-vlan 1000 inbound traffic-table name ftth_iptv outbound traffic-
table name ftth_iptv
```

f. Create an MVLAN and configure the IGMP version.

Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses
in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

g. Configure a program library.

Set the mode for obtaining multicast programs to dynamic.

NOTE

You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

h. Set the IGMP mode.

Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

i. (Optional) Configure the IGMP upstream port.

In this example, the IGMP upstream port uses default value default.

Run the **display igmp config global** command to query the IGMP upstream port mode. If this mode does not meet the requirement, run the **igmp uplink-port-mode** command to configure it.

j. Configure multicast users.

Add service ports 1 and 2 as multicast users.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

k. Save the data.

```
huawei(config)#save
```

- Configure the HGW.

a. Log in to the web configuration window.

i. Enter the default IP address in the address bar of the browser, and then press **Enter**.

ii. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.

b. Set parameters for the BTV service.

i. Choose BTV service configuration from the navigation tree.

ii. Set parameters for the BTV service.

Parameter	Value
Bearing service	OTHER: It is used for the BTV service.
VLAN enabling (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	Enabled: VLAN tags are added to upstream packets. **NOTE** When BTV service flows are configured on the OLT, if the value of **uservlan** is **untagged**, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID[1-4094] (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	The BTV VLAN ID on the HGW. In this example, set this parameter to **43**.

Parameter	Value
VPI/VCI (Set this parameter when the HGW uses ADSL2+ for upstream transmission)	Set the VPI/VCI to be the same as that configured on the devices at the central office. In this example, set this parameter to **0/35**.
Binding item	LAN3 (Example: LAN3 interface serves as the BTV interface)
Mode	Bridge
DHCP transparent transmission	Enabled

iii. Submit the configuration.

----End

1.4.1.7 Configuring the VoD Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the VoD service.

Prerequisites

- The OLT is connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **1.4.1.3 Adding an ONT to an OLT**.
- HGWs have different models and appearance and therefore, their configuration processes are not the same. This topic describes how to configure the Internet access service on an HGW generally. The actual configuration varies depending on different HGWs.

Data Plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID: 13

Item	Data
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common ● UVLAN (upstream VLAN of the HGW): 41 ● CVLAN=UVLAN VLAN translation policy: ● ONT: transparently transmits the UVLAN of the HGW. ● OLT: implements VLAN translation: U<->S.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Set the profile name to ftth_iptv. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip name ftth_iptv cir off priority 4 priority-policy local-setting
   ```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 41 is mapped to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 41
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the HGW through Ethernet port 2, add Ethernet port 2 to VLAN 41.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#port vlan eth 2 41
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/9 0
```

5. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 41, and use traffic profile ftth_iptv.

```
huawei(config)#service-port vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service user-vlan 41 inbound traffic-table name ftth_iptv
outbound traffic-table name ftth_iptv
huawei(config)#service-port vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service user-vlan 41 inbound traffic-table name ftth_iptv
outbound traffic-table name ftth_iptv
```

6. Save the data.

```
huawei(config)#save
```

Step 2 Configure the HGW.

1. Log in to the web configuration window.
   a. Enter the default IP address in the address bar of the browser, and then press **Enter**.
   b. In the login window, enter the user name and password (the default value is provided by ISP) of the administrator and click **OK**.
2. Set parameters for the VoD service.
   a. Choose VoD service configuration from the navigation tree.
   b. Set parameters for the VoD service.

Parameter	Value
Bearing service	OTHER: It is used for the VoD service.
VLAN enabling (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	Enabled: VLAN tags are added to upstream packets. **NOTE** When VoD service flows are configured on the OLT, if the value of **uservlan** is **untagged**, set this parameter to **Disabled**; otherwise, set it to **Enabled**.
VLANID[1-4094] (Set this parameter when the HGW uses the LAN or VDSL2 for upstream transmission)	The VoD VLAN ID on the HGW. In this example, set this parameter to **41**.

Parameter	Value
VPI/VCI (Set this parameter when the HGW uses ADSL2+ for upstream transmission)	Set the VPI/VCI to be the same as that configured on the devices at the central office. In this example, set this parameter to **0/35**.
Binding item	LAN4 (Example: LAN4 interface serves as the VoD interface)
Mode	Bridge
DHCP transparent transmission	Enabled

c. Submit the configuration.

----End

1.4.1.8 Configuring Link Aggregation, Congestion Control, and Security Policies

The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG).

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **1.2.6 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/9/0 and 0/9/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/9 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling.

According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **1.2.2 Principle of QoS Planning**.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.
    i. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    ii. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    iii. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on the OLT.
    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on the OLT.
    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    i. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    ii. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
      1) In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
      2) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
      3) Perform the following operations to enable MAC address anti-spoofing in VLAN service profile mode:
        1) Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
        2) Run the **commit** command to make the profile configuration take effect.
        3) Run the **quit** command to quit the VLAN service profile mode.
        4) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    iii. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    iv. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on the OLT.
    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three

levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

i. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.

ii. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

iii. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.

    i. Enable DHCP Option 82 on the OLT.

    DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

    - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

      When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
    - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
    - The VLAN level:

      1) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

      2) Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.

      3) Run the **commit** command to make the profile configuration take effect.

      4) Run the **quit** command to quit the VLAN service profile mode.

      5) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

    ii. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT DHCP packets to carry Option 82 information.
  - Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.

    i. Enable PITP on the OLT.

    PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four

levels. Among the four levels, PITP is disabled only at the global level by default.

- The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

  In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
- The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
- The VLAN level:
  1) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
  2) Run the **pitp enable** command to enable PITP at the VLAN level.
  3) Run the **commit** command to make the profile configuration take effect.
  4) Run the **quit** command to quit the VLAN service profile mode.
  5) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

ii. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT PPPoE packets to carry a vendor tag.

----End

1.4.1.9 Verifying Services

In the FTTH scenario, ONTs are installed in users' houses which are far away from the central equipment room. ONTs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONTs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONT simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONT supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONT simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONT can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel is. ● An ONT supports a maximum of a call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONT. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test1234	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONT POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.

Item	Data	Remarks
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  a. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test1234
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 192.168.100.101
  Gateway IP           : 192.168.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  a. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
     - If a native VLAN is configured for the Ethernet port on the ONT, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.
  b. Check the upstream and downstream ports by checking the MAC address learning status.

i. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
   - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
   - If the downstream port does not learn a MAC address, check whether the ONT is activated, whether the PC is connected to the right port on the ONT, and whether the PC is working properly.

ii. Run the **display ont-learned-mac** command to check whether the ONT connecting to the PON port learned any MAC addresses.

   If not, check whether the ONT properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.

  a. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
77730020
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 77730020
```

  b. The ONT outputs the call emulation result after the test is complete.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 77730020
  Reported number      : 77730020
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.

  a. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

  b. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
     - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
     - If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
     - If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONT and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.

c. Check the registration status of the voice service.

- You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
- If the ONT uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONT. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
- You can query the registration status of the voice service on the ONT web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- Verify the multicast service using multicast emulation.

a. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan
1000
```

NOTE

If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

b. Run the **display igmp user** command to query the status of the multicast user.

```
huawei(config-btv)#display igmp user service-port 1
  User                        : 0/1/0/1
  State                       : online
  Authentication              : no-auth
  Quick leave                 : MAC-based
  IGMP flow ID                : 1
  Video flow ID               : 1
  Log switch                  : enable
  Bind profiles               : -
  IGMP version                : IGMP v3
  Current version             : IGMP v3
  Current IGMP IPv6 version   : IGMP IPv6 v2
  Available programs          : 8
  Global leave                : disable
  User max bandwidth          : no-limit
  Used bandwidth(kbps)        : 0
  Used bandwidth
  to max bandwidth(%)         : -
  Total video bandwidth       : -
  Mcast video bandwidth       : -
  Active program list

------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start time

------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                         16:33:41+08:00

------------------------------------------------------------------------
--
  Total: 1
```


c. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

1.5 Configuring FTTH IPv6 Services in Bridging-type ONT Scenario (Dual Stack/DS-Lite)

This topic describes how to configure FTTH IPv6 services when the ONT is a bridging-type ONT and the dual stack or DS-Lite solution is used.

Dual Stack Application Scenario

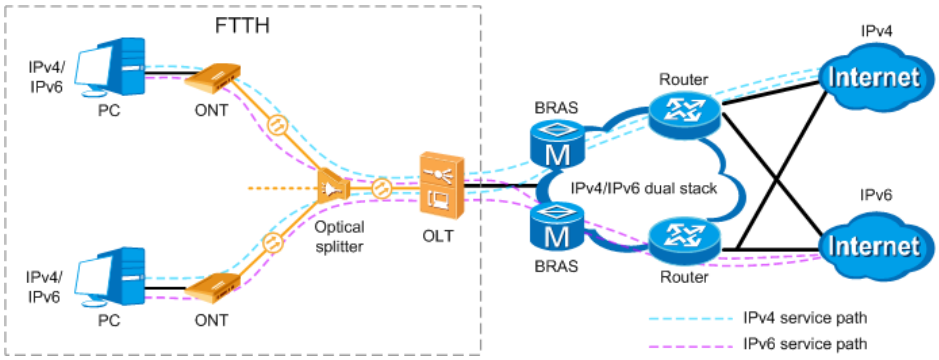
Networking description:

- All NEs must support both IPv4 and IPv6.
- The BRAS directly assigns IPv4 and IPv6 addresses to PCs, and the ONT transparently transmits IPv4 and IPv6 packets.
- PCs use IPv4 and IPv6 addresses to access the IPv4 Internet and IPv6 Internet respectively.
- Both the OLT and ONT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction: All NEs on the network need to be upgraded to support IPv4 and IPv6 dual stacks.

Figure 1-6 shows the dual-stack networking diagram.

Figure 1-6 Dual-stack networking diagram



DS-Lite Application Scenario

Networking description:

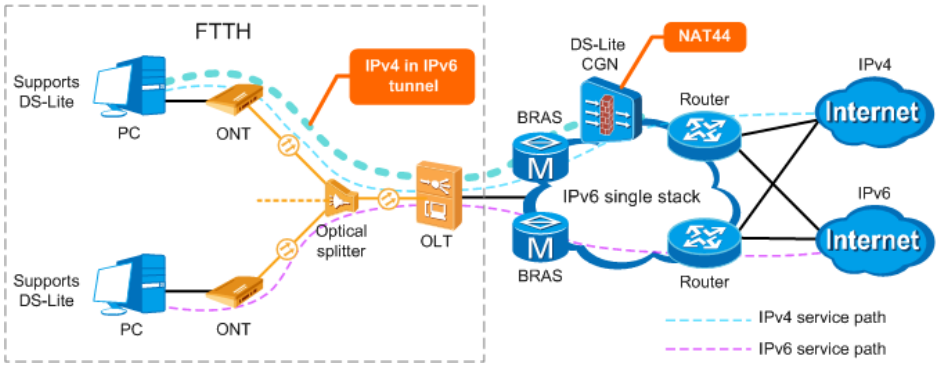
- Devices below the DS-Lite CGN must support the IPv6 single stack.
- The BRAS directly assigns IPv6 address prefixes (without IPv4 address) to PCs, and the ONT transparently transmits IPv6 packets.
- IPv4 addresses are encapsulated into IPv6 packets for forwarding, decapsulated on the DS-Lite CGN, and forwarded to the IPv4 Internet after NAT44 translation. IPv6 addresses are directly forwarded to the IPv6 Internet through IPv6 devices.
- Both the OLT and ONT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction:

- A special software needs to be installed on the PC to support DS-Lite.
- The CGN needs to be upgraded to support DS-Lite.
- Devices between the CGN and PC need to be upgraded to support IPv6.
- The DS-Lite CGN device needs to be added.

Figure 1-7 shows the DS-Lite networking diagram.

Figure 1-7 DS-Lite networking diagram



Procedure

- Configuration using the U2000

NOTE

In the dual stack and DS-Lite scenarios, both the OLT and ONT implement Layer 2 transparent transmission. Configurations in the FTTH scenario are the same as those for IPv4.

When the access mode of IPv6 users is IPoE and the BRAS uses the binding authentication mode, users do not need to enter user names or passwords for authentication because the BRAS performs authentication based on users' physical information. In this case, DHCPv6 Option18 needs to be configured on the OLT. For the mapping relationship between DHCPv6 Option and the BRAS, see **Table 1-8**.

Table 1-8 DHCPv6 Option mapping

DHCPv6 Option	OLT	BRAS
Option17	N/A	Optional

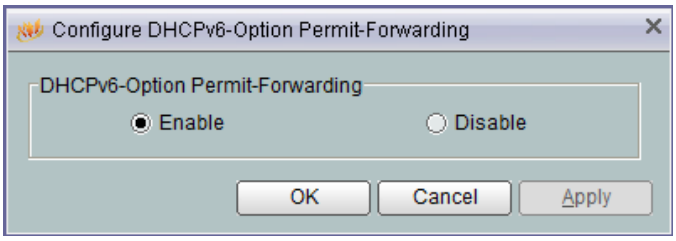
DHCPv6 Option	OLT	BRAS
Option18	Mandatory	Mandatory
Option37	Optional	Optional

NOTE

By default, the global DHCPv6 Option configuration is **disable**, the VLAN-level DHCPv6 Option configuration is **enable**, and the upstream/cascaded port-level DHCPv6 Option configuration is **enable**. Therefore, you only need to enable DHCPv6 Option globally.

After DHCPv6 Option is enabled, the OLT inserts Option18 and Option37 into DHCPv6 packets for authentication by the BRAS.

1. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT 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 GPON ONUs.
4. Right-click a required ONT and choose **Configure DHCPv6–Option Permit-Forwarding**.
5. In the dialog box that is displayed, select **Enable**.



6. Click **OK**.

- Configuration using OLT commands

NOTE

In the dual stack and DS-Lite scenarios, both the OLT and ONT implement Layer 2 transparent transmission. Configurations in the FTTH scenario are the same as those for IPv4.

When the access mode of IPv6 users is IPoE and the BRAS uses the binding authentication mode, users do not need to enter user names or passwords for authentication because the BRAS performs authentication based on users' physical information. In this case, DHCPv6 Option18 needs to be configured on the OLT. Table 1-9 describes the mapping between the BRAS, OLT, and DHCPv6 Option.

Table 1-9 DHCPv6 Option mapping

DHCPv6 Option	OLT	BRAS
Option17	N/A	Optional
Option18	Mandatory	Mandatory
Option37	Optional	Optional

NOTE

By default, the global DHCPv6 Option configuration is **disable**, the VLAN-level DHCPv6 Option configuration is **enable**, and the upstream/cascaded port-level DHCPv6 Option configuration is **enable**. Therefore, you only need to enable DHCPv6 Option globally.

After DHCPv6 Option is enabled, the OLT inserts Option18 and Option37 into DHCPv6 packets for authentication by the BRAS.

```
huawei(config)#raio-mode common dhcpv6-option
huawei(config)#dhcpv6 option enable
```

- The ONT implements Layer 2 transparent transmission. Therefore, no configuration needs to be performed on the ONT Web page.

2 Configuring the Bridging+Voice ONT

About This Chapter

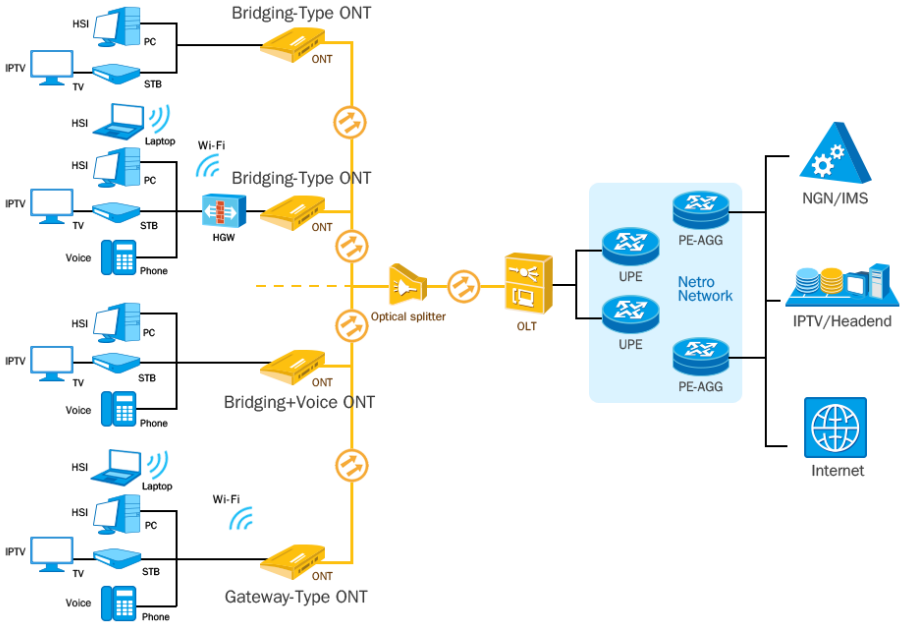
This topic describes the configuration of bridging+voice ONTs and their web pages. Bridging +voice ONTs only support Layer 2 and voice features.

2.1 FTTH Networking and Configuration Scenarios

Typical FTTH Networking

Figure 2-1 shows the typical FTTH networking.

Figure 2-1 Typical FTTH networking diagram



Networking Scenario	Description
Bridging ONT + HGW Network Scenario	The HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users. Services are implemented on the HGW, and the bridging ONT works with the OLT to provide Layer 2 channels.
Bridging +Voice ONT Network Scenario	The ONT integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users. The bridging+voice ONT provides Layer 2 data and voice services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking. ● For data services, a PC directly performs dial-up. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address. ● The ONT with a built-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).
Gateway ONT Network Scenario	The ONT integrating an IAD provides Internet, VoIP, and IPTV services to users. The HGW ONT facilitates interconnection of home devices by providing Layer 3 services, such as Point-to-Point Protocol over Ethernet (PPPoE)/ DHCP dial-up, network address translation (NAT), and Internet Group Management Protocol (IGMP) snooping. This scenario provides fine-grained management channels and service control, and applies to Layer 3 networking.

FTTH Deployment Schemes

FTTH service application includes the deployment process and service provisioning process. The FTTH deployment process includes OLT deployment (configuration) and configuration of basic data. No deployment, however, is required on the ONT and the ONT is plug and play once services are provisioned.

Table 2-1lists the FTTH deployment schemes and service provisioning methods.

Table 2-1 FTTH deployment schemes

-	Scheme	Parameter
Pre-configuration	● **On the NMS**: Profiles can be issued in batches. ● **Using commands on the OLT**: Configuration scripts containing commands can be imported to the OLT.	● DBA profile ● Line profile ● Service profile ● IP traffic profile ● Service level profile ● Global OLT configurations (rather than FTTH user configurations) such as multicast VLAN, multicast mode, and policy of forwarding unknown packets ● FTTH user service VLAN configurations including adding VLANs, setting the attributes of VLANs, and adding upstream ports for VLANs

-	Scheme	Parameter
Service Provisioning	● **Using the OSS**: This method is recommended and it can implement automatic service provisioning, and eliminate problems caused by manual service provisioning, such as large workload, low efficiency, and difficult management. ● **Using OSS+ITMS**: This method is recommended if the multiple private nodes are customized for carriers. Using a TR069 server, new gateways and value-added voice services can be simply added. – Layer 2 configuration data is issued on the NMS or OLT. – Other configuration data such as voice, Layer 3, and Wi-Fi data is issued using the ITMS. ● **On the NMS**: It applies to the scenario when no OSS is available and services need to be provisioned manually on the NMS. ● **On the ONT web page**: When it is not feasible to provision services on the OSS or NMS, you can log in to the ONT web page and configure or modify parameters to provision services.	See **Table 2-2**. ONT service provisioning parameters are classified into common parameters and customized parameters: ● Customized parameters are usually issued by the upper-layer system during service provisioning. ● Common parameters are usually configured at delivery

Table 2-2 Parameters required for ONT service provisioning

Parameter Type	Layer 2	Voice	Above Layer 2 (Layer 3, Wi-Fi, and User Security)
Customized parameters	Parameters for adding ONTs, adding service flows, activating ports, configuring port rate limitation, and adding multicast users	● **Registration information**: IP address and port number of the local end and the proxy ● **User data**: SIP user name and H.248 TID	Login user name and password
Common parameters	Various pre-configured profile data	● **Digitmap**: includes the digitmap timer and digitmap character strings. ● **Time configuration**: includes registration heartbeat and protocol timers. ● **Encoding and decoding**: includes voice encoding and decoding priorities and packetization period, G.711/G.729/G.722. ● Fax/Modem. ● Service permission and service data. ● **VAG**: implements multiple virtual AG devices on one physical device. ● Configurations for the interconnection between IMSs of softswitches of different specifications.	● WAN port configurations (routes, bridge WANs, and VLANs) ● LAN/WAN binding ● IGMP mode ● URL for the ITMS ● NTP server ● Default Wi-Fi configurations ● Local login IP address
ONT type	● Bridging ONTs (SFUs) ● Bridging+voice ONTs ● Gateway-type ONTs (HGUs)	● Bridging+voice ONTs. ● Gateway-type ONTs.	Gateway-type ONTs

The following describes the involved configuration scenarios:

- Service configuration on the NMS: Pre-configurations and service provisioning are implemented on the NMS. The ONT software version V300R018C00 is used as an example to describe how to provision the services on the NMS.
- Service configuration using commands: Pre-configurations are implemented using commands, and service provisioning is implemented on the ONT web pages.
- Service provisioning on the ITMS: Pre-configurations are implemented on the NMS or using commands, and Layer 3 and voice services are provisioned on the ITMS. Huawei U2560 is used as an example to describe how to provision the services on the ITMS.

Recommended tool: FTTx Script Generation Tool

This tool can generate configuration scripts through the configuration wizard for you efficiently or instantly transform any configuration page into a command script, making your configuration easy and improving your configuration efficiency.

Click to experience (for Carrier) : **FTTx Script Generation Tool**.

Click to experience (for Enterprise) : **FTTx Script Generation Tool**.

2.2 Principle of FTTH Data Plan

2.2.1 Data Plan Principles for IP Addresses

This section describes how to obtain an IP address in various scenarios.

Terminal Type	Service	Recommended Solution
Bridging +Voice ONT	Internet access	A PC obtains an IP address through PPPoE dialup. The ONT transparently transmits the packets.
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The set top box (STB) obtains an IP address from the DHCP server for ordering programs. The ONT transparently transmits the packets.
Bridging ONT+HGW	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. At the same time, the HGW functions as a DHCP server and allocates IP addresses to PCs through the network cable and wireless fidelity (Wi-Fi) access. The ONT transparently transmits the packets.

Terminal Type	Service	Recommended Solution
	VoIP	The HGW functions as a DHCP client and obtains an IP address from the DHCP server, or the application control server (ACS) issues a static IP address to the HGW using TR069. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port. The ONT transparently transmits the packets.
	IPTV	The HGW is configured with a bridging WAN port. The STB obtains an IP address from the DHCP server. The HGW transparently transmits packets. The ONT also transparently transmits the packets.
Gateway ONT	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. The ONT functions as a DHCP server and allocates IP addresses to PCs through the network cable.
	Wi-Fi access	● Layer 3 bridge Wi-Fi access service: A mobile equipment (ME) searches the SSID. After the ME is authenticated, the DHCP server assigns this ME the IP address by IPoE. ● Layer 3 route Wi-Fi access service: An ME searches the SSID. After the ME is authenticated, the DHCP address pool of an ONT assigns this ME the IP address and then PPPoE dialup is automatically performed on the ONT.
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The ONT functions as a DHCP client and obtains an IP address from the DHCP server. At the same time, the ONT functions as a DHCP server and allocates IP addresses to STBs.

2.2.2 Principle of QoS Planning

The QoS planning is an E2E planning, and it can be divided into following policies: traffic classification, marking, and scheduling policy; and traffic monitoring and DBA policy.

Traffic Classification, Marking, and Scheduling Policy

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONT Queue.ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Wi-Fi access service	1	PQ	1	1	1
Internet access service	0	PQ	0	0	0

NOTE

The greater the priority value, the higher the priority. The service priorities in this table are the recommended values. The service priorities are arranged according to the operators's actual plan.

Traffic Monitoring and DBA Policy

Items	Management service	Internet access service	Wi-Fi access service	VoIP service	IPTV service
GEM port	11 [Remark 1]	14	15	12	13
TCONT	Select a DBA type based on service types. For example, select Type1 for the management service, Type4 for the Internet access service, and Type2 for the VoIP and IPTV services.				
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)				
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is larger than or equal to the maximum bandwidth that users apply.				

Items	Management service	Internet access service	Wi-Fi access service	VoIP service	IPTV service
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit
Rate limit on ONU upstream port	No rate restriction				
Rate limit on ONU downstream port	No rate restriction				

Remark 1: GEM port value depends on the planning of the service provider, but in principle, use different GEM ports for different services.

Remark 2: **Table 2-3** shows the reference service bandwidth of each service for each user.

Table 2-3 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service/ Wi—Fi access service	Determined based on the service tariff package.	Determined based on the service tariff package.	Available bandwidth of Internet access service or Wi—Fi access service = Committed bandwidth of the service tariff package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 kbit/s	200 kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth is related to the coding format. This bandwidth is calculated for two POTS ports.

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
IPTV service (standard definition program)	N/A	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture information, 10% bandwidth burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires little bandwidth. Therefore, the bandwidth occupied by IGMP packets can be neglected.
IPTV service (high definition program)	N/A	9.7 Mbit/s per channel	

NOTE

- The rate restriction on the BRAS or SR is recommended. OLTs and ONTs do not restrict the rate for service streams.
- If BRAS does not support rate restriction, OLTs can restrict the rate for service streams through the traffic profile.
- Different service packets on the ONT are distinguished by different VLAN IDs. The service packets are mapped to GEM ports based on VLAN IDs so that different service packets are transmitted to different GEM ports. Each GEM port (each service) corresponds to a T-CONT or all GEM ports share a T-CONT.
- The sum of the assured bandwidth of all ONTs connected to a PON port and the fixed bandwidth of OMCI management channel is less than the GPON upstream bandwidth. Some bandwidth must be reserved for the future service expansion.

2.2.3 Principles of Internet and Wi-Fi Access Services Data Planning

This topic describes the principles of data planning for Internet and Wi-Fi access services and will focus on the VLAN planning and VLAN translation policy planning in different network scenarios.

Table 2-4 Planning of VLANs and VLAN translation policies for Internet access service

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+Voice ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.
Bridging ONT + HGW	Double-tagged VLAN	ONT: The upstream packets sent from the HGW carry user-VLANs and the ONT transparently transmits them. OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.
Gateway ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Table 2-5 Planning of VLANs and VLAN translation policies for Wi-Fi access service

Application Scenario	VLAN Plan	VLAN Translation Policy
Gateway ONT	Single-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S.

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.

- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- To ensure traceability of users and finer-grained QoS control and management of users and services, plan per user per service per VLAN (PUPSPV) for the Internet access service. Considering OLT capacity and VLAN scalability, use dual VLANs (S-VLAN+C-VLAN) on the OLT to differentiate users for the Internet access service.
- The outer VLAN (S-VLAN), which identifies services and physical location, can be allocated based on the OLT, PON board, or PON port. The inner VLAN (C-VLAN) identifies users. C-VLANs must be unique in one S-VLAN.
- It is recommended that you use stacking VLANs as S-VLANs so that security features, such as PPPoE+/option82, and anti-MAC attacks and anti-MAC spoofing, can be easily deployed.
- The 802.1q in 802.1q (QinQ) VLAN is used in the enterprise private line scenario, such as transparent LAN service (TLS), in which the device transparently transmits packets. It is not recommended that you use QinQ VLANs as S-VLANs for the triple play services of residential users.

2.2.4 Principle of Voice Service Data Plan

The voice service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios, and the plan of voice protocol.

VLAN and VLAN Translation Policy

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+voice ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have different C-VLANs. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT +HGW	Single-tagged VLAN (recommended)	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> S-VLAN). All the ONTs connected to the same OLT have the same voice service S-VLAN; ONTs connected to different OLTs may have different voice service S-VLANs. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> C-VLAN). The C-VLAN is an inner VLAN tag that differentiates users. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
Gateway ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN+C-VLAN').

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- The voice service is a closed service operated by carriers. The single-tagged S-VLAN is the mainstream application and is recommended.
- When the planned VLAN is single-tagged VLAN, the S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-VLANs identify services and physical locations. It is recommended that you set different voice VLANs for the OLTs connected to one voice SR to avoid an excessively large broadcast domain of the SR and convergence switch.
- When the planned VLAN is S-VLAN+C-VLAN (that is, double-tagged VLAN), the outer S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-+VLANs identify services and physical locations. It is recommended to allocate S-VLANs based on PON board or PON port. The inner C-VLAN is used to identify services (a fixed value) or users.

Voice Data Plan Based on H.248 or SIP

Item			Description
MG interface/SIP interface data **NOTE** must be consistent with the data on the MGC/IMS core network devices.	Media and signaling parameters	Media and signaling upstream VLANs	Upstream VLANs of the voice service
		Media and signaling upstream port	Upstream ports of the voice service
		Media IP addresses and signaling IP addresses	Supports separating media from signaling.
		Default gateway IP address.	The next hop IP address from an ONU/HGW to an MGC/IMS.
	MG interface/SIP interface ID		N/A
	Signaling port ID		Choose the transmission mode according to the requirement of the MGC/IMS side.

Item		Description
	IP address of active MGC (H.248)/IP address of active IMS device (SIP)	If the dual homing is not configured, only one MGC parameter needs to be configured. If the dual homing is configured, the IP address and port ID of the standby MGC need to be configured.
	Port ID of active MGC (H248)/port ID of active IMS device (SIP)	
	Coding	Choose the coding method according to the requirement on the MGC/IMS side. Generally, the text coding method is adopted.
	Transmission mode	Choose the transmission mode according to the requirement on the MGC/IMS side. Generally, the UDP transmission mode is adopted.
	Home domain (SIP)	N/A
	Profile index	N/A
	The version of H248 protocol that MG starts to negotiate	V1, V2 or V3 (by default). The interface may fail to be registered because some softswitches do not support V3.
Voice user configuration data	Phone number	For H248 protocol: The phone numbers allocated by the MGC need to be determined, and the paging numbers for users' emergency standalone need to be planned if the emergency standalone function is provided. For SIP protocol: The phone number that the IMS core network device allocates to the user must be configured.
	Terminal ID (H248)	If the TID template with which the POTS user is bound does not support terminal layering, this parameter needs to be configured.
	User priority	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)

Item		Description
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
Common parameter	system parameter	The system parameters including the overseas version flag and message waiting indication (MWI) mode need to be configured according to the local standard to ensure that the response of the user terminal complies with the local standard.
	Overseas parameters	The attributes such as the upper and lower thresholds of the flash-hooking duration need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	POTS port attributes	If the POTS port needs to support the polarity reversal accounting, the POTS port needs to be configured to support the polarity reversal pulse. Other attributes need not be modified if there is no special requirement.
	Ringing current attributes	When the attributes of ring current are changed, ring volume is changed accordingly. Generally, no adjustment is required for the ringing tone volume. You need to modify the parameters of the ringing current attributes according to the local standard only when the default ringing current attributes do not comply with the local standard.

2.2.5 Principle of IPTV Service Data Plan

The IPTV service data plan mainly include the plan of VLAN and VLAN translation policy in different network scenario, and the plan of IPTV service.

IPTV services include multicast service and video on demand (VoD) service. These two services are relevant but independent in VLAN planning.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
Bridging +Voice ONT	Multicast service	Single-tagged VLAN	ONTs replicate multicast packets based on user ports and multicast VLANs (M-VLANs) are removed downstream. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs add S-VLAN tags to iTV service packets. The OLT transparently transmits packets with S-VLANs.
		Double-tagged VLAN	All ONTs add the same C-VLAN tag to packets. The OLT implements VLAN translation: C->S+C'.
Bridging ONT + HGW	Multicast service	Single-tagged VLAN	ONTs transparently transmit upstream packets with M-VLANs sent from HGW. Multicast packets are replicated downstream with M-VLAN unchanged. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
		Single-tagged VLAN	ONTs translate the upstream VLANs sent from HGW to M-VLANs. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S.
		Double-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S+C.
Gateway ONT	Multicast service	Single-tagged VLAN	ONTs replicate packets based on user ports and M-VLANs are removed in downstream direction. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs add C-VLAN tags to packets. Untagged VLANs are translated to C-VLANs. The OLT implements VLAN translation: C -> S.

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- IPTV service is a closed service self-operated by carriers, and single-tagged S-VLAN is recommended.
- The same S-VLAN or different S-VLANs can be used as the M-VLAN and VoD VLAN. It is recommended that you use different S-VLANs as M-VLAN and VoD VLAN so that the upper-level device easily differentiates between the BTV service and VoD service.
- S-VLANs of VoD service can identify services and physical locations based on an entire network or an OLT. It is recommended that you set different VoIP VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the VoIP SR and convergence switch.

2.2.6 Principle of Security Data Plan

The security plan involves system security plan, user security plan, and service security plan. Security policy ensures service security from different aspects.

NOTE

The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:

- The security measures can be used on the live network.
- The security measures are easy to deploy.
- The security measures are effective.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.

Security Vulnerability	Solution	Description and Usage Suggestion
IP attack	Enable the anti-IP-attack function for OLT.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT.	After anti-MAC-duplicate is enabled, the system records the first MAC address learned from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
MAC attack	Enable the anti-MAC spoofing function for OLT.	After anti-MAC spoofing is enabled, the system can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
IP spoofing	Enable the anti-IP spoofing function for OLT.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

Service Security

Security Vulnerability	Solution	Description and Usage Suggestion
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on OLT, and the BRAS implements user authentication based on the RAIO information.	In the DHCP option 82 mode, user's physical location is added to the option 82 field carried in the DHCP request packet initiated by a user. The physical location, used for user authentication on the upper-layer authentication server, can help implement the following functions: ● The DHCP relay forwards DHCP response packets to devices with specified CID and RID. ● Prevents DHCP address exhaustion. ● Achieves static allocation of DHCP addresses. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the DHCP Internet access service.
Broadband access of residential users (PPPoE), user account theft/ borrowing	PPPoE+ (PITP) is enabled on OLT, and the BRAS implements user authentication based on binding of the RAIO information to the user account.	The BRAS responds to request packets of users with specified CID and RID. In this way, the following functions are implemented: ● Prevents IP address exhaustion. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the PPPoE Internet access service.

2.3 Configuring the Service by Using the NMS

This topic describes how to configure Internet access service, VoIP service and IPTV service by using the NMS.

2.3.1 Configuring FTTH Services (GPON Access)

This topic describes how to configure the Internet service, voice service, and multicast service in GPON access mode in the FTTH network scenario using the U2000.

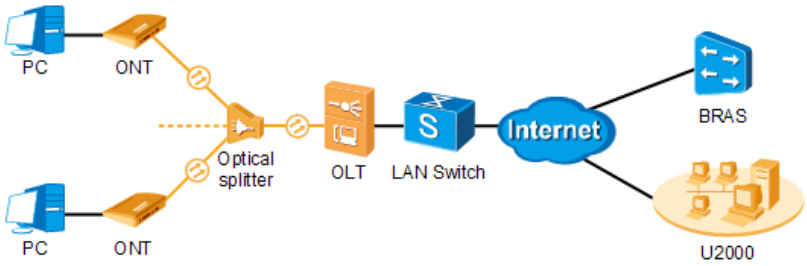
2.3.1.1 Configuring the GPON FTTH Layer 2 Internet Access Service on the NMS

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Networking

- The PC gains access to the Internet in PPPoE dialup mode.
- The ONT is connected to the GPBC card of the OLT through an optical fiber.
- The broadband remote access server (BRAS) provides broadband user access and functions of authentication and accounting.

Figure 2-2 Configuring the GPON FTTH Internet service



Data Plan

Table 2-6 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA Type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1 ID of the port on the ONT that is connected to the PC: 1

Item	Data
VLAN plan	Double-tagged VLAN ● S-VLAN ID: 100 ● S-VLAN type: Smart ● S-VLAN attribute: Stacking ● C-VLAN ID: 1001 ● C'VLAN ID: 1010 **NOTE** VLAN translation policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

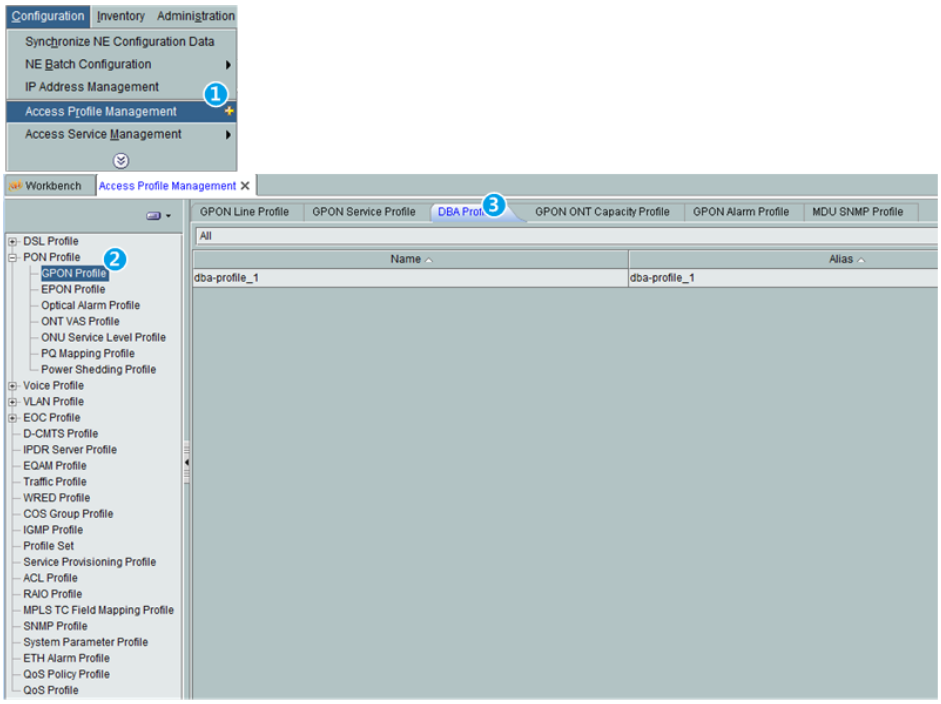
- **Implement pre-configurations.**

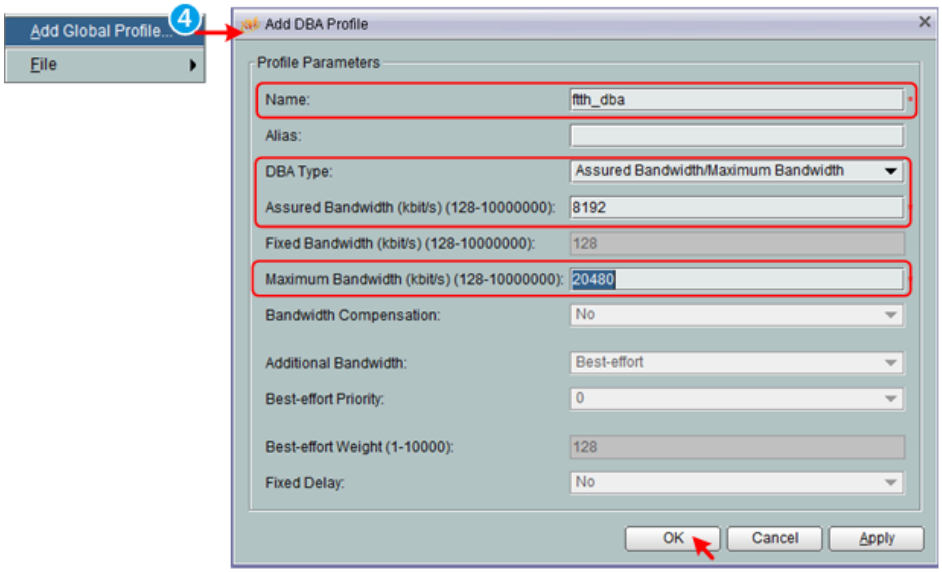
NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

1. **Configure a DBA profile.**

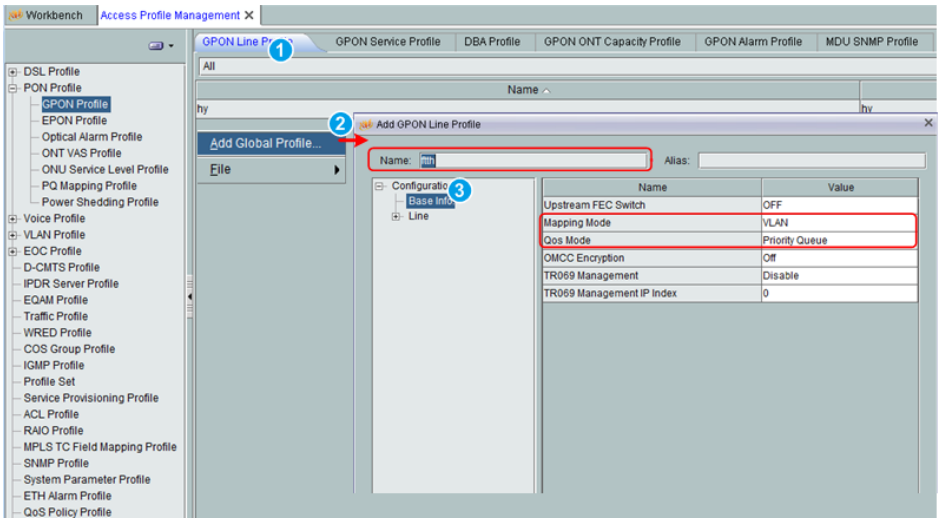


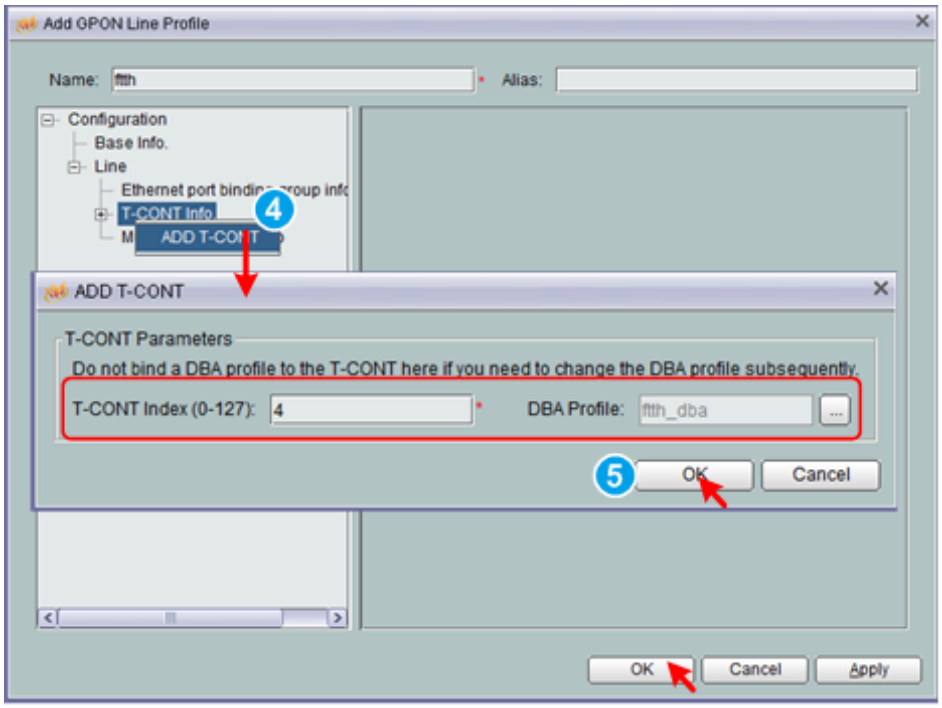


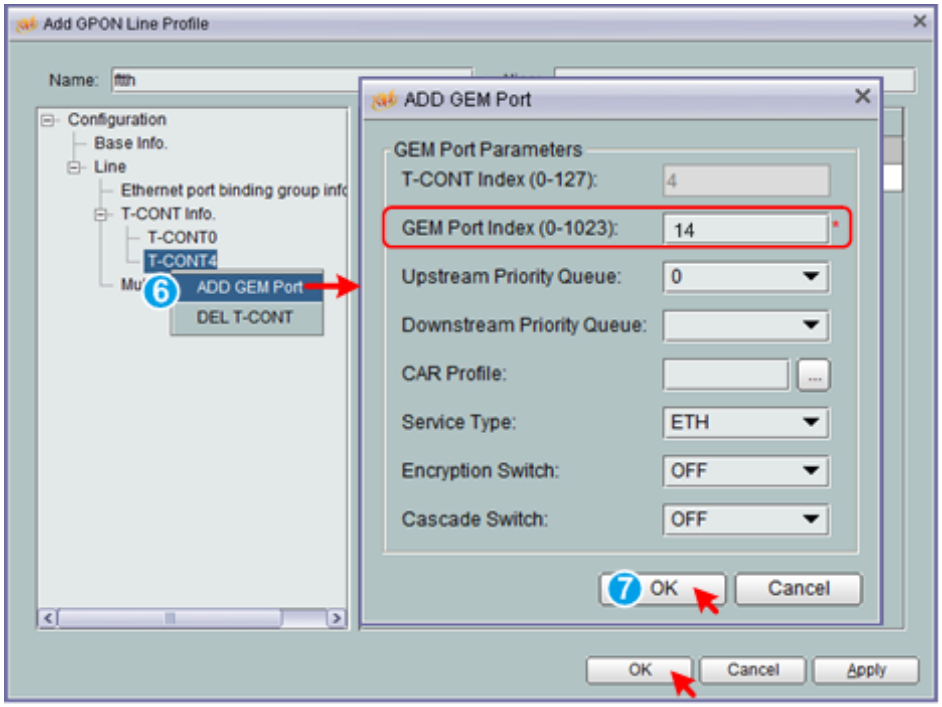
2. **Configure a line profile.**

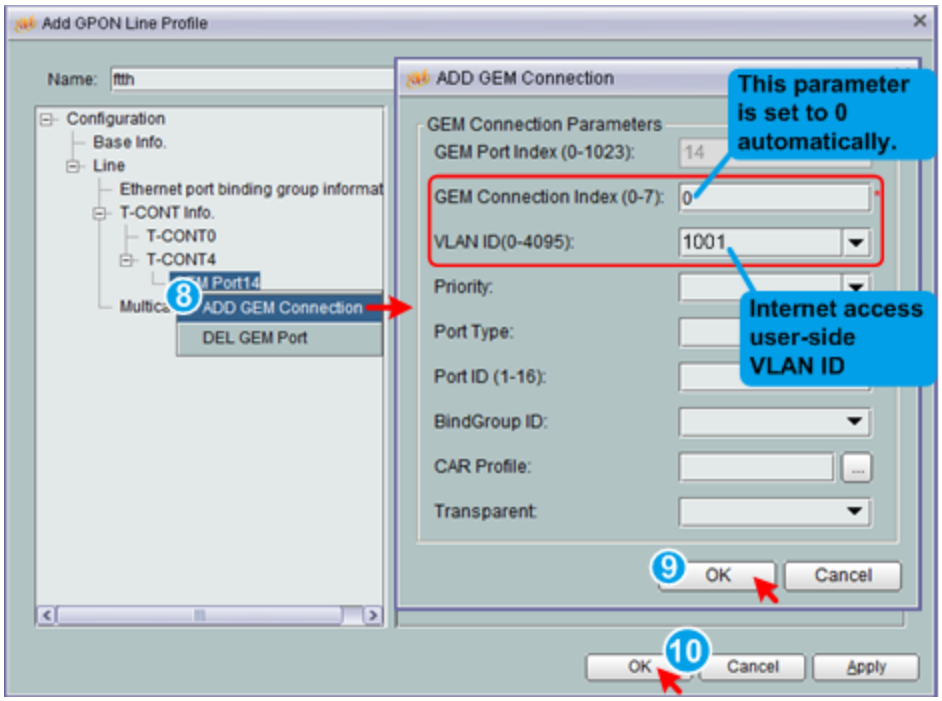
   In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

   In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 14. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.



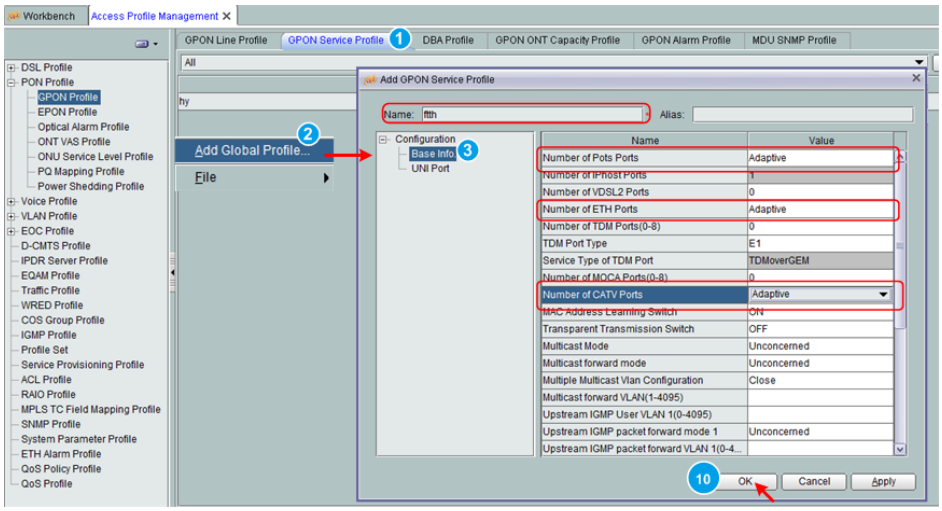

Add GPON Line Profile
Name: ftth
Alias:
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info.
ADD T-CONT
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127): 4
DBA Profile: ftth_dba
5
OK
Cancel
OK
Cancel
Apply

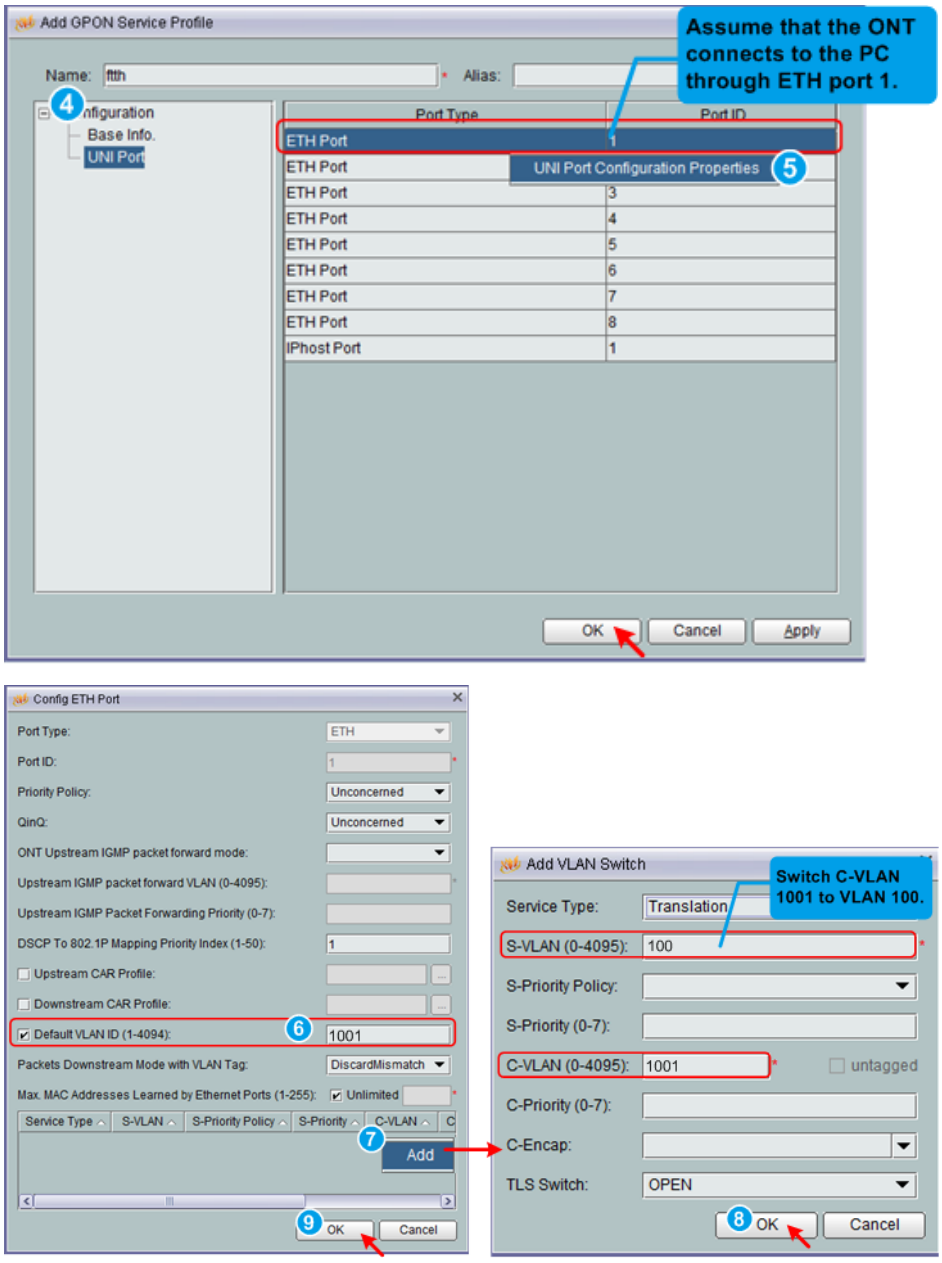

Add GPON Line Profile
Name: ftth
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info.
T-CONT0
T-CONT4
6
ADD GEM Port
DEL T-CONT
ADD GEM Port
GEM Port Parameters
T-CONT Index (0-127): 4
GEM Port Index (0-1023): 14
Upstream Priority Queue: 0
Downstream Priority Queue:
CAR Profile:
Service Type: ETH
Encryption Switch: OFF
Cascade Switch: OFF
7
OK
Cancel
OK
Cancel
Apply



3. **Configure a service profile.**

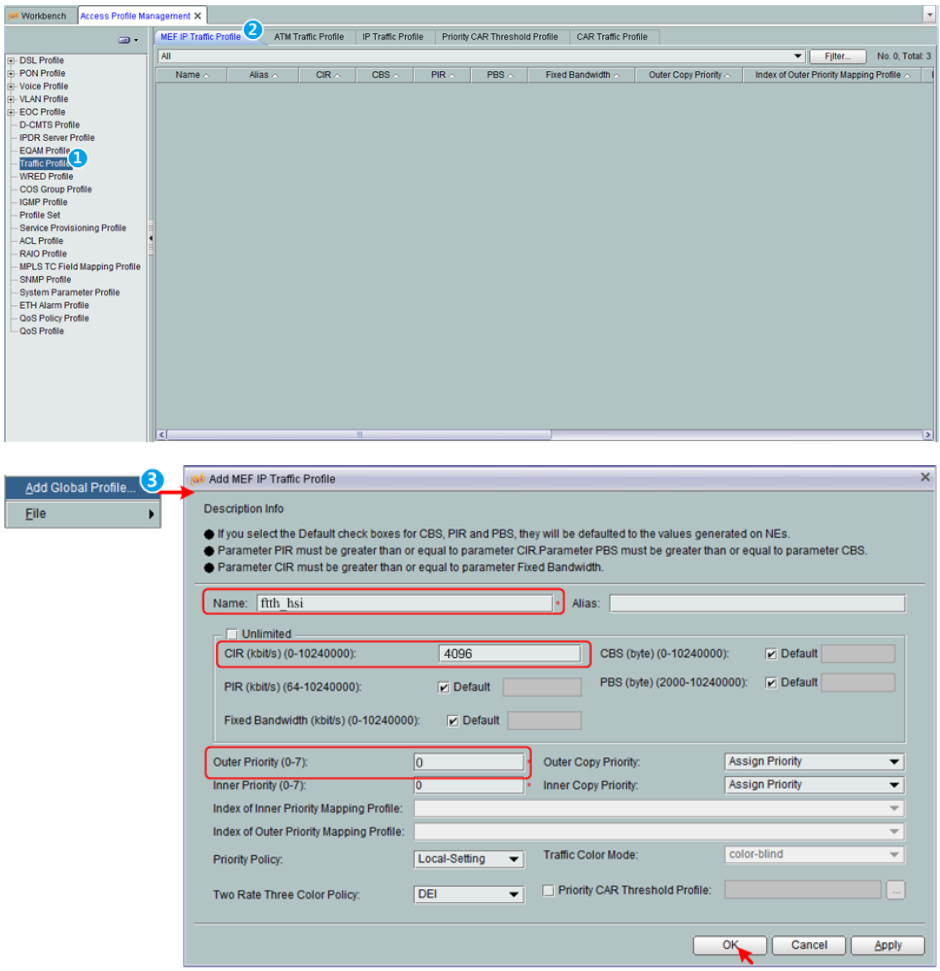
   Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability. Then, in the ONT service profile, configure a VLAN translation policy to translate C-VLAN 1001 to VLAN 100.





4. **Configure an MEF IP traffic profile.**

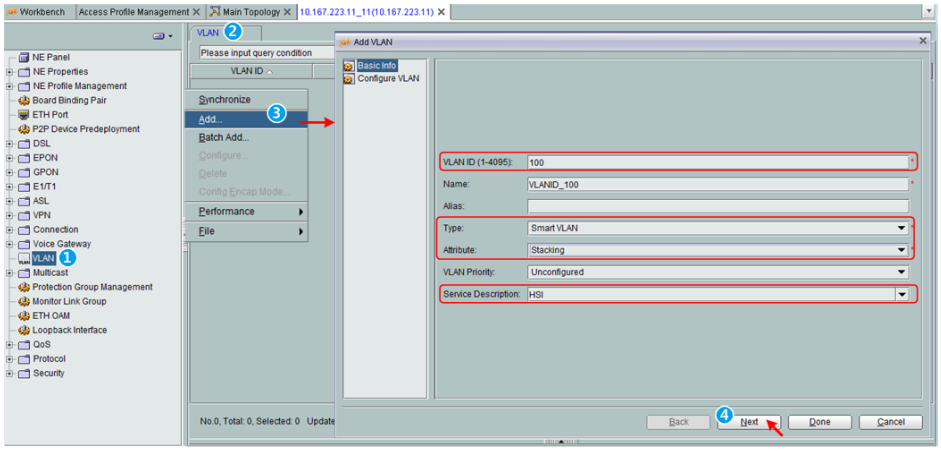
   The profile name is ftth_hsi, CIR is 4 Mbit/s, and the priority is 0. Traffic is scheduled based on the priority specified in the profile.

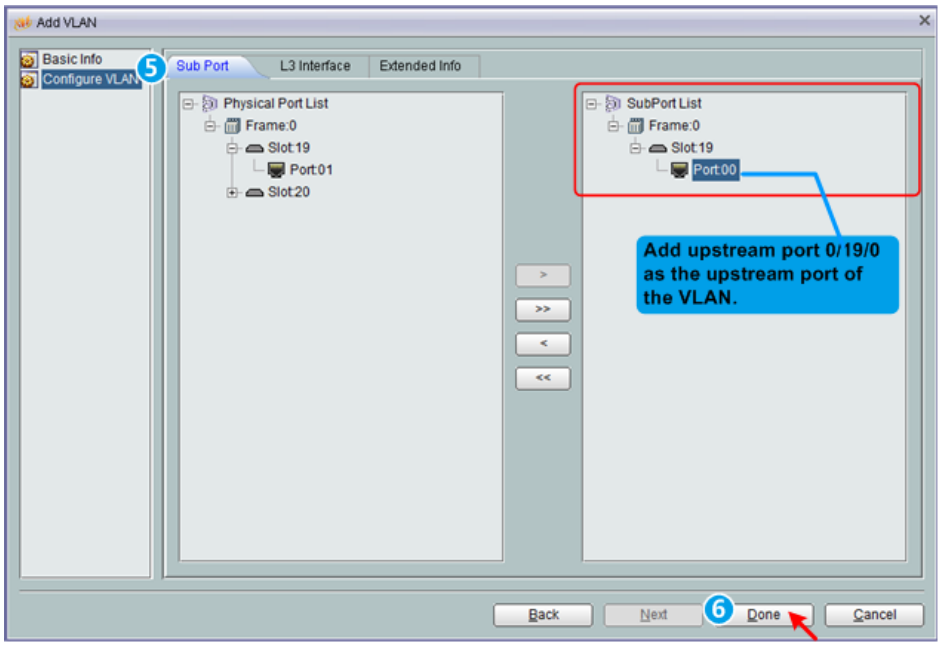


5. **Configure a service VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   A service VLAN is the VLAN used for the Internet service.



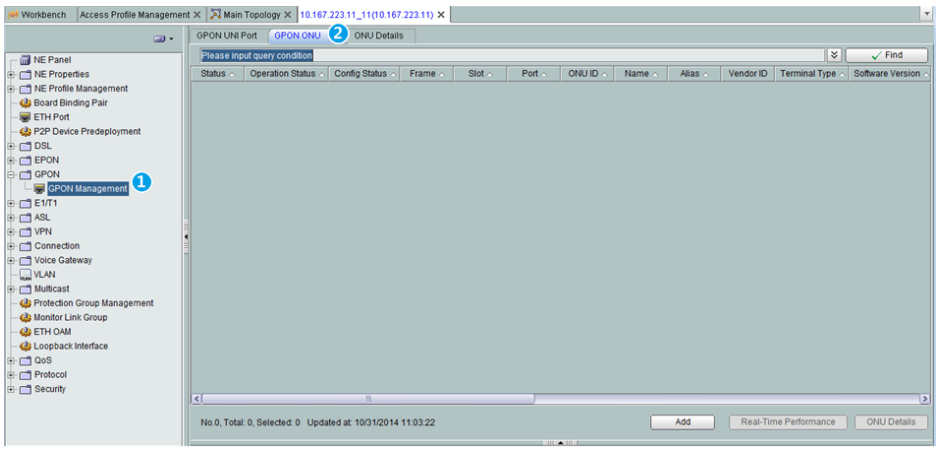


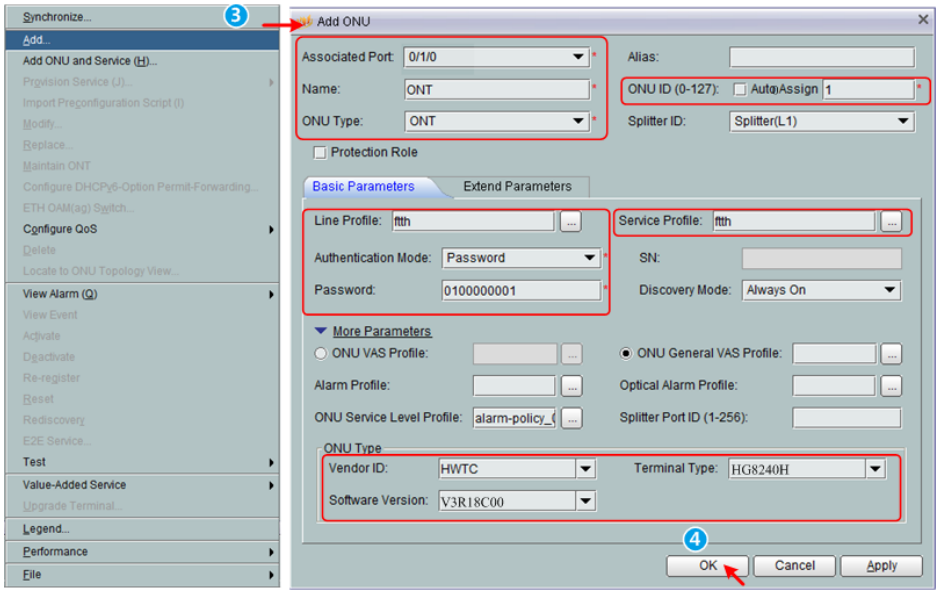
- **Configure the Internet access service.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

  The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



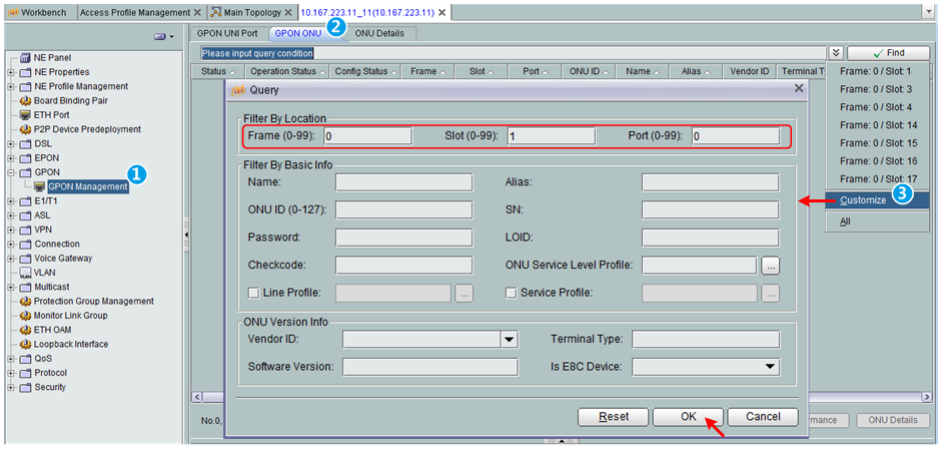


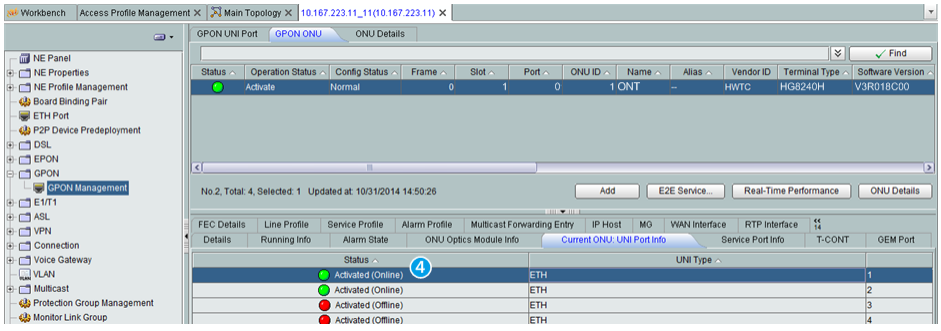
NOTE

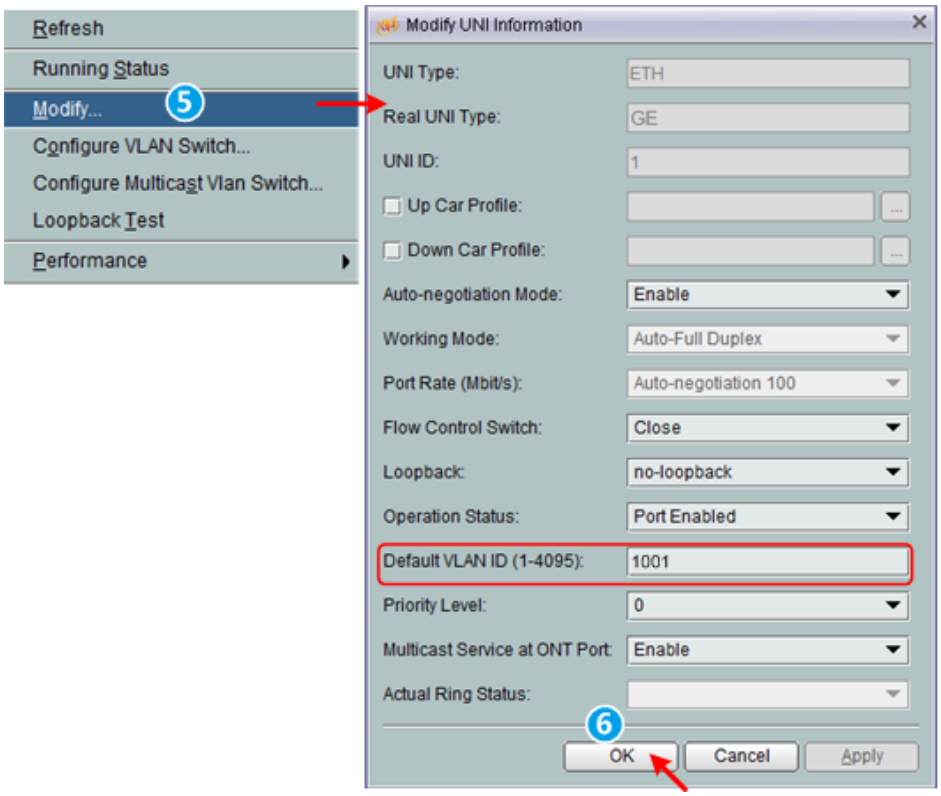
HG8240H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

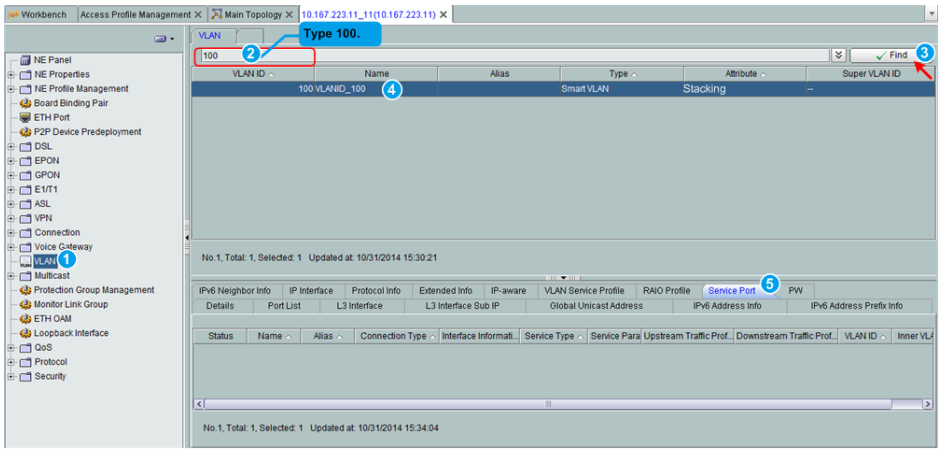
b. **Configure an ETH port of the GPON ONU.**

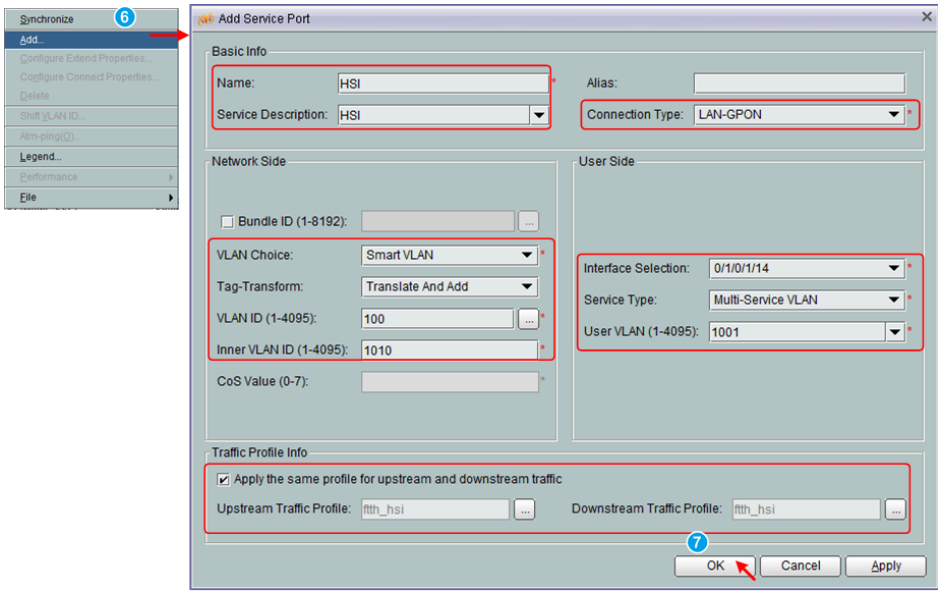






c. **Add a service virtual port on the OLT side.**





Result

Check whether the user successfully gains access to the Internet through dialup on the PC.

1. The LAN1 port of the ONT is connected to the Ethernet port of the PC properly.
2. Dial up on the PC using the PPPoE dialup software.
3. The user gains access to the Internet on the PC after the dialup is successful.

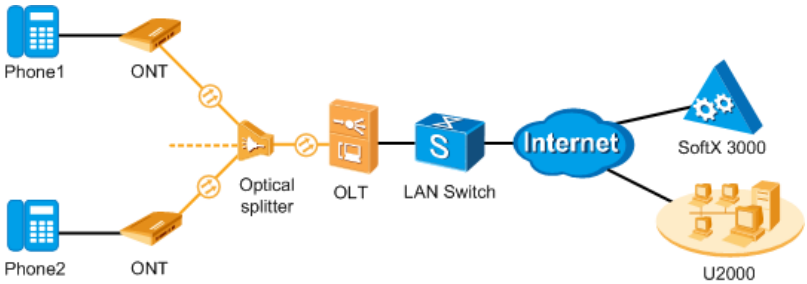
2.3.1.2 Configuring the GPON FTTH Voice Service (H.248 Protocol) on the NMS

This topic describes how to configure the voice service when an ONT is connected to an OLT through a GPON port.

Networking

- The phones connected to different ONTs can communicate with each other.
- The ONT obtains an IP address in Dynamic Host Configuration Protocol (DHCP) mode.

Figure 2-3 Configuring the GPON FTTH voice service (H.248 protocol)



Data Plan

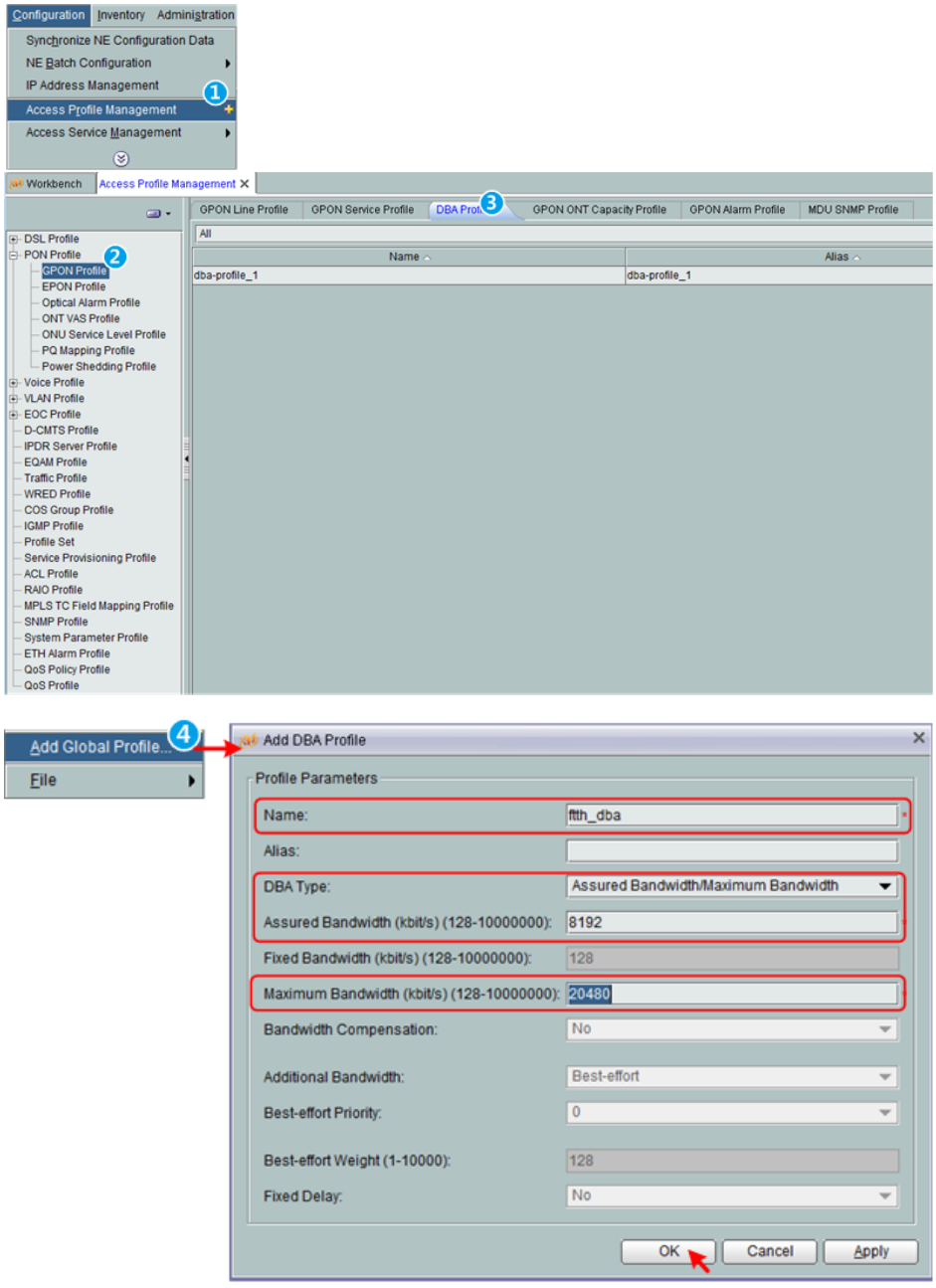
Table 2-7 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for voice services: 12
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1
VLAN plan	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: Smart ● S-VLAN attribute: Common ● C-VLAN=S-VLAN **NOTE** VLAN translation policy: ● ONT: uses the same VLAN configurations and adds C-VLAN tags to packets. All ONTs use the same C-VLAN. ● OLT: transparently transmits VLAN (C-VLAN is the same as the planned S-VLAN).
ONT value-added services	Profile Name: ONT-VoIP WAN VLAN ID: 300 Service Type: VoIP Connection Type: Routed Priority: 5 Signaling Protocol: H.248 IP address of the MGC server: 10.10.100.10/24 Port ID of the MGC server: 2944 MID Format: Domain name MG Domain name: 0100000001 TID: A0 and A1

Procedure

- **Implement pre-configurations.**

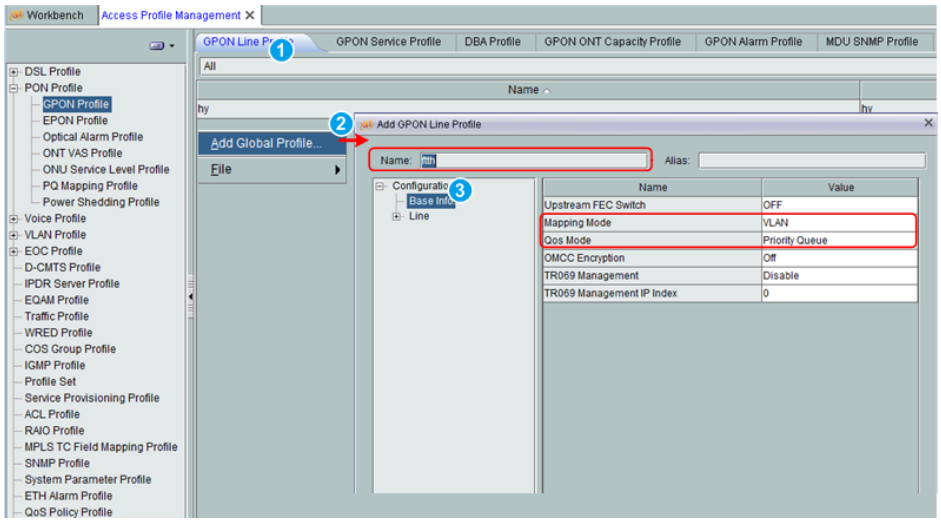
  a. **Configure a DBA profile.**

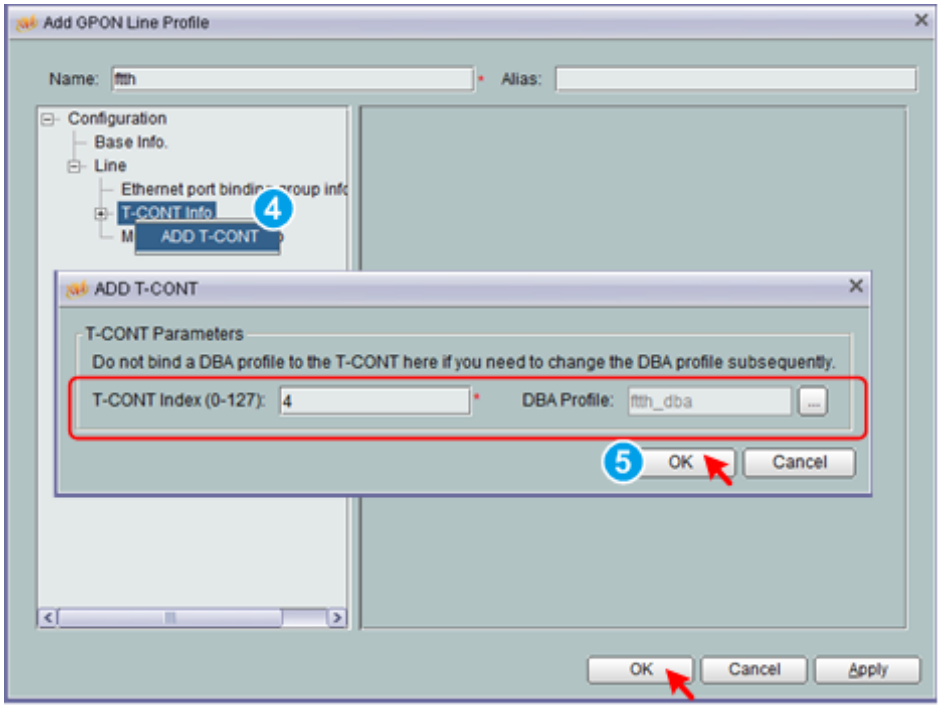


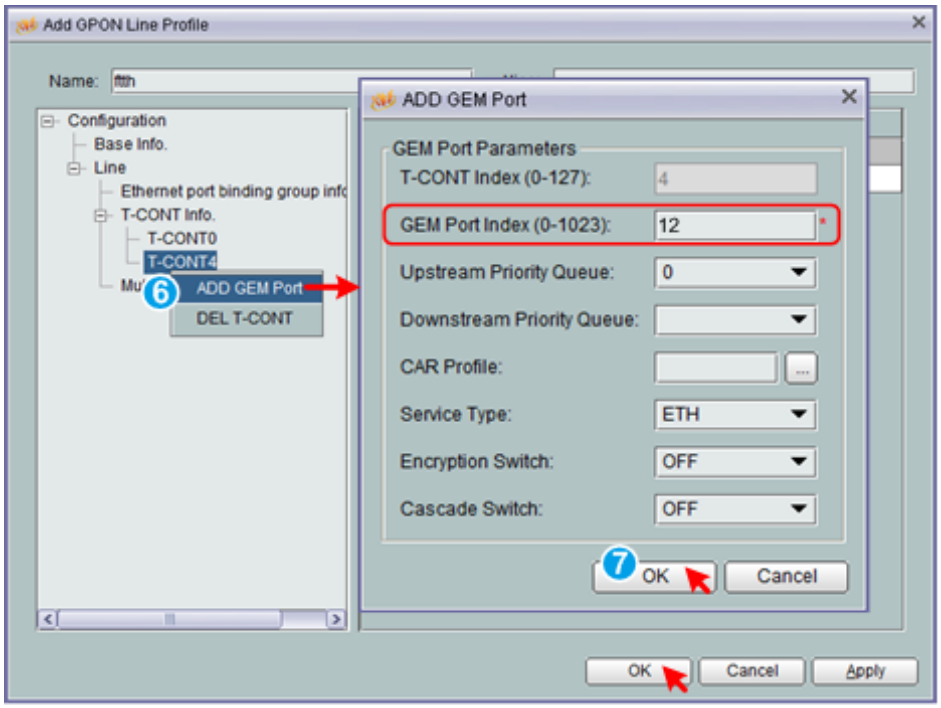
  b. **Configure a line profile.**

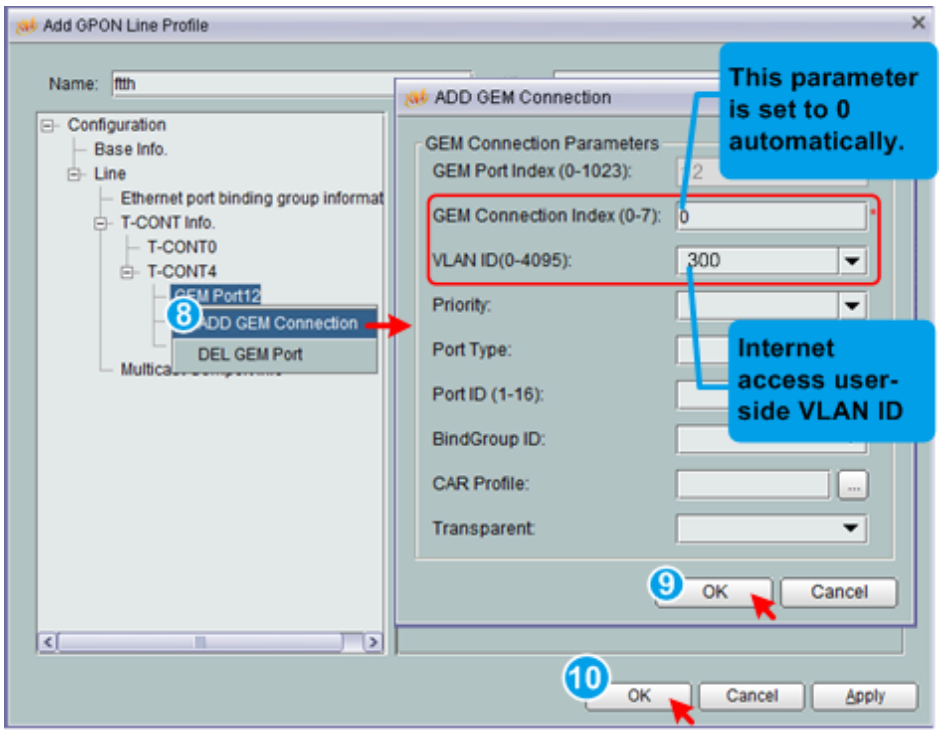
  In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

  In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 12. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.


Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
Add Global Profile...
File
Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
Name
Value
Upstream FEC Switch
OFF
Mapping Mode
VLAN
Qos Mode
Priority Queue
OMCC Encryption
Off
TR069 Management
Disable
TR069 Management IP Index
0
1
2
3

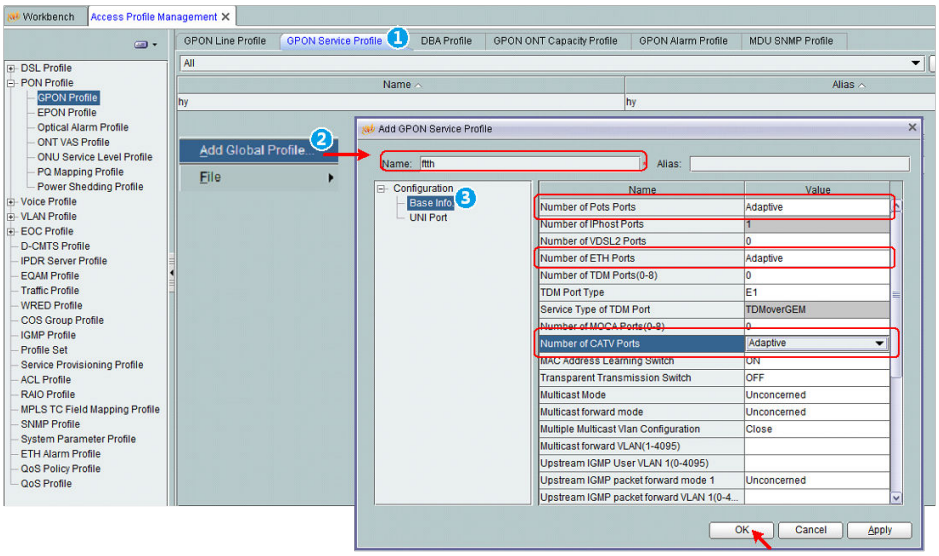

Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
T-CONT Info
ADD T-CONT
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127):
DBA Profile:
5
OK
Cancel
OK
Cancel
Apply





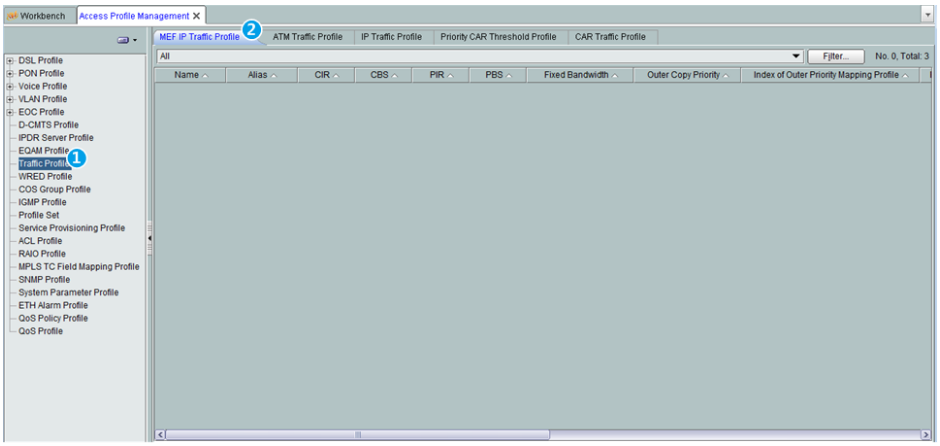
c. **Configure a service profile.**

Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability.



d. **Configure an MEF IP traffic profile.**

The profile name is ftth_voip, upstream/downstream traffic rate is not limited, and the priority is 5. Traffic is scheduled based on the priority specified in the profile.

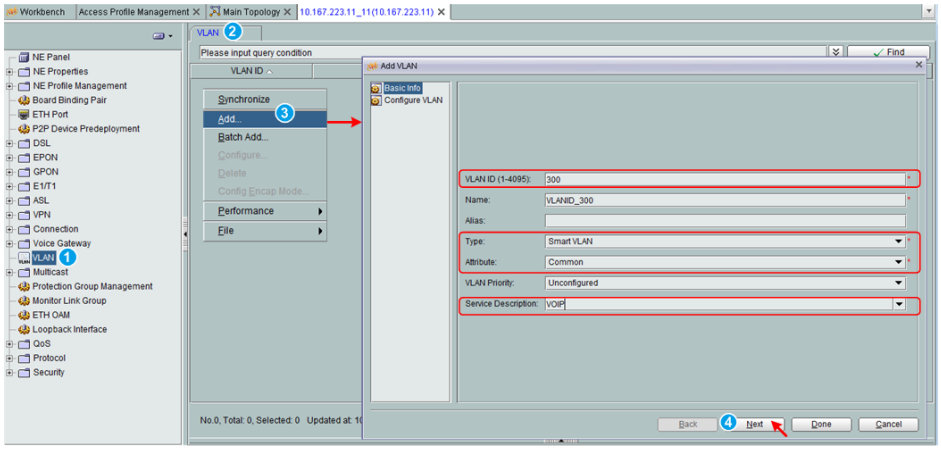


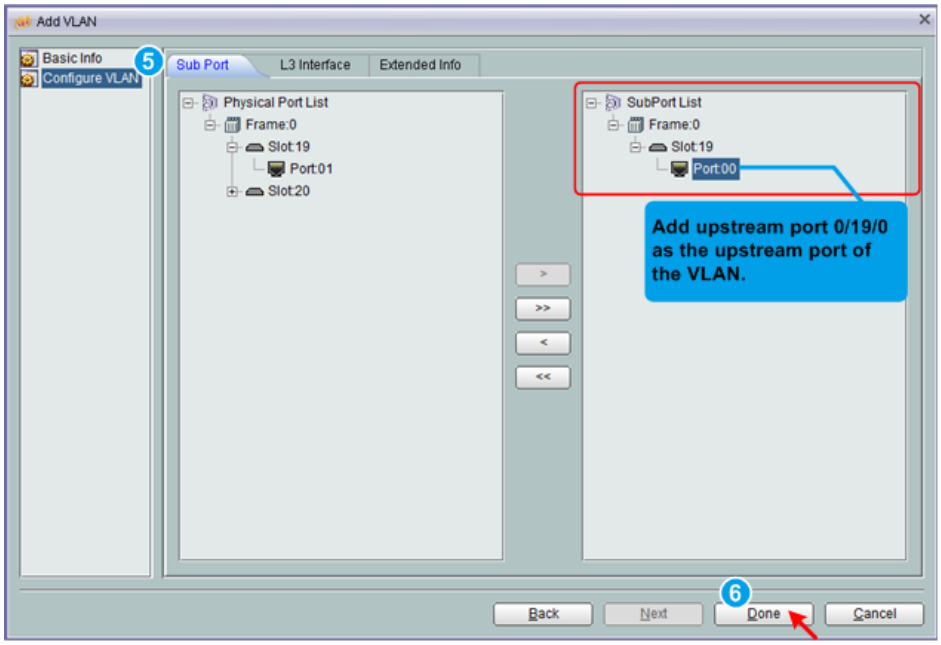
e. **Configure an S-VLAN on the OLT side.**

The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as

follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

The S-VLAN is used for the voice service.



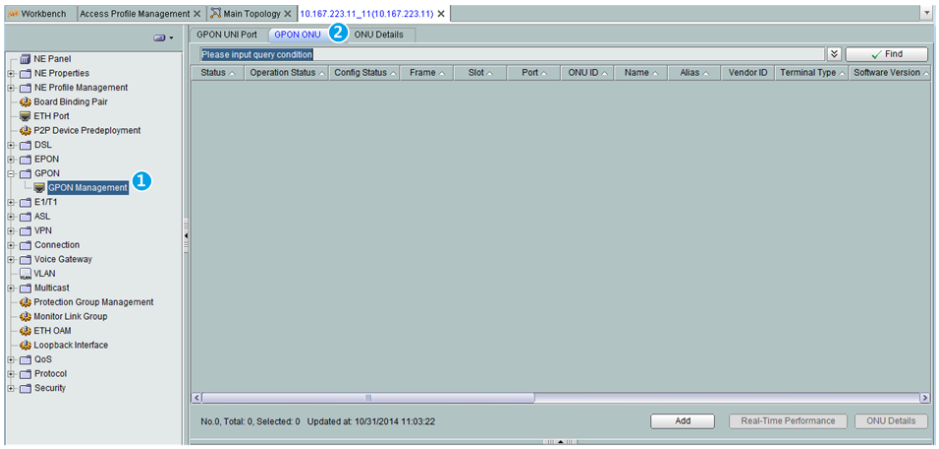


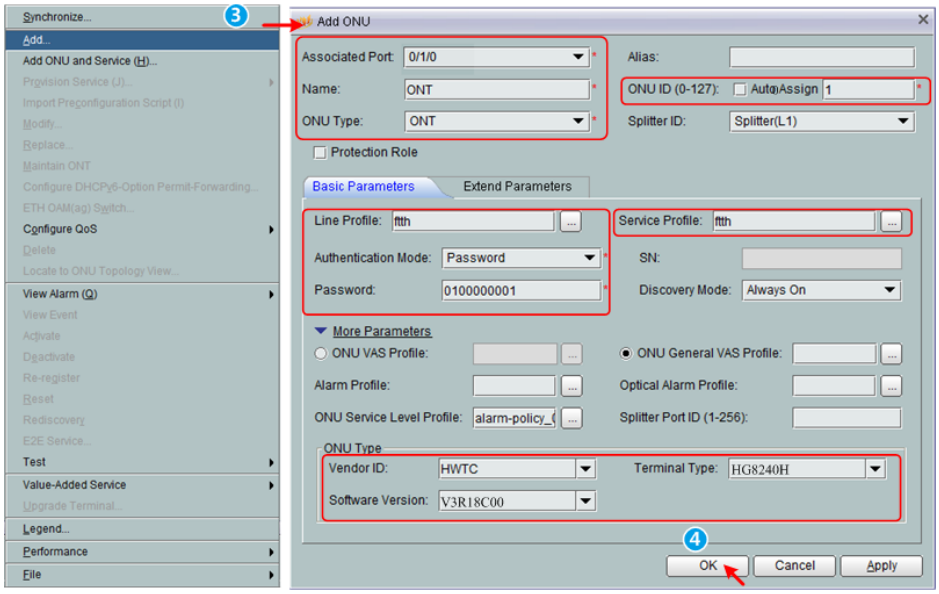
- **Provision services.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

     The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



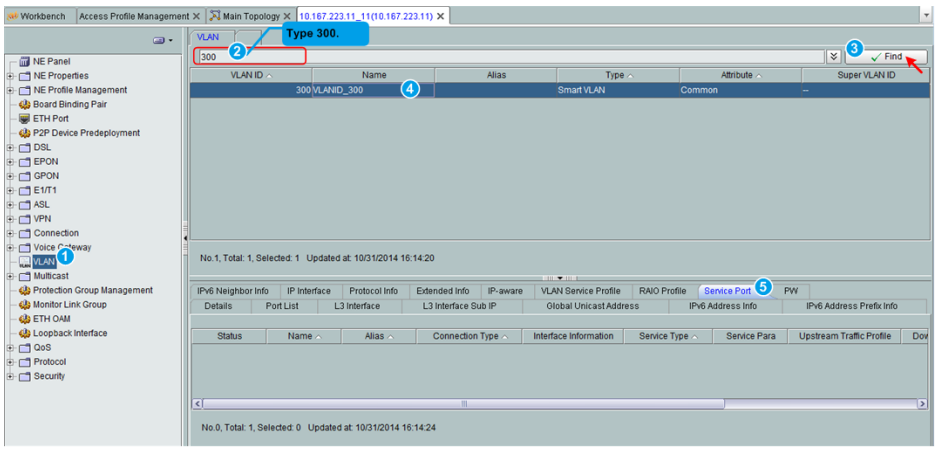


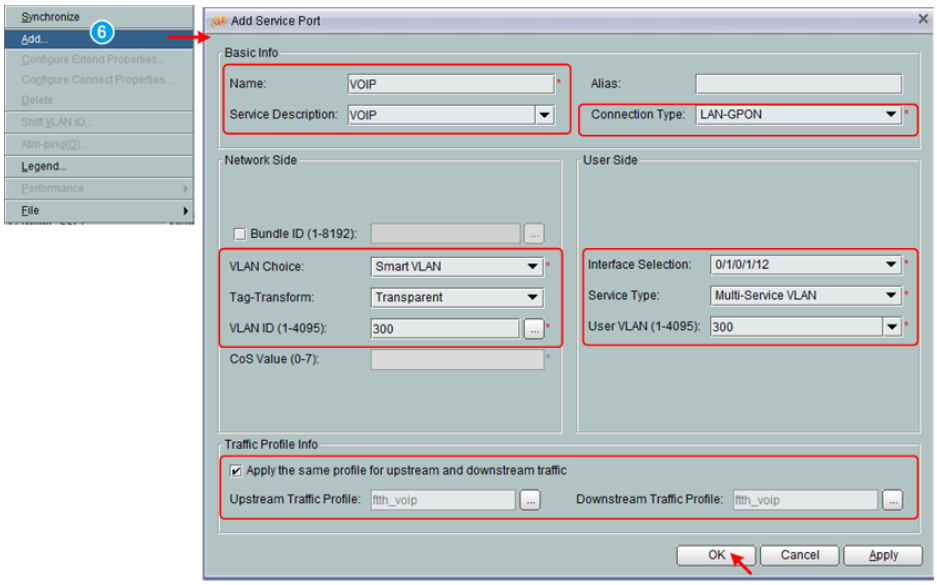
NOTE

HG8240H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

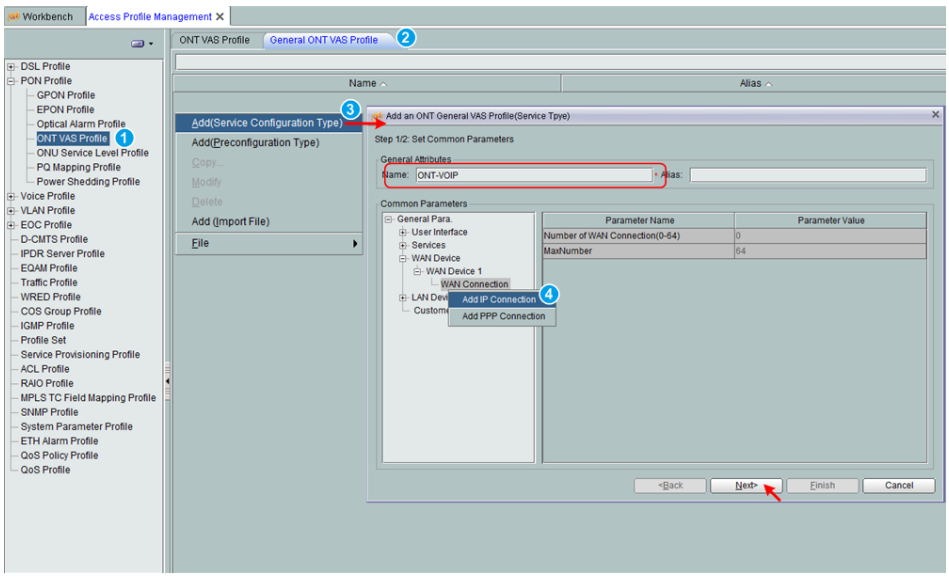
The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

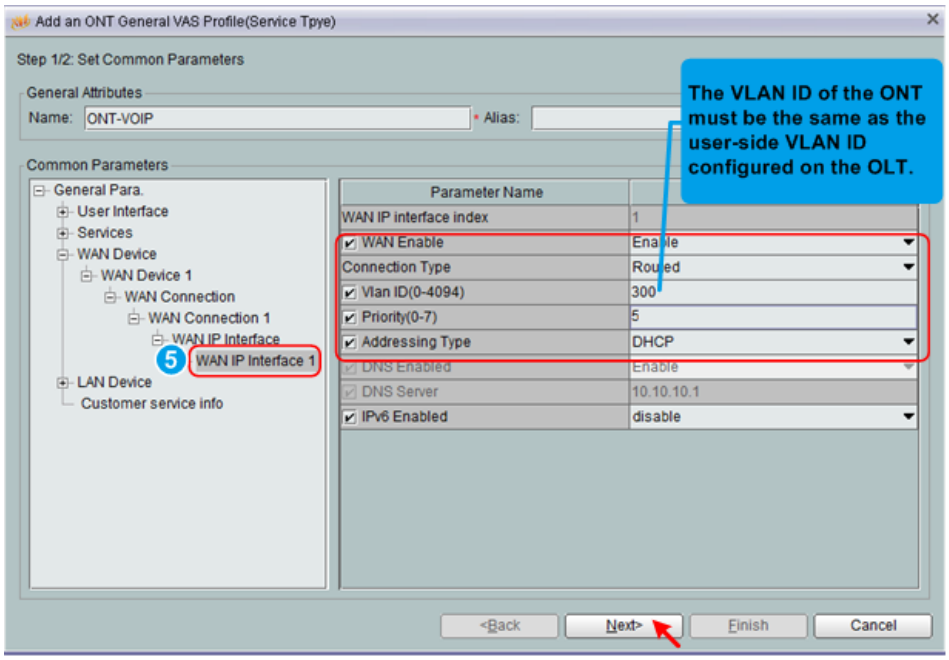
b. **Add a service port on the OLT side.**

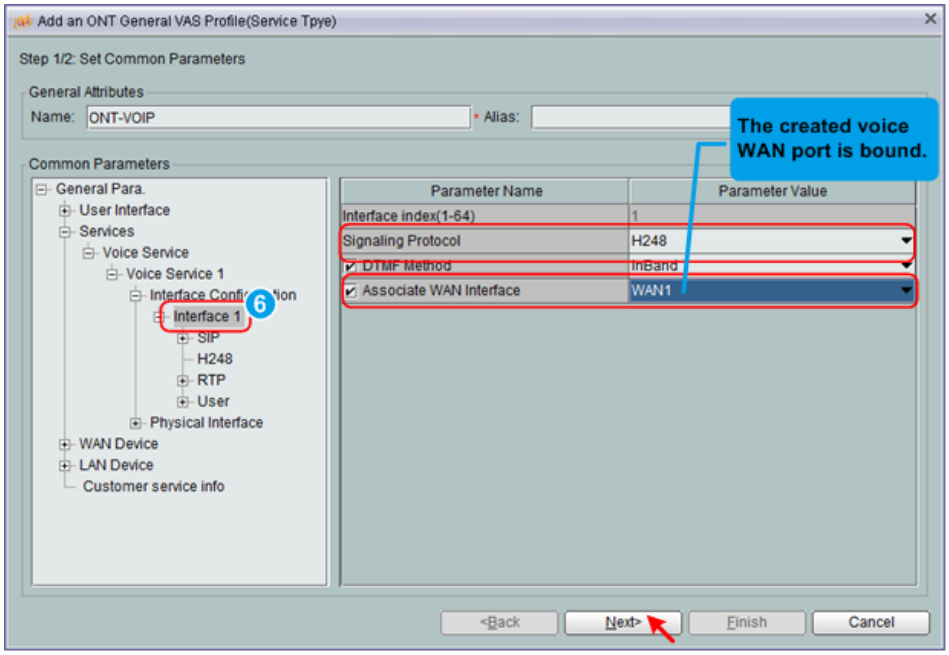


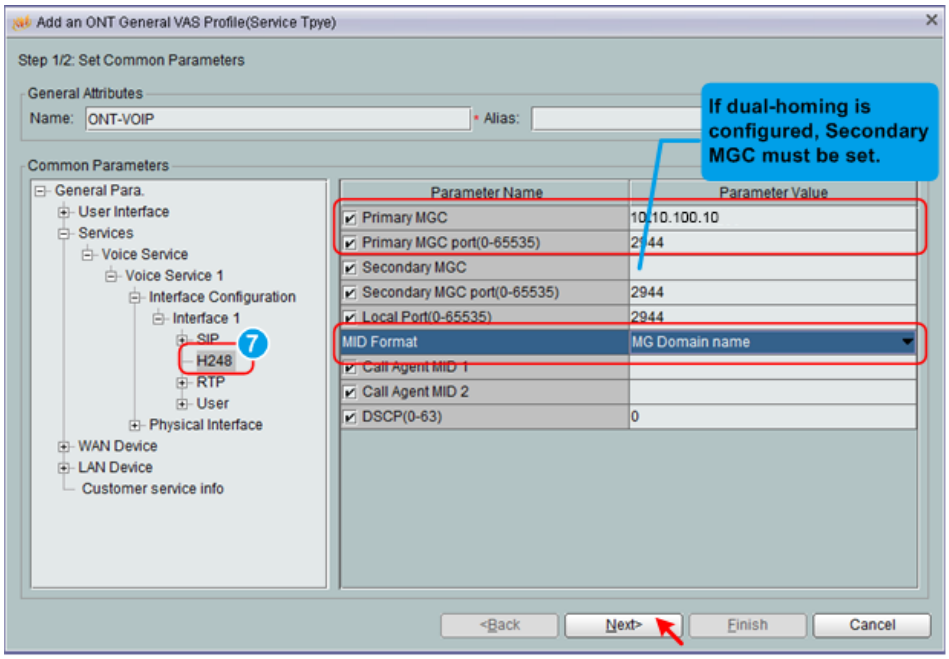


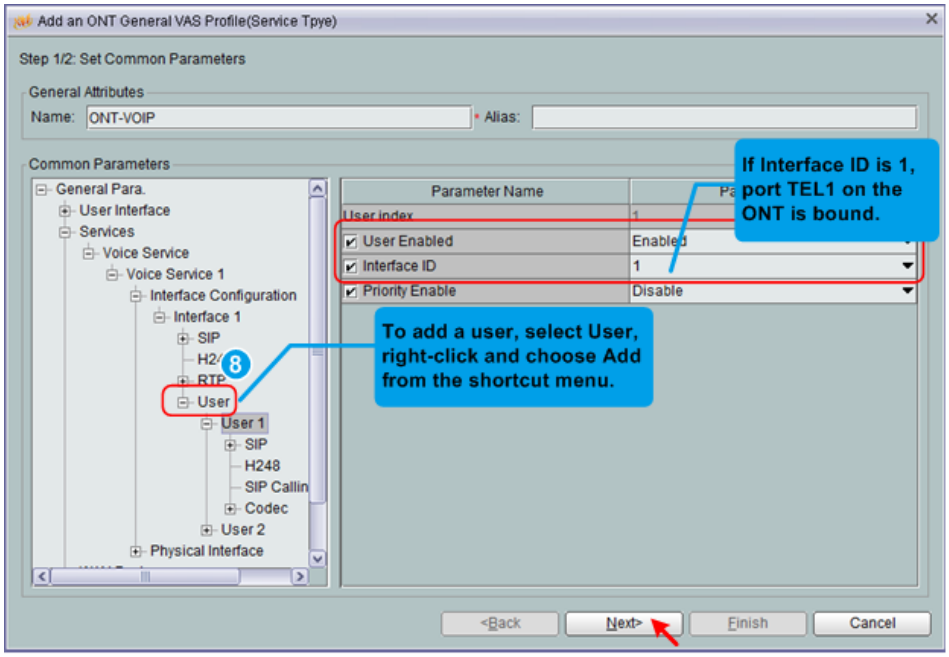
c. **Configure and bind a general value-added service (VAS) profile for the ONT.**

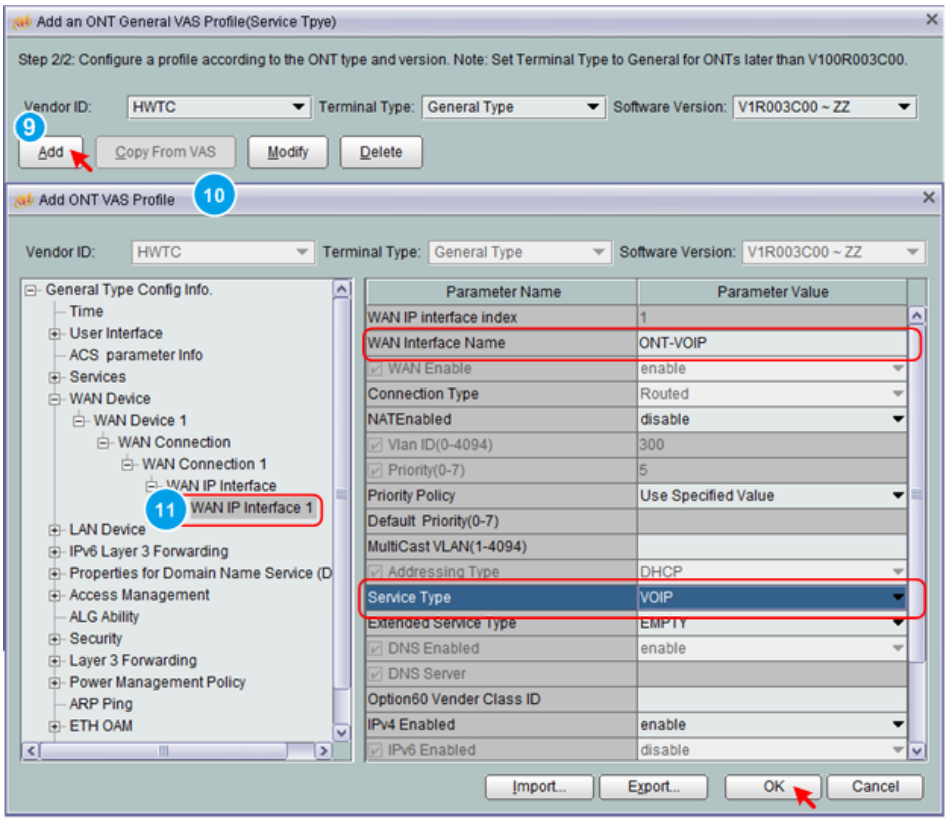



Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN IP Interface
5
WAN IP Interface 1
LAN Device
Customer service info
Parameter Name
WAN IP interface index
WAN Enable
Connection Type
Vlan ID(0-4094)
Priority(0-7)
Addressing Type
DNS Enabled
DNS Server
IPv6 Enabled
1
Enable
Routed
300
5
DHCP
Enable
10.10.10.1
disable
The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.
<Back
Next>
Finish
Cancel


Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
Voice Service
Voice Service 1
Interface Confi ion
6
Interface 1
SIP
H248
RTP
User
Physical Interface
WAN Device
LAN Device
Customer service info
Parameter Name
Parameter Value
Interface index(1-64)
Signaling Protocol
DTMF Method
Associate WAN Interface
1
H248
inBand
WAN1
The created voice WAN port is bound.
<Back
Next>
Finish
Cancel



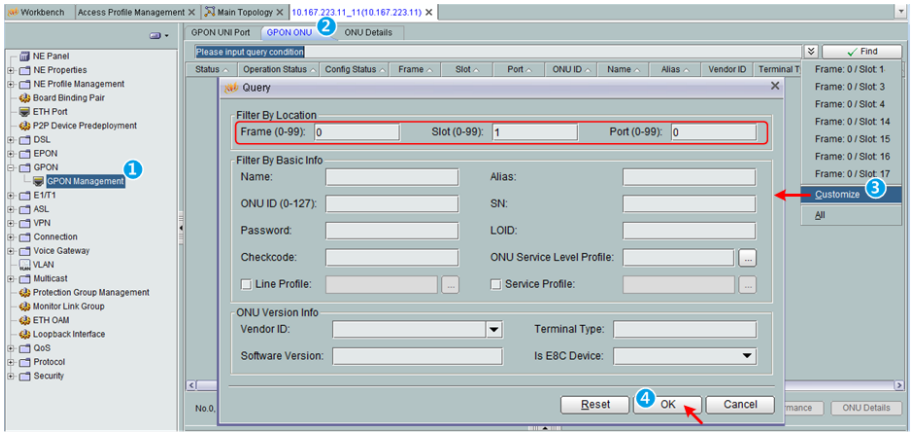


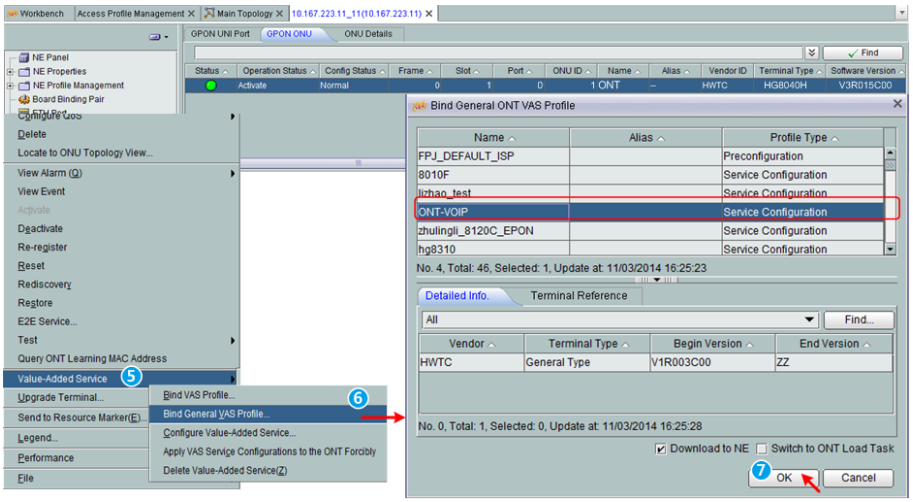


NOTE

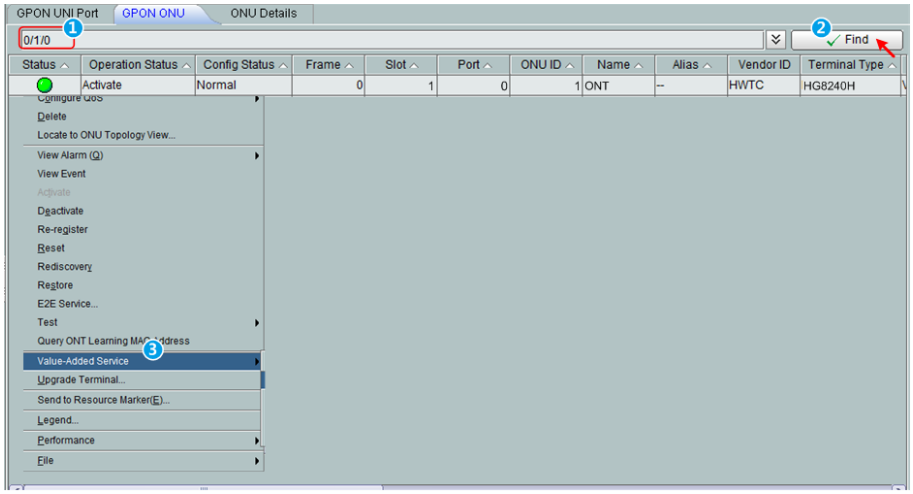
If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default. Create a WAN port named **WAN-RTP** on the ONT, and set this WAN port to a media WAN port. Specifically, choose **Interface 1** > **RTP** and set **Associate WAN Interface** to **WAN2**.

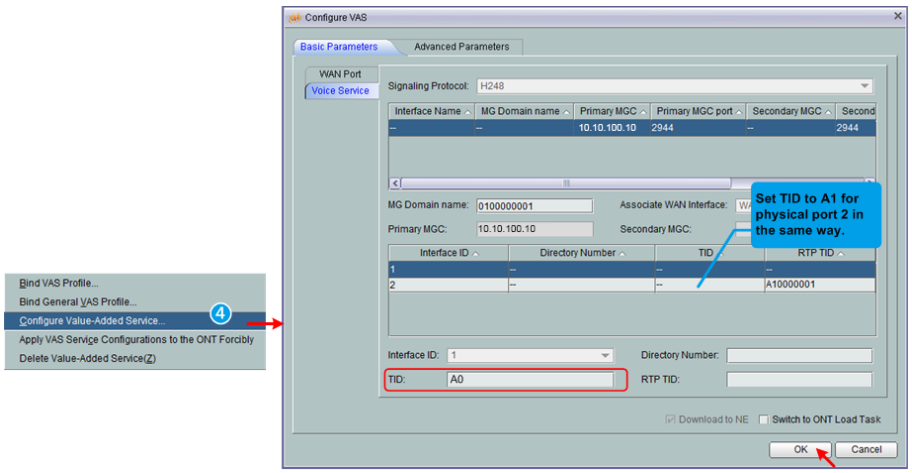
d. **Bind a general VAS profile.**





e. **Configure the ONT VAS service.**





NOTE

Domain Name is ONT's domain name registered with the MGC. It is globally unique. **MG Domain Name** in this example is ONT's password.

Pay attention to the RTP TID configuration when the ONT is interconnected with a softswitch of other vendors. The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.

Do not configure **Directory Number**.

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

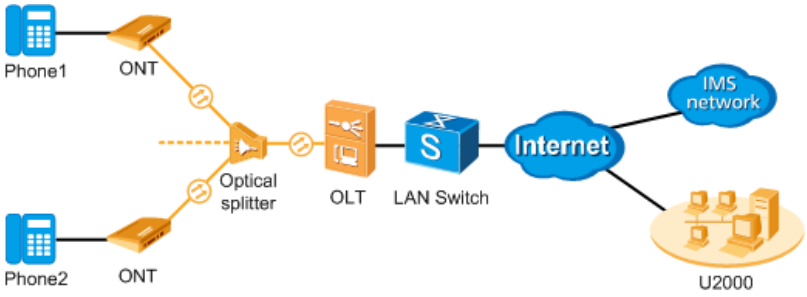
2.3.1.3 Configuring the GPON FTTH Voice Service (SIP Protocol) on the NMS

This topic describes how to configure the voice service when an ONT is connected to an OLT through a GPON port.

Networking

- The phones connected to different ONTs can communicate with each other.
- The ONT obtains an IP address in Dynamic Host Configuration Protocol (DHCP) mode.

Figure 2-4 Configuring the GPON FTTH voice service (SIP protocol)



Data Plan

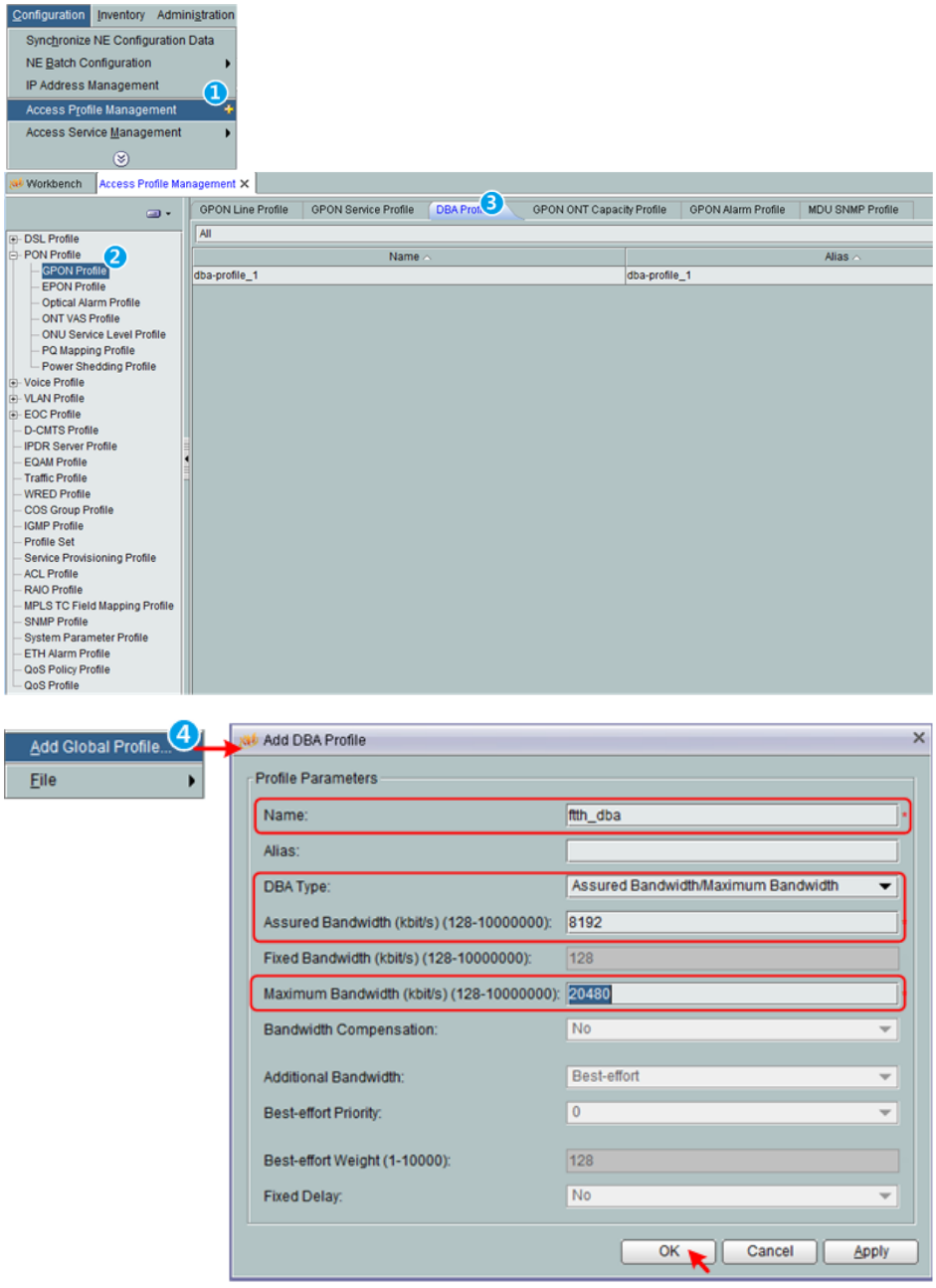
Table 2-8 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for voice services: 12
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1
VLAN Plan	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: Smart ● S-VLAN attribute: Common ● C-VLAN=S-VLAN **NOTE** VLAN translation policy: ● ONT: uses the same VLAN configurations and adds C-VLAN tags to packets. All ONTs use the same C-VLAN. ● OLT: transparently transmits VLAN (C-VLAN is the same as the planned S-VLAN).
ONT value-added services	Profile Name: ONT-VoIP WAN VLAN ID: 300 Service Type: VoIP Connection Type: Routed Priority: 5 IP address of the SIP server: 10.10.100.10/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010; Auth User Name is +8675577730010@huawei.com; Auth Password is iadtest1 User phone number 2: 77730020; Auth User Name is +8675577730020@huawei.com; Auth Password is iadtest2

Procedure

- **Implement pre-configurations.**

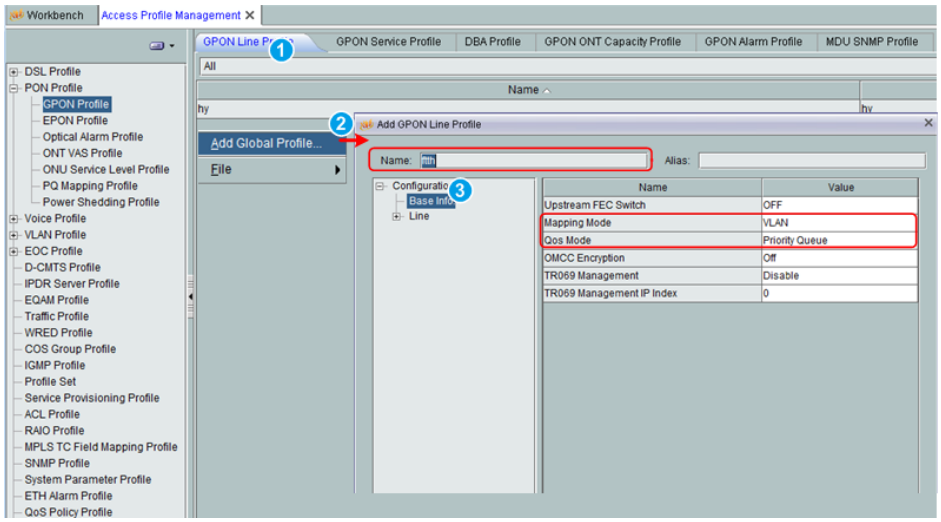
  a. **Configure a DBA profile.**

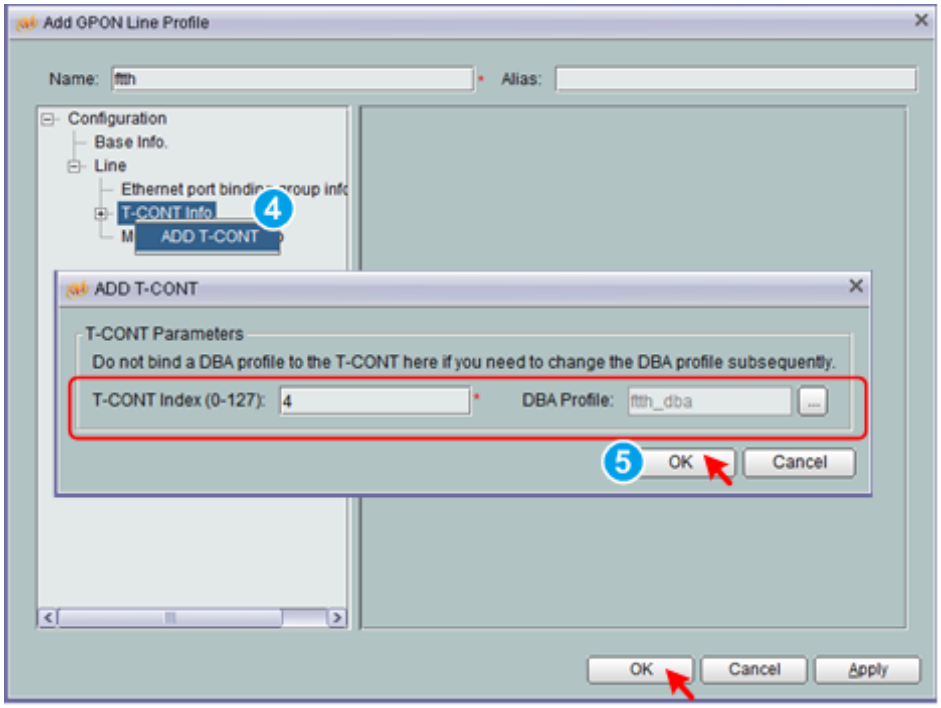


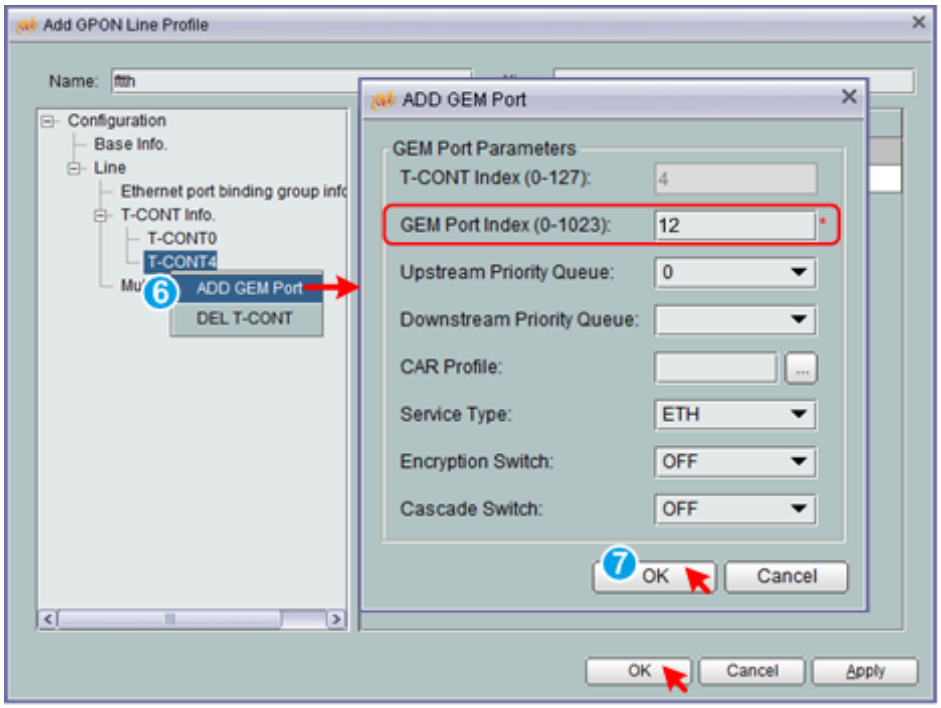
  b. **Configure a line profile.**

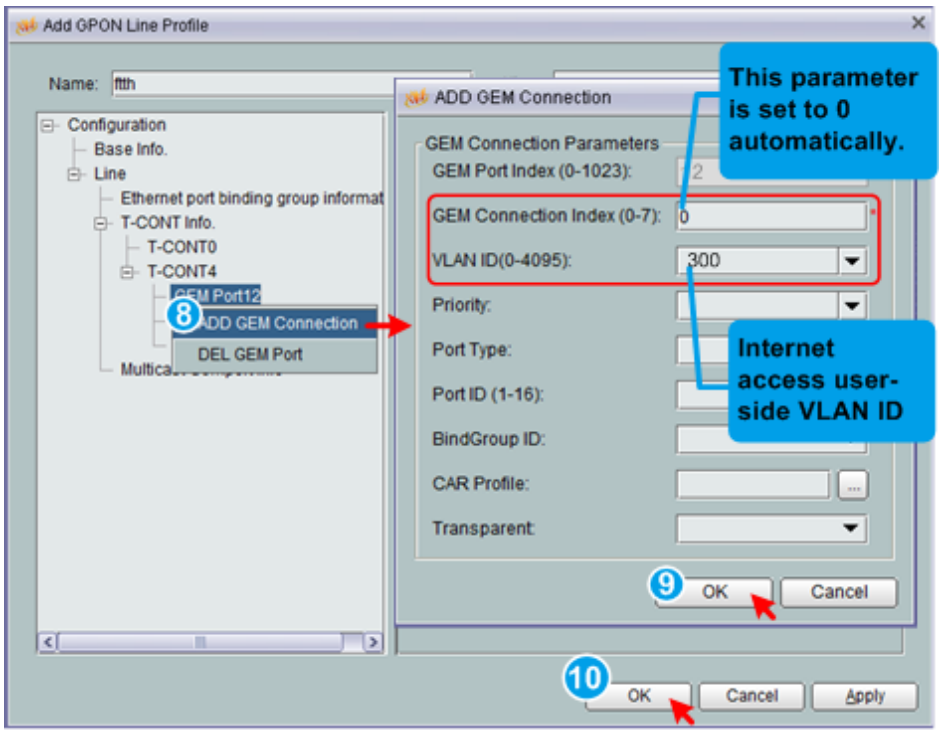
  In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

  In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 12. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.



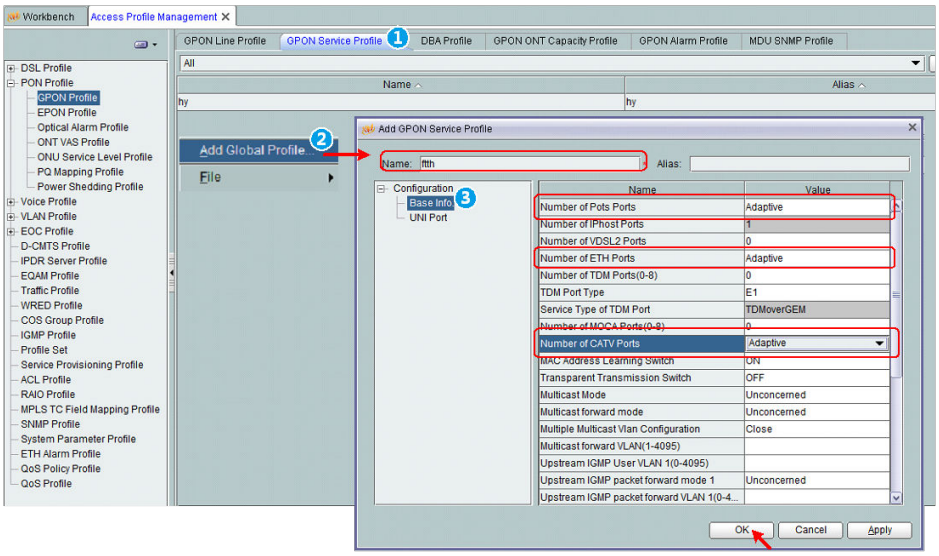






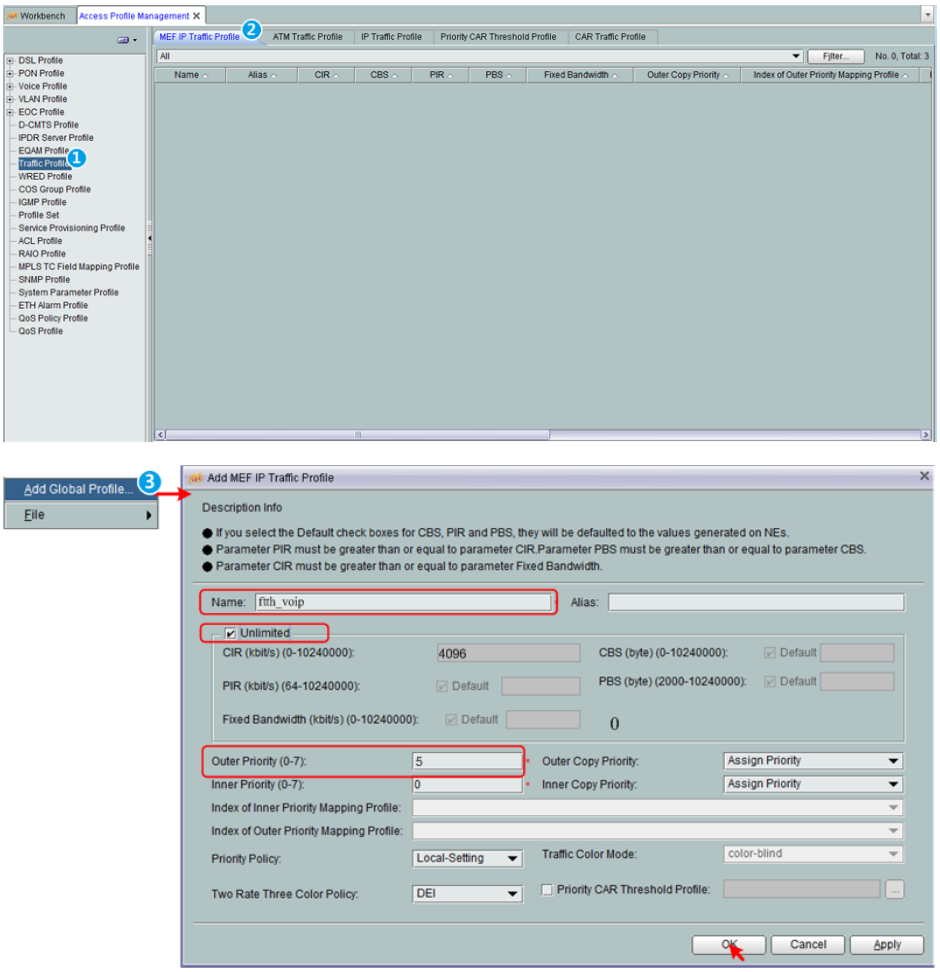
c. **Configure a service profile.**

Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability.



d. **Configure an MEF IP traffic profile.**

The profile name is ftth_voip, upstream/downstream traffic rate is not limited, and the priority is 5. Traffic is scheduled based on the priority specified in the profile.

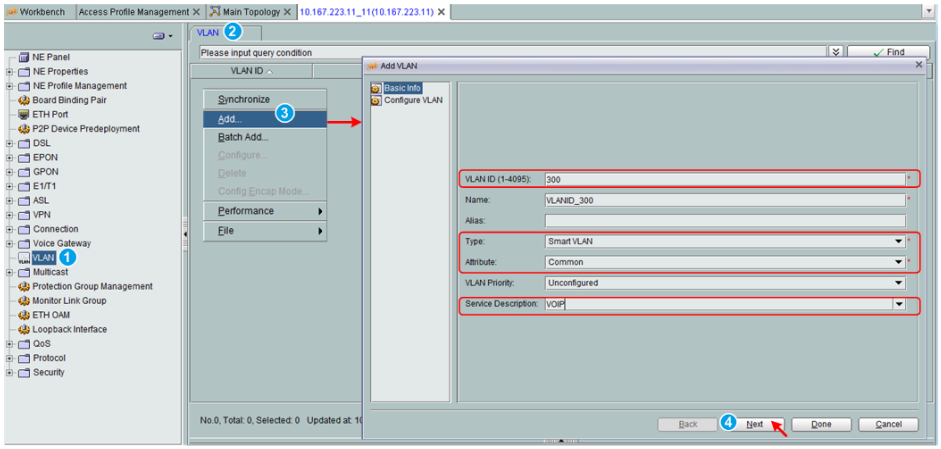


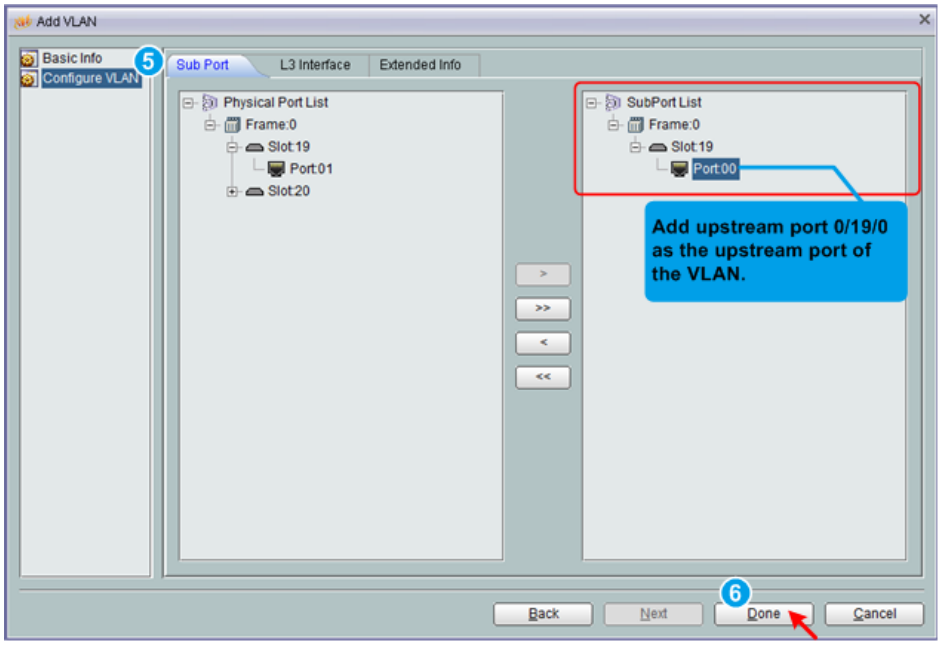
e. **Configure an S-VLAN on the OLT side.**

The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as

follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

The S-VLAN is used for the voice service.



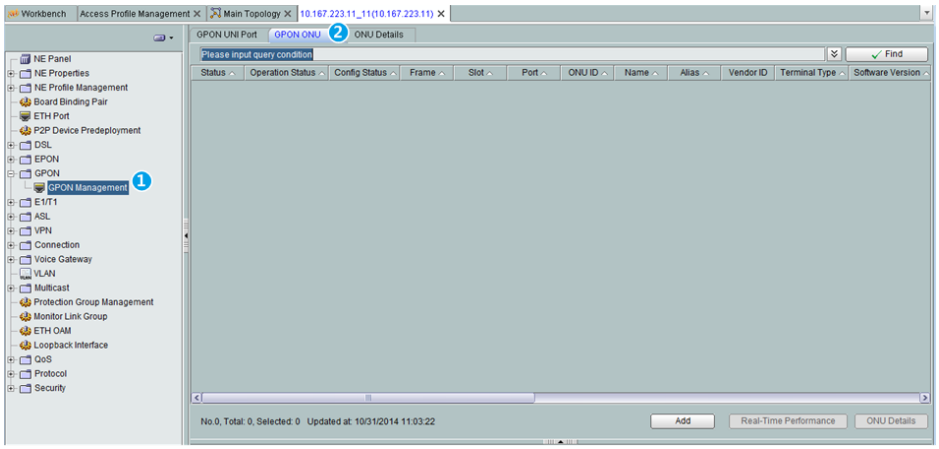


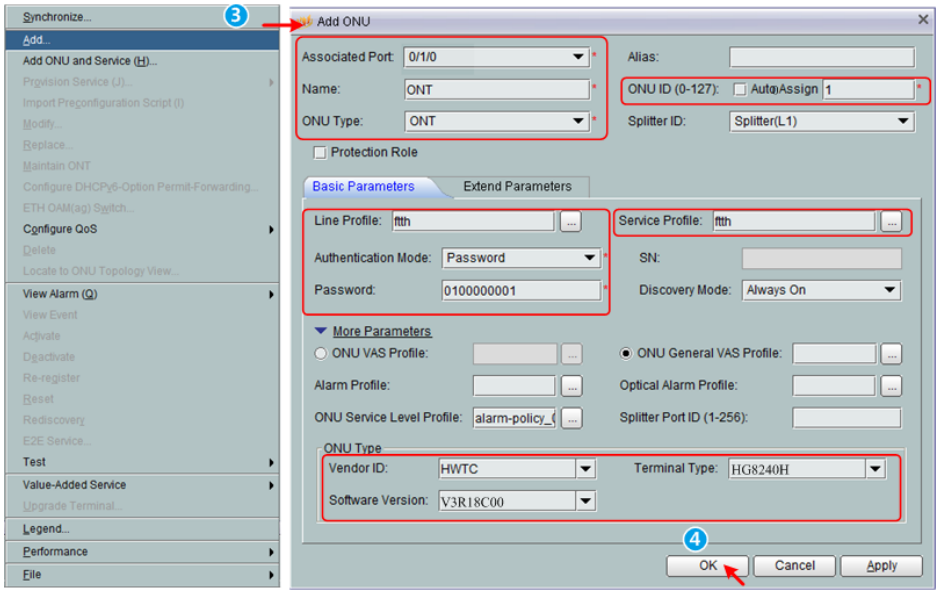
- **Provision services.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

     The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



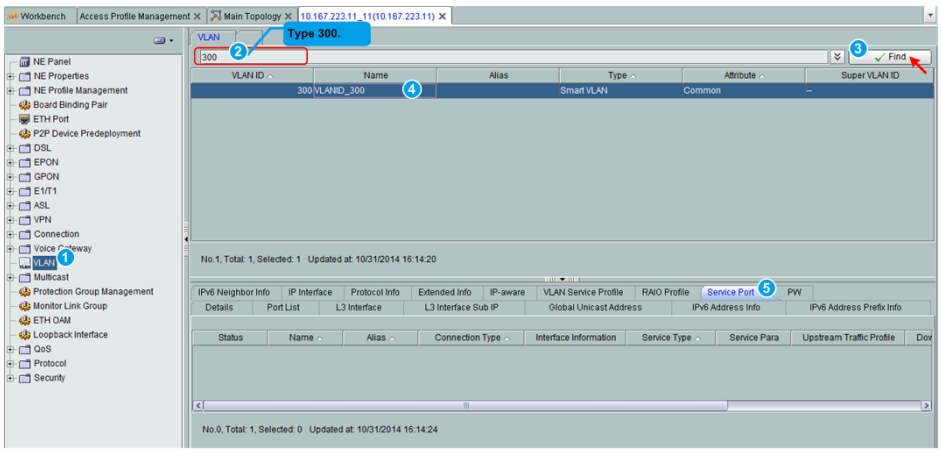


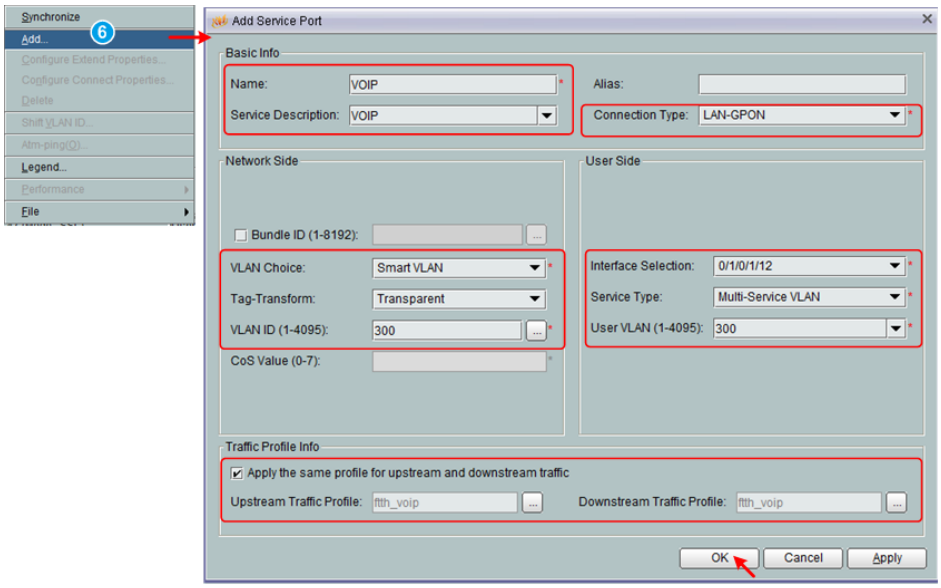
NOTE

HG8240H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

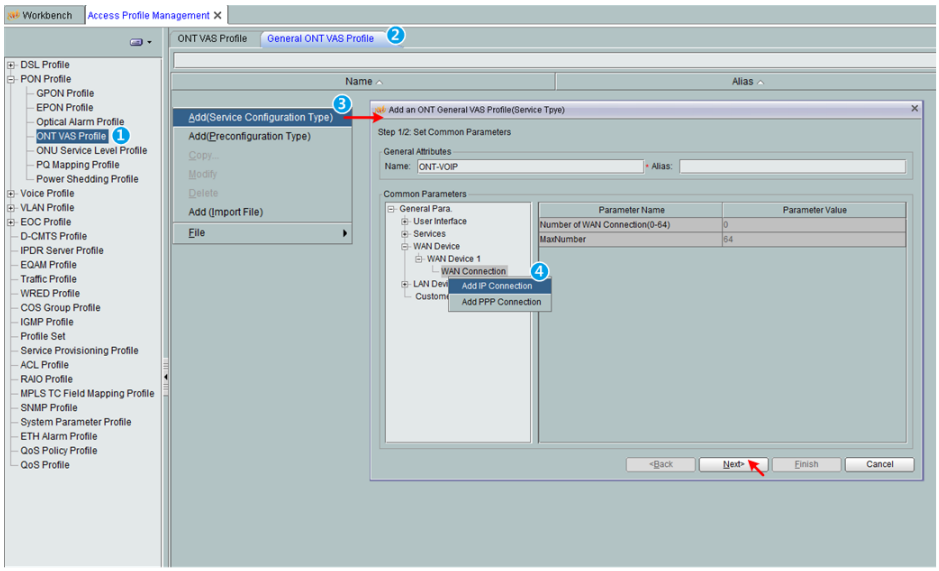
The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

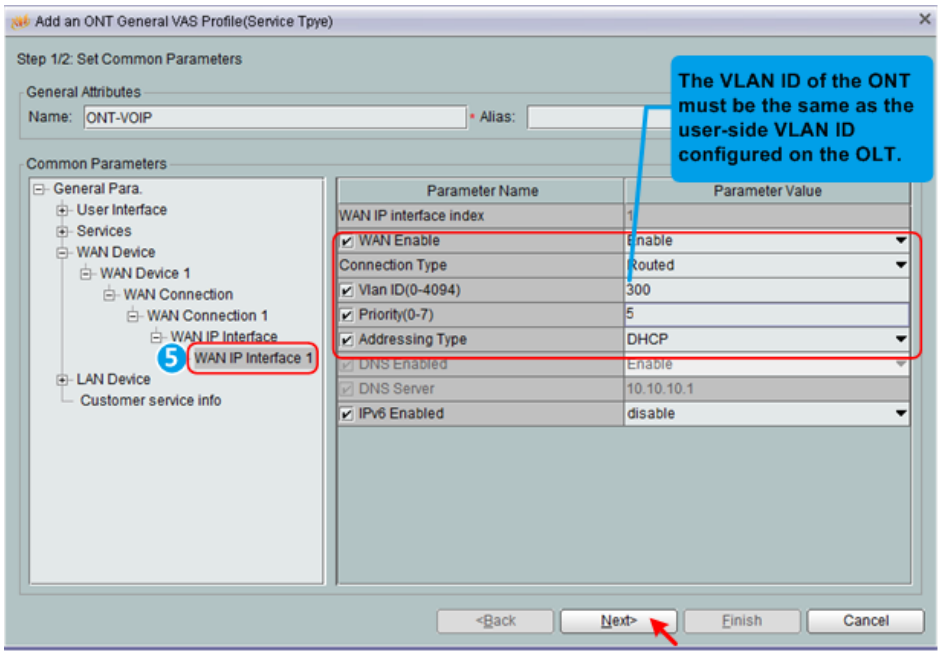
b. **Add a service port on the OLT side.**

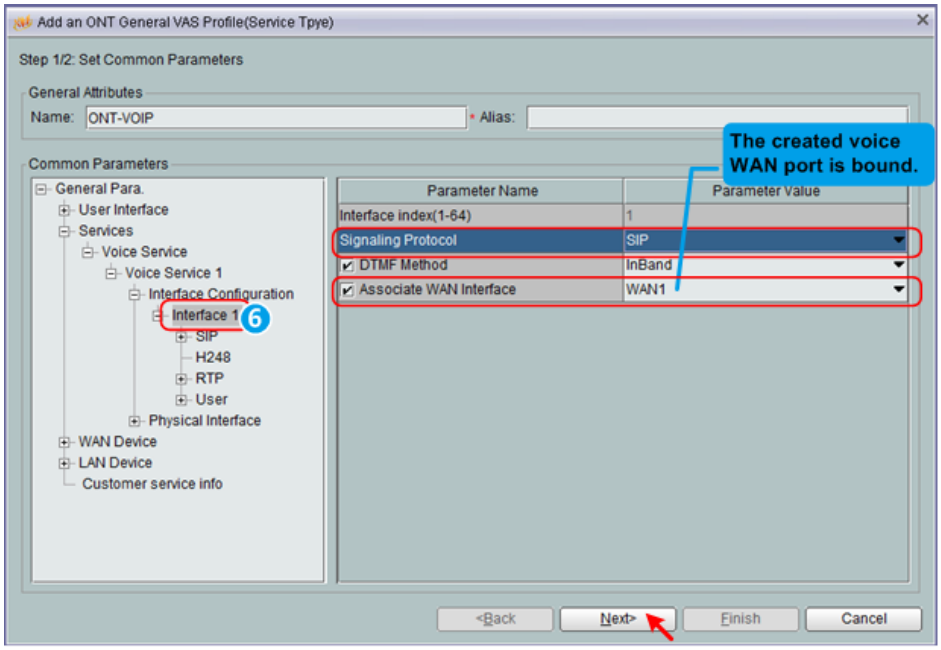


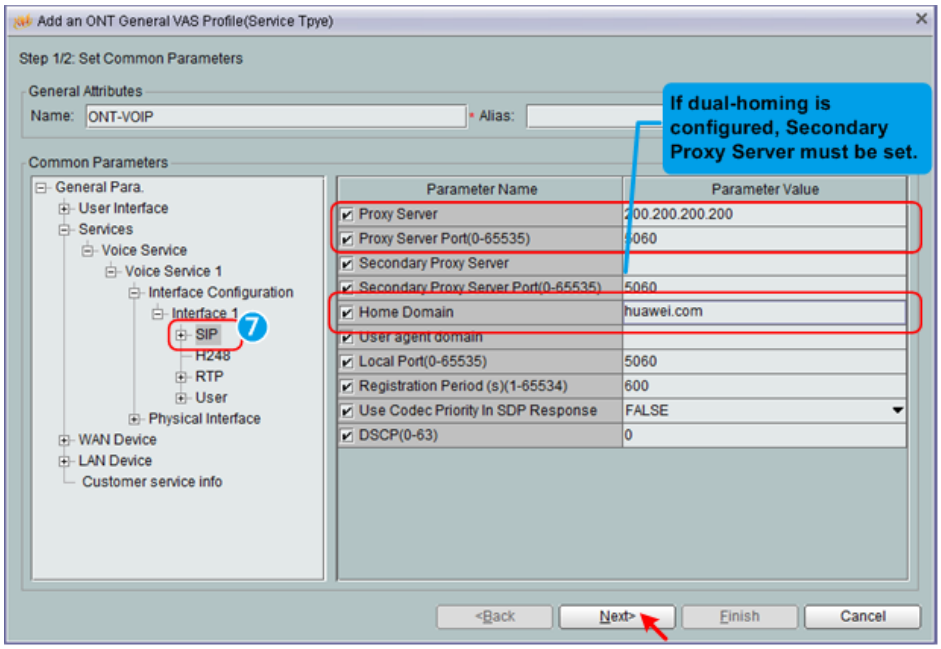


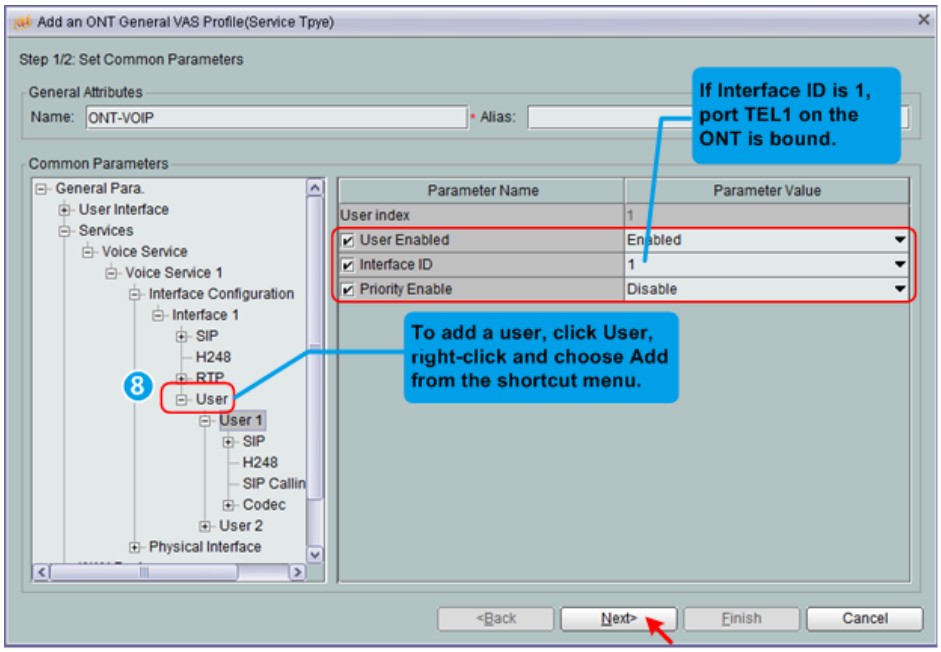
c. **Configure a general VAS profile for the ONT.**

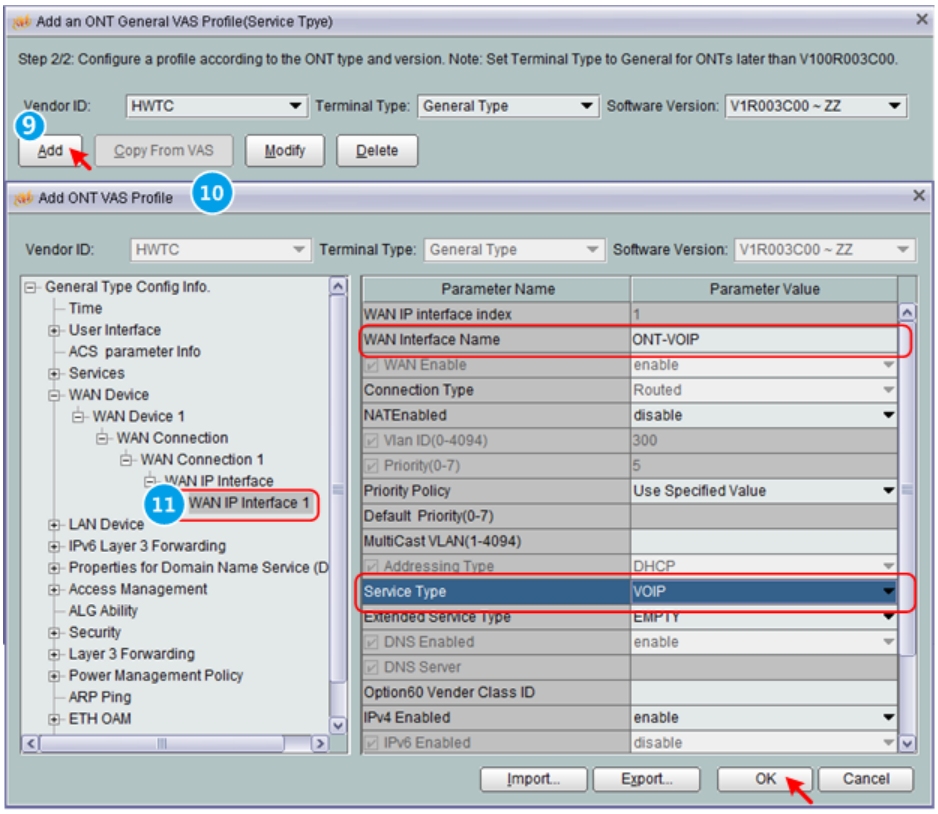




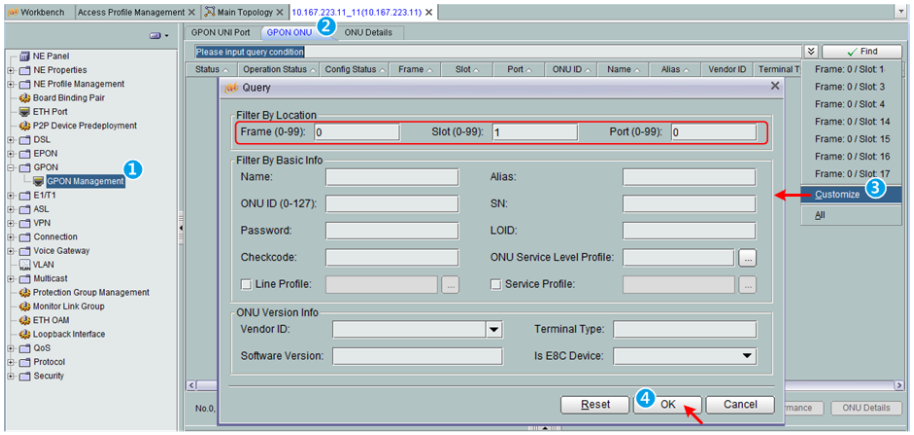


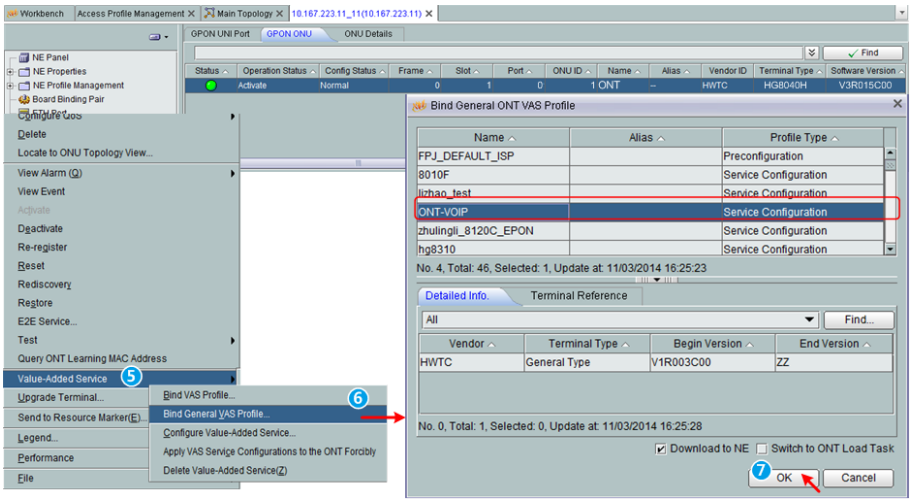

Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
Voice Service
Voice Service 1
Interface Configuration
Interface 1
SIP
H248
RTP
User
Physical Interface
WAN Device
LAN Device
Customer service info
Parameter Name
Parameter Value
Proxy Server
200.200.200.200
Proxy Server Port(0-65535)
5060
Secondary Proxy Server
Secondary Proxy Server Port(0-65535)
5060
Home Domain
huawei.com
User agent domain
Local Port(0-65535)
5060
Registration Period (s)(1-65534)
600
Use Codec Priority In SDP Response
FALSE
DSCP(0-63)
0
If dual-homing is configured, Secondary Proxy Server must be set.
7
<Back
Next>
Finish
Cancel


Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
Voice Service
Voice Service 1
Interface Configuration
Interface 1
SIP
H248
RTP
User
User 1
SIP
H248
SIP Callin
Codec
User 2
Physical Interface
Parameter Name
Parameter Value
User index
1
User Enabled
Enabled
Interface ID
1
Priority Enable
Disable
If Interface ID is 1, port TEL1 on the ONT is bound.
To add a user, click User, right-click and choose Add from the shortcut menu.
8
<Back
Next>
Finish
Cancel

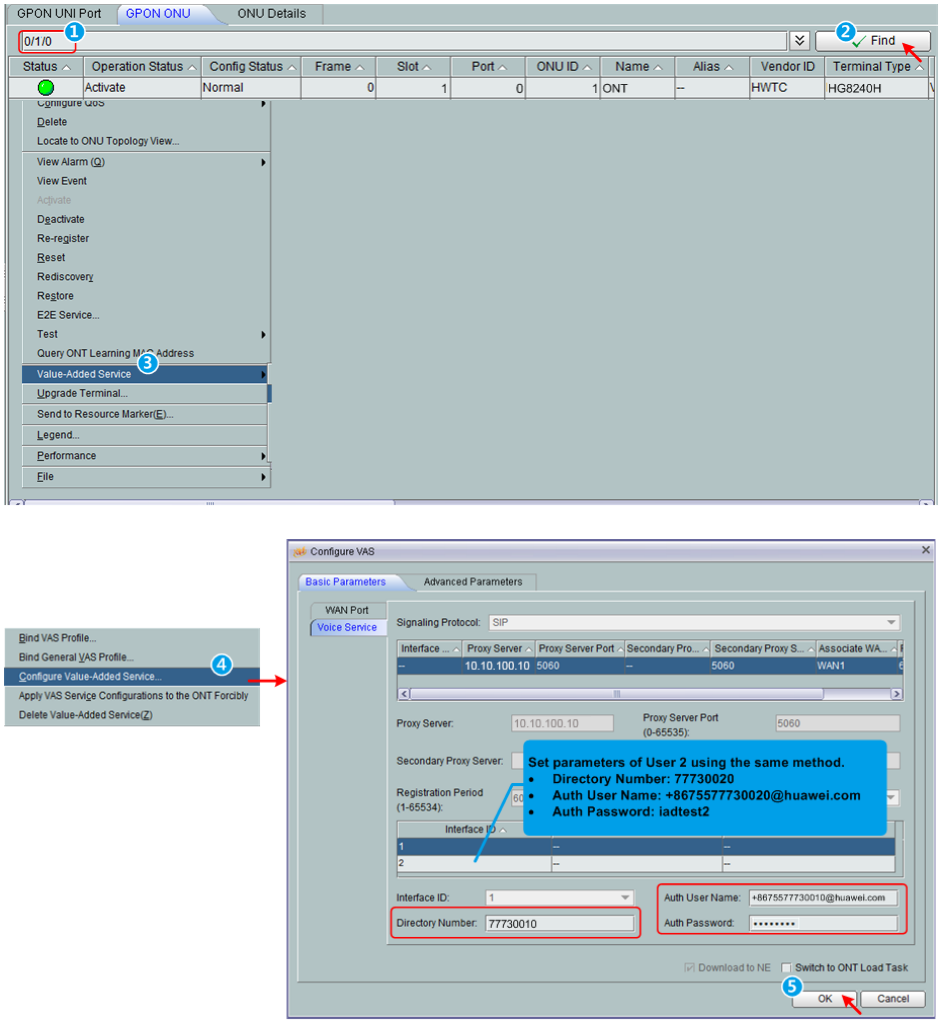


d. **Bind a general VAS profile.**





e. **Configure the ONT VAS service.**



NOTE

The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

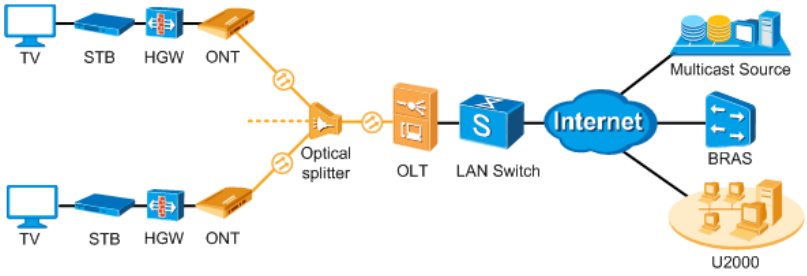
2.3.1.4 Configuring the GPON FTTH Layer 2 Multicast Service on the NMS

This topic describes how to configure the multicast service when an ONT is connected to an OLT through a GPON port.

Networking

- The ONT is connected to the OLT in Layer 2 mode.
- The OLT uses IGMP proxy, which is a Layer 2 multicast protocol.
- The IGMP version of the multicast VLAN is IGMPv2.
- The multicast programs are obtained in the dynamic mode.

Figure 2-5 Configuring the GPON FTTH multicast service



Data Plan

Table 2-9 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA Type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for video services: 13

Item	Data
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1 ID of the port on the ONT that is connected to the PC: 2
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode
VLAN Plan	● S-VLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: Smart ● VLAN attribute: Common **NOTE** VLAN translation policy: ● ONT: transparently transmits the MVLAN of the HGW. Multicast packets are duplicated downstream with MVLAN unchanged. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.

Procedure

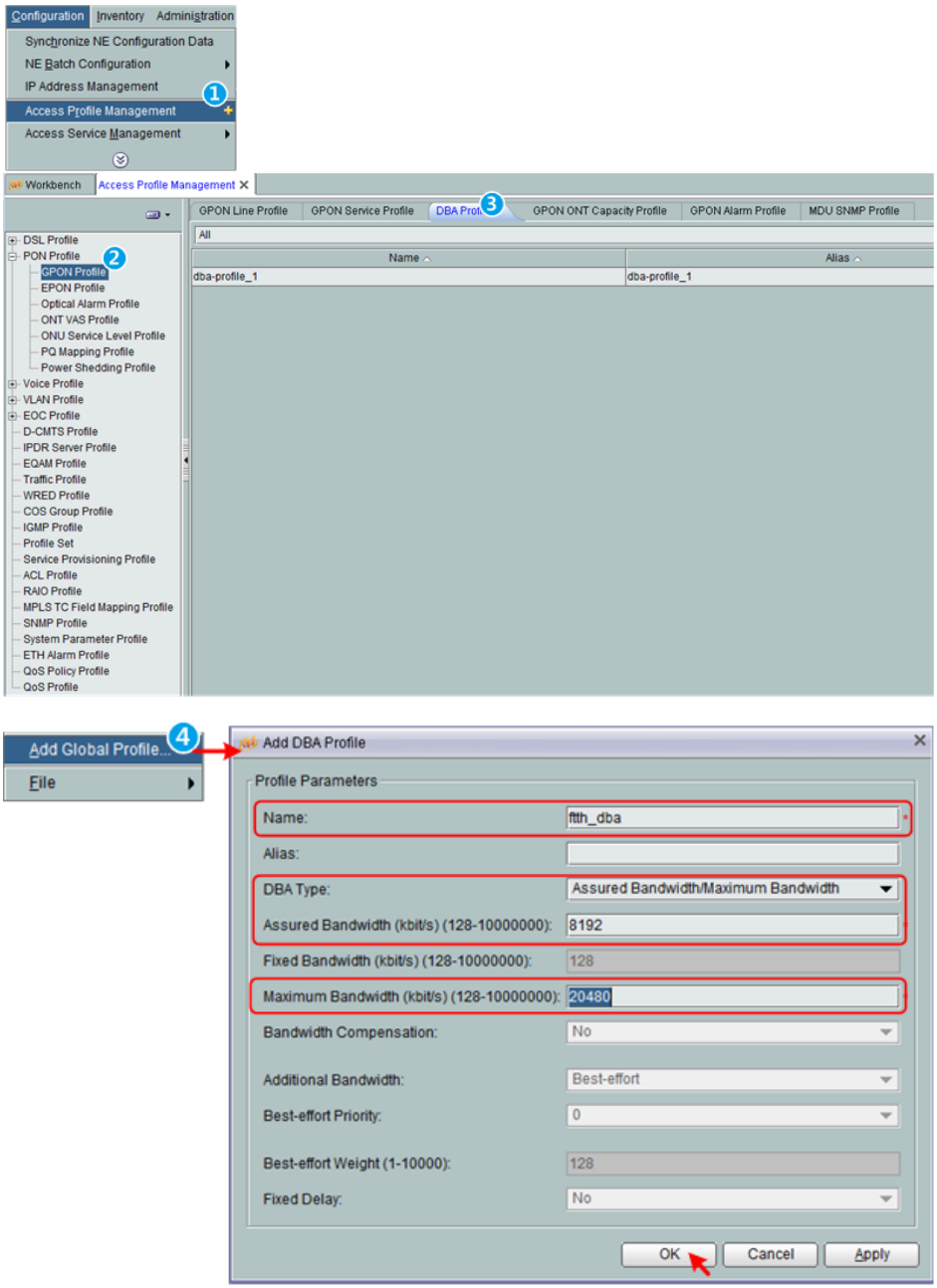
- **Implement pre-configurations.**

NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

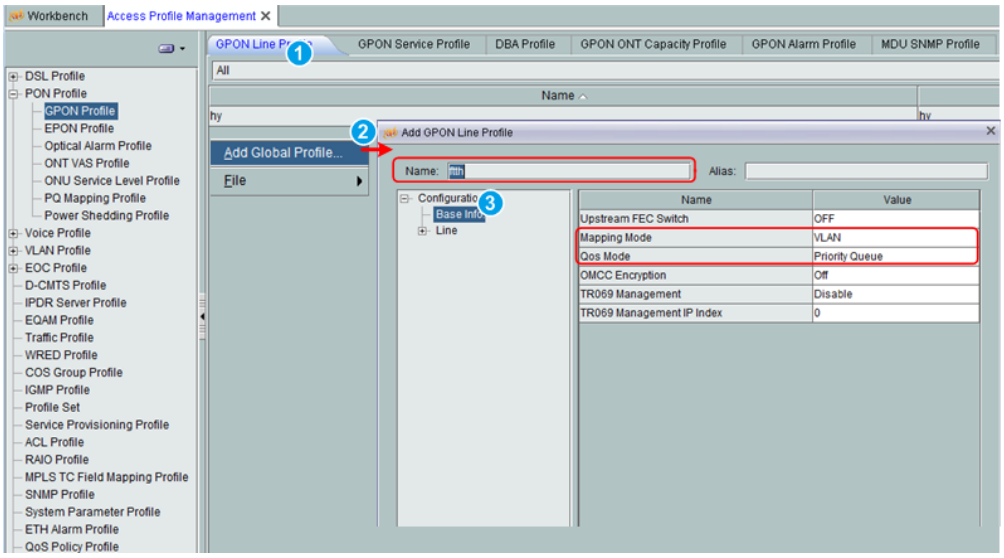
1. **Configure a DBA profile.**

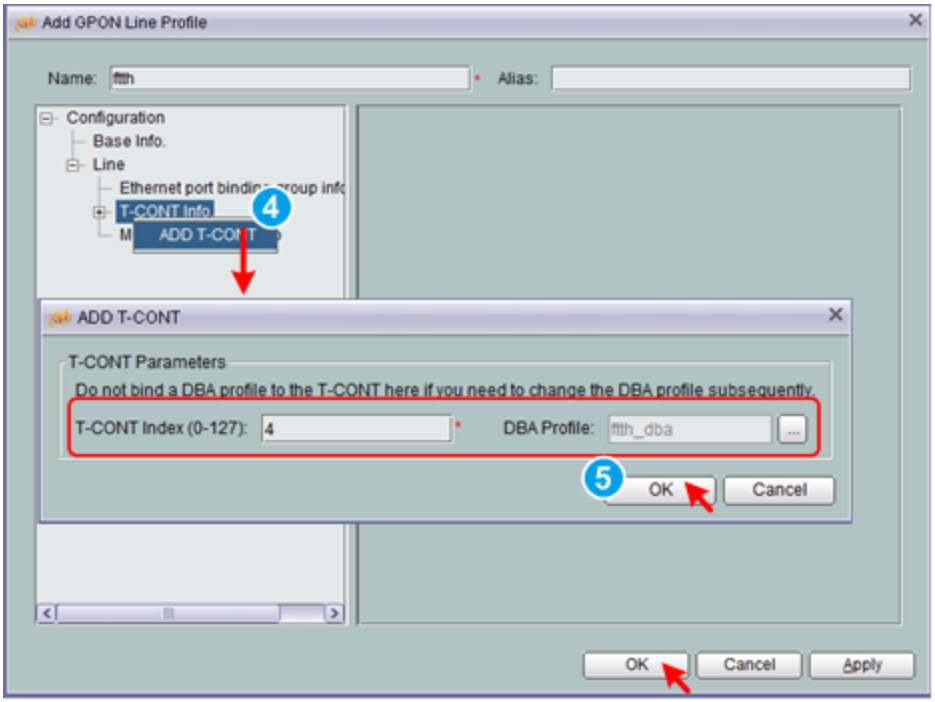


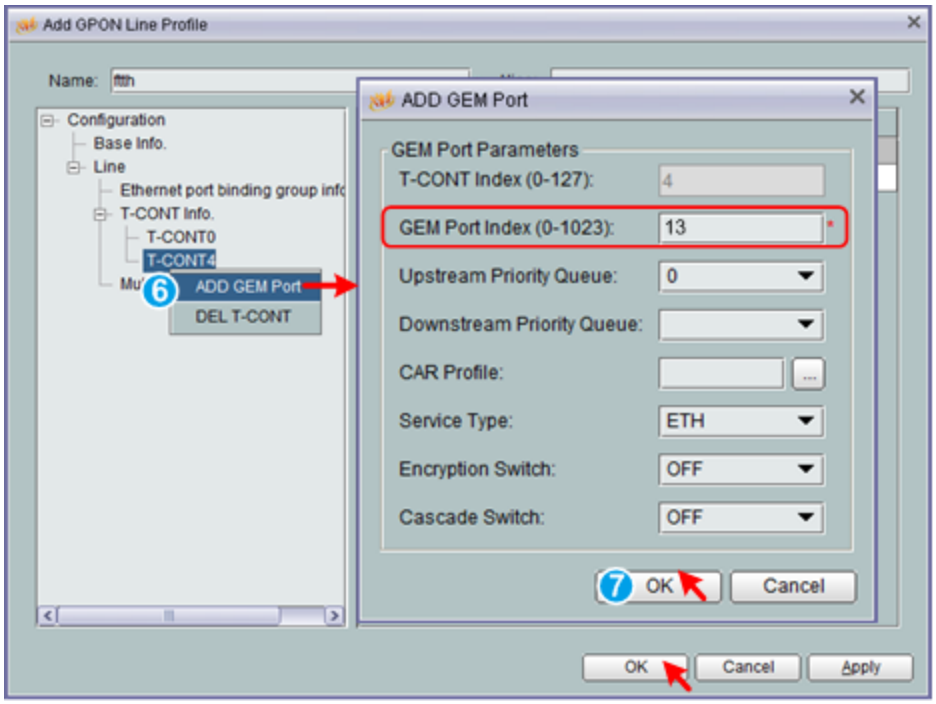
2. **Configure a line profile.**

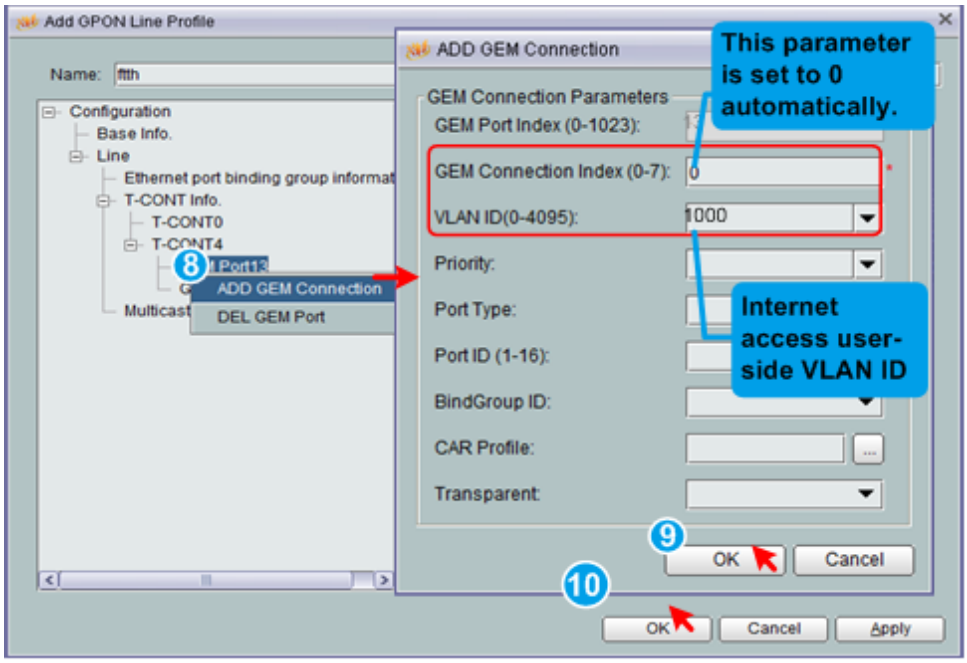
   In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

   In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 13. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.


Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
Add Global Profile...
File
Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
Name
Value
Upstream FEC Switch
OFF
Mapping Mode
VLAN
Qos Mode
Priority Queue
OMCC Encryption
Off
TR069 Management
Disable
TR069 Management IP Index
0
1
2
3

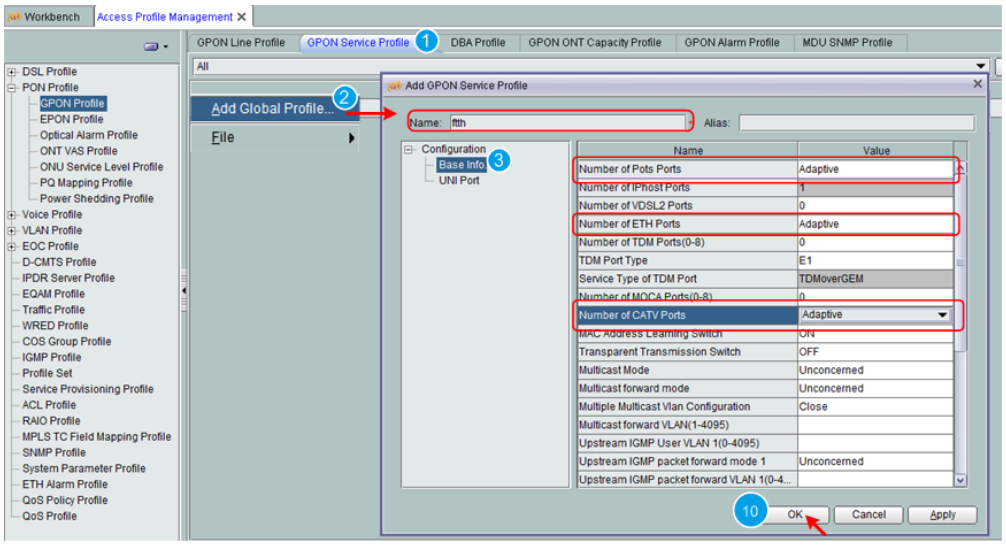

Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
T-CONT Info
ADD T-CONT
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127):
4
DBA Profile:
ftth_dba
5
OK
Cancel
OK
Cancel
Apply

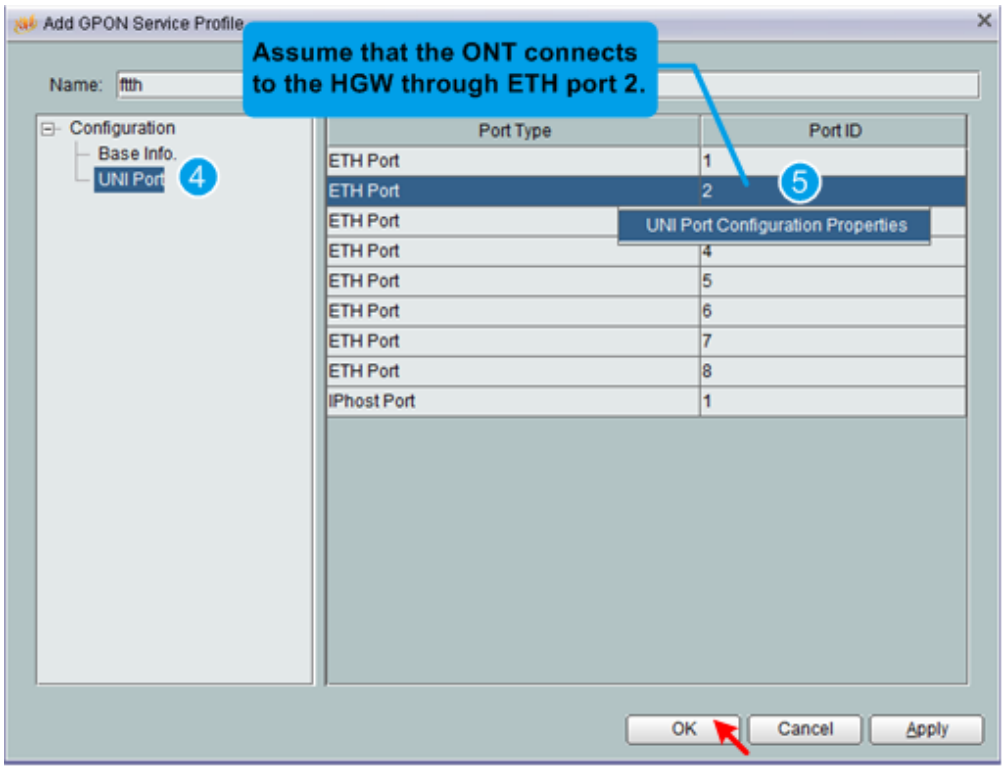


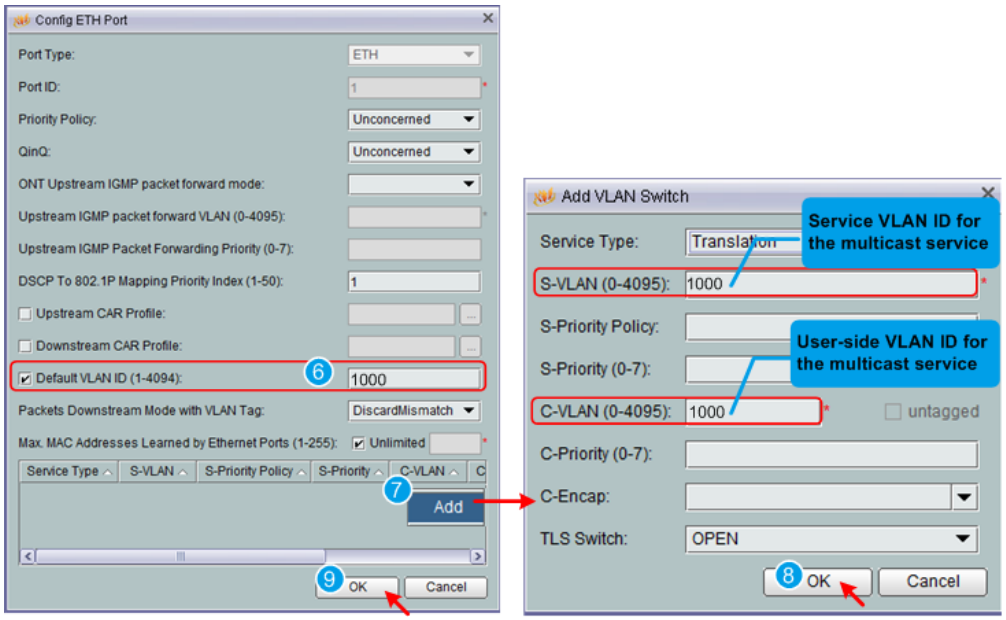


3. **Configure a service profile.**

   Configure a VLAN translation policy for the ONT ETH port. Assume that the ONT connects to the HGW through ETH port 2. Configure a VLAN translation policy to make the ONT transparently transmit the MVLAN of the HGW in the upstream direction, and replicate multicast packets with the MVLAN unchanged in the downstream direction.

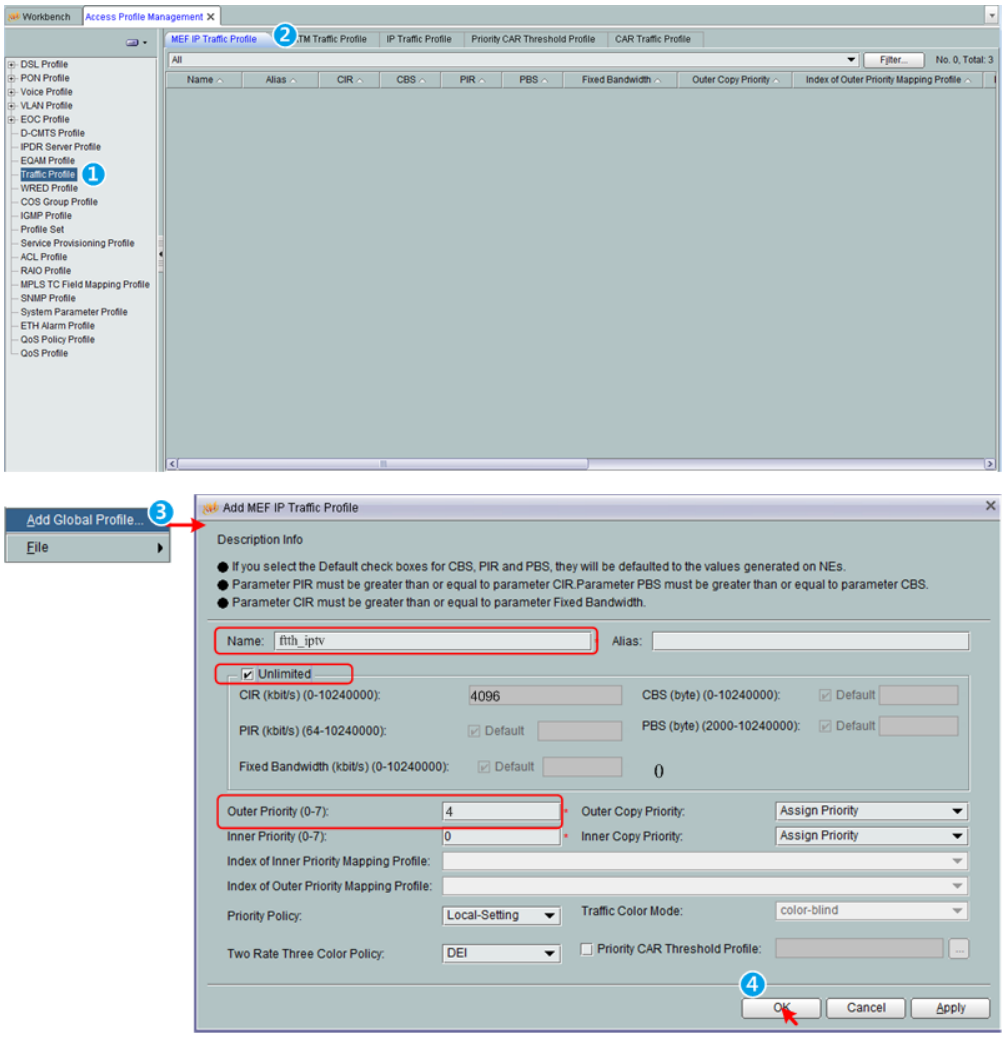






4. **Configure an MEF IP traffic profile.**

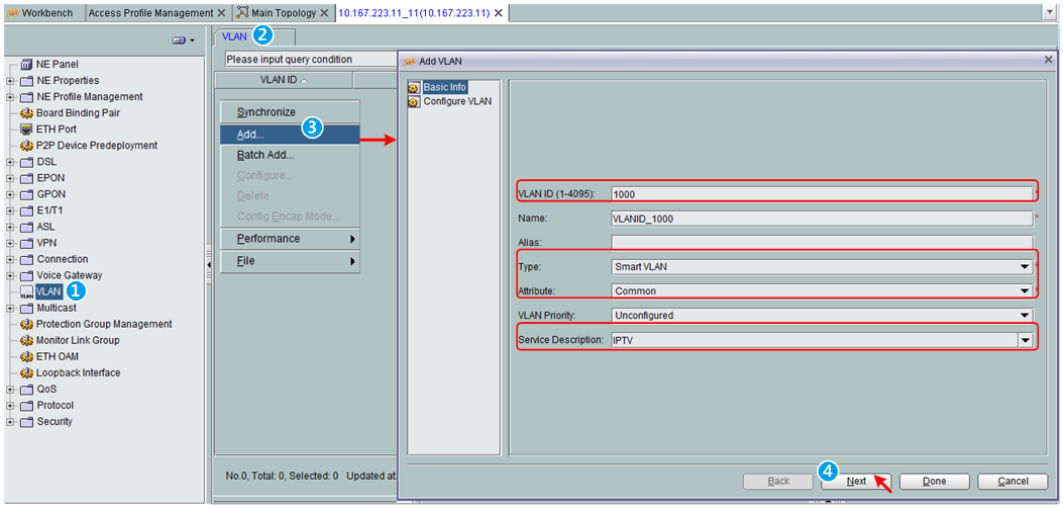
   The profile name is ftth_iptv, CIR is off, priority is 4, and priority-based scheduling policy is Local-Setting. Traffic is scheduled based on the priority specified in the profile.

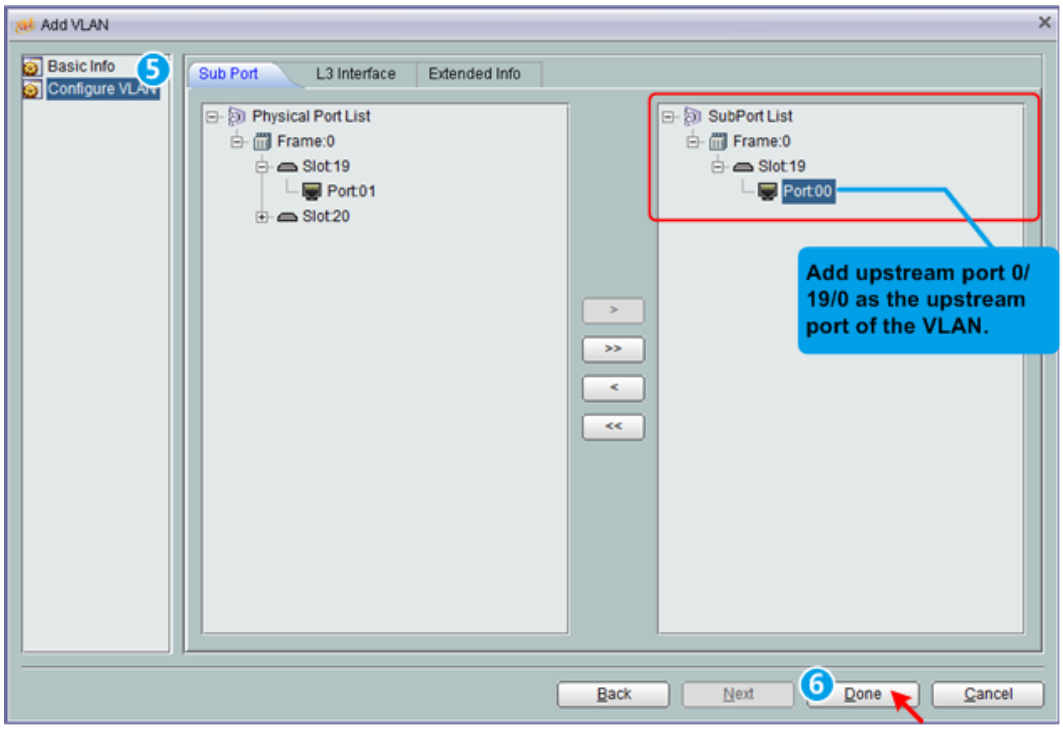


5. **Configure an S-VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   The S-VLAN is used for the multicast service.



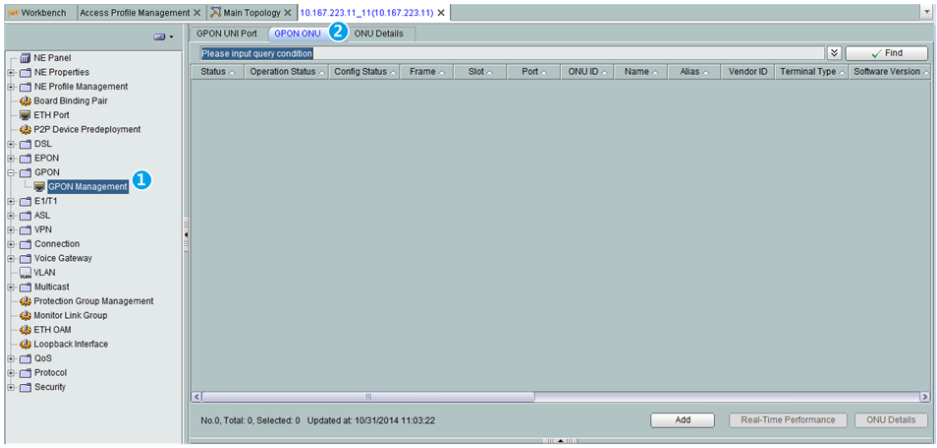


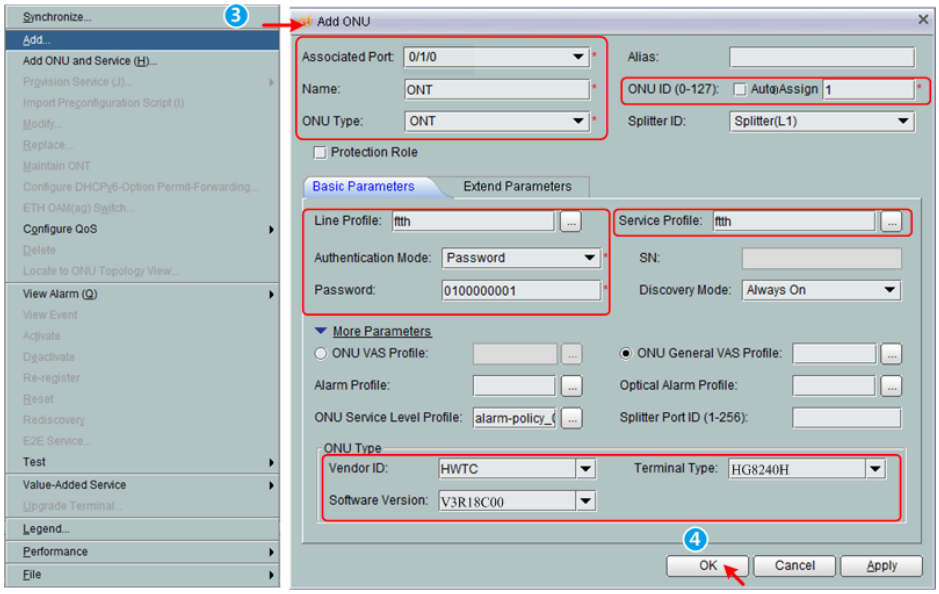
- **Provision services.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



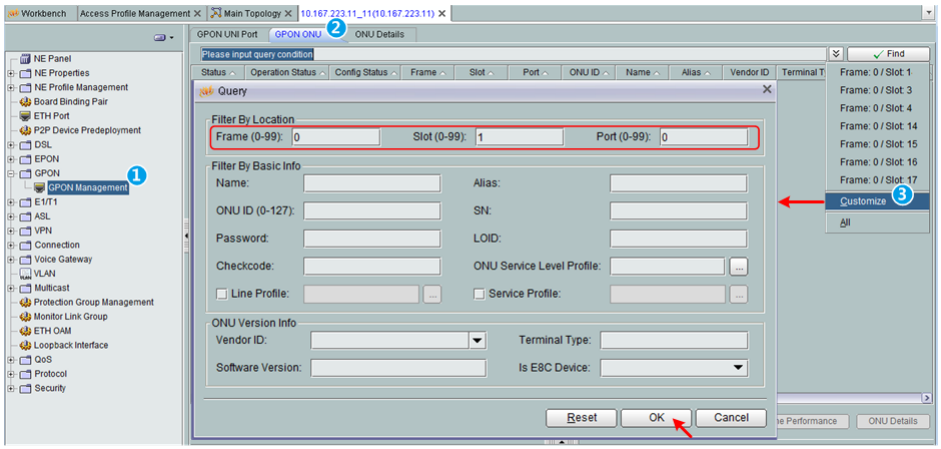


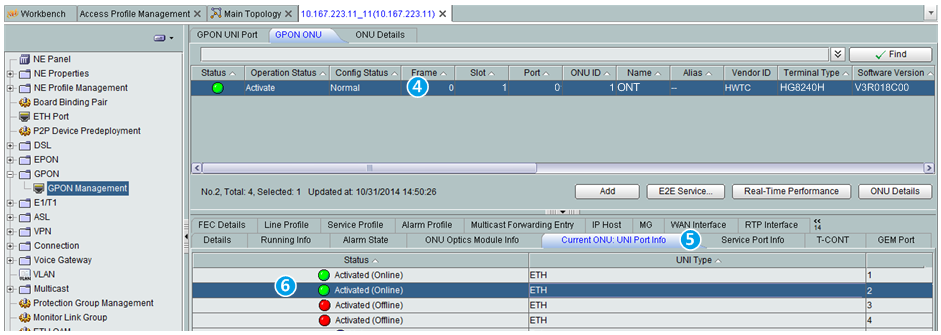
NOTE

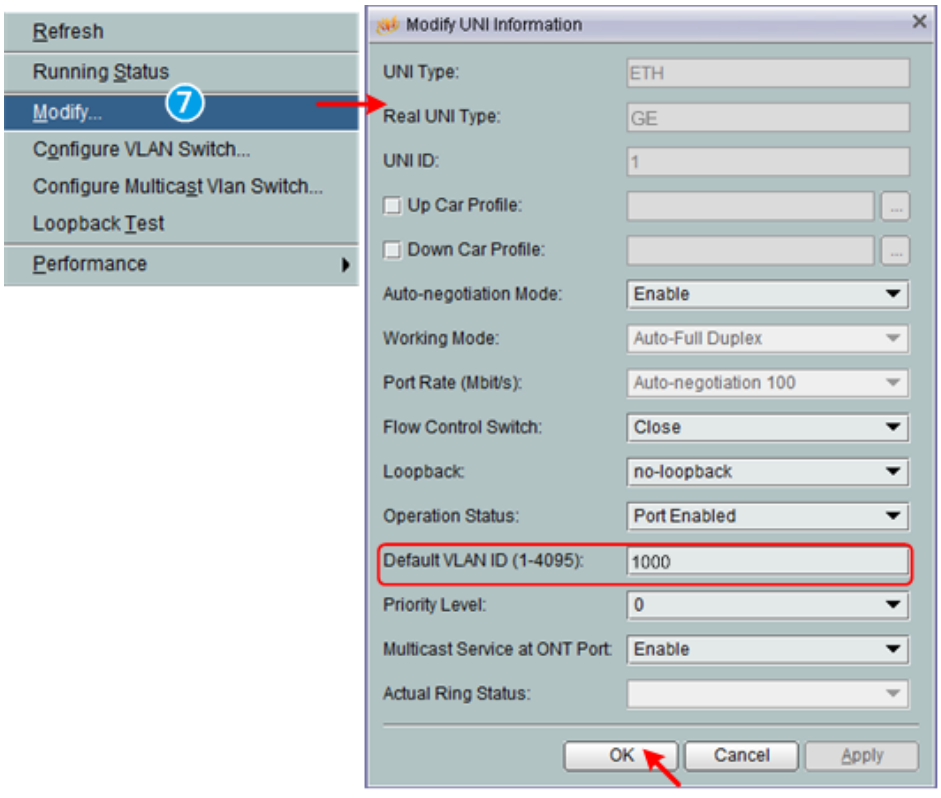
HG8240H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

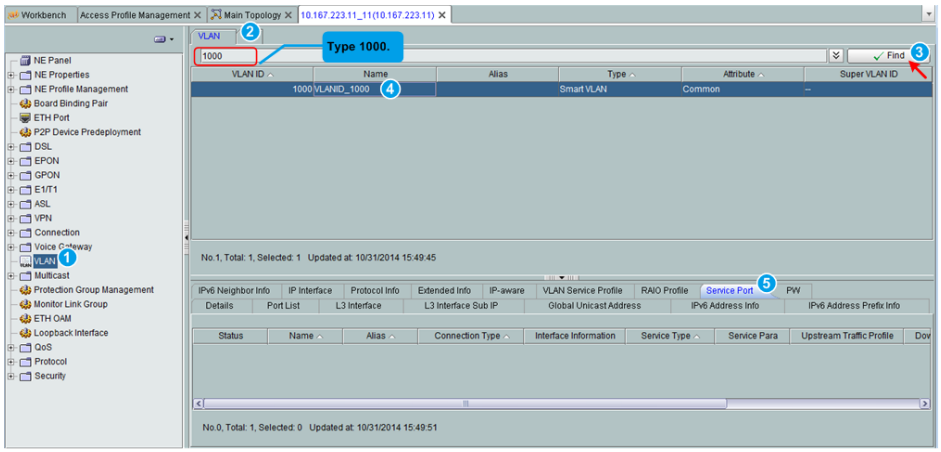
b. **Configure Ethernet port attributes and service channels of a GPON ONU.**

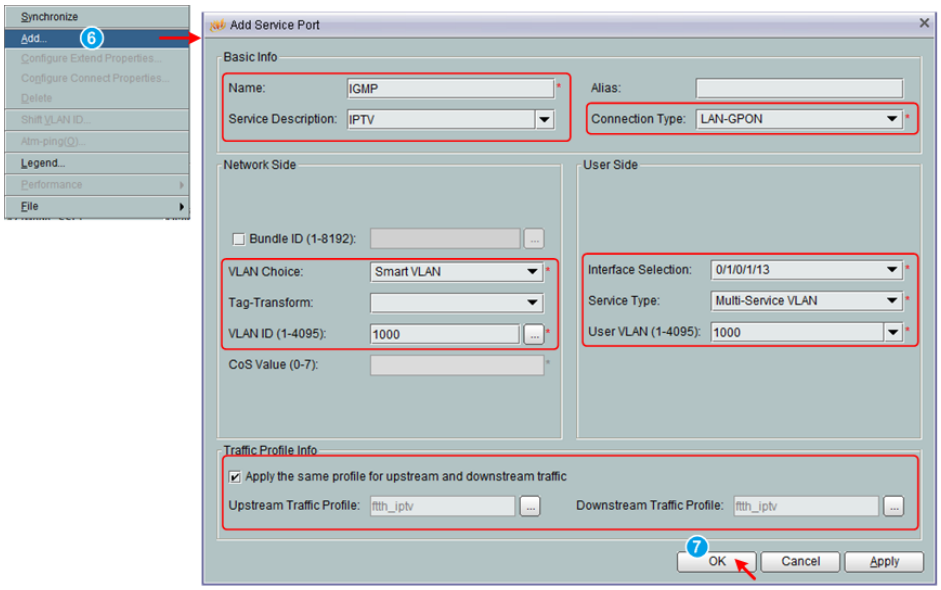




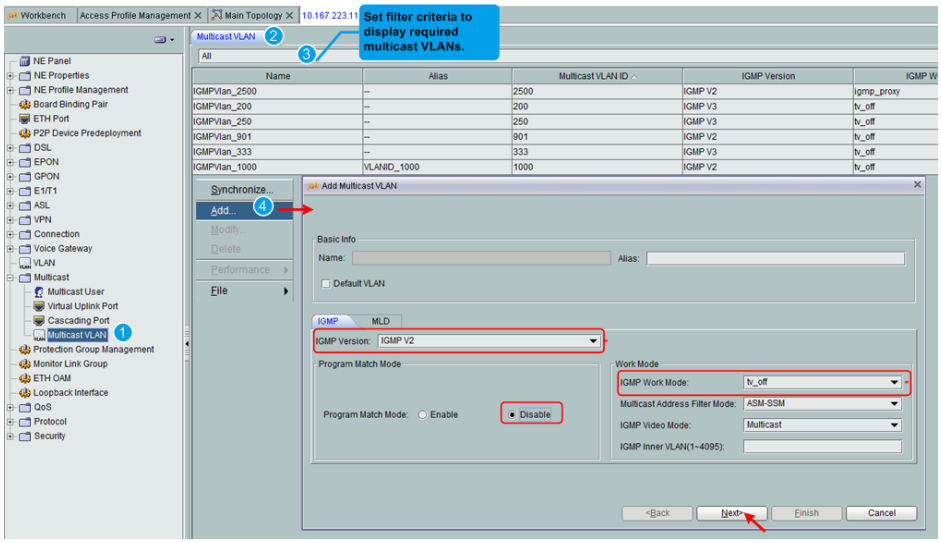


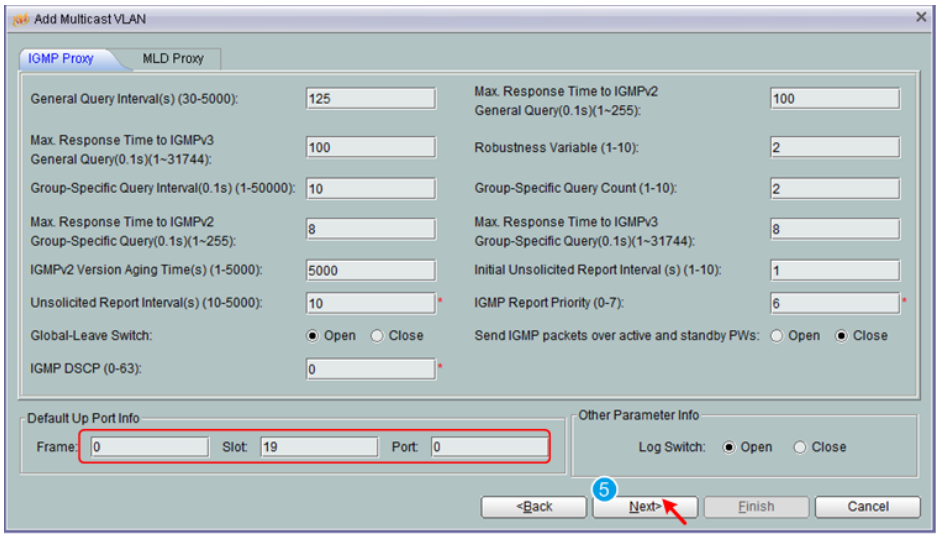
c. **Add a service virtual port on the OLT side.**

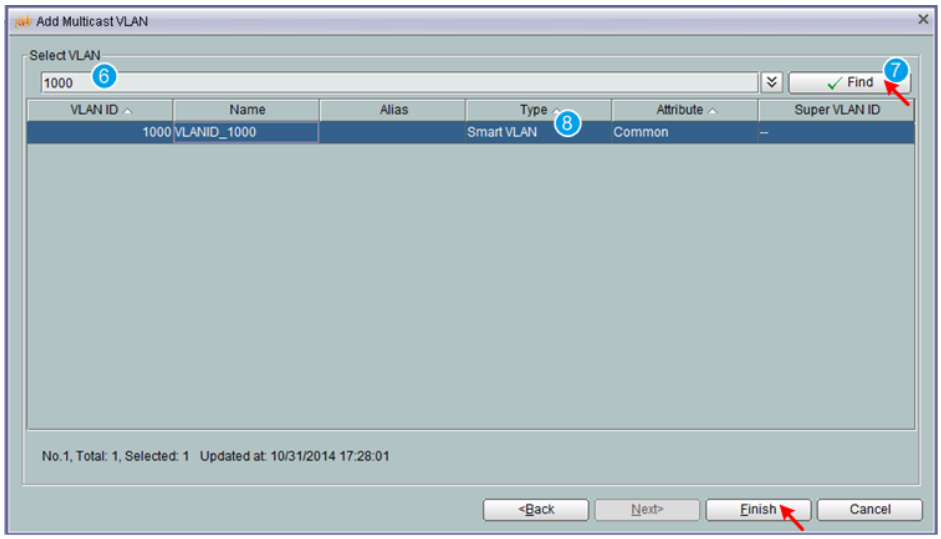




d. **Add a multicast VLAN on the OLT side.**







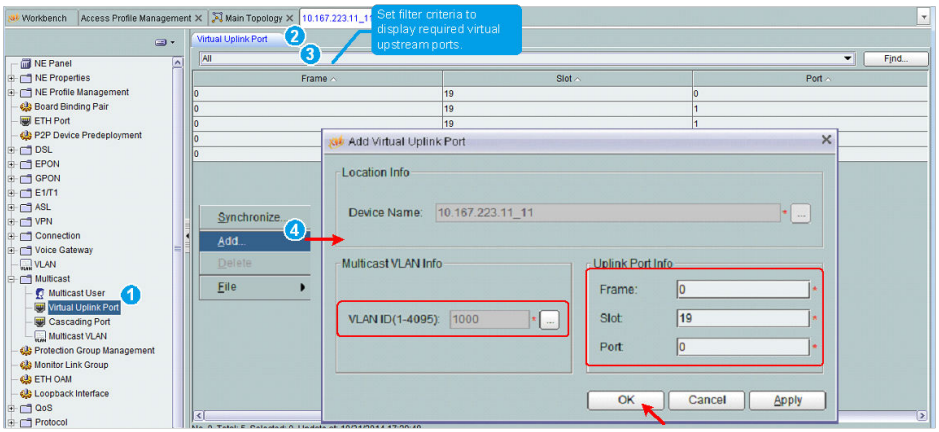
NOTE

Program match mode can be set when **IGMP Work Mode** is **tv_off**. The values of **Program match mode** are as follows:

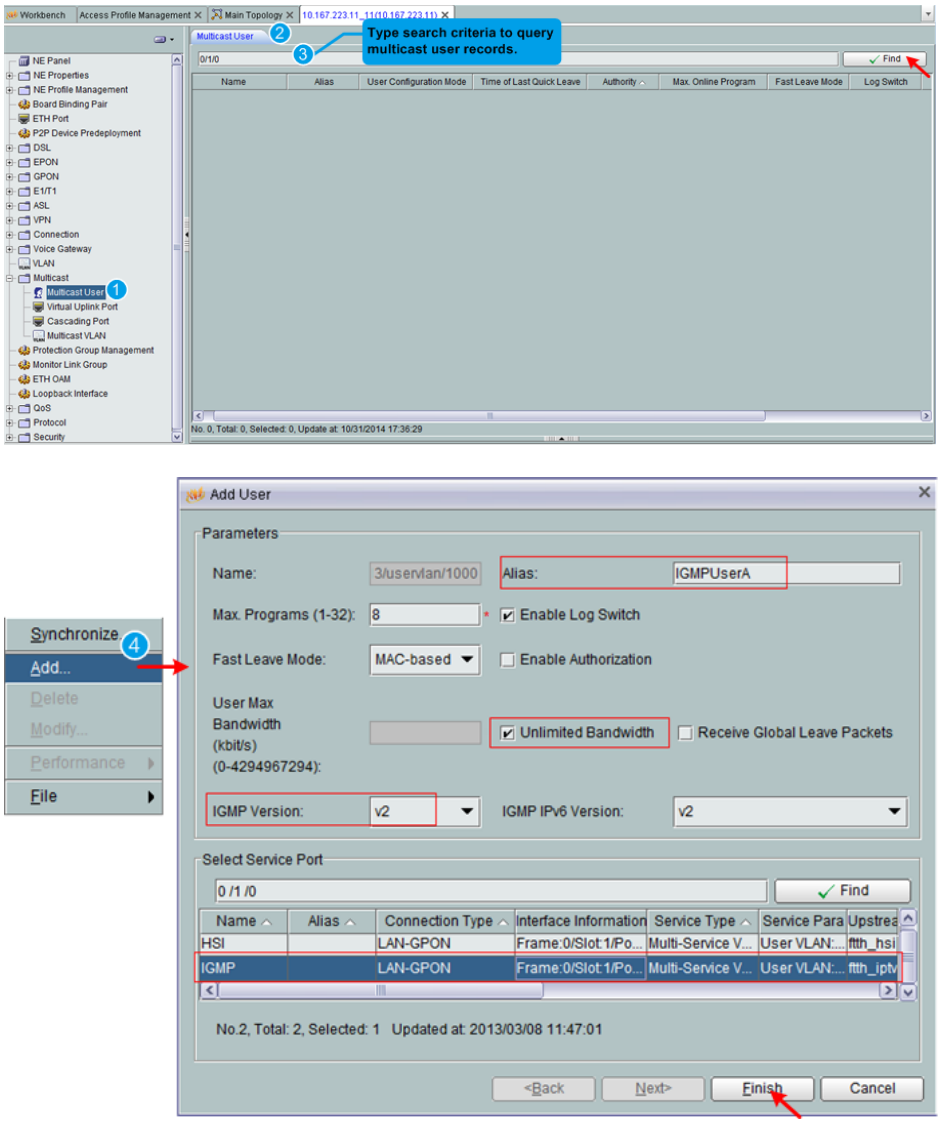
- Enable: Multicast programs are configured statically. Dynamic program generation is not supported.
- Disable: Multicast programs are dynamically generated. Static program configuration is not supported.

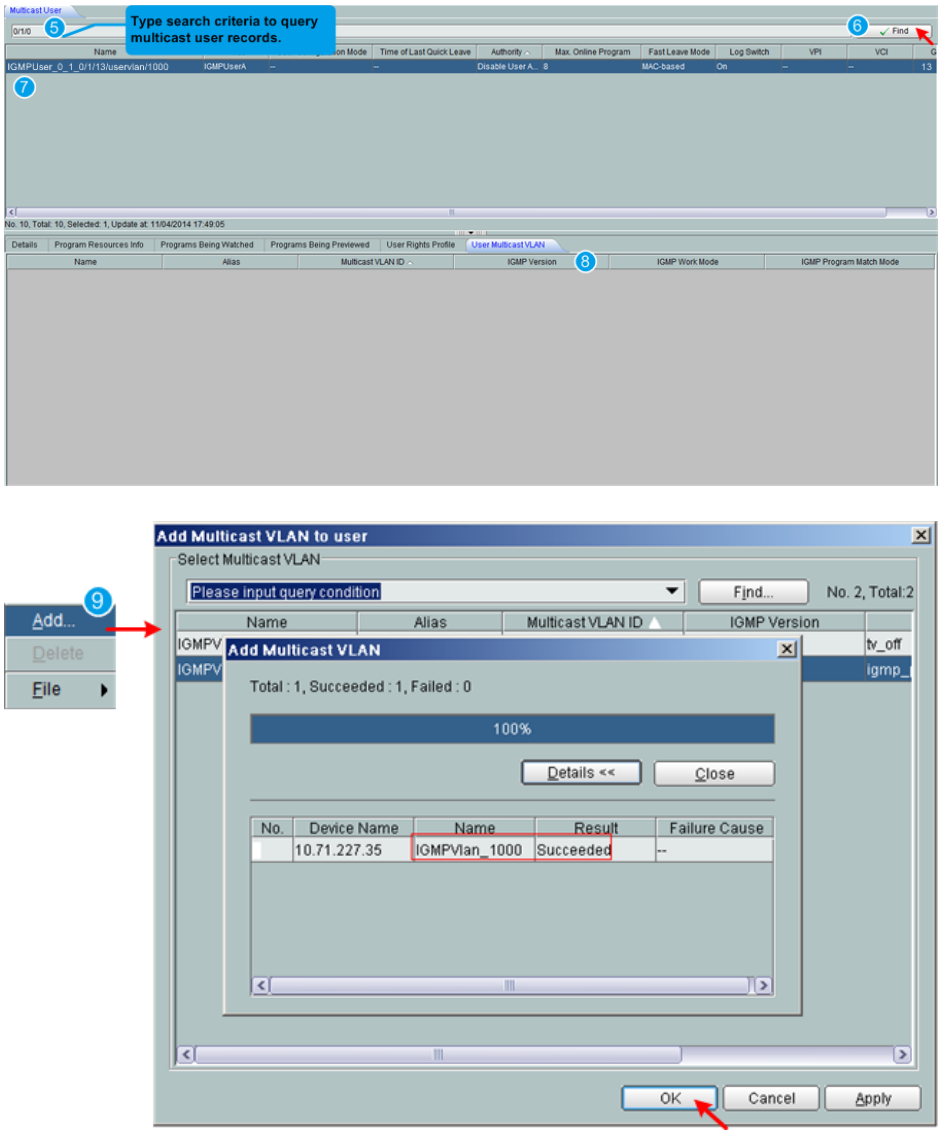
After Configuration, **IGMP Work Mode** should be set to **Proxy** again, otherwise IGMP work abnormally.

e. **Add a virtual multicast upstream port on the OLT side.**



f. **Configure a multicast user on the OLT side.**





Result

The user can watch programs on TV.

2.4 Configuration by Using OLT Commands

This topic describes how to configure the Internet access service, VoIP service and IPTV service by using OLT commands.

2.4.1 Bridging + Voice ONT Network Scenario (GPON and 10G GPON Access)

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when bridging + voice ONTs are used to build an FTTH network.

The FTTH GPON and 10G GPON access have the same configuration procedure. ONT web pages for configuring them have differences; however, they have the same configuration

parameters. The following uses GPON ONT configuration as an example. For differences on web pages, see the related ONT manuals.

2.4.1.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to users' home and triple play services are required. The following provides detailed service requirements:

- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service expansibility is supported and different services do not affect each other.
- Proper service security is ensured.
  - Internet access services are protected against unauthorized access, user account theft or borrowing, MAC/IP spoofing, and malicious attacks.
  - Voice and IPTV services are protected against MAC/IP spoofing, malicious attack, and traffic flooding attacks.
- Service faults are easy to locate and services are easy to maintain.

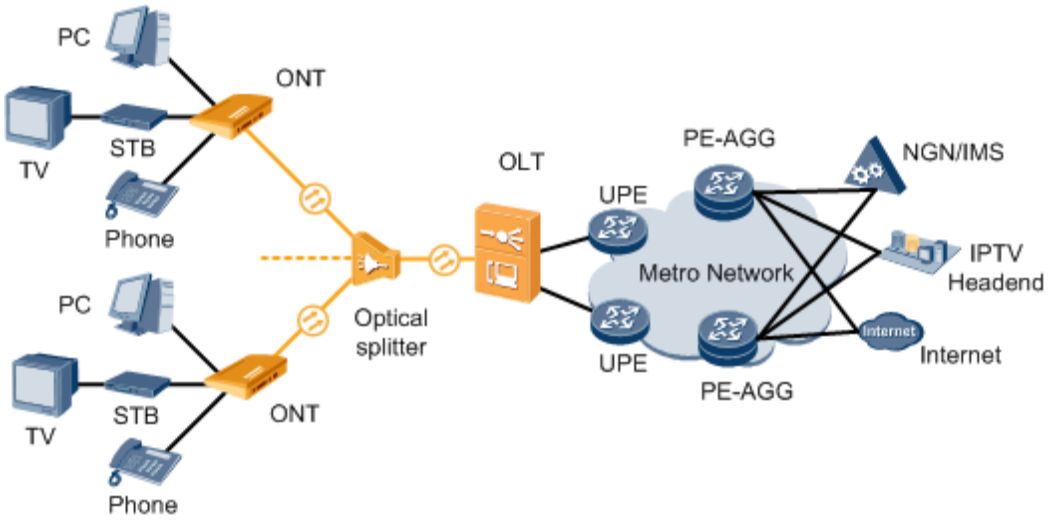
Application Scenario

As shown in **Figure 2-6**, the ONT integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users.

The bridging+voice ONT provides Layer 2 data (Internet and IPTV services) and VoIP services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking.

- For Internet services, a PC directly performs dial-up. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address.
- For VoIP services, the ONT with a built-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).
- For IPTV services, the set top box (STB) obtains an IP address from the DHCP server for ordering programs. The ONT transparently transmits the packets.

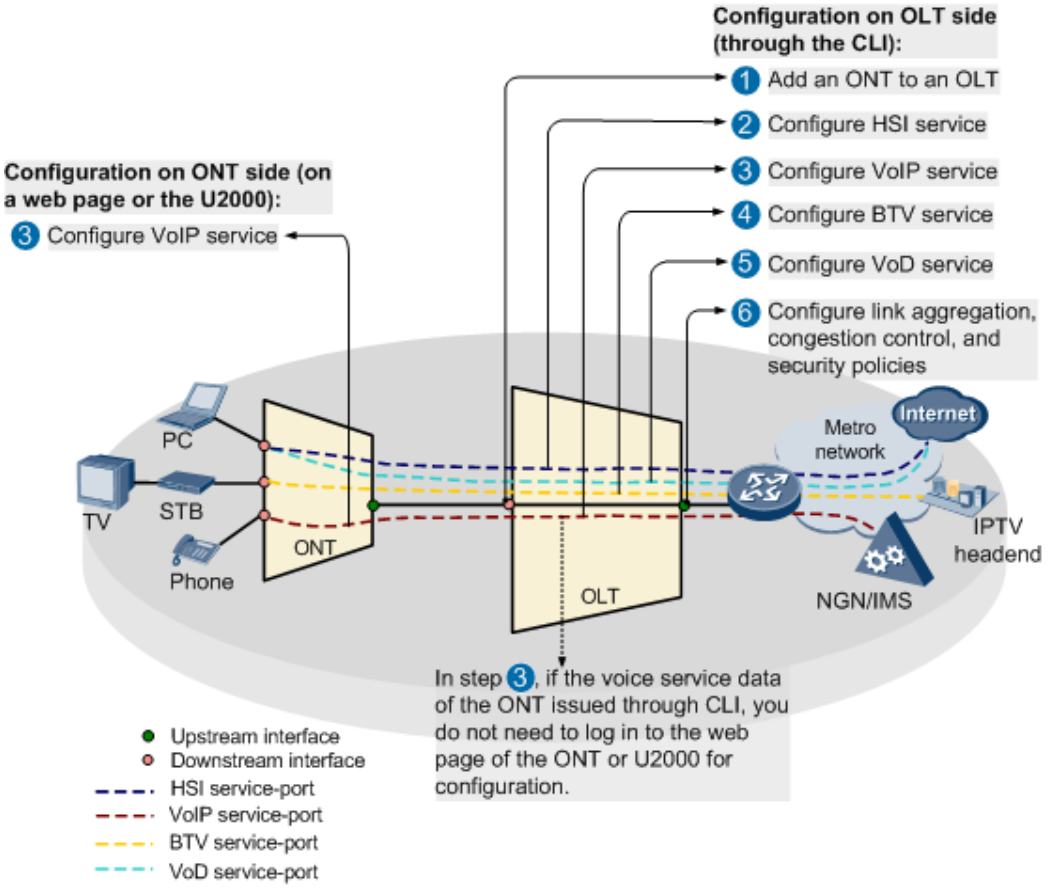
Figure 2-6 Bridging+Voice ONT



2.4.1.2 Configuration Process

Figure 2-7 shows the configuration roadmap in fiber to the home (FTTH) networking using a bridging+voice optical network terminal (ONT).

Figure 2-7 Configuration roadmap in FTTH networking using a bridging+voice ONT



The following table describes the configuration steps.

Item	Step		Description
Optical line terminal (OLT)	Adding an ONT to an OLT		Services can be configured for an ONT only after the ONT is successfully added to an OLT.
OLT	Configuring the Internet Access Service		None

OLT
ONT
U2000
	Configure the VoIP service.	Configuring the H.248-based Voice Service (on a Web Page or the U2000)	**NOTE**
			● The H.248 and Session Initiation Protocol (SIP) protocols are mutually exclusive for the VoIP service. Either of them is configured at a time.
			● The voice service can be configured through command line interface (CLI) on an OLT, web page, or U2000. Select a configuration mode based on site requirements.
			  ● OLT CLI: This mode can be used for site deployment or the U2000 has not been deployed.
			  ● Web page: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for site deployment.
			  ● U2000: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for service provisioning in batches.

		Configuring the H.248-based Voice Service (Through the CLI)	
		Configuring the SIP-based Voice Service (on a Web Page or the U2000)	
		Configuring the SIP-based Voice Service (Through the CLI)	
OLT	Configure the IPTV service.	Configuring the BTV Service	IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.
		Configuring the VoD Service	
OLT	Configuring Link Aggregation, Congestion Control, and Security Policies		The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.
OLT	Verifying Services		The OLT provides remote verification methods including ONT PPPoE/DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.

2.4.1.3 Adding an ONT to an OLT

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Data Plan

Item	Data
DBA profile	Profile name: ftth_dba_mngt ● Profile type: Type1 ● Fixed bandwidth: 1 Mbit/s Profile name: ftth_dba_hsi ● Profile type: Type4 ● Maximum bandwidth: 32 Mbit/s Profile name: ftth_dba_voip ● Profile type: Type2 ● Assured bandwidth: 1 Mbit/s Profile name: ftth_dba_iptv ● Profile type: Type2 ● Assured bandwidth: 1 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID for management services: 4 T-CONT ID for voice services: 5 T-CONT ID for video services: 6 T-CONT ID for Internet access services: 7 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: adaptive
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2

Procedure

Step 1 Configure GPON ONT profiles.

GPON ONT profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONT-side service.
- Service profile: A service profile provides the service configuration channel for the ONT that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONT lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query the existing DBA profiles in the system. If the existing DBA profiles in the system cannot meet the requirements, run the **dba-profile add** command to add a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name ftth_dba_mngt type1 fix 1024
   huawei(config)#dba-profile add profile-name ftth_dba_voip type2 assure 1024
   huawei(config)#dba-profile add profile-name ftth_dba_iptv type2 assure 1024
   huawei(config)#dba-profile add profile-name ftth_dba_hsi type4 max 32768
   ```

   NOTE

   Select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONT. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba_mngt
   huawei(config-gpon-lineprofile-1)#tcont 5 dba-profile-name ftth_dba_voip
   huawei(config-gpon-lineprofile-1)#tcont 6 dba-profile-name ftth_dba_iptv
   huawei(config-gpon-lineprofile-1)#tcont 7 dba-profile-name ftth_dba_hsi
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 5
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 6
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 7
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameters settings.


```
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure an ONT service profile.

   Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port and POTS port to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.

   ```
   huawei(config)#ont-srvprofile gpon profile-name ftth
   huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive
   ```

   After the configurations are complete, run the **commit** command to apply the parameters setting.

   ```
   huawei(config-gpon-srvprofile-1)#commit
   huawei(config-gpon-srvprofile-1)#quit
   ```

4. (Optional) Add an alarm profile.
   - The default GPON alarm profile 1 is used. The alarm thresholds for the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONT line.

Step 2 Add an ONT.

The procedures for configuring GPON, XG-PON, and XGS-PON services are the same. The difference lies in this step. Here, the GPON service is used as an example. When configuring XG-PON and XGS-PON services, you need to configure the ONT network-side interface type parameter (ont-type) in the **ont add** and **ont confirm** commands. Select a value based on the actual ONT capability or service data plan, for example, 10g/2.5g.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **3230313126595540** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-
  aging omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-
  aging omci ont-lineprofile-name
   ftth ont-srvprofile-name ftth
  ```

- Confirm automatically discovered ONTs.

  If the password or SN of an ONT is unknown, run the **port** *portid* **ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

  ```
  huawei(config)#interface gpon 0/1
  huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
  huawei(config-if-gpon-0/1)#display ont autofind 0
    //After this command is executed, the information about all ONTs connected
  to the GPON port through optical splitters is displayed.
  ```



```
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 3230313126595540
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

NOTE

If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-
name ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of
the ONT is normal.
  Match state          : match     //Indicates that the capability profile bound
to the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactivated**, run the **ont activate** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.

----End

2.4.1.4 Configuring the Internet Access Service

The OLT is connected to the remote ONT through a GPON port to provide users with high-speed Internet access services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.
- The ONT has been added to the OLT. For details, see **2.4.1.3 Adding an ONT to an OLT**.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID for Internet access services: 14
Network topology data	Upstream port: 0/9/0 PON port: 0/1/0 ONT IDs: 1 and 2 ID of the port on the ONT that is connected to the PC: 1
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● CVLAN ID: 1001 ● C'-VLAN ID: 1010-1011 VLAN Translation Policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the profile ID to ftth_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.


```
huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0
priority-policy local-setting
```

b. Configure the mapping between a GEM port and a VLAN.

The service flow of C-VLAN 1001 is mapped to GEM port 14 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

c. Configure the VLAN of the Ethernet port on the ONT.

If the ONT is connected to the PC through Ethernet port 1, add Ethernet port 1 to VLAN 1001 in the ONT service profile.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 1 1001
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

d. Configure the native VLAN of the ONT port.

Set the native VLAN ID of Ethernet port 1 to 1001.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 1 vlan 1001
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 1 vlan 1001
huawei(config-if-gpon-0/1)#quit
```

e. Create an Internet access service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/9 0
```

f. Create service flows.

Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001. Use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound
traffic-table name
ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1011 inbound
traffic-table name
ftth_hsi outbound traffic-table name ftth_hsi
```

g. Save the data.

```
huawei(config)#save
```

- The ONT does not need to be configured.

----End

2.4.1.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see **2.4.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.
Voice parameter	IP address of the MGC server: 10.10.100.10/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.


```
huawei(config)#traffic table ip name ftth_voip cir off priority 5
priority-policy
 local-setting
```

b. Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

c. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/9 0
```

d. Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-
table name ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-
table name ftth_voip
```

e. Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

f. Save the data.

```
huawei(config)#save
```

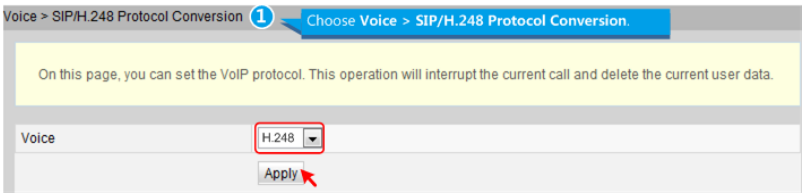
- Configure the ONT on the Web page.

a. Log in to the Web configuration page.

i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

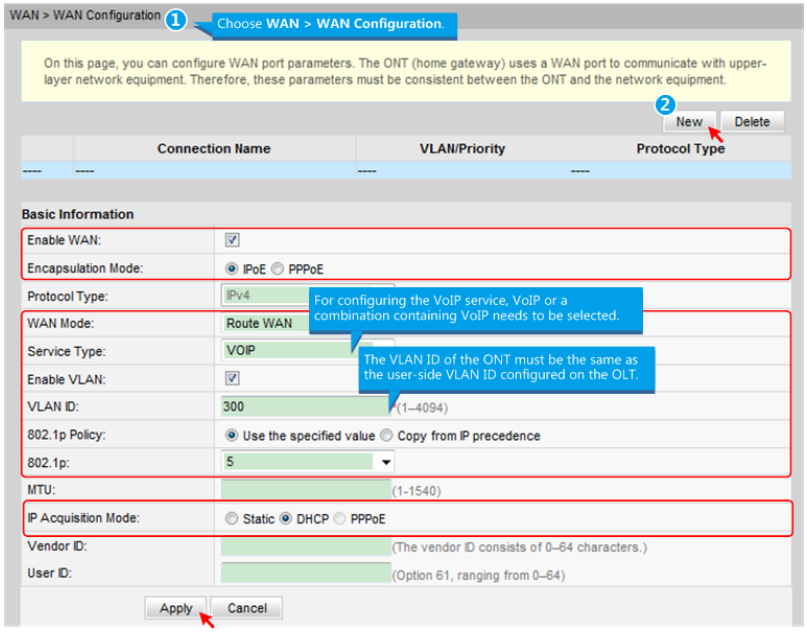
b. Configure the voice protocol.



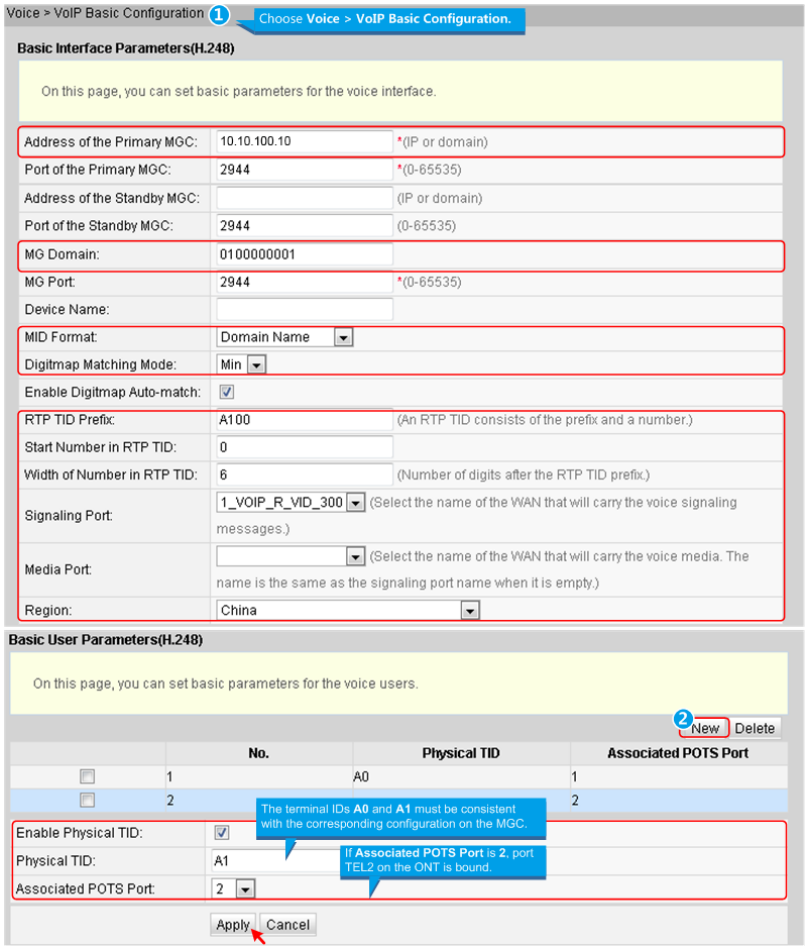
NOTE

The default voice protocol is SIP. Therefore, change the voice protocol first.

c. Configure parameters for the voice WAN interface.



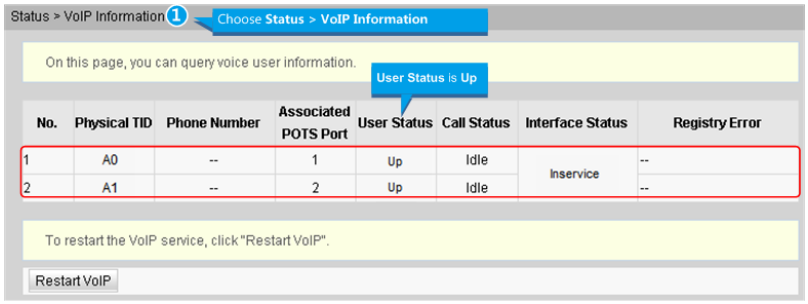
d. Configure parameters for the H.248-based voice interface.



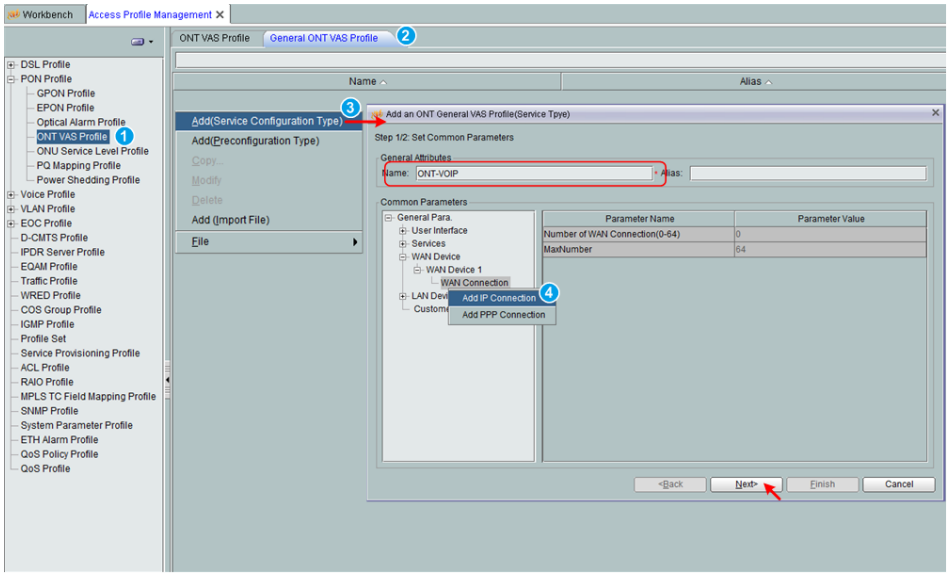
NOTE

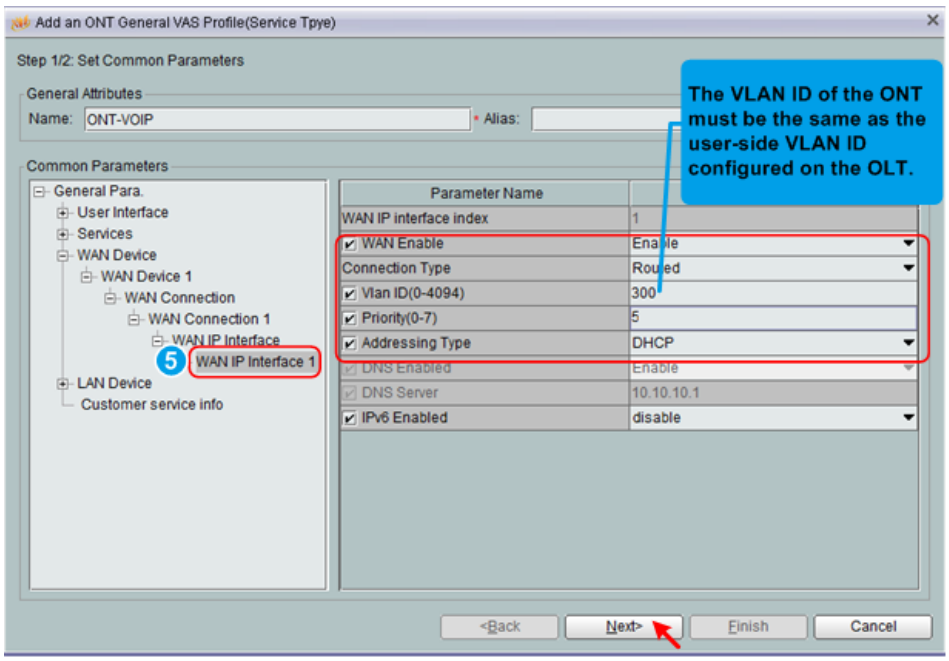
- The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
- If dual-homing is configured, **Address of the Standby MGC** must be configured.
- **MID Format** can be set to **Domain Name**, **IP**, or **Device Name**. If **MID Format** is set to **Domain Name** or **Device Name**, the setting must be consistent with the corresponding configuration on the MGC.
- **MG Domain** is ONT's domain name registered with the MGC. It is globally unique. **MG Domain** in this example is ONT's password.
- If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.
- When the ONT is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.

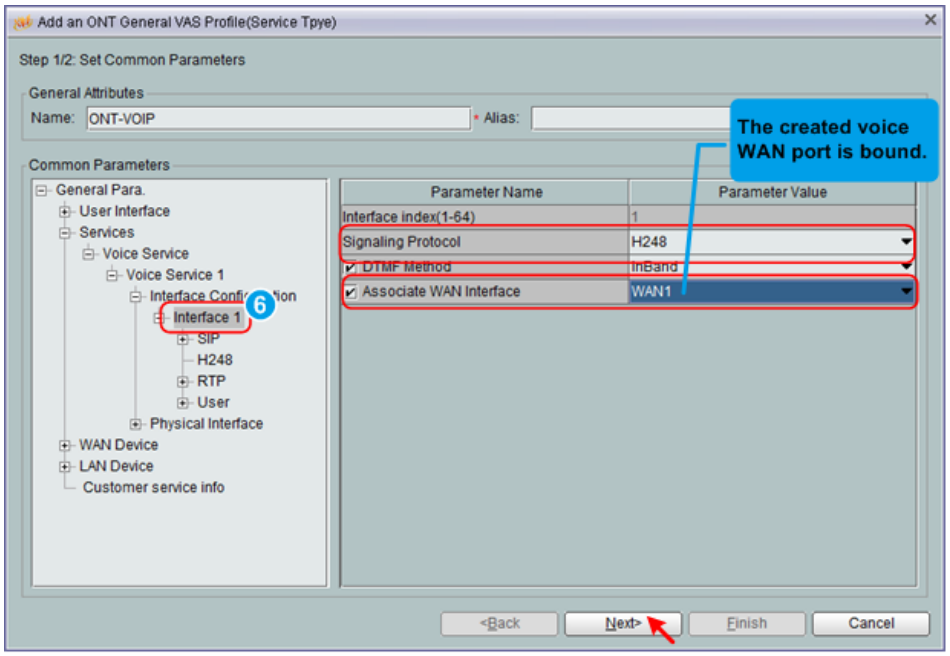
e. Check the registration status of the voice user.

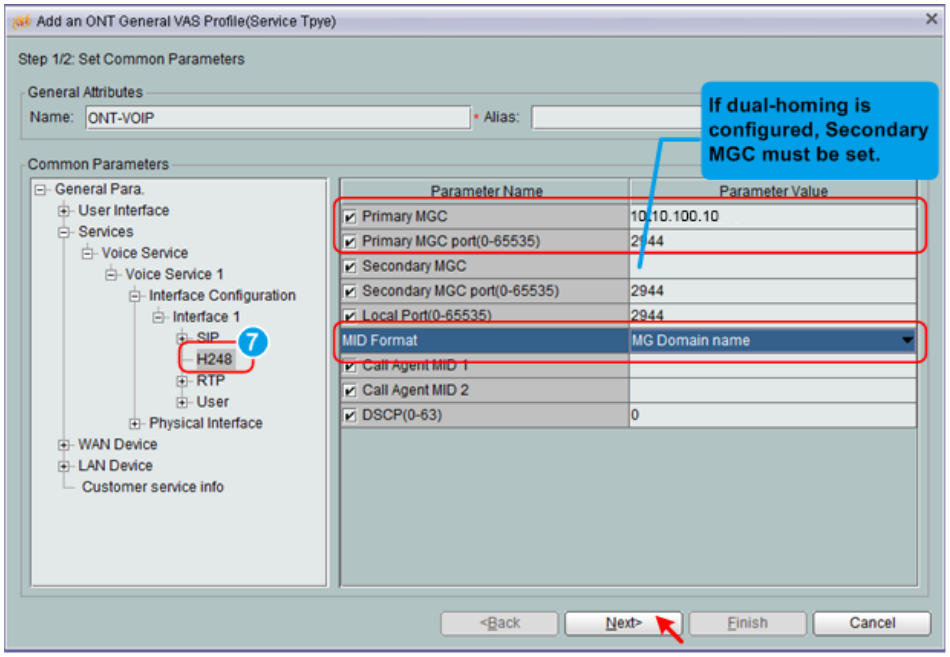


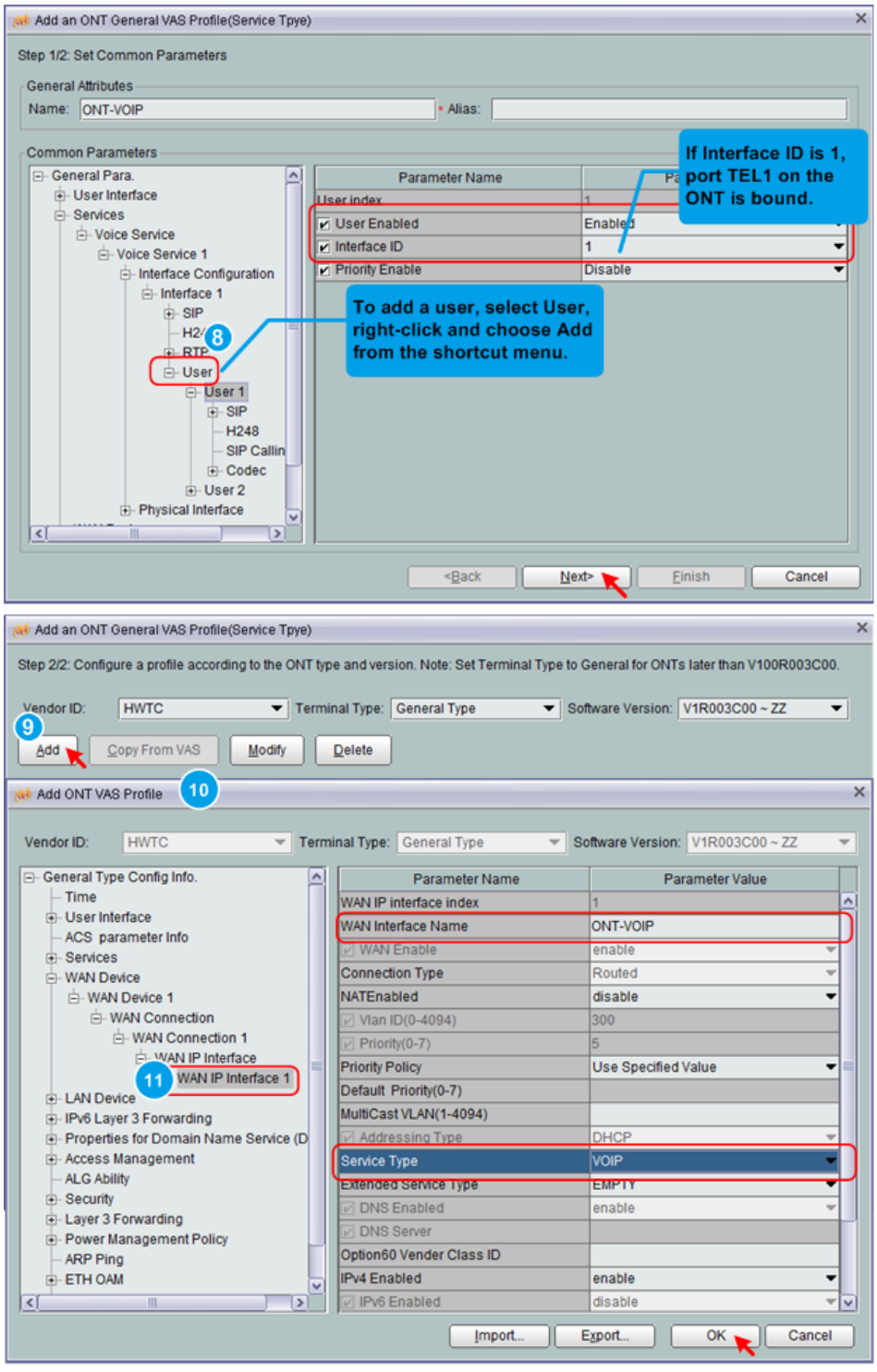
- Configure the ONT on the U2000.
  a. **Configure and bind a general value-added service (VAS) profile for the ONT.**







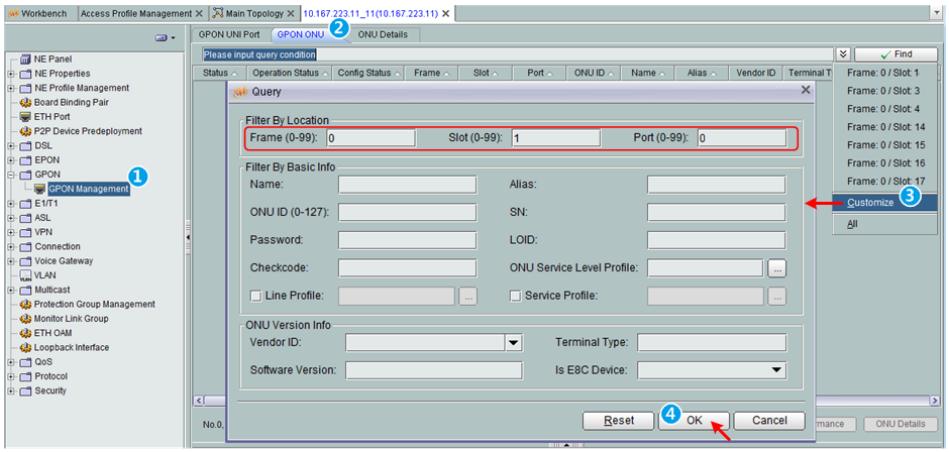


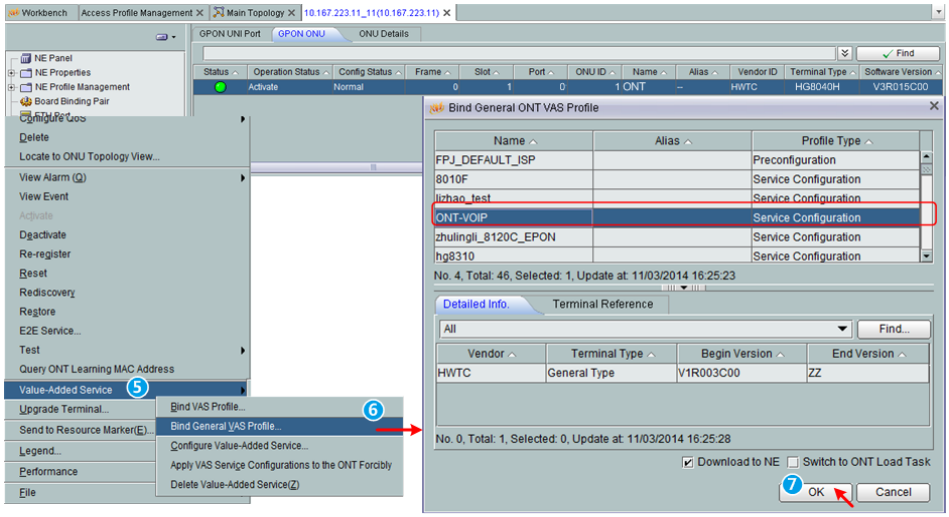


NOTE

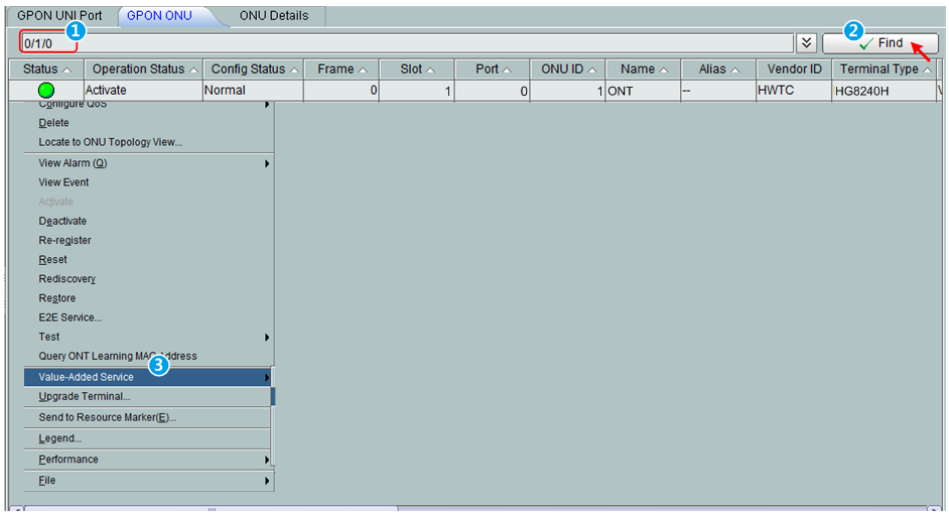
If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default. Create a WAN port named **WAN-RTP** on the ONT, and set this WAN port to a media WAN port. Specifically, choose **Interface 1** > **RTP** and set **Associate WAN Interface** to **WAN2**.

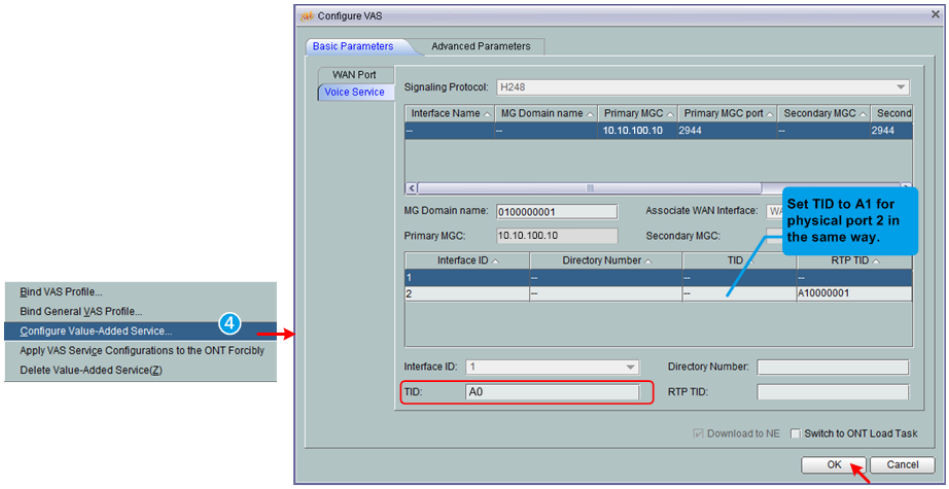
b. **Bind a general VAS profile.**





c. **Configure the ONT VAS service.**





NOTE

Domain Name is ONT's domain name registered with the MGC. It is globally unique. **MG Domain Name** in this example is ONT's password.

Pay attention to the RTP TID configuration when the ONT is interconnected with a softswitch of other vendors. The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.

Do not configure **Directory Number**.

----End

2.4.1.6 Configuring the H.248-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the H.248-based voice service.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see **2.4.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.
Voice parameter	IP address of the MGC server: 10.10.100.10/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/9 0
```

Step 4 Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
```

Step 5 Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

Step 6 Configure ONT voice profiles.

ONT voice service configurations include the VoIP service provisioning mode, ONT voice profiles, voice users, and voice-related parameters.

ONT voice profiles include the common MG interface attribute profile, POTS port profile, MGC profile, and voice signal profile.

- Common MG interface attribute profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, Tx gain, Rx gain, and signaling type of a POTS port.
- MGC profile: saves the IP address or domain name of an MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- Voice signal profile: saves the ONT signal tone and ringing tone.

Currently, the common MG interface attribute profile, POTS port profile, and MGC profile can be applied to an H.248 interface, and the voice signal profile can be bound to an H.248 interface.

For profiles that can be applied to an H.248 interface, if parameters in those profiles are changed, those profiles must be reapplied to the H.248 interface so that the changed parameters can take effect. For profiles that can be bound to an H.248 interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the H.248 interface and the changed parameters can take effect.

1. Configure the VoIP service provisioning mode.

   Run the **ont voip config-method** command to configure the VoIP service provisioning mode. Run the **display ont info** command to query the mode of issuing VoIP services.

   In this example, the mode is **default**, that is, the VoIP service provisioning mode is depended on the actual service provisioning mode on the ONT. Run this command to select a proper mode if the system supports multiple voice service provisioning modes. The service provisioning modes can be OMCI, FTP, and TR069.

2. Configure and apply an MG interface public attribute profile.

   In this example, the default profile 1 is used.

   a. Configure an MG interface public attribute profile.

      Run the **display ont-mg-attribute-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add a profile.

   b. Apply a common MG interface attribute profile.

      Run the **ont-if-h248 bat-apply** command to apply profiles in batches to H.248 interfaces and run the **if-h248 attribute** command to apply a profile to an H.248

interface or configure customized parameters on an H.248 interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

3. Configure and apply a POTS port profile.

   In this example, the default profile 1 is used.

   a. Configure a POTS port profile.

      Run the **display ont-pots-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a profile.

   b. Apply a POTS port profile.

      Run the **ont-pstnport electric bat-apply** command to apply POTS port profiles in batches and run the **pstnport electric** command to apply a POTS port profile to an H.248 interface or configure customized parameters on an H.248 interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

4. Configure the voice WAN port of the ONT.

   For ONT 1 and ONT 2, configure the IP address obtaining mode to DHCP, set the management VLAN to VLAN 300, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 300
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 300
```

5. Configure and apply an MGC profile.

   a. Configure and apply an MGC profile.

      Run the **display ont-mgc-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add a profile.

      Create MGC profile 2, set the IP address of the MGC to 10.10.100.10, and use default values for other parameters.

```
huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 10.10.100.10
```

   b. Add an H.248 interface and apply an MGC profile to the interface.

      For ONT 1 and ONT 2, set the MG ID to 1, apply MGC profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

```
huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
```

1. Add POTS users.

   For ONT 1 and ONT 2, create a POTS user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

```
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

-------------------------------------------------------------------------------
  F/S/P                     : 0/1/0
  ONT ID                    : 1
  Port ID                   : 1
```



```
  MG ID                       : 1
  Terminal ID                 : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

---------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A1
...//The rest of the response information is omitted.
```

1. Configure and bind the voice signal profile.

   In this example, the default profile 1 is used.

   a. Configure the voice signal profile.

      Run the **display ont-voipsignal-profile** command to query the existing profiles in the system. If the existing profile in the system does not meet the requirement, run the **ont-voipsignal-profile** command to add a profile.

   b. Configure the ONT signal tone.

      Run the **display ont-tone** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-tone add** command to add signal tone parameters. The ONT signal tone will not be configured independently in this example.

   c. Configure ONT ringing parameters.

      Run the **display ont-ring** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-ring add** command to add ringing parameters. The ONT ringing parameter will not be configured independently in this example.

   d. Run the **commit** command to save parameters of the voice signal profile to the database.

   e. Bind the voice signal profile.

      Run the **ont-voipsignal bat-bind** command to bind voice signal profiles in batches or run the **voipsignal** command to bind a voice signal profile to an ONT. If you run these two commands to bind profiles in batches or bind a voice signal profile to an ONT repeatedly, the last configurations take effect.

2. (Optional) Configure the H.248 user codec.

   Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

3. (Optional) Configure the global VoIP media attributes of the ONT.

   Run the **ont-voip-media attribute** command to configure the global VoIP media attributes of the ONT. Before configuration, ensure that the configured media attributes are supported by the corresponding ONT. Otherwise, the ONT configuration will fail. The global VoIP media attributes of the ONT will not be configured independently in this example.

Step 7 Save the data.

```
huawei(config)#save
```

----End

2.4.1.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the SIP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see **2.4.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.
Voice parameter	IP address of the SIP server: 10.10.100.10/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.

a. Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

```
huawei(config)#traffic table ip name ftth_voip cir off priority 5
priority-policy
 local-setting
```

b. Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

c. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/9 0
```

d. Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-
table name ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-
service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-
table name ftth_voip
```

e. Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

f. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the Web page.

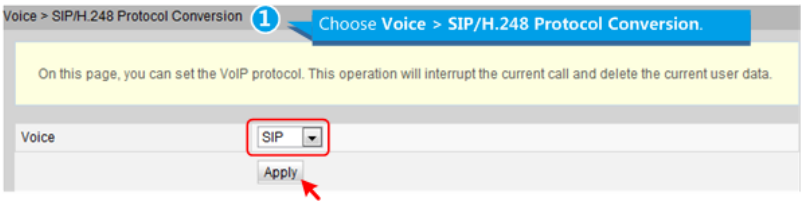
a. Log in to the Web configuration page.

i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login

window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

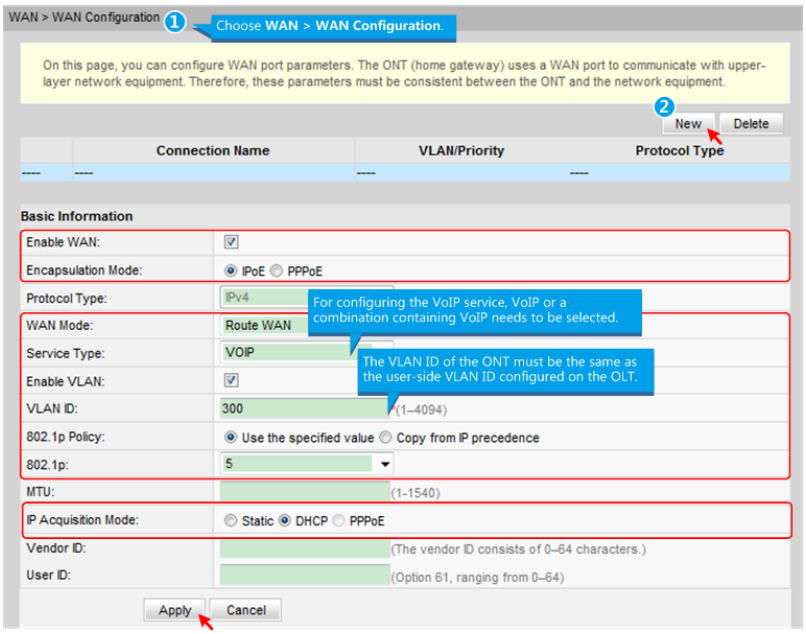
b. **Optional:** Configure the voice protocol.



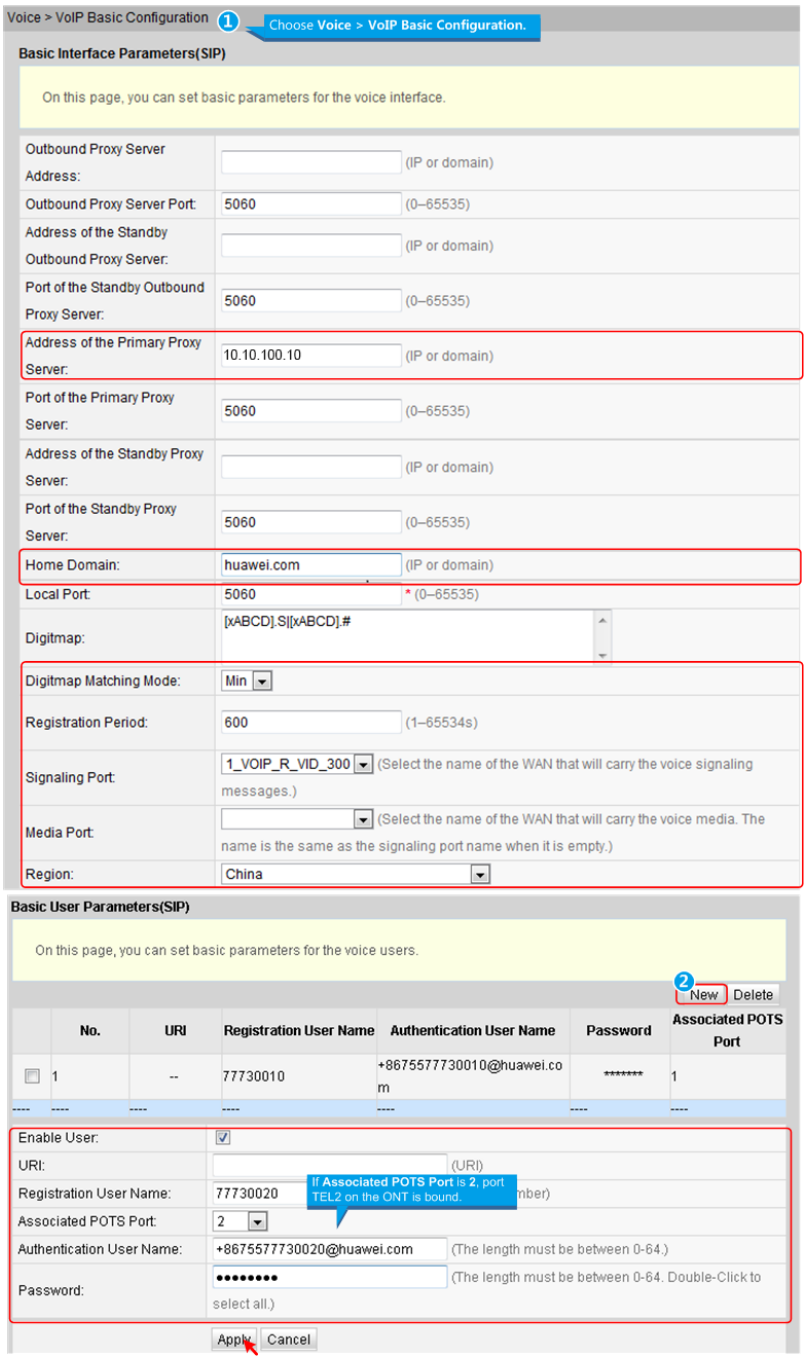
NOTE

The default voice protocol is SIP. If the protocol is not changed, skip this step.

c. Configure parameters for the voice WAN interface.



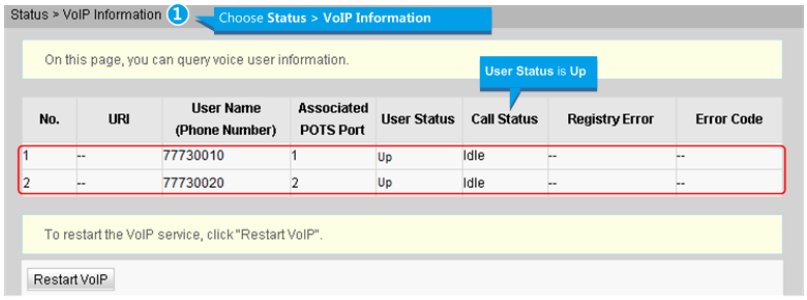
d. Configure parameters for the SIP-based voice interface.



NOTE

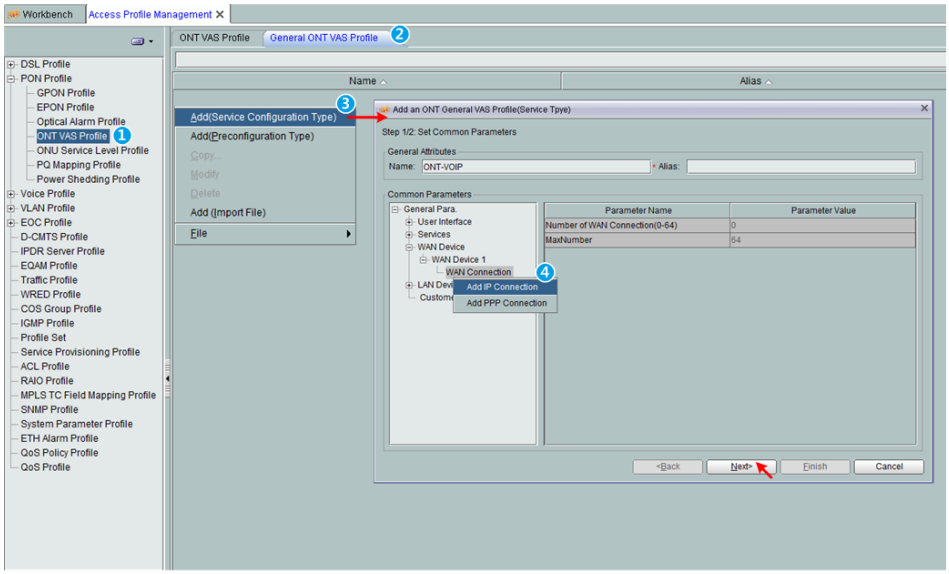
- The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
- If dual-homing is configured, **Address of the Standby Proxy Server** must be configured.
- If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.
- If **Associated POTS Port** is **1**, port TEL1 on the ONT is bound. If **Associated POTS Port** is **2**, port TEL2 on the ONT is bound.

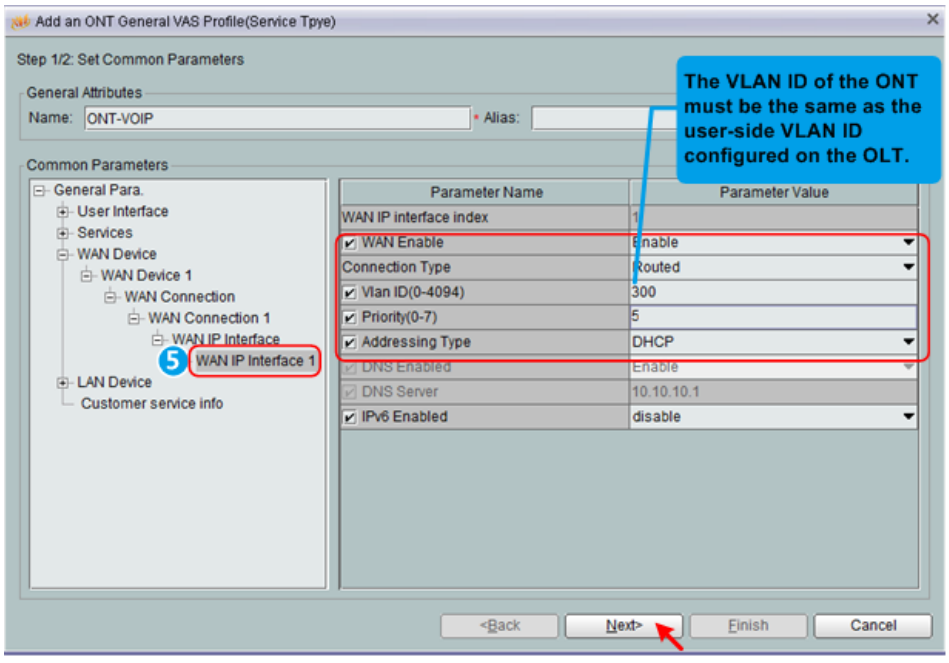
e. Check the registration status of the voice user.

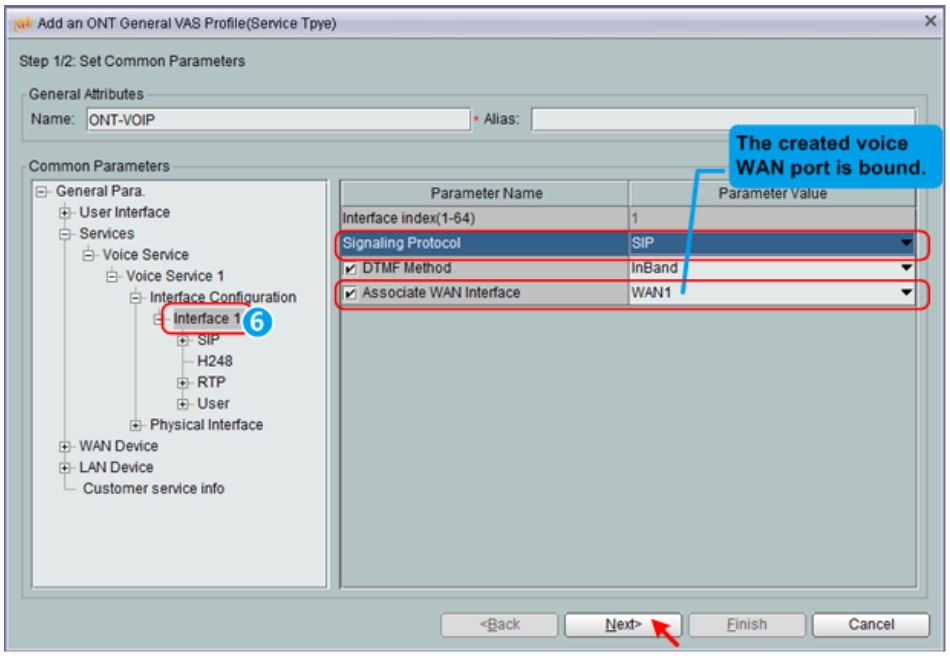


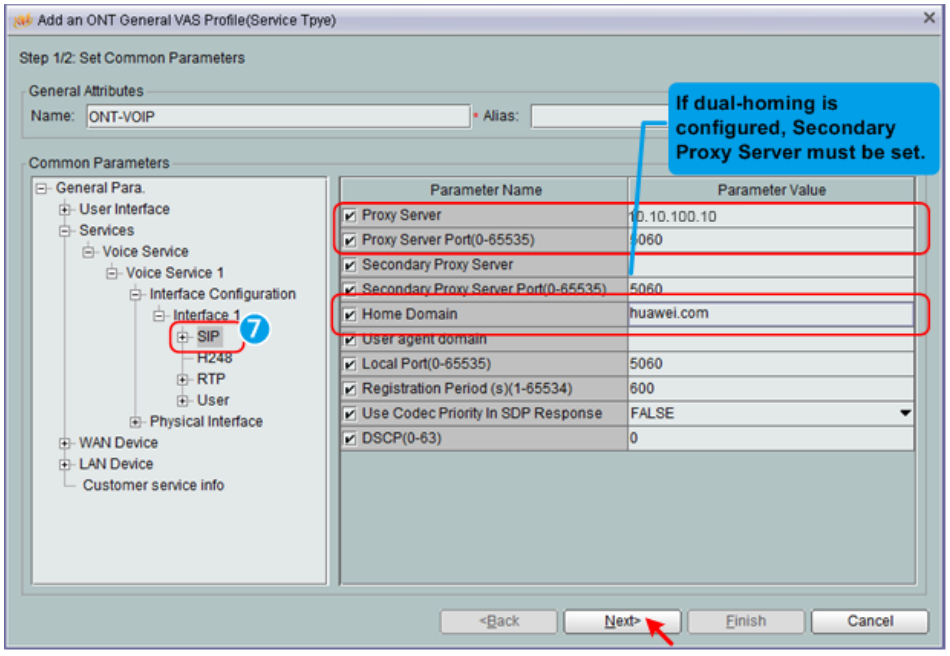
- Configure the ONT on the U2000.

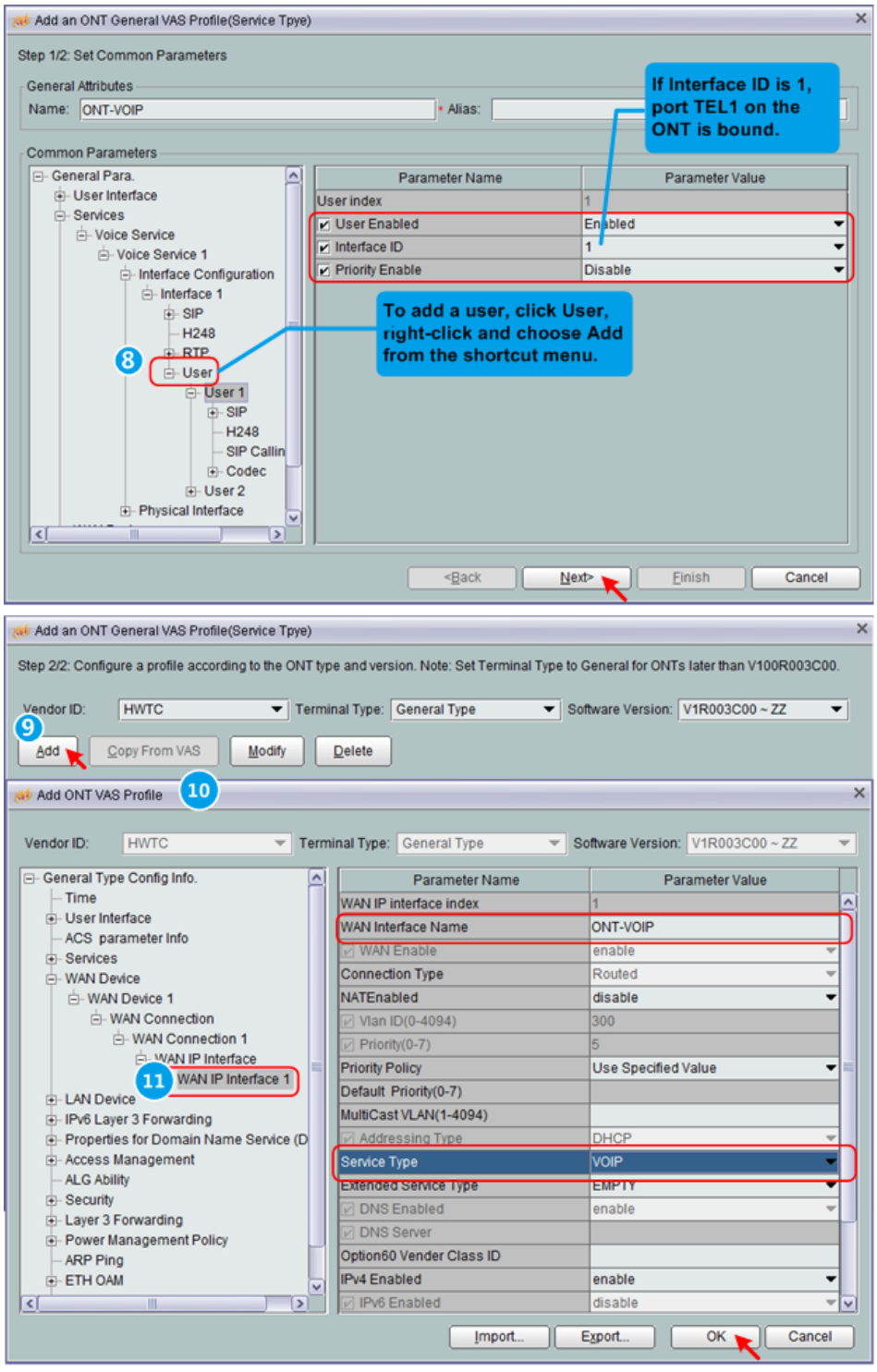
  a. **Configure a general VAS profile for the ONT.**



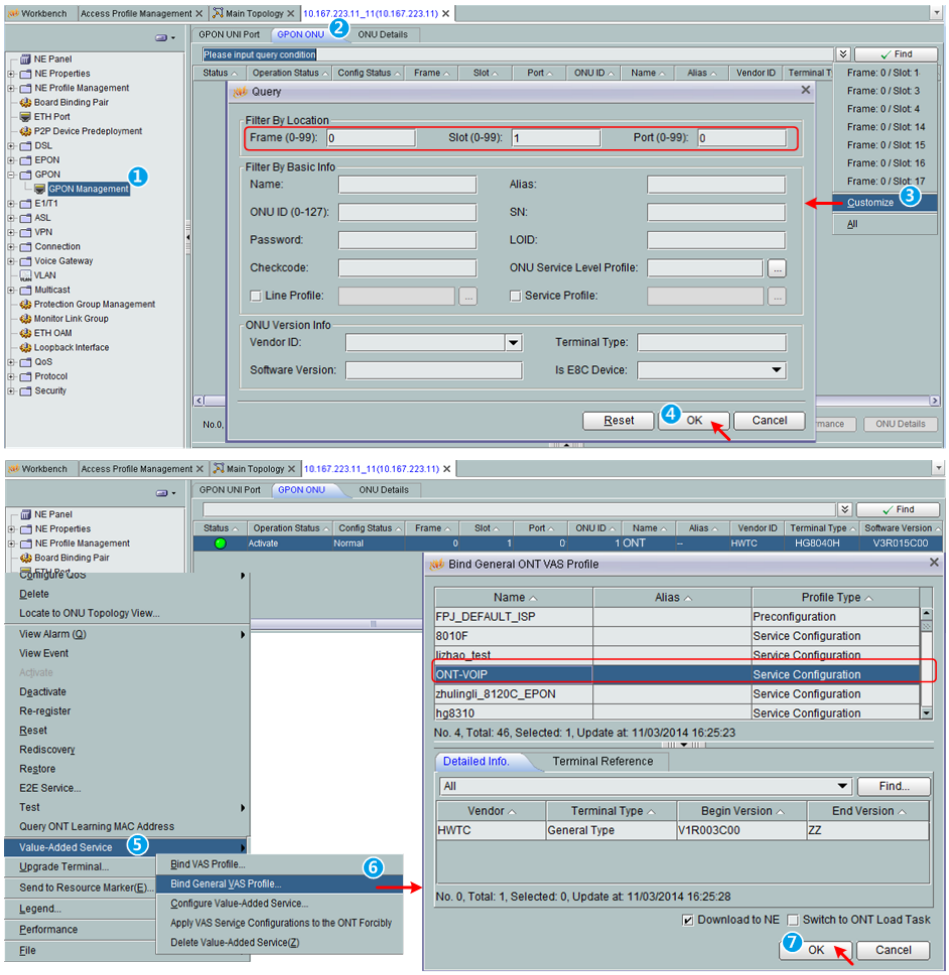




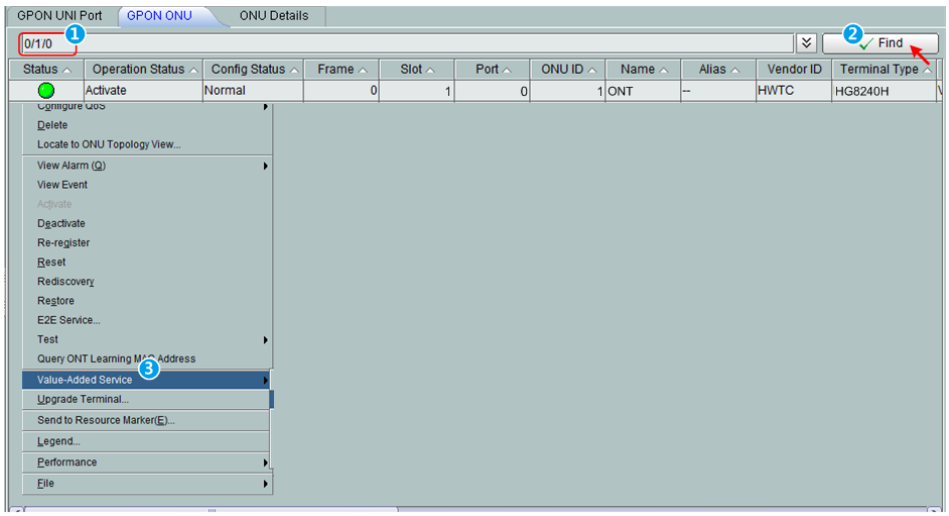


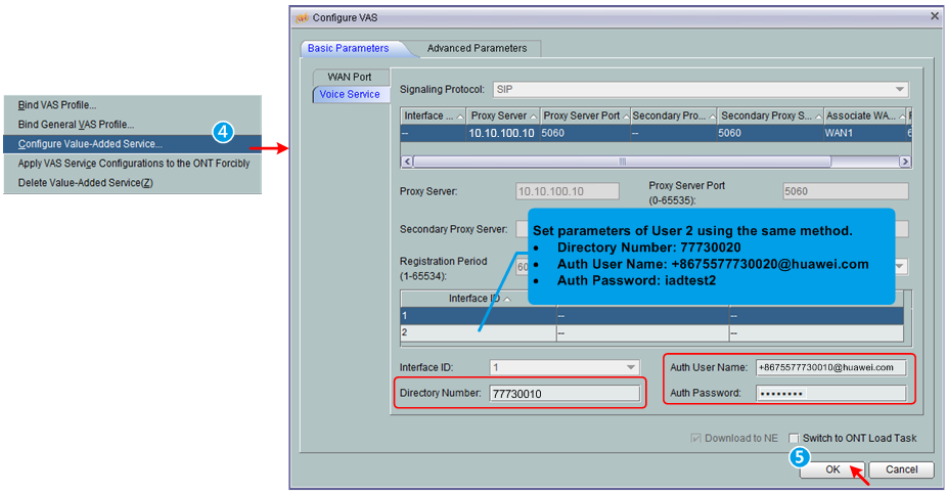


b. **Bind a general VAS profile.**



c. **Configure the ONT VAS service.**





NOTE

The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.

----End

2.4.1.8 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see **2.4.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12

Item	Data
VLAN plan	Single VLAN tag: ● VLAN ID: 300 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: transparently transmits the VLAN.
Voice parameter	IP address of the SIP server: 10.10.100.10/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 300.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/9 0
```

Step 4 Create service flows.

Set the service VLAN to 300, GEM port ID to 12, and user VLAN to 300, and use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 1 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
huawei(config)#service-port vlan 300 gpon 0/1/0 ont 2 gemport 12 multi-service
 user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
```


Step 5 Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#arp proxy enable
huawei(config-if-vlanif300)#quit
```

Step 6 Configure ONT voice profiles.

ONT voice service configurations include the VoIP service provisioning mode, ONT voice profiles, voice users, and voice-related parameters.

ONT voice profiles include the common MG interface attribute profile, POTS port profile, SIP service profile, SIP agent profile, digitmap profile, and voice signal profile.

- Common MG interface attribute profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, Tx gain, Rx gain, and signaling type of a POTS port.
- SIP service data profile: saves the data information about the ONT voice service, including the rights of call waiting (CW), three-way calling (3WC), call transfer (CT), and call hold (CH).
- SIP agent profile: saves the SIP agent information about an ONT, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- Digitmap profile: saves the digitmap information about an ONT, including the timeout time of the digitmap timer and the digitmap format.
- Voice signal profile: saves the ONT signal tone and ringing tone.

Currently, the common MG interface attribute profile, POTS port profile, SIP service profile, and SIP agent profile can be applied to an SIP interface, and the digitmap profile and voice signal profile can be bound to an SIP interface.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

1. Configure the VoIP service provisioning mode.

   Run the **ont voip config-method** command to configure the VoIP service provisioning mode. Run the **display ont info** command to query the mode of issuing VoIP services.

   In this example, the mode is **default**, that is, the VoIP service provisioning mode is depended on the actual service provisioning mode on the ONT. Run this command to select a proper mode if the system supports multiple voice service provisioning modes. The service provisioning modes can be OMCI, FTP, and TR069.

2. Configure and apply an MG interface public attribute profile.

   In this example, the default profile 1 is used.

a. Configure an MG interface public attribute profile.

Run the **display ont-mg-attribute-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add a profile.

b. Apply a common MG interface attribute profile.

Run the **ont-if-sip bat-apply** command to apply profiles in batches to SIP interfaces and run the **if-sip attribute** command to apply a profile to an SIP interface or configure customized parameters on an SIP interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

3. Configure and apply a POTS port profile.

In this example, the default profile 1 is used.

a. Configure a POTS port profile.

Run the **display ont-pots-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a profile.

b. Apply a POTS port profile.

Run the **ont-pstnport electric bat-apply** command to apply POTS port profiles in batches and run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure customized parameters on an SIP interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

4. Configure the voice WAN port of the ONT.

For ONT 1 and ONT 2, configure the IP address obtaining mode to DHCP, set the management VLAN to VLAN 300, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 300
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 300
```

5. Configure and apply an SIP agent profile.

a. Configure an SIP agent profile.

Run the **display ont-sipagent-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add a profile.

Create SIP agent profile 2, set the IP address of the SIP server to 10.10.100.10, and use default values for other parameters.

```
huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
10.10.100.10
```

b. Add an SIP interface and apply an SIP agent profile to the interface.

For ONT 1 and ONT 2, set the MG ID to 1, apply SIP agent profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

```
huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
huawei(config-if-gpon-0/1)#if-sip add 0 2 1 sipagent-profile profile-id 2
```

6. Add POTS users.

For ONT 1 and ONT 2, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1 and huawei2, set passwords to user1 and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.


```
huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1
telno 77730010
huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2
telno 77730020
```

Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

-------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730010
  User name                   : huawei1
  Password                    : user1
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 2 1

-------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730020
  User name                   : huawei2
  Password                    : user2
...//The rest of the response information is omitted.
```

1. Configure and apply an SIP service profile.

   In this example, the default profile 1 is used.

   a. Configure an SIP service profile.

      Run the **display ont-siprightflag-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add a profile.

   b. Apply an SIP service profile.

      Run the **ont-sippstnuser bat-apply from** command to apply profiles in batches to SIP interfaces and run the **sippstnuser rightflag** command to apply a profile to a SIP interface or configure customized parameters on a SIP interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

2. Configure and bind a digitmap profile.

   In this example, the default profile 1 is used.

   a. Configure a digitmap profile.

      Run the **display ont-digitmap-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a profile.

   b. Bind a digitmap profile.

      Run the **ont-sippstnuser bat-bind from** command to apply profiles in batches to SIP interfaces, or run the **sippstnuser digitmap** command to bind a profile to an SIP interface. If you use these two commands to bind the profile to SIP ports repeatedly, the last configurations take effect.

3. Configure and bind the voice signal profile.

   In this example, the default profile 1 is used.

   a. Configure the voice signal profile.

      Run the **display ont-voipsignal-profile** command to query the existing profiles in the system. If the existing profile in the system does not meet the requirement, run the **ont-voipsignal-profile** command to add a profile.

   b. Configure the ONT signal tone.

      Run the **display ont-tone** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-tone add** command to add signal tone parameters. The ONT signal tone will not be configured independently in this example.

   c. Configure ONT ringing parameters.

      Run the **display ont-ring** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-ring add** command to add ringing parameters. The ONT ringing parameter will not be configured independently in this example.

   d. Run the **commit** command to save parameters of the voice signal profile to the database.

   e. Bind the voice signal profile.

      Run the **ont-voipsignal bat-bind** command to bind voice signal profiles in batches or run the **voipsignal** command to bind a voice signal profile to an ONT. If you run these two commands to bind profiles in batches or bind a voice signal profile to an ONT repeatedly, the last configurations take effect.

4. (Optional) Configure the SIP user codec.

   Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

5. (Optional) Configure the global VoIP media attributes of the ONT.

   Run the **ont-voip-media attribute** command to configure the global VoIP media attributes of the ONT. Before configuration, ensure that the configured media attributes are supported by the corresponding ONT. Otherwise, the ONT configuration will fail. The global VoIP media attributes of the ONT will not be configured independently in this example.

Step 7 Save the data.

```
huawei(config)#save
```

----End

2.4.1.9 Configuring the BTV Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the multicast service.

Prerequisites

- The OLT is connected to the BRAS and the multicast source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.

- The ONT has been added to the OLT. For details, see **2.4.1.3 Adding an ONT to an OLT**.

Data Plan

Table 2-10 Data plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONT: duplicates packets based on user ports and multicast VLANs (MVLANs) are stripped off downstream. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Set the profile name to ftth_iptv. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     NOTE

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     ```
     huawei(config)#traffic table ip name ftth_iptv cir off priority 4
     priority-policy local-setting
     ```


b. Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 1000 is mapped to GEM port 13 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1000
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

c. Configure the VLAN of the Ethernet port on the ONT and the multicast forwarding mode.

If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000. Configure the multicast forwarding mode is untagged.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#multicast-forward untag
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

d. Configure the native VLAN of the ONT port.

If the ONT is connected to the STB through Ethernet port 2, the native VLAN ID is 1000.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#quit
```

e. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/9 0
```

f. Create service flows.

Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile ftth_iptv.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13
multi-service
user-vlan 1000 inbound traffic-table name ftth_iptv outbound traffic-
table name ftth_iptv
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13
multi-service
user-vlan 1000 inbound traffic-table name ftth_iptv outbound traffic-
table name ftth_iptv
```

g. Create an MVLAN and configure the IGMP version.

Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses
in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

h. Configure a program library.

Set the mode for obtaining multicast programs to dynamic.

NOTE

You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

i. Set the IGMP mode.

Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

j. (Optional) Configure the IGMP upstream port.

In this example, the IGMP upstream port uses default value default.

Run the **display igmp config global** command to query the IGMP upstream port mode. If this mode does not meet the requirement, run the **igmp uplink-port-mode** command to configure it.

k. Configure multicast users.

Add service ports 1 and 2 as multicast users.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

l. Save the data.

```
huawei(config)#save
```

- The ONT does not need to be configured.

----End

2.4.1.10 Configuring the VoD Service

The OLT is connected to the remote bridging ONT through a GPON port to provide users with the VoD service.

Prerequisites

- The OLT is connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.

- The ONT has been added to the OLT. For details, see **2.4.1.3 Adding an ONT to an OLT**.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common ● CVLAN=SVLAN VLAN translation policy: ● ONT: adds CVLAN tags to iTV service packets. ● OLT: transparently transmits packets with SVLANs.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Set the profile name to ftth_iptv. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip name ftth_iptv cir off priority 4 priority-policy local-setting
   ```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 1000 is mapped to GEM port 13 in the ONT line profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1000
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000.


```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Configure the native VLAN of the ONT port.

   If the ONT is connected to the STB through Ethernet port 2, the native VLAN ID is 1000.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont port native-vlan 0 1 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#ont port native-vlan 0 2 eth 2 vlan 1000
huawei(config-if-gpon-0/1)#quit
```

5. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/9/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/9 0
```

6. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and VLAN translation mode to transparent transmission, and use traffic profile ftth_iptv.

```
huawei(config)#service-port vlan 1000 gpon 0/1/0 ont 1 gemport 13 inbound
traffic-table name ftth_iptv
outbound traffic-table name ftth_iptv tag-transform transparent
huawei(config)#service-port vlan 1000 gpon 0/1/0 ont 2 gemport 13 inbound
traffic-table name ftth_iptv
outbound traffic-table name ftth_iptv tag-transform transparent
```

7. Save the data.

```
huawei(config)#save
```

Step 2 The ONT does not need to be configured.

----End

2.4.1.11 Configuring Link Aggregation, Congestion Control, and Security Policies

The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG).

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **2.2.6 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

- Uplink ports 0/9/0 and 0/9/1 are added to a LAG.
- The two ports send packets upstream based on the packets' source MAC addresses.
- The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

```
huawei(config)#link-aggregation 0/9 0-1 ingress workmode lacp-static
```

- Configure queue scheduling.

  According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **2.2.2 Principle of QoS Planning**.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.
    i. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    ii. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    iii. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on the OLT.

    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on the OLT.

    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    i. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    ii. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
      1) In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
      2) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
      3) Perform the following operations to enable MAC address anti-spoofing in VLAN service profile mode:
        1) Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
        2) Run the **commit** command to make the profile configuration take effect.
        3) Run the **quit** command to quit the VLAN service profile mode.
        4) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    iii. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.

iv. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.

- Enable IP address anti-spoofing on the OLT.

  IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

  i. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.

  ii. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

  iii. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.

    i. Enable DHCP Option 82 on the OLT.

    DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

    - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

      When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
    - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
    - The VLAN level:

      1) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

      2) Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.

      3) Run the **commit** command to make the profile configuration take effect.

      4) Run the **quit** command to quit the VLAN service profile mode.

      5) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

    ii. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT DHCP packets to carry Option 82 information.

- Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.
  i. Enable PITP on the OLT.

     PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, PITP is disabled only at the global level by default.

     - The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

       In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
     - The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
     - The VLAN level:
       1) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
       2) Run the **pitp enable** command to enable PITP at the VLAN level.
       3) Run the **commit** command to make the profile configuration take effect.
       4) Run the **quit** command to quit the VLAN service profile mode.
       5) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
     - The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

  ii. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT PPPoE packets to carry a vendor tag.

----End

2.4.1.12 Verifying Services

In the FTTH scenario, ONTs are installed in users' houses which are far away from the central equipment room. ONTs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONTs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONT simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONT supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONT simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONT can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel is. ● An ONT supports a maximum of a call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONT. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test1234	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONT POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.

Item	Data	Remarks
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  a. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test1234
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 192.168.100.101
  Gateway IP           : 192.168.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  a. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
     - If a native VLAN is configured for the Ethernet port on the ONT, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.
  b. Check the upstream and downstream ports by checking the MAC address learning status.

i. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
   - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
   - If the downstream port does not learn a MAC address, check whether the ONT is activated, whether the PC is connected to the right port on the ONT, and whether the PC is working properly.

ii. Run the **display ont-learned-mac** command to check whether the ONT connecting to the PON port learned any MAC addresses.

   If not, check whether the ONT properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.

  a. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
77730020
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 77730020
```

  b. The ONT outputs the call emulation result after the test is complete.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 77730020
  Reported number      : 77730020
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.

  a. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

  b. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
     - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
     - If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
     - If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONT and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.

c. Check the registration status of the voice service.

- You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
- If the ONT uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONT. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
- You can query the registration status of the voice service on the ONT web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- Verify the multicast service using multicast emulation.

a. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan
1000
```

NOTE

If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

b. Run the **display igmp user** command to query the status of the multicast user.

```
huawei(config-btv)#display igmp user service-port 1
  User                        : 0/1/0/1
  State                       : online
  Authentication              : no-auth
  Quick leave                 : MAC-based
  IGMP flow ID                : 1
  Video flow ID               : 1
  Log switch                  : enable
  Bind profiles               : -
  IGMP version                : IGMP v3
  Current version             : IGMP v3
  Current IGMP IPv6 version   : IGMP IPv6 v2
  Available programs          : 8
  Global leave                : disable
  User max bandwidth          : no-limit
  Used bandwidth(kbps)        : 0
  Used bandwidth
  to max bandwidth(%)         : -
  Total video bandwidth       : -
  Mcast video bandwidth       : -
  Active program list

------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start time

------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                         16:33:41+08:00

------------------------------------------------------------------------
--
  Total: 1
```


c. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

2.5 Configuration by U2560

This topic describes how to configure the Internet access service, VoIP service and Wi-Fi service by using U2560.

2.5.1 Prerequisites

Before configuring services on the U2560, plan data of the entire network in a unified manner and add the ONT to the U2560.

Before adding the ONT to the U2560, complete pre-configuration on the NMS or using commands to set up Layer 2 service channels. For details, see **Table 2-11**.

Table 2-11 Pre-configuration

Configuration Method	Procedure
On the NMS	GPON ONT: **2.3.1.1 Configuring the GPON FTTH Layer 2 Internet Access Service on the NMS**
Using commands	See the following to configure ONTs on the OLT: GPON ONT:**2.4.1.3 Adding an ONT to an OLT**, **2.4.1.4 Configuring the Internet Access Service**, **2.4.1.5 Configuring the H.248-based Voice Service (on a Web Page or the U2000)** and **2.4.1.7 Configuring the SIP-based Voice Service (on a Web Page or the U2000)**

2.5.2 Commissioning Interoperation Between the U2560 and the ONT

To configure and issue ONT services using the U2560, you need to add the ONT on the U2560 so that the U2560 can manage the ONT.

Data Plan

Table 2-12 provides the data plan for commissioning interoperation between the U2560 and the ONT through the web page.

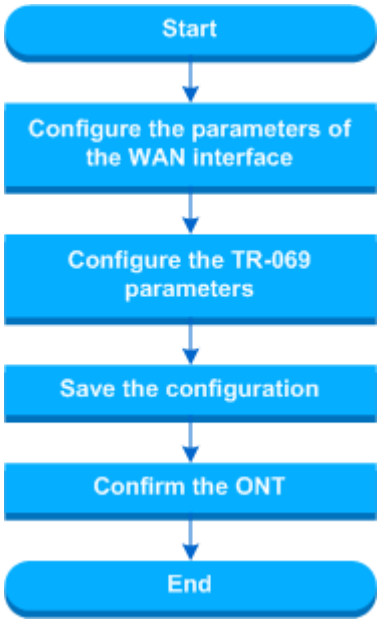
Table 2-12 Data plan for commissioning interoperation between the U2560 and the ONT through the web page

Parameter	Data	Description
Service type of the WAN interface	TR069	When configuring the U2560 management channel, you need to select only TR069 or a combination with TR069. In this example, TR069 is selected.
Connection mode	Route	-
VLAN ID of the WAN interface	50	The VLAN ID of the WAN interface must be the same as the C-VLAN ID configured on the OLT.
Mode of obtaining an IP address	DHCP	There are three modes to obtain an IP address: ● DHCP: Obtain an IP address dynamically. ● Static: Configure an IP address manually. ● PPPoE: Access in the PPPoE dialup mode. In this example, the DHCP mode is configured. You can also select the static or PPPoE mode according to the data plan of the upper-layer network.
ACS URL	http://10.11.11.1:9070	It can be the IP address, port ID, domain name of the ACS server.
Periodical notification interval	43200	It is the default value of the system.
ACS user name	hgw	It is the default value of the system.
ACS password	hgw	It is the default value of the system.
User name of a requested connection	server	It must be the same as that planned on the U2560.
Password of a requested connection	server	It must be the same as that planned on the U2560.

Process

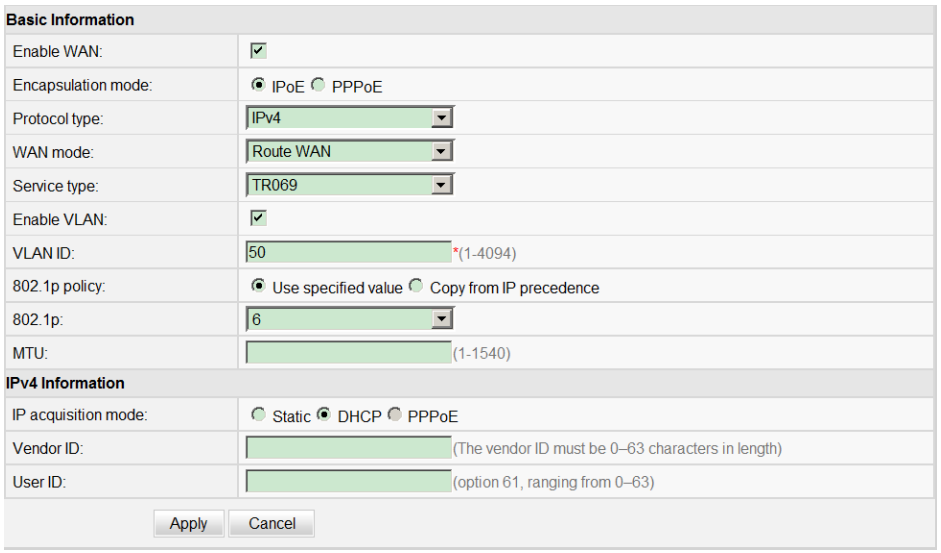
Figure 2-8 shows the flowchart for commissioning interoperation between the U2560 and the ONT through the web page.

Figure 2-8 Process for commissioning interoperation between the U2560 and the ONT through the web page



Procedure

1. Configure the parameters of the WAN interface.
   a. In the navigation tree on the left, choose **WAN** > **WAN Configuration**.
   b. In the pane on the right, click **New**. In the dialog box that is displayed, configure the parameters of the WAN interface as follows:
      - Enable WAN: enabled
      - Encapsulation mode: IPoE
      - WAN mode: Route WAN
      - Service type: TR069
      - VLAN ID: 50
      - 802.1p: 6
      - IP acquisition mode: DHCP



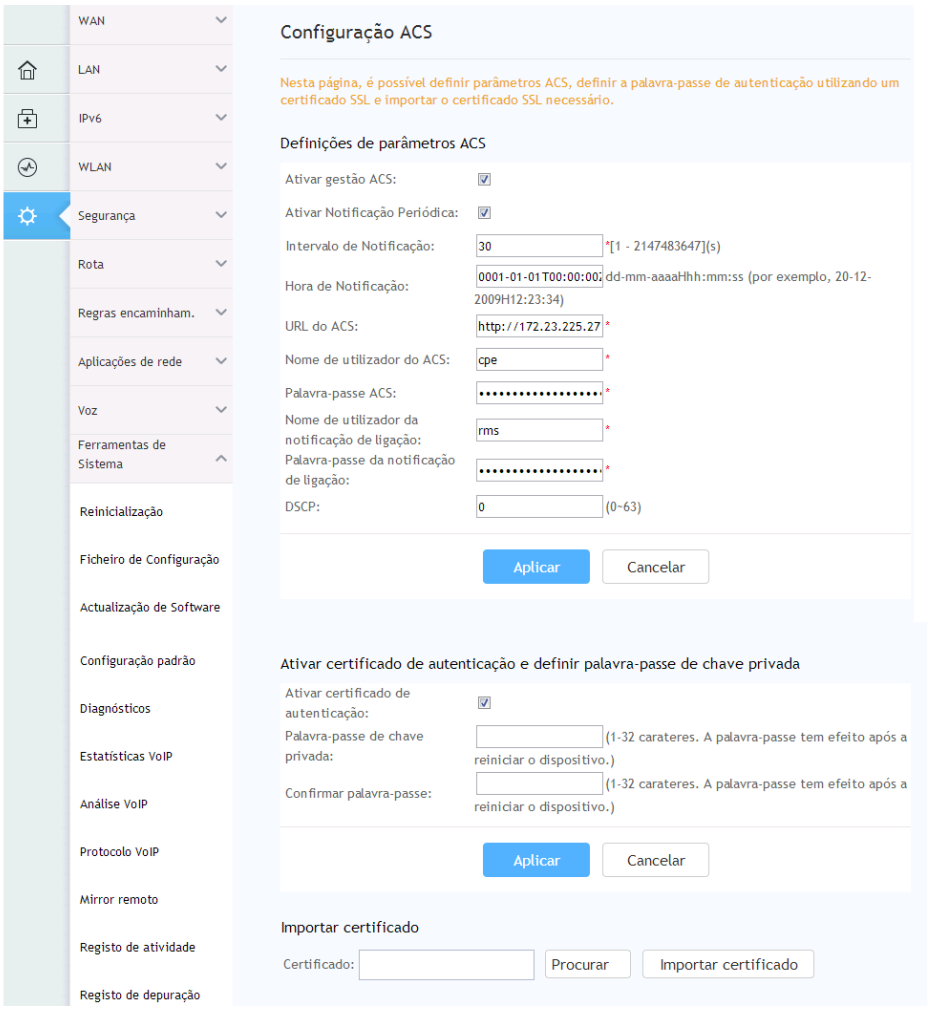
c. Click **Apply**.

2. Configure the TR-069 parameters.

   a. In the navigation tree on the left, choose **System Tools** > **TR-069**.

   b. In the pane on the right, set the TR-069 client parameters (other parameters use the default values) as follows:

      - ACS URL: http://10.11.11.1:9070
      - Connection Request User Name: server
      - Connection Request Password: server



c. Click **Apply**.

3. Confirm the ONT.

Log in to the U2560 and then choose **Subnet view** > **TR-069 Subnet** from **WLAN and Home Network View** in the navigation tree on the left. In the pane on the right, right-click and choose **Refresh** from the shortcut menu. The reported ONT list is displayed. Then, select the ONT list, right-click, and choose **Confirm** from the shortcut menu.

Result

On the U2560, you can configure ONT services. For details, see the configuration examples.

2.5.3 Data Plan

This topic plans the data in a unified manner for various example networks of connecting ONTs in an FTTH network. Subsequent examples are configured based on the following data plan.

Table 2-13 shows the unified data plan for the HSI service, VoIP service and Wi-Fi service in an FTTH network.

Table 2-13 Data plan for connecting ONTs in the FTTH network

Configuration Item	Data Item	Detailed Data	Remarks
WAN port data	HSI service (Layer 3 routing)	● Service type: Internet ● Connection mode: routing ● VLAN ID: 10 ● IP address obtainment mode: PPPoE (user name: iadtest@pppoe, password: iadtest) ● 802.1p: 1 ● NAT function: enable ● Bound port: LAN1 (LAN1 is a Layer 3 LAN)	● For configuring HSI service or Wi-Fi service, Internet or a combination containing Internet must be selected as the service type. For configuring VoIP service, VoIP or a combination containing VoIP must be selected as the service type. ● The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT. ● PPPoE must use the same user name and password as the upper-layer BRAS. ● The HSI service involves the Layer 2, Layer 3 bridge and Layer 3 routing modes. In the Layer 2 mode, all configurations are required only on the OLT. The application mode of the Layer 3 bridge mode is similar to the Layer 2 mode. It is recommended that you use the Layer 2 mode. ● The Wi-Fi service does not support the Layer 2 mode.
	VoIP service	● Service type: VoIP ● Connection mode: routing ● VLAN ID: 20 ● IP address obtaining mode: DHCP ● 802.1p: 6	
	Wi-Fi service (Layer 3 bridge)	● Service type: Internet (not configurable) ● Connection mode: bridge ● VLAN ID: 40 ● 802.1p: 1 ● Bound port: SSID1	
	Wi-Fi service (Layer 3 routing)	● Service type: Internet ● Connection mode: routing ● VLAN ID: 40 ● IP address Obtainment mode: PPPoE (user name: iadtest@pppoe, password: iadtest) ● 802.1p: 1 ● NAT function: enable ● Bound port: SSID1	

Configuration Item	Data Item	Detailed Data	Remarks
VoIP service data	SIP parameters	● IP address of the primary server: 10.10.100.10 ● Port ID of the primary server: 5060 ● Home domain name: softx3000.huawei.com ● Digitmap: x.S|x.# (Default) ● User 1: – Phone number: 88001234 – Authentication user name: 88001234@softx3000.huawei.com – Password: iadtest1 ● User 2: – Phone number: 88001235 – Authentication user name: 88001235@softx3000.huawei.com – Password: iadtest2	-
	H.248 parameters	● Primary MGC address: 10.10.100.10 ● Primary MGC port: 2944 ● MID format: domain name ● MG domain name: 6877687714852901 ● TID: A0 and A1	-
Wi-Fi service	SSID1	ChinaNet-huawei	-
	Security mode	WPA Pre-Shared Key	
	WPA encryption mode	● TKIP&AES ● Key: chinahuawei	

2.5.4 Configuring SIP-based Voice Service Through the U2560

This topic provides an example of how to configure the SIP-based voice service through the U2560.

Prerequisites

- The ONT is auto discovered on the U2560. For details, see **2.5.2 Commissioning Interoperation Between the U2560 and the ONT**.
- Two telephone sets must be available and each must be connected to ports TEL1 and TEL2 respectively on the ONT.

Context

Every data change must be saved. You can click **Save** in a window to save data changes. If you navigate to another node without saving data changes, a dialog box will be displayed prompting you to save the data changes. In this case, click **YES** in the dialog box. New data will be automatically applied to the ONTs after the data changes are saved.

NOTICE

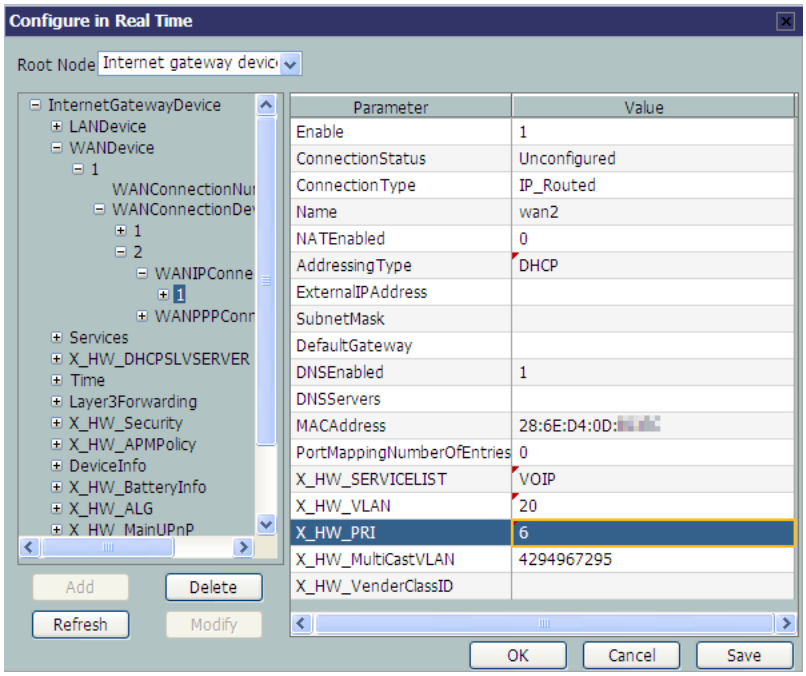
When configuring services on the U2560, do not modify the WAN interface connecting the U2560 and the ONT. Otherwise, the U2560 loses communication with the ONT.

Procedure

1. Log in to the U2560 and choose **Subnet View** > **TR069 Subnet** from the navigation tree. In the terminal list, right-click an ONT and choose **Tools** > **Configure in Real Time** from the shortcut menu.
2. In the **Configure in Real Time** dialog box, set **Root Node** to **Internet gateway device**.
3. Configure the parameters of the voice WAN interface.
   a. Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** from the navigation tree. Click **Add** in the lower left part to create an instance.
   b. Choose **2** > **WANIPConnection** from the navigation tree. Click **Add** in the lower left part. Choose **1** from the navigation tree. In the right pane, set the parameters as follows:
      - Set **Enable** to **1**, indicating that the WAN connection is enabled.
      - Set **Connection Type** to **IP_Routed**, indicating that the connection type of the WAN interface is in routing mode.
      - Set **Addressing Type** to **DHCP**, indicating that the WAN interface obtains IP addresses in DHCP mode.
      - Set **X_HW_SERVICELIST** to **VOIP**, indicating that the WAN interface provides the VoIP access service.
      - Set **X_HW_VLAN** to **20**, indicating the VLAN ID of the WAN interface is 20.
      - Set **X_HW_PRI** to **6**, indicating that the priority level of the WAN interface is 6.

   NOTE

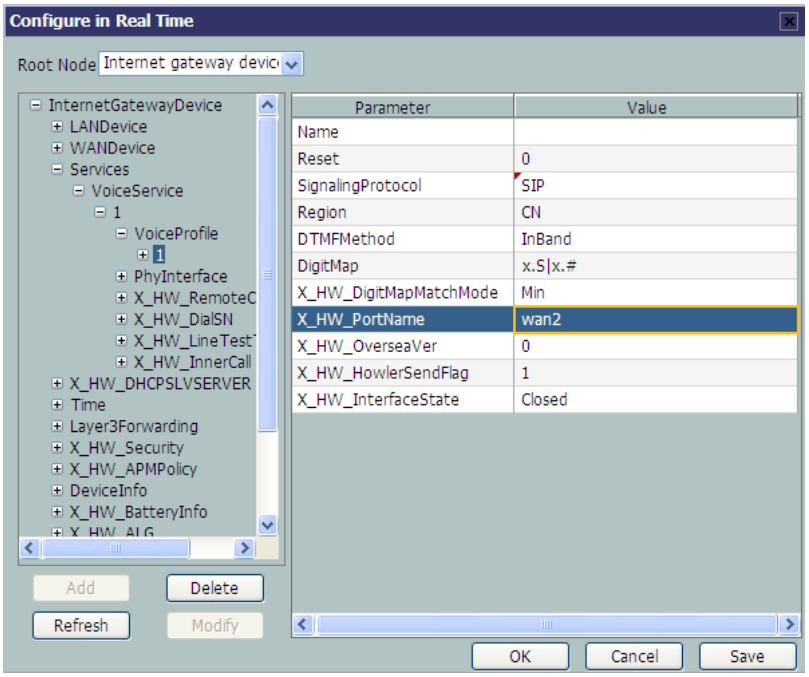
   - If the WAN interface obtains IP addresses in static or DHCP mode, choose **WANIPConnection** to set the parameters of the voice WAN interface.
   - If the WAN interface obtains IP addresses in PPPoE mode, choose **WANPPPConnection** to set the parameters of the voice WAN interface.



4. Configure the voice protocol parameters.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set the parameters as follows:

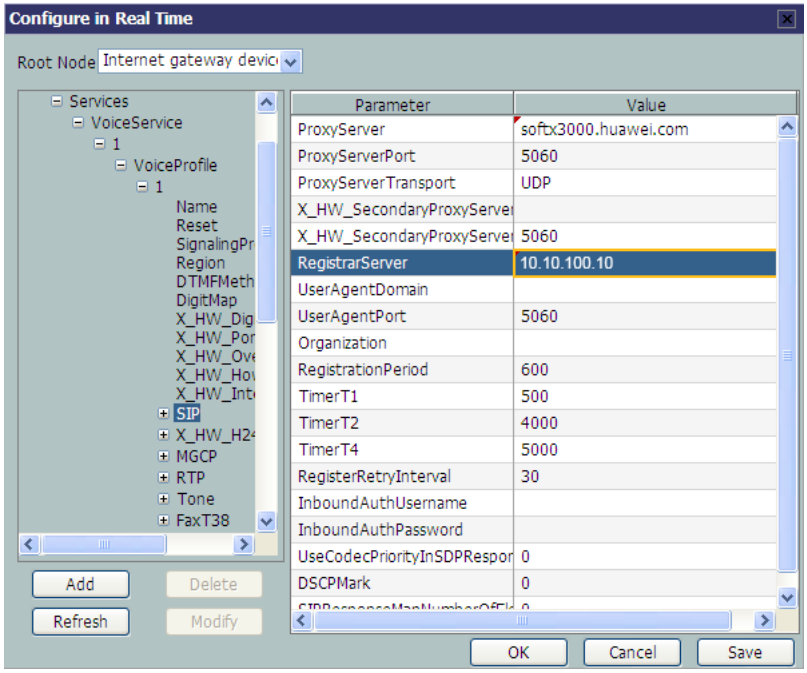
- Set **SignalingProtocol** to **SIP**, indicating that the SIP protocol is used.
- Set **Region** to **CN**, indicating the country code of China.
- Set **X_HW_PortName** to **wan2**, indicating that the new WAN interface 2 is bound.



5. Configure the SIP service parameters.

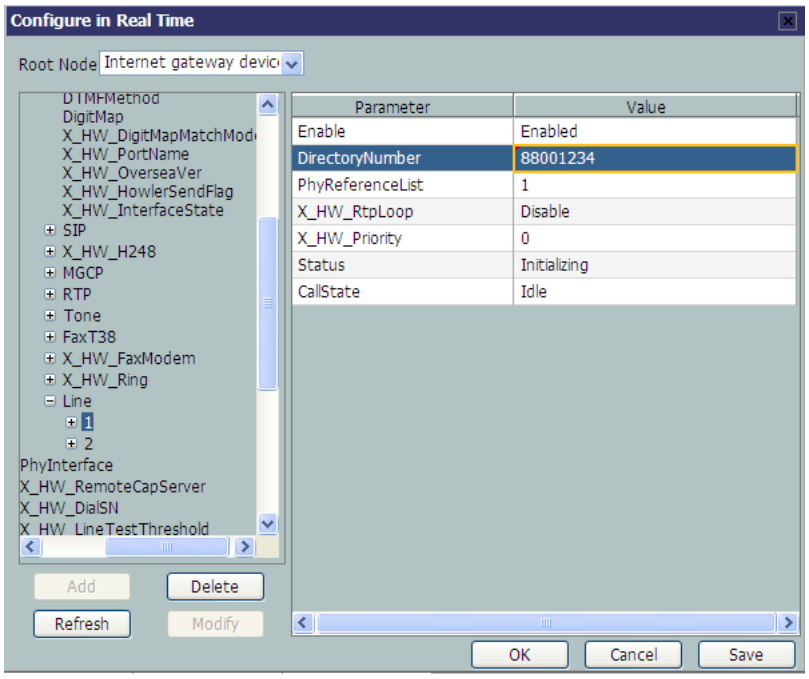
Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** > **SIP** from the navigation tree. In the right pane, set the parameters as follows:

- Set **ProxyServer** to **softx3000.huawei.com**, indicating that the address of the SIP proxy server is **softx3000.huawei.com**.
- Set **RegistarServer** to **10.10.100.10**, indicating that the SIP registration address is **10.10.100.10**.



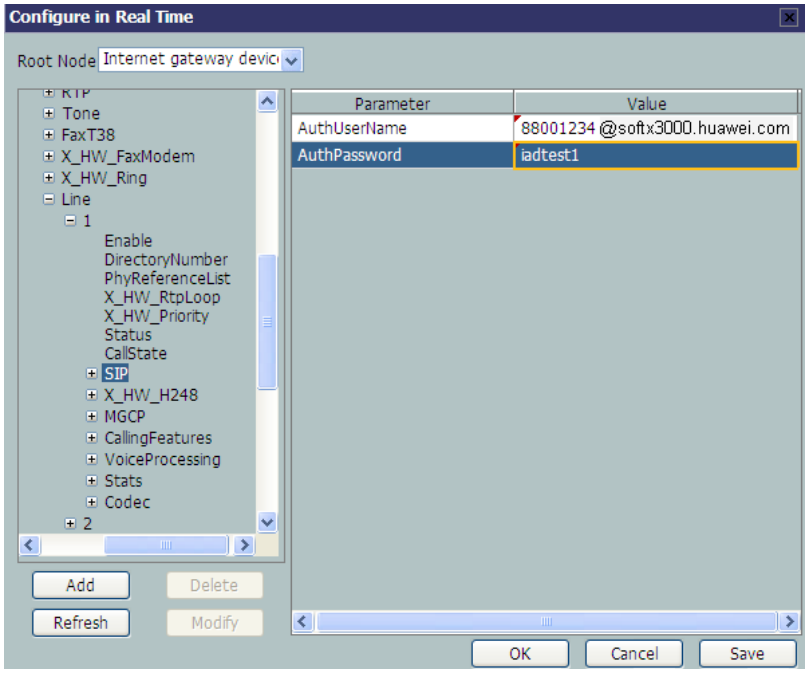
6. Configure the information about SIP voice users.

   a. Choose **InternetGatewayDevice** > **Service** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** > **1** from the navigation tree. In the right pane, set **DirectoryNumber** to **88001234**, indicating that the telephone number of SIP user 1 is 88001234.



   b. Choose **1** > **SIP** from the navigation tree. In the right pane, set **AuthUserName** to **88001234@softx3000.huawei.com** and **AuthPassword** to **iadtest1**, indicating that

the user name and password of user 1 for authentication are **88001234@softx3000.huawei.com** and **iadtest1** respectively.



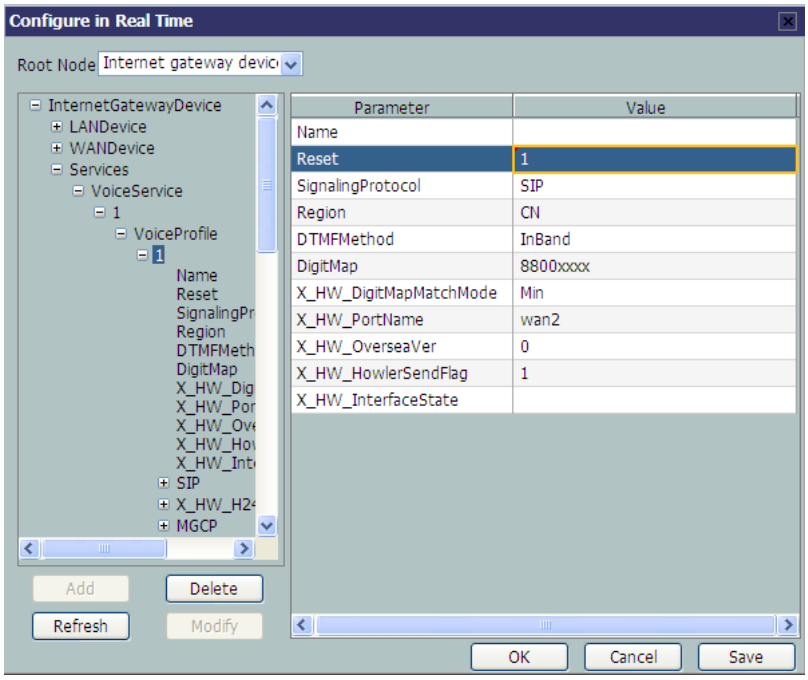
c. Set information about SIP user 2 in the same way.

   Choose **InternetGatewayDevice** > **Service** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** from the navigation tree. Click **Add** in the lower left part. Choose **2** from the navigation tree. In the right pane, set **DirectoryNumber** to **88001235**, indicating the telephone number of SIP user 2 is 88001235.

   Choose **2** > **SIP** from the navigation tree. In the right pane, set **AuthUserName** to **88001235@softx3000.huawei.com** and **AuthPassword** to **iadtest2**, indicating that the user name and password of user 2 for authentication are **88001235@softx3000.huawei.com** and **iadtest2** respectively.

7. Restart the voice process.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set **Reset** to **1**, indicating that the voice process will be restarted.



8. Click **OK** after the configuration.

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

2.5.5 Configuring the H.248-based Voice Service Through the U2560

This topic provides an example of how to configure the H.248-based voice service through the U2560.

Prerequisites

- The ONT is auto discovered on the U2560. For details, see **2.5.2 Commissioning Interoperation Between the U2560 and the ONT**.
- Two telephone sets must be available and each must be connected to ports TEL1 and TEL2 respectively on the ONT.

Context

Every data change must be saved. You can click **Save** in a window to save data changes. If you navigate to another node without saving data changes, a dialog box will be displayed

prompting you to save the data changes. In this case, click **YES** in the dialog box. New data will be automatically applied to the ONTs after the data changes are saved.

NOTICE

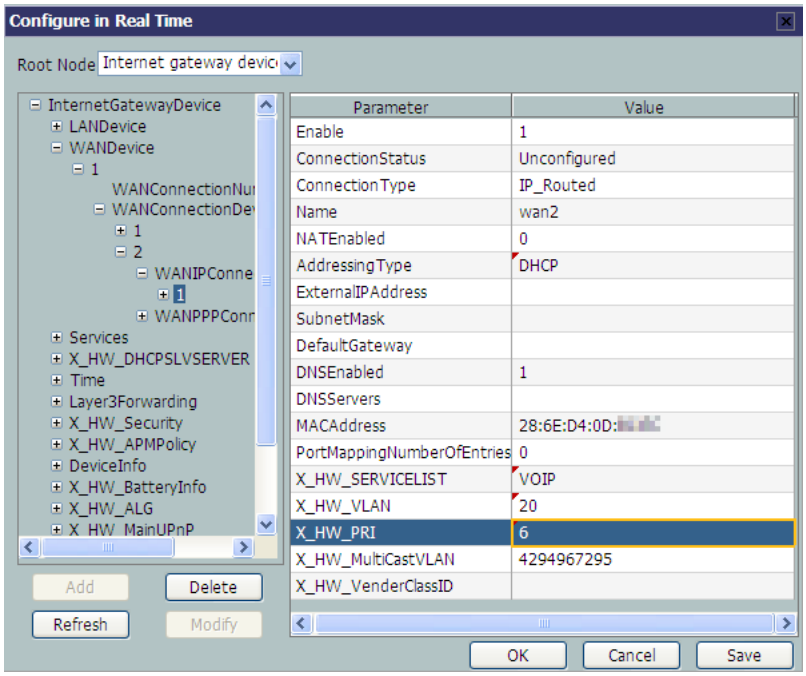
When configuring services on the U2560, do not modify the WAN interface connecting the U2560 and the ONT. Otherwise, the U2560 loses communication with the ONT.

Procedure

1. Log in to the U2560 and choose **Subnet View** > **TR069 Subnet** from the navigation tree. In the terminal list, right-click an ONT and choose **Tools** > **Configure in Real Time** from the shortcut menu.
2. In the **Configure in Real Time** dialog box, set **Root Node** to **Internet gateway device**.
3. Configure the parameters of the voice WAN interface.
   a. Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** from the navigation tree. Click **Add** in the lower left part to create an instance.
   b. Choose **2** > **WANIPConnection** from the navigation tree. Click **Add** in the lower left part. Choose **1** from the navigation tree. In the right pane, set the parameters as follows:
      - Set **Enable** to **1**, indicating that the WAN connection is enabled.
      - Set **Connection Type** to **IP_Routed**, indicating that the connection type of the WAN interface is in routing mode.
      - Set **Addressing Type** to **DHCP**, indicating that the WAN interface obtains IP addresses in DHCP mode.
      - Set **X_HW_SERVICELIST** to **VOIP**, indicating that the WAN interface provides the VoIP access service.
      - Set **X_HW_VLAN** to **20**, indicating the VLAN ID of the WAN interface is 20.
      - Set **X_HW_PRI** to **6**, indicating that the priority level of the WAN interface is 6.

   NOTE

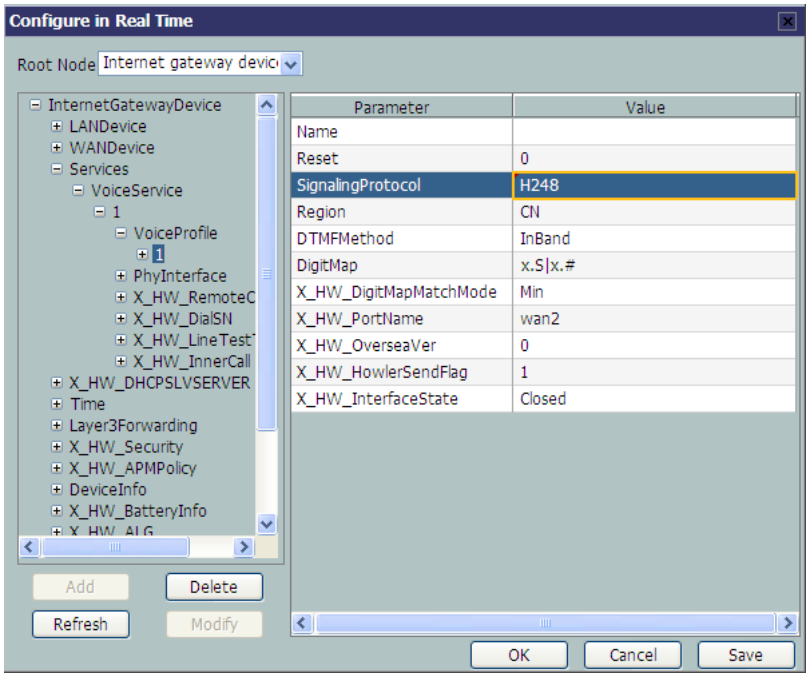
   - If the WAN interface obtains IP addresses in static or DHCP mode, choose **WANIPConnection** to set the parameters of the voice WAN interface.
   - If the WAN interface obtains IP addresses in PPPoE mode, choose **WANPPPConnection** to set the parameters of the voice WAN interface.



4. Configure the voice protocol parameters.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set the parameters as follows:

- Set **SignalingProtocol** to **H248**, indicating that the H.248 protocol is used.
- Set **Region** to **CN**, indicating the country code of China.
- Set **X_HW_PortName** to **wan2**, indicating that the new WAN interface 2 is bound.



5. Configure the H.248 service parameters.

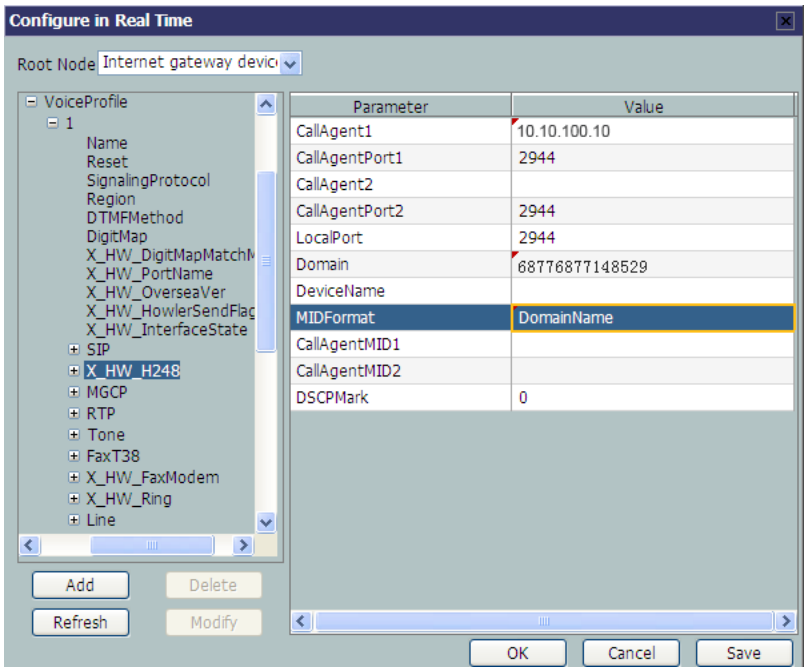
Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** > **X_HW_H248** from the navigation tree. In the right pane, set the parameters as follows:

- Set **CallAgent1** to **10.10.100.10**, indicating that the IP address of the MGC server is **10.10.100.10**.
- Set **Domain** to **6877687714852901**, indicating that the MG registration address is **6877687714852901**.

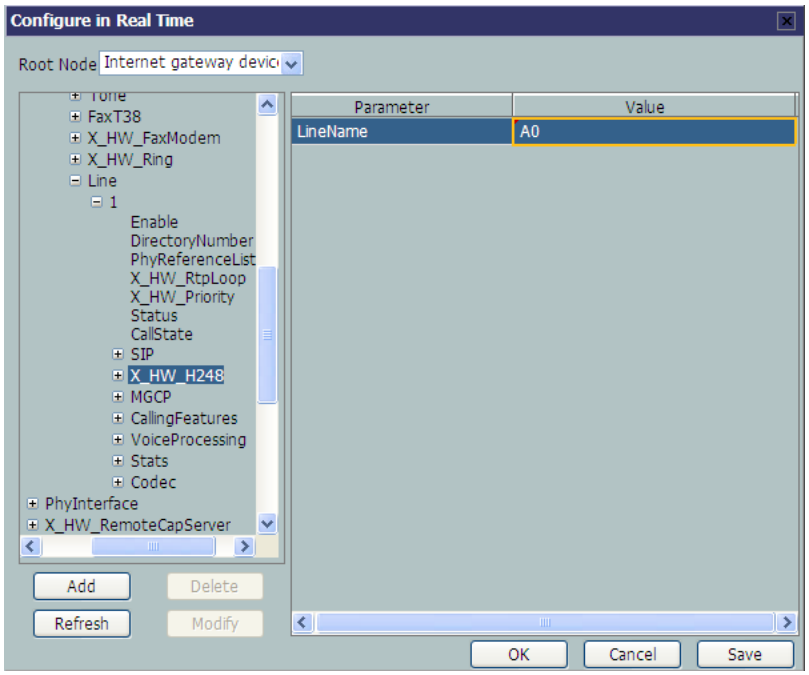
NOTE

Domain is ONT's domain name registered on the MGC. It is globally unique. **Domain** in this example is ONT's SN.

- Set **MIDFormat** to **DomainName**, indicating that the MG uses its domain name to register.

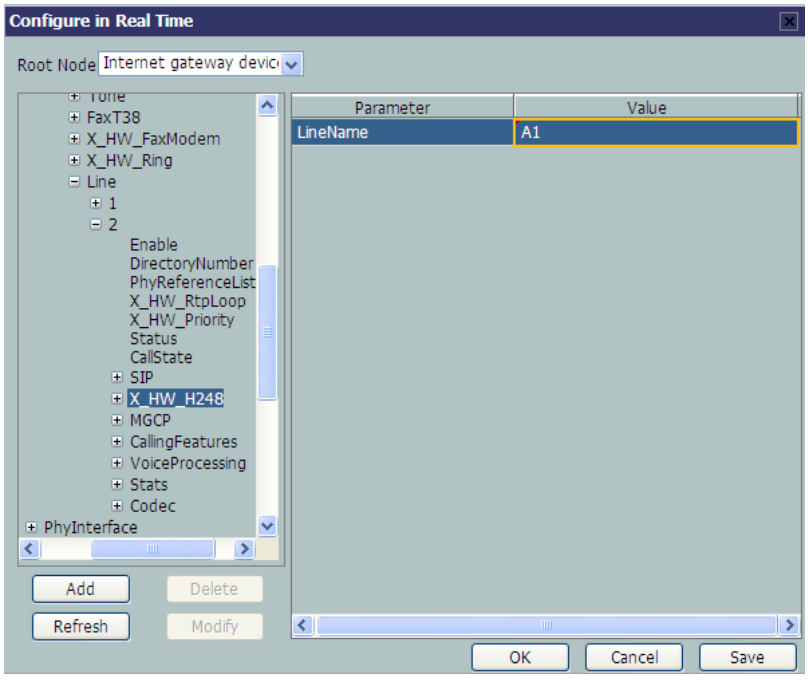


6. Configure the TIDs of H.248 voice users.
   a. Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** > **1** > **X_HW_H248** from the navigation tree. In the right pane, set **LineName** to **A0**, indicating that the TID of H.248 voice user 1 is A0. The user telephone number set on the MGC is 88001234.



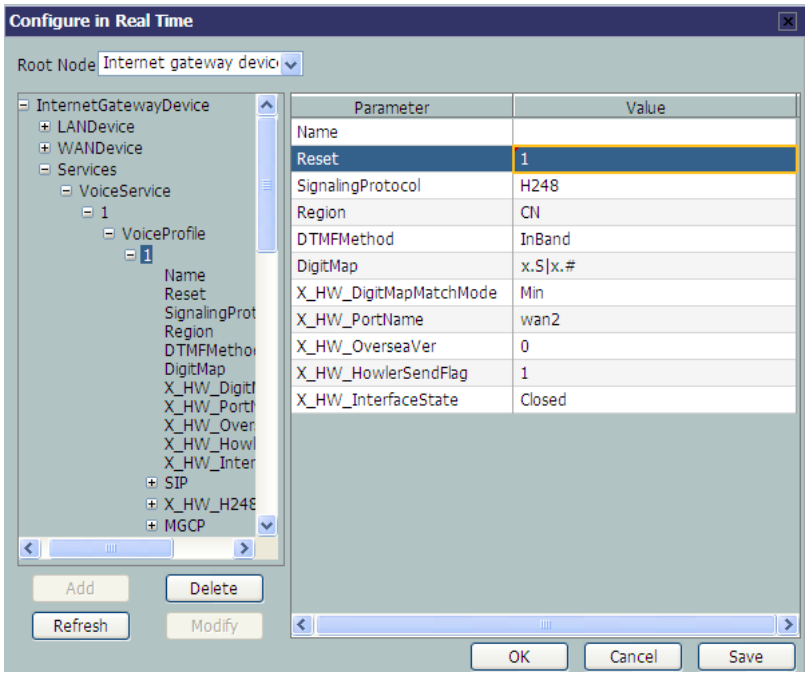
b. Configure the TID of H.248 voice user 2 in the same way.

Choose **InternetGatewayDevice** > **Service** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** from the navigation tree. Click **Add** in the lower left part. Choose **2** > **X_HW_H248** from the navigation tree. In the right pane, set **LineName** to **A1**, indicating that the TID of H.248 voice user 2 is A1. The user telephone number set on the MGC is 88001235.



7. Restart the voice process.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set **Reset** to **1**, indicating that the voice process will be restarted.



8. Click **OK** after the configuration.

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

2.6 Configuring FTTH IPv6 Services in Bridging-type ONT Scenario (Dual Stack/DS-Lite)

This topic describes how to configure FTTH IPv6 services when the ONT is a bridging-type ONT and the dual stack or DS-Lite solution is used.

Dual Stack Application Scenario

Networking description:

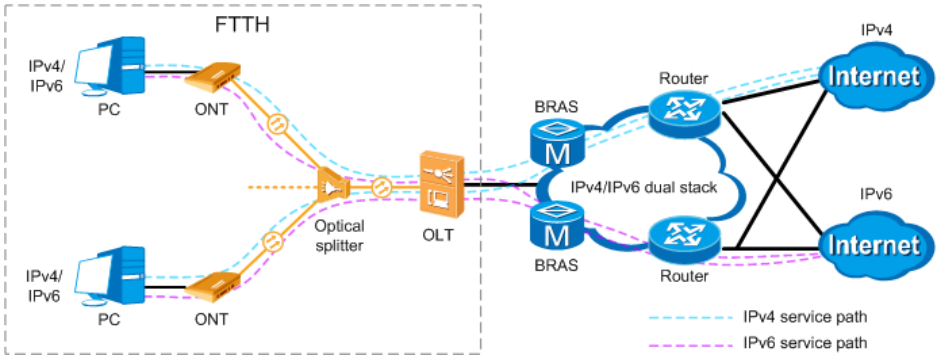
- All NEs must support both IPv4 and IPv6.
- The BRAS directly assigns IPv4 and IPv6 addresses to PCs, and the ONT transparently transmits IPv4 and IPv6 packets.
- PCs use IPv4 and IPv6 addresses to access the IPv4 Internet and IPv6 Internet respectively.

- Both the OLT and ONT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction: All NEs on the network need to be upgraded to support IPv4 and IPv6 dual stacks.

Figure 2-9 shows the dual-stack networking diagram.

Figure 2-9 Dual-stack networking diagram



DS-Lite Application Scenario

Networking description:

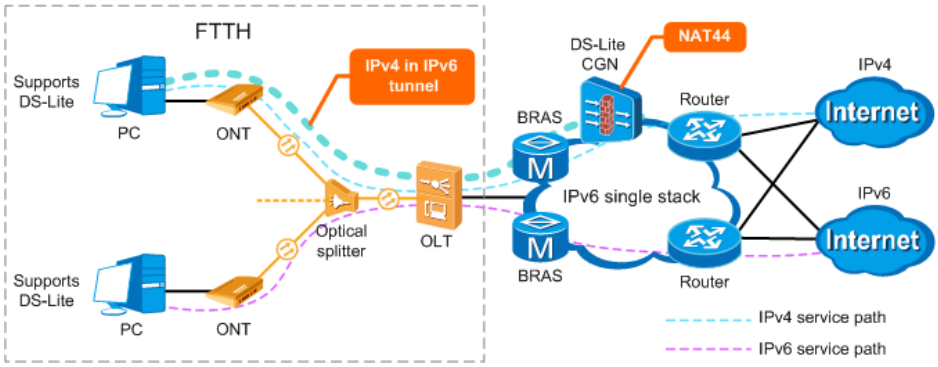
- Devices below the DS-Lite CGN must support the IPv6 single stack.
- The BRAS directly assigns IPv6 address prefixes (without IPv4 address) to PCs, and the ONT transparently transmits IPv6 packets.
- IPv4 addresses are encapsulated into IPv6 packets for forwarding, decapsulated on the DS-Lite CGN, and forwarded to the IPv4 Internet after NAT44 translation. IPv6 addresses are directly forwarded to the IPv6 Internet through IPv6 devices.
- Both the OLT and ONT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction:

- A special software needs to be installed on the PC to support DS-Lite.
- The CGN needs to be upgraded to support DS-Lite.
- Devices between the CGN and PC need to be upgraded to support IPv6.
- The DS-Lite CGN device needs to be added.

Figure 2-10 shows the DS-Lite networking diagram.

Figure 2-10 DS-Lite networking diagram



Procedure

- Configuration using the U2000

NOTE

In the dual stack and DS-Lite scenarios, both the OLT and ONT implement Layer 2 transparent transmission. Configurations in the FTTH scenario are the same as those for IPv4.

When the access mode of IPv6 users is IPoE and the BRAS uses the binding authentication mode, users do not need to enter user names or passwords for authentication because the BRAS performs authentication based on users' physical information. In this case, DHCPv6 Option18 needs to be configured on the OLT. For the mapping relationship between DHCPv6 Option and the BRAS, see **Table 2-14**.

Table 2-14 DHCPv6 Option mapping

DHCPv6 Option	OLT	BRAS
Option17	N/A	Optional
Option18	Mandatory	Mandatory
Option37	Optional	Optional

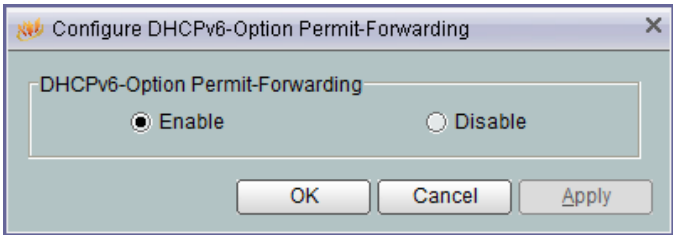
NOTE

By default, the global DHCPv6 Option configuration is **disable**, the VLAN-level DHCPv6 Option configuration is **enable**, and the upstream/cascaded port-level DHCPv6 Option configuration is **enable**. Therefore, you only need to enable DHCPv6 Option globally.

After DHCPv6 Option is enabled, the OLT inserts Option18 and Option37 into DHCPv6 packets for authentication by the BRAS.

1. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT 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 GPON ONUs.
4. Right-click a required ONT and choose **Configure DHCPv6–Option Permit-Forwarding**.

5. In the dialog box that is displayed, select **Enable**.



6. Click **OK**.

- Configuration using OLT commands

NOTE

In the dual stack and DS-Lite scenarios, both the OLT and ONT implement Layer 2 transparent transmission. Configurations in the FTTH scenario are the same as those for IPv4.

When the access mode of IPv6 users is IPoE and the BRAS uses the binding authentication mode, users do not need to enter user names or passwords for authentication because the BRAS performs authentication based on users' physical information. In this case, DHCPv6 Option18 needs to be configured on the OLT. **Table 2-15** describes the mapping between the BRAS, OLT, and DHCPv6 Option.

Table 2-15 DHCPv6 Option mapping

DHCPv6 Option	OLT	BRAS
Option17	N/A	Optional
Option18	Mandatory	Mandatory
Option37	Optional	Optional

NOTE

By default, the global DHCPv6 Option configuration is **disable**, the VLAN-level DHCPv6 Option configuration is **enable**, and the upstream/cascaded port-level DHCPv6 Option configuration is **enable**. Therefore, you only need to enable DHCPv6 Option globally.

After DHCPv6 Option is enabled, the OLT inserts Option18 and Option37 into DHCPv6 packets for authentication by the BRAS.

```
huawei(config)#raio-mode common dhcpv6-option
huawei(config)#dhcpv6 option enable
```

- The ONT implements Layer 2 transparent transmission. Therefore, no configuration needs to be performed on the ONT Web page.

3 Configuring the Gateway-Type ONT

About This Chapter

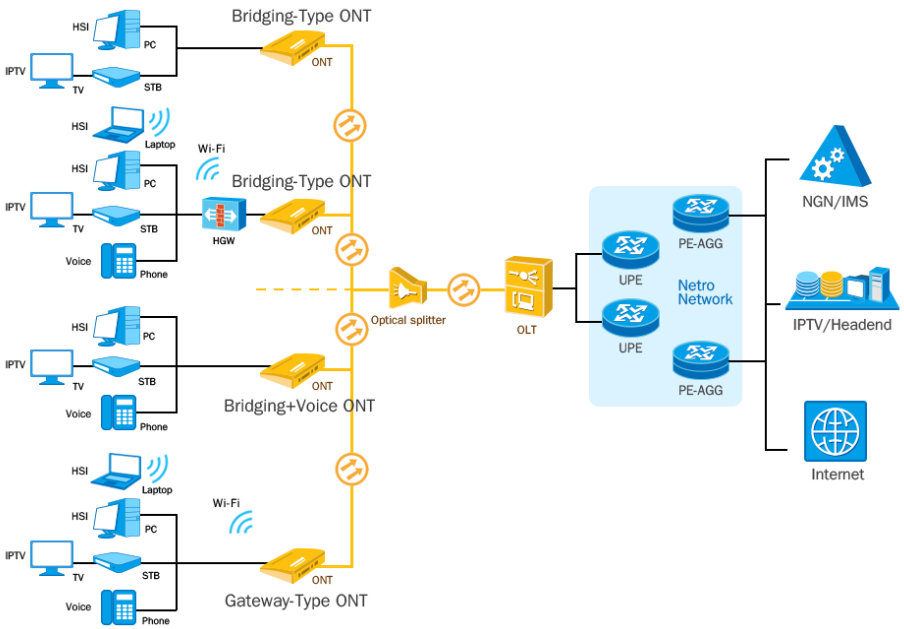
This topic describes the configuration of gateway-type ONTs and their web pages. Gateway-type ONTs only support Layer 2 and Layer 3 features.

3.1 FTTH Networking and Configuration Scenarios

Typical FTTH Networking

Figure 3-1 shows the typical FTTH networking.

Figure 3-1 Typical FTTH networking diagram



Networking Scenario	Description
Bridging ONT + HGW Network Scenario	The HGW integrating an IAD provides Internet, voice over Internet Protocol (VoIP), and Internet Protocol television (IPTV) services to users. Services are implemented on the HGW, and the bridging ONT works with the OLT to provide Layer 2 channels.
Bridging+Voice ONT Network Scenario	The ONT integrating an integrated access device (IAD) provides Internet, VoIP, and IPTV services to users. The bridging+voice ONT provides Layer 2 data and voice services. This scenario provides transparent transmission channels and requires simple service configuration, so this scenario applies to Layer 2 networking. ● For data services, a PC directly performs dial-up. Then, the upper-layer broadband remote access server (BRAS) device authenticates and accesses the PC. The PC can also access the Internet using the Dynamic Host Configuration Protocol (DHCP) or static IP address. ● The ONT with a built-in voice module encapsulates voice service packets, and the OLT transmits them to the upstream next generation network (NGN) or IP multimedia subsystem (IMS).
Gateway ONT Network Scenario	The ONT integrating an IAD provides Internet, VoIP, and IPTV services to users. The HGW ONT facilitates interconnection of home devices by providing Layer 3 services, such as Point-to-Point Protocol over Ethernet (PPPoE)/DHCP dial-up, network address translation (NAT), and Internet Group Management Protocol (IGMP) snooping. This scenario provides fine-grained management channels and service control, and applies to Layer 3 networking.

FTTH Deployment Schemes

FTTH service application includes the deployment process and service provisioning process. The FTTH deployment process includes OLT deployment (configuration) and configuration of basic data. No deployment, however, is required on the ONT and the ONT is plug and play once services are provisioned.

Table 3-1lists the FTTH deployment schemes and service provisioning methods.

Table 3-1 FTTH deployment schemes

-	Scheme	Parameter
Pre-configuration	● **On the NMS**: Profiles can be issued in batches. ● **Using commands on the OLT**: Configuration scripts containing commands can be imported to the OLT.	● DBA profile ● Line profile ● Service profile ● IP traffic profile ● Service level profile ● Global OLT configurations (rather than FTTH user configurations) such as multicast VLAN, multicast mode, and policy of forwarding unknown packets ● FTTH user service VLAN configurations including adding VLANs, setting the attributes of VLANs, and adding upstream ports for VLANs

-	Scheme	Parameter
Service Provisioning	● **Using the OSS**: This method is recommended and it can implement automatic service provisioning, and eliminate problems caused by manual service provisioning, such as large workload, low efficiency, and difficult management. ● **Using OSS+ITMS**: This method is recommended if the multiple private nodes are customized for carriers. Using a TR069 server, new gateways and value-added voice services can be simply added. – Layer 2 configuration data is issued on the NMS or OLT. – Other configuration data such as voice, Layer 3, and Wi-Fi data is issued using the ITMS. ● **On the NMS**: It applies to the scenario when no OSS is available and services need to be provisioned manually on the NMS. ● **On the ONT web page**: When it is not feasible to provision services on the OSS or NMS, you can log in to the ONT web page and configure or modify parameters to provision services.	See **Table 3-2**. ONT service provisioning parameters are classified into common parameters and customized parameters: ● Customized parameters are usually issued by the upper-layer system during service provisioning. ● Common parameters are usually configured at delivery or during data pre-configuration.

Table 3-2 Parameters required for ONT service provisioning

Parameter Type	Layer 2	Voice	Above Layer 2 (Layer 3, Wi-Fi, and User Security)
Customized parameters	Parameters for adding ONTs, adding service flows, activating ports, configuring port rate limitation, and adding multicast users	● **Registration information**: IP address and port number of the local end and the proxy ● **User data**: SIP user name and H.248 TID	Login user name and password
Common parameters	Various pre-configured profile data	● **Digitmap**: includes the digitmap timer and digitmap character strings. ● **Time configuration**: includes registration heartbeat and protocol timers. ● **Encoding and decoding**: includes voice encoding and decoding priorities and packetization period, G.711/G.729/G.722. ● Fax/Modem. ● Service permission and service data. ● **VAG**: implements multiple virtual AG devices on one physical device. ● Configurations for the interconnection between IMSs of softswitches of different specifications.	● WAN port configurations (routes, bridge WANs, and VLANs) ● LAN/WAN binding ● IGMP mode ● URL for the ITMS ● NTP server ● Default Wi-Fi configurations ● Local login IP address
ONT type	● Bridging ONTs (SFUs) ● Bridging +voice ONTs ● Gateway-type ONTs (HGUs)	● Bridging+voice ONTs. ● Gateway-type ONTs.	Gateway-type ONTs

The following describes the involved configuration scenarios:

- Service configuration on the NMS: Pre-configurations and service provisioning are implemented on the NMS. The ONT software version V300R018C00 is used as an example to describe how to provision the services on the NMS.
- Service configuration using commands: Pre-configurations are implemented using commands, and service provisioning is implemented on the ONT web pages.
- Service provisioning on the ITMS: Pre-configurations are implemented on the NMS or using commands, and Layer 3 and voice services are provisioned on the ITMS. Huawei U2560 is used as an example to describe how to provision the services on the ITMS.

Recommended tool: FTTx Script Generation Tool

This tool can generate configuration scripts through the configuration wizard for you efficiently or instantly transform any configuration page into a command script, making your configuration easy and improving your configuration efficiency.

Click to experience (for Carrier) : **FTTx Script Generation Tool**.

Click to experience (for Enterprise) : **FTTx Script Generation Tool**.

3.2 Principle of FTTH Data Plan

3.2.1 Data Plan Principles for IP Addresses

This section describes how to obtain an IP address in various scenarios.

Terminal Type	Service	Recommended Solution
Bridging +Voice ONT	Internet access	A PC obtains an IP address through PPPoE dialup. The ONT transparently transmits the packets.
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The set top box (STB) obtains an IP address from the DHCP server for ordering programs. The ONT transparently transmits the packets.
Bridging ONT+HGW	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. At the same time, the HGW functions as a DHCP server and allocates IP addresses to PCs through the network cable and wireless fidelity (Wi-Fi) access. The ONT transparently transmits the packets.

Terminal Type	Service	Recommended Solution
	VoIP	The HGW functions as a DHCP client and obtains an IP address from the DHCP server, or the application control server (ACS) issues a static IP address to the HGW using TR069. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port. The ONT transparently transmits the packets.
	IPTV	The HGW is configured with a bridging WAN port. The STB obtains an IP address from the DHCP server. The HGW transparently transmits packets. The ONT also transparently transmits the packets.
Gateway ONT	Internet access	The HGW functions as a PPPoE client and obtains an IP address through PPPoE dialup. The ONT functions as a DHCP server and allocates IP addresses to PCs through the network cable.
	Wi-Fi access	● Layer 3 bridge Wi-Fi access service: A mobile equipment (ME) searches the SSID. After the ME is authenticated, the DHCP server assigns this ME the IP address by IPoE. ● Layer 3 route Wi-Fi access service: An ME searches the SSID. After the ME is authenticated, the DHCP address pool of an ONT assigns this ME the IP address and then PPPoE dialup is automatically performed on the ONT.
	VoIP	The ONT functions as a DHCP client and obtains an IP address from the DHCP server, or the NMS issues a static IP address to the ONT using the configuration file. Voice signaling and media streams at multiple POTS ports share one IP address. Media streams are distinguished by port.
	IPTV	The ONT functions as a DHCP client and obtains an IP address from the DHCP server. At the same time, the ONT functions as a DHCP server and allocates IP addresses to STBs.

3.2.2 Principle of QoS Planning

The QoS planning is an E2E planning, and it can be divided into following policies: traffic classification, marking, and scheduling policy; and traffic monitoring and DBA policy.

Traffic Classification, Marking, and Scheduling Policy

Service Type	802.1p Priority	Queue Scheduling Method	OLT Queue ID (8 Queues)	ONT Queue.ID	
				When Eight Queues Are Supported	When Four Queues Are Supported
Management service	6	PQ	6	6	3
VoIP service	5	PQ	5	5	2
IPTV service	4	PQ	4	4	2
Wi-Fi access service	1	PQ	1	1	1
Internet access service	0	PQ	0	0	0

NOTE

The greater the priority value, the higher the priority. The service priorities in this table are the recommended values. The service priorities are arranged according to the operators's actual plan.

Traffic Monitoring and DBA Policy

Items	Management service	Internet access service	Wi-Fi access service	VoIP service	IPTV service
GEM port	11 [Remark 1]	14	15	12	13
TCONT	Select a DBA type based on service types. For example, select Type1 for the management service, Type4 for the Internet access service, and Type2 for the VoIP and IPTV services.				
DBA type	Type 3 (DBA profile: assured bandwidth + maximum bandwidth. Users are allowed to preempt the bandwidth on condition that the users' assured bandwidth is guaranteed. However, the total bandwidth cannot exceed the maximum bandwidth.)				
DBA bandwidth planning	Configure the DBA bandwidth according to the user's bandwidth package. The assured bandwidth is the maximum bandwidth required by management packets, VoIP, and IPTV upstream packets. The maximum bandwidth is larger than or equal to the maximum bandwidth that users apply.				

Items	Management service	Internet access service	Wi-Fi access service	VoIP service	IPTV service
Rate limit on OLT downstream	No rate limit	Configure rate limit by a traffic profile as required. [Remark 2]	Configure rate limit by a traffic profile as required. [Remark 2]	No rate limit	No rate limit
Rate limit on ONU upstream port	No rate restriction				
Rate limit on ONU downstream port	No rate restriction				

Remark 1: GEM port value depends on the planning of the service provider, but in principle, use different GEM ports for different services.

Remark 2: **Table 3-3** shows the reference service bandwidth of each service for each user.

Table 3-3 Reference service bandwidth of each service for each user

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
Internet access service/ Wi—Fi access service	Determined based on the service tariff package.	Determined based on the service tariff package.	Available bandwidth of Internet access service or Wi—Fi access service = Committed bandwidth of the service tariff package - VoIP bandwidth - IPTV bandwidth
VoIP service	200 kbit/s	200 kbit/s	The upstream bandwidth and the downstream bandwidth of VoIP service are symmetrical. The actual bandwidth is related to the coding format. This bandwidth is calculated for two POTS ports.

Service Type	Upstream Bandwidth	Downstream Bandwidth	Bandwidth Description
IPTV service (standard definition program)	N/A	2.5 Mbit/s per channel	IPTV service mainly occupies the downstream bandwidth. The actual bandwidth depends on the coding format, the picture in picture information, 10% bandwidth burst traffic, and the number of programs that can be concurrently watched by one user (in the case of multiple STBs). The upstream bandwidth is mainly used for transmitting IGMP packets, which requires little bandwidth. Therefore, the bandwidth occupied by IGMP packets can be neglected.
IPTV service (high definition program)	N/A	9.7 Mbit/s per channel	

NOTE

- The rate restriction on the BRAS or SR is recommended. OLTs and ONTs do not restrict the rate for service streams.
- If BRAS does not support rate restriction, OLTs can restrict the rate for service streams through the traffic profile.
- Different service packets on the ONT are distinguished by different VLAN IDs. The service packets are mapped to GEM ports based on VLAN IDs so that different service packets are transmitted to different GEM ports. Each GEM port (each service) corresponds to a T-CONT or all GEM ports share a T-CONT.
- The sum of the assured bandwidth of all ONTs connected to a PON port and the fixed bandwidth of OMCI management channel is less than the GPON upstream bandwidth. Some bandwidth must be reserved for the future service expansion.

3.2.3 Principles of Internet and Wi-Fi Access Services Data Planning

This topic describes the principles of data planning for Internet and Wi-Fi access services and will focus on the VLAN planning and VLAN translation policy planning in different network scenarios.

Table 3-4 Planning of VLANs and VLAN translation policies for Internet access service

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+Voice ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.
Bridging ONT + HGW	Double-tagged VLAN	ONT: The upstream packets sent from the HGW carry user-VLANs and the ONT transparently transmits them. OLT: The OLT translates the U-VLAN to S-VLAN+C-VLAN.
Gateway ONT	Double-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Table 3-5 Planning of VLANs and VLAN translation policies for Wi-Fi access service

Application Scenario	VLAN Plan	VLAN Translation Policy
Gateway ONT	Single-tagged VLAN	ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. OLT: The OLT performs VLAN translation: C<->S.

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.

- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- To ensure traceability of users and finer-grained QoS control and management of users and services, plan per user per service per VLAN (PUPSPV) for the Internet access service. Considering OLT capacity and VLAN scalability, use dual VLANs (S-VLAN+C-VLAN) on the OLT to differentiate users for the Internet access service.
- The outer VLAN (S-VLAN), which identifies services and physical location, can be allocated based on the OLT, PON board, or PON port. The inner VLAN (C-VLAN) identifies users. C-VLANs must be unique in one S-VLAN.
- It is recommended that you use stacking VLANs as S-VLANs so that security features, such as PPPoE+/option82, and anti-MAC attacks and anti-MAC spoofing, can be easily deployed.
- The 802.1q in 802.1q (QinQ) VLAN is used in the enterprise private line scenario, such as transparent LAN service (TLS), in which the device transparently transmits packets. It is not recommended that you use QinQ VLANs as S-VLANs for the triple play services of residential users.

3.2.4 Principle of Voice Service Data Plan

The voice service plan mainly includes the plan of the VLAN and VLAN translation policy in different network scenarios, and the plan of voice protocol.

VLAN and VLAN Translation Policy

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging+voice ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have different C-VLANs. The ONT adds a C-VLAN tag to packets. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).

Application Scenario	VLAN Plan	VLAN Translation Policy
Bridging ONT +HGW	Single-tagged VLAN (recommended)	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> S-VLAN). All the ONTs connected to the same OLT have the same voice service S-VLAN; ONTs connected to different OLTs may have different voice service S-VLANs. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT transparently transmits the user VLAN. OLT: translates the VLAN tag (user VLAN <-> S-VLAN+C-VLAN).
	Double-tagged VLAN	ONT: Packets that are sent upstream by the HGW are tagged with a user VLAN. The ONT translates the user VLAN (user VLAN <-> C-VLAN). The C-VLAN is an inner VLAN tag that differentiates users. OLT: adds an S-VLAN tag to the packets (C-VLAN <-> S-VLAN+C-VLAN).
Gateway ONT	Single-tagged VLAN (recommended)	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
	Single-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: transparently transmits the VLAN.
	Double-tagged VLAN	ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. OLT: translates the VLAN tag (C-VLAN <-> S-VLAN+C-VLAN').

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- The voice service is a closed service operated by carriers. The single-tagged S-VLAN is the mainstream application and is recommended.
- When the planned VLAN is single-tagged VLAN, the S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-VLANs identify services and physical locations. It is recommended that you set different voice VLANs for the OLTs connected to one voice SR to avoid an excessively large broadcast domain of the SR and convergence switch.
- When the planned VLAN is S-VLAN+C-VLAN (that is, double-tagged VLAN), the outer S-VLANs can be allocated based on the OLT device, PON board or PON port. The S-+VLANs identify services and physical locations. It is recommended to allocate S-VLANs based on PON board or PON port. The inner C-VLAN is used to identify services (a fixed value) or users.

Voice Data Plan Based on H.248 or SIP

Item			Description
MG interface/SIP interface data **NOTE** must be consistent with the data on the MGC/IMS core network devices.	Media and signaling parameters	Media and signaling upstream VLANs	Upstream VLANs of the voice service
		Media and signaling upstream port	Upstream ports of the voice service
		Media IP addresses and signaling IP addresses	Supports separating media from signaling.
		Default gateway IP address.	The next hop IP address from an ONU/HGW to an MGC/IMS.
	MG interface/SIP interface ID		N/A
	Signaling port ID		Choose the transmission mode according to the requirement of the MGC/IMS side.

Item		Description
	IP address of active MGC (H.248)/IP address of active IMS device (SIP)	If the dual homing is not configured, only one MGC parameter needs to be configured. If the dual homing is configured, the IP address and port ID of the standby MGC need to be configured.
	Port ID of active MGC (H248)/port ID of active IMS device (SIP)	
	Coding	Choose the coding method according to the requirement on the MGC/IMS side. Generally, the text coding method is adopted.
	Transmission mode	Choose the transmission mode according to the requirement on the MGC/IMS side. Generally, the UDP transmission mode is adopted.
	Home domain (SIP)	N/A
	Profile index	N/A
	The version of H248 protocol that MG starts to negotiate	V1, V2 or V3 (by default). The interface may fail to be registered because some softswitches do not support V3.
Voice user configuration data	Phone number	For H248 protocol: The phone numbers allocated by the MGC need to be determined, and the paging numbers for users' emergency standalone need to be planned if the emergency standalone function is provided. For SIP protocol: The phone number that the IMS core network device allocates to the user must be configured.
	Terminal ID (H248)	If the TID template with which the POTS user is bound does not support terminal layering, this parameter needs to be configured.
	User priority	According to the service requirements, user priorities must be specified. The user priorities include the following: ● cat1: government1 (category 1 government users) ● cat2: government2 (category 2 government users) ● cat3: common (common users)

Item		Description
	User type	According to the service requirements, user type needs to be specified. The user type includes the following: ● DEL: direct exchange lines (default) ● ECPBX: earth calling PBX ● LCPBX: loop calling PBX ● PayPhone: pay phone
Common parameter	system parameter	The system parameters including the overseas version flag and message waiting indication (MWI) mode need to be configured according to the local standard to ensure that the response of the user terminal complies with the local standard.
	Overseas parameters	The attributes such as the upper and lower thresholds of the flash-hooking duration need to be configured according to the local standards to ensure that the response of the user terminal complies with the local standards.
	POTS port attributes	If the POTS port needs to support the polarity reversal accounting, the POTS port needs to be configured to support the polarity reversal pulse. Other attributes need not be modified if there is no special requirement.
	Ringing current attributes	When the attributes of ring current are changed, ring volume is changed accordingly. Generally, no adjustment is required for the ringing tone volume. You need to modify the parameters of the ringing current attributes according to the local standard only when the default ringing current attributes do not comply with the local standard.

3.2.5 Principle of IPTV Service Data Plan

The IPTV service data plan mainly include the plan of VLAN and VLAN translation policy in different network scenario, and the plan of IPTV service.

IPTV services include multicast service and video on demand (VoD) service. These two services are relevant but independent in VLAN planning.

Application Scenario	Service Type	VLAN Plan	VLAN Translation Policy
Bridging +Voice ONT	Multicast service	Single-tagged VLAN	ONTs replicate multicast packets based on user ports and multicast VLANs (M-VLANs) are removed downstream. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs add S-VLAN tags to iTV service packets. The OLT transparently transmits packets with S-VLANs.
		Double-tagged VLAN	All ONTs add the same C-VLAN tag to packets. The OLT implements VLAN translation: C->S+C'.
Bridging ONT + HGW	Multicast service	Single-tagged VLAN	ONTs transparently transmit upstream packets with M-VLANs sent from HGW. Multicast packets are replicated downstream with M-VLAN unchanged. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
		Single-tagged VLAN	ONTs translate the upstream VLANs sent from HGW to M-VLANs. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S.
		Double-tagged VLAN	ONTs transparently transmit the upstream U-VLANs sent from HGW. The OLT implements VLAN translation: U->S+C.
Gateway ONT	Multicast service	Single-tagged VLAN	ONTs replicate packets based on user ports and M-VLANs are removed in downstream direction. The OLT replicates multicast packets based on PON ports with M-VLAN unchanged.
	VoD	Single-tagged VLAN	ONTs add C-VLAN tags to packets. Untagged VLANs are translated to C-VLANs. The OLT implements VLAN translation: C -> S.

Note:

- User VLAN: VLAN carried by packets going upstream from user-side devices (such as a home gateway), U-VLAN for short.
- C-VLAN: VLAN added based on the ONT/ONU port. For details, see the description of the Double-tagged VLAN S+C.
- Double-tagged VLAN S+C: C indicates the inner VLAN (C-VLAN) and S indicates the outer VLAN (S-VLAN).
- Double-tagged VLAN S+C': C' indicates the translated inner VLAN (C'-VLAN) and S indicates the outer VLAN (S-VLAN).
- Single-tagged S-VLAN: Single-tagged VLAN marked or translated by the OLT. It is generally used in a single-tagged VLAN translation scenario.
- C<->S+C': Bidirectional VLAN translation: translates the C-VLAN and then adds an S-VLAN.
- C<->S+C: Bidirectional VLAN translation: maintains the C-VLAN and adds an S-VLAN.

NOTE

- IPTV service is a closed service self-operated by carriers, and single-tagged S-VLAN is recommended.
- The same S-VLAN or different S-VLANs can be used as the M-VLAN and VoD VLAN. It is recommended that you use different S-VLANs as M-VLAN and VoD VLAN so that the upper-level device easily differentiates between the BTV service and VoD service.
- S-VLANs of VoD service can identify services and physical locations based on an entire network or an OLT. It is recommended that you set different VoIP VLANs for the OLTs connected to one VoIP SR to avoid an excessively large broadcast domain of the VoIP SR and convergence switch.

3.2.6 Principle of Security Data Plan

The security plan involves system security plan, user security plan, and service security plan. Security policy ensures service security from different aspects.

NOTE

The device provides complete security measures, but not all security measures need to be deployed. Only the security measures that meet the following requirements need to be deployed:

- The security measures can be used on the live network.
- The security measures are easy to deploy.
- The security measures are effective.

System Security

Security Vulnerability	Solution	Description and Usage Suggestion
DoS attack	Enable the anti-DoS-attack function for OLT.	After the anti-DoS-attack function is enabled, control packets are monitored and those exceeding the number threshold are discarded. Use this solution for new site deployment.

Security Vulnerability	Solution	Description and Usage Suggestion
IP attack	Enable the anti-IP-attack function for OLT.	After the anti-IP-attack function is enabled, a device discards the IP packets received from the user side whose destination IP address is the IP address of the device, and therefore the system is protected. Use this solution for new site deployment.

User Security

Security Vulnerability	Solution	Description and Usage Suggestion
MAC spoofing	Enable the anti-MAC-duplicate function for OLT.	After anti-MAC-duplicate is enabled, the system records the first MAC address learned from the port and binds the MAC address to the port and VLAN. If receiving packets sent from the host that has the same MAC address with the port, the system discards the packets directly. In this case, it can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
MAC attack	Enable the anti-MAC spoofing function for OLT.	After anti-MAC spoofing is enabled, the system can prevent users from forging MAC addresses to perform malicious attacks. Use this solution for new site deployment.
IP spoofing	Enable the anti-IP spoofing function for OLT.	After anti-IP spoofing is enabled, the system can prevent users from forging IP addresses to perform malicious attacks. Use this solution for new site deployment.

Service Security

Security Vulnerability	Solution	Description and Usage Suggestion
Unauthorized broadband access of small enterprises (IPoE)	DHCP option 82 is enabled on OLT, and the BRAS implements user authentication based on the RAIO information.	In the DHCP option 82 mode, user's physical location is added to the option 82 field carried in the DHCP request packet initiated by a user. The physical location, used for user authentication on the upper-layer authentication server, can help implement the following functions: ● The DHCP relay forwards DHCP response packets to devices with specified CID and RID. ● Prevents DHCP address exhaustion. ● Achieves static allocation of DHCP addresses. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the DHCP Internet access service.
Broadband access of residential users (PPPoE), user account theft/ borrowing	PPPoE+ (PITP) is enabled on OLT, and the BRAS implements user authentication based on binding of the RAIO information to the user account.	The BRAS responds to request packets of users with specified CID and RID. In this way, the following functions are implemented: ● Prevents IP address exhaustion. ● Implements anti-IP spoofing. ● Implements anti-user ID spoofing. ● Implements anti-MAC spoofing. Use this solution for the PPPoE Internet access service.

3.3 IPv4 Scenarios

This topic describes how to configure services through the NMS, the OLT CLI or the U2560.

Context

NOTE

- The procedures for configuring ONT are similar. The following sections consider HG8245H as an example.
- The following descriptions use V300R019C00&V500R019C00 as the OLT, U2000 V200R015C50 as the BMS, and U2560 V100R002C00 as the TR-069 server. Screen shots may vary with different versions but the configuration procedures are similar. For details about configuration procedures, see the BMS configuration manuals.
- Each ONT has a different capability set. For example, a bridging ONT does not support Layer 3 configurations; an ONT without a voice port does not support voice configurations. For capability set supported by ONTs, see Reference of GPON ONT Capability Sets.

3.3.1 Configuring the Service by Using the NMS

This topic describes how to configure Internet access service, VoIP service and IPTV service by using the NMS.

3.3.1.1 Configuring FTTH Services (GPON Access)

This topic describes how to configure the Internet service, voice service, and multicast service in GPON access mode in the FTTH network scenario using the U2000.

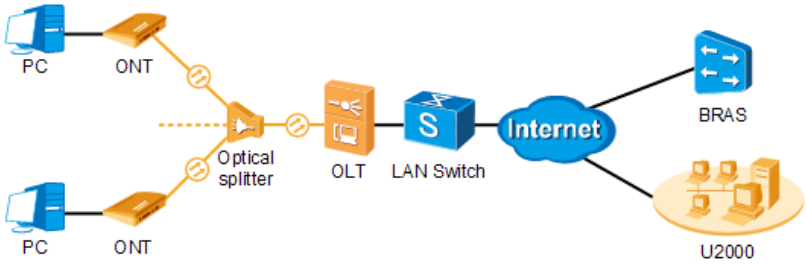
3.3.1.1.1 Configuring the GPON FTTH Layer 2 Internet Access Service on the NMS

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Networking

- The PC gains access to the Internet in PPPoE dialup mode.
- The ONT is connected to the GPBC card of the OLT through an optical fiber.
- The broadband remote access server (BRAS) provides broadband user access and functions of authentication and accounting.

Figure 3-2 Configuring the GPON FTTH Internet service



Data Plan

Table 3-6 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA Type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1 ID of the port on the ONT that is connected to the PC: 1
VLAN plan	Double-tagged VLAN ● S-VLAN ID: 100 ● S-VLAN type: Smart ● S-VLAN attribute: Stacking ● C-VLAN ID: 1001 ● C'VLAN ID: 1010 **NOTE** VLAN translation policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

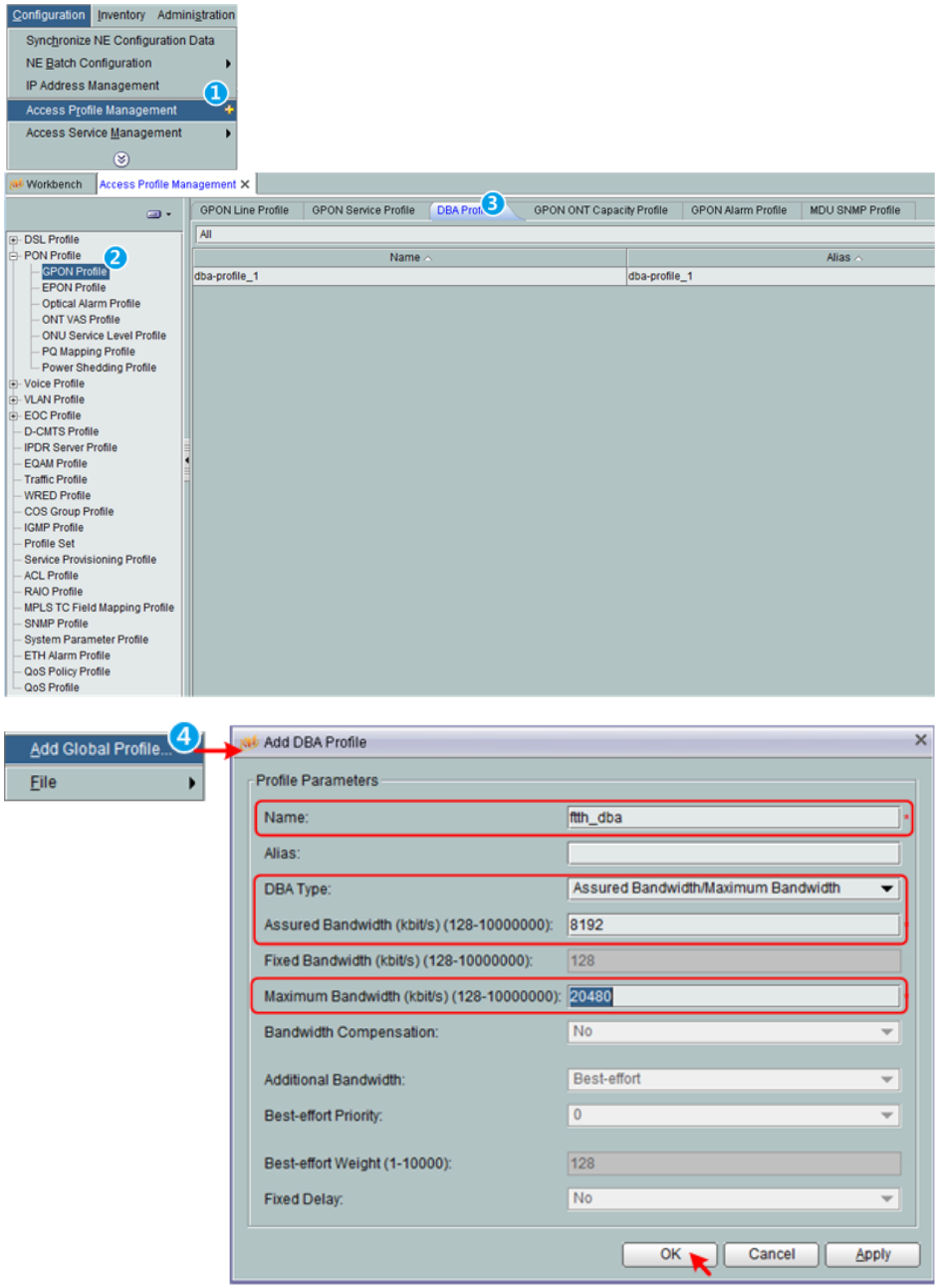
- **Implement pre-configurations.**

NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

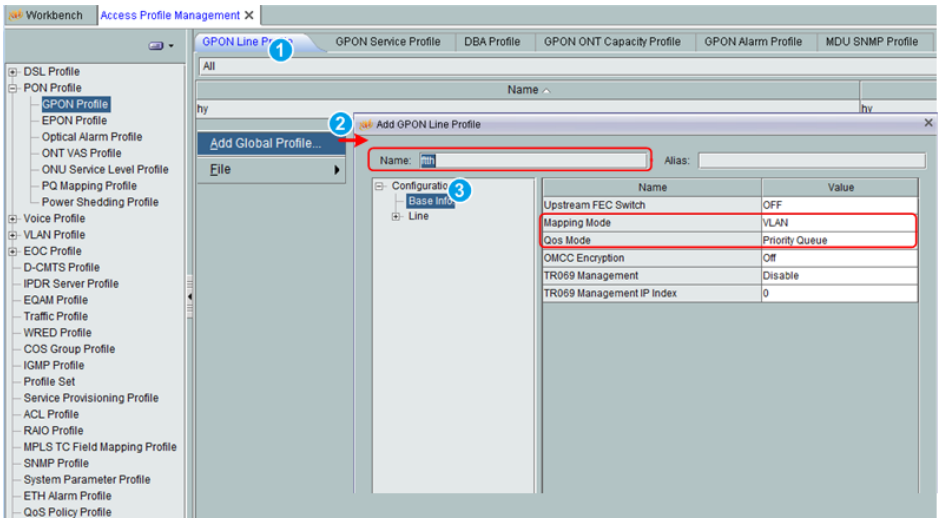
1. **Configure a DBA profile.**

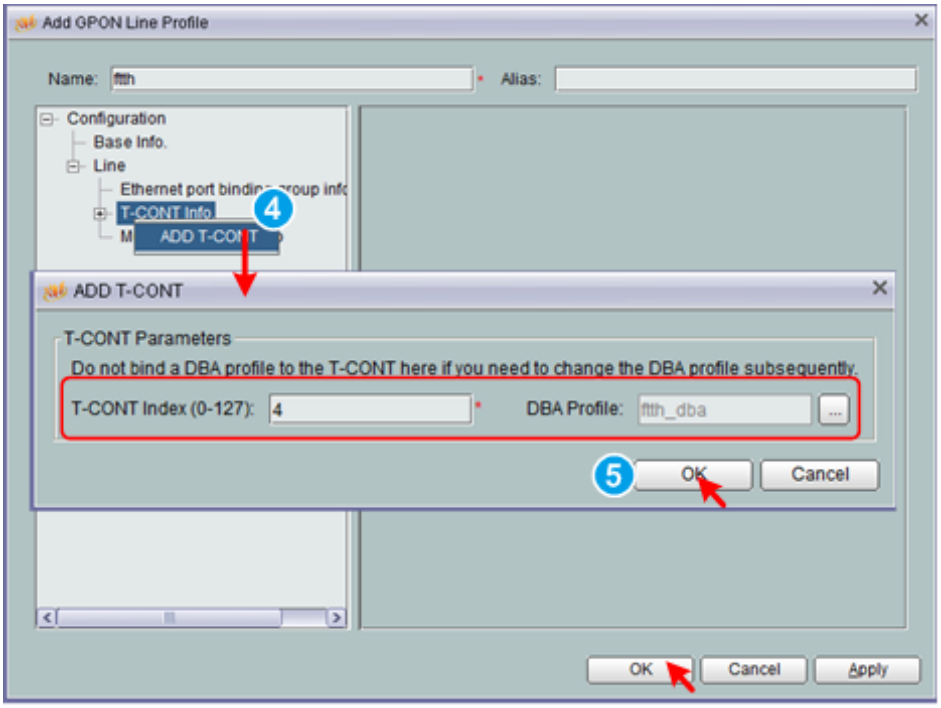


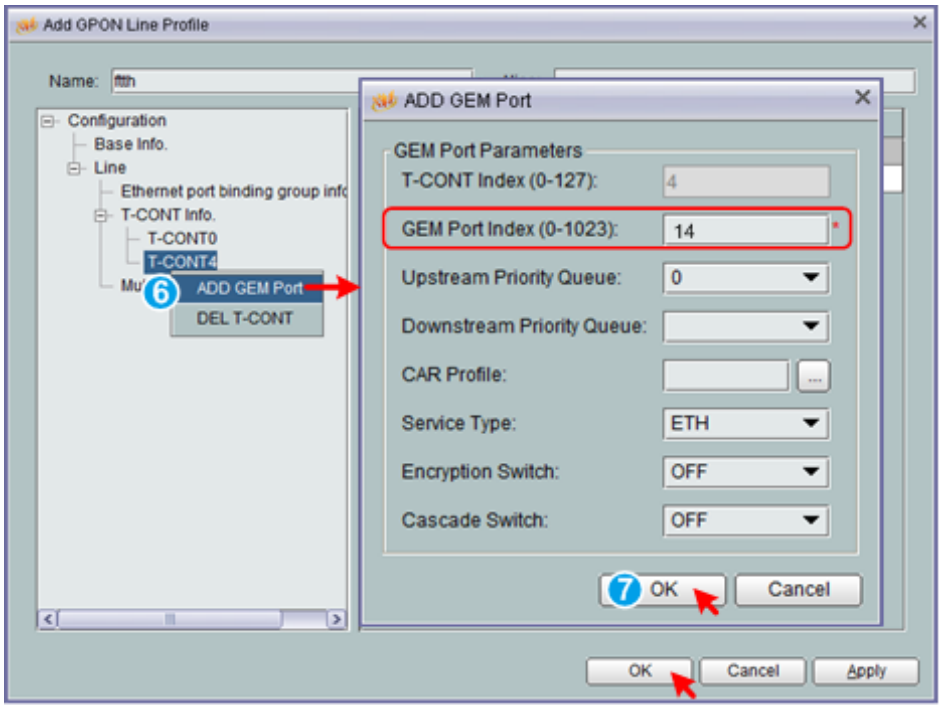
2. **Configure a line profile.**

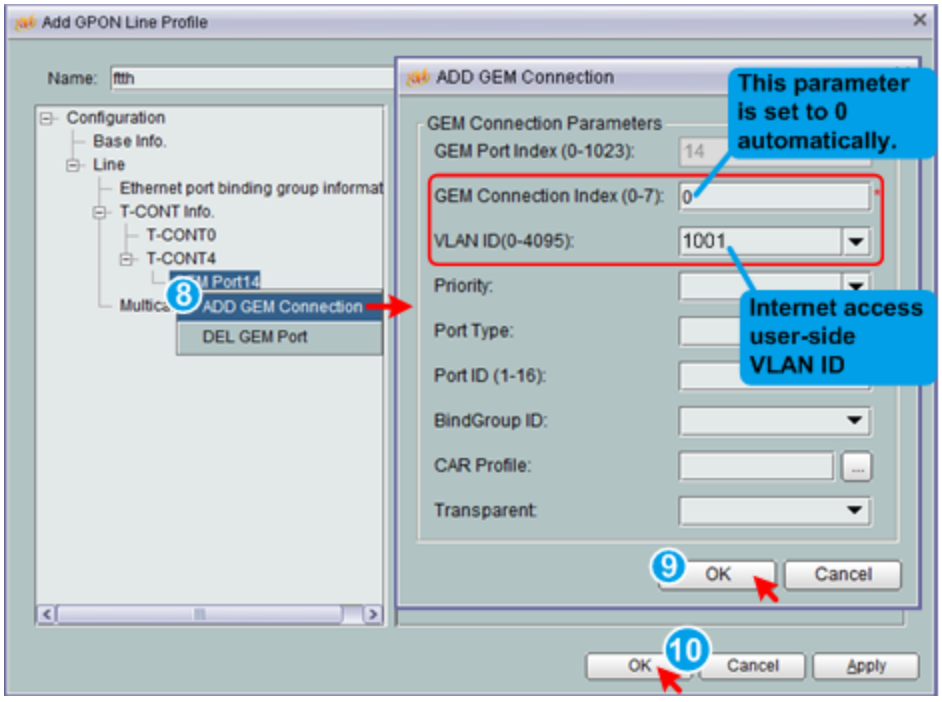
   In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

   In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 14. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.


Workbench
Access Profile Management
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
Add Global Profile...
File
Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
Name
Value
Upstream FEC Switch
OFF
Mapping Mode
VLAN
Qos Mode
Priority Queue
OMCC Encryption
Off
TR069 Management
Disable
TR069 Management IP Index
0
1
2
3

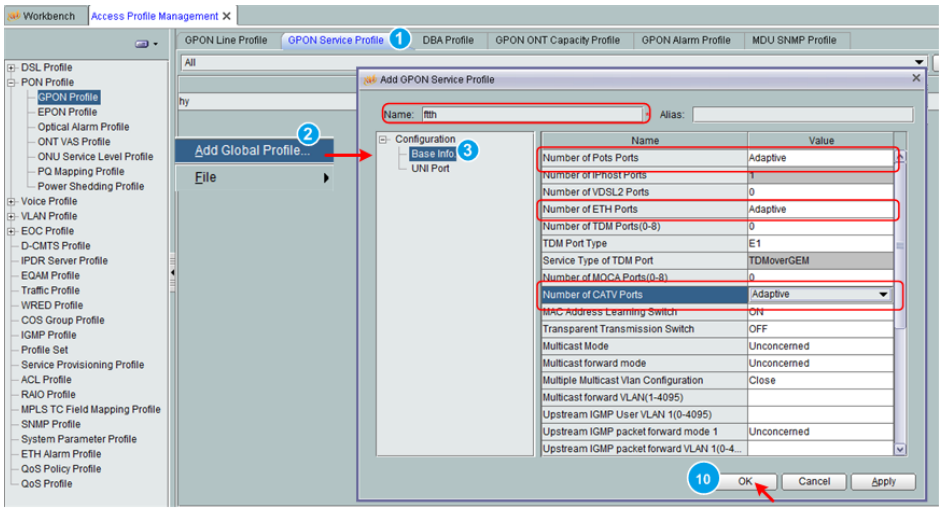

Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
T-CONT Info
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127):
4
DBA Profile:
ftth_dba
5
OK
Cancel
OK
Cancel
Apply

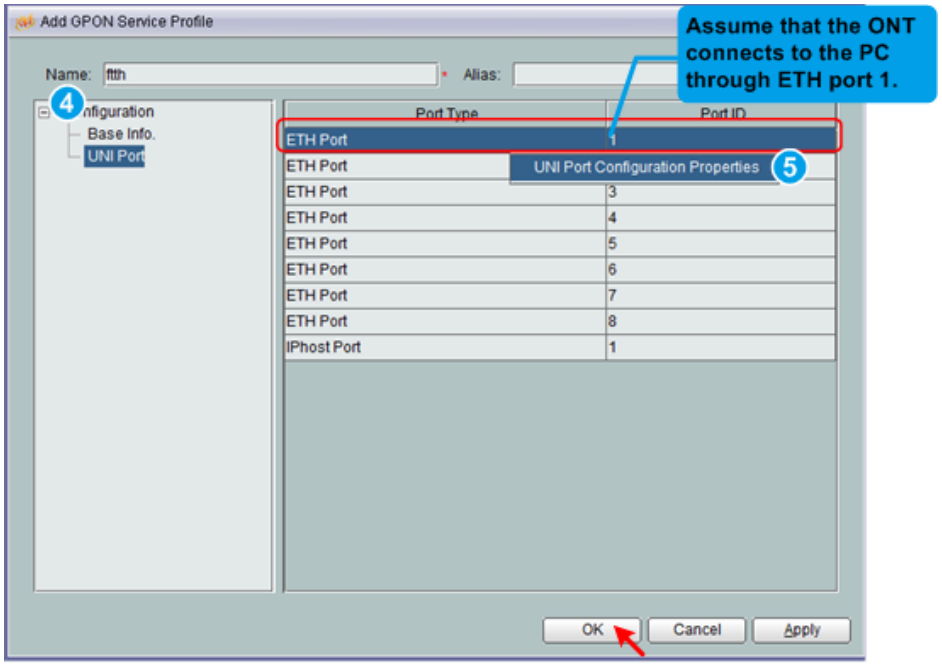


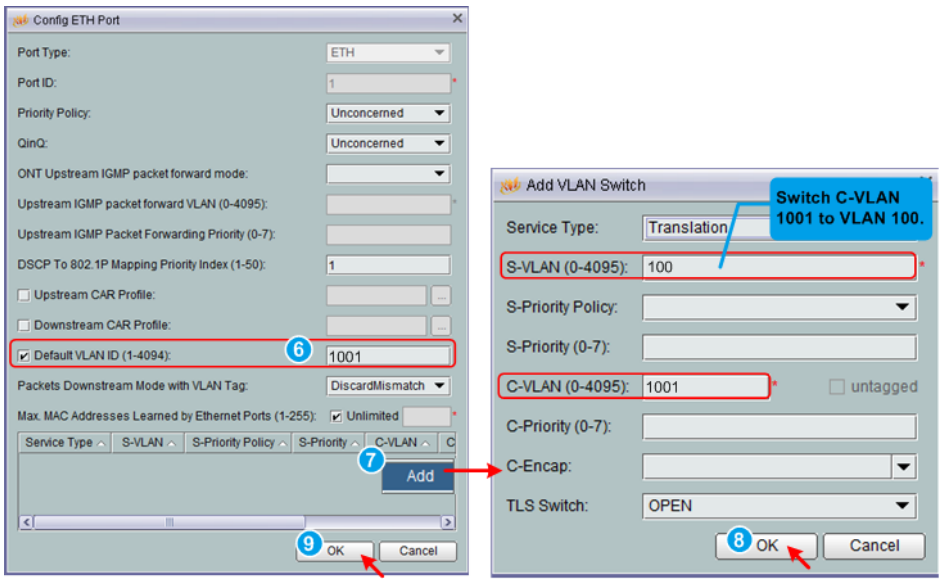


3. **Configure a service profile.**

   Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability. Then, in the ONT service profile, configure a VLAN translation policy to translate C-VLAN 1001 to VLAN 100.

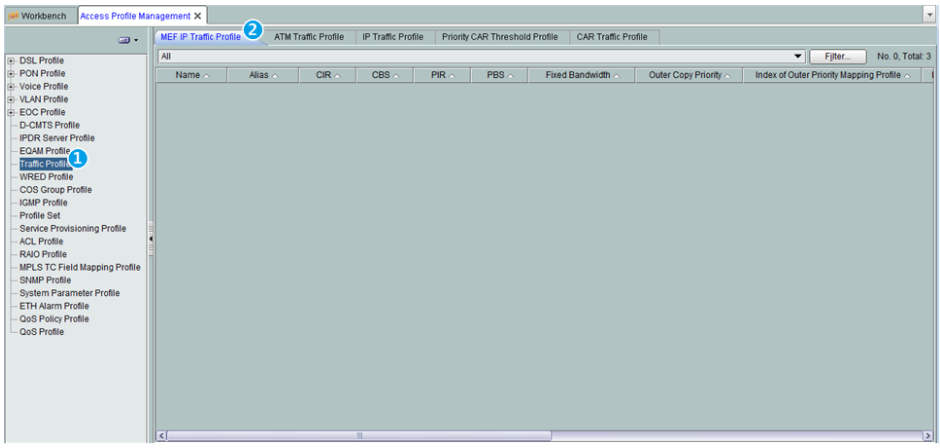

Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
Add Global Profile...
File
Add GPON Service Profile
Name: ftth
Alias:
Configuration
Base Info
UNI Port
Number of Pots Ports
Number of VDSL2 Ports
Number of ETH Ports
Number of TDM Ports(0-8)
TDM Port Type
Service Type of TDM Port
Number of CATV Ports
Transparent Transmission Switch
Multicast Mode
Multicast forward mode
Multiple Multicast Vlan Configuration
Multicast forward VLAN(1-4095)
Upstream IGMP User VLAN 1(0-4095)
Upstream IGMP packet forward mode 1
OK
Cancel
Apply

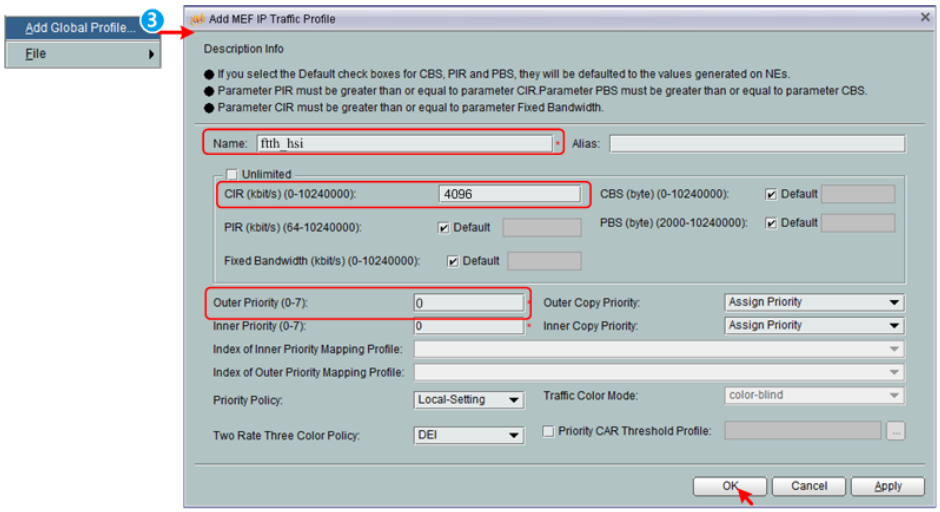

Add GPON Service Profile
Assume that the ONT connects to the PC through ETH port 1.
Name: ftth
Alias:
Base Info.
UNI Port
Port Type
Port ID
ETH Port
IPhost Port
UNI Port Configuration Properties
OK
Cancel
Apply


Config ETH Port
Port Type:
Port ID:
Priority Policy:
QinQ:
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):
Upstream CAR Profile:
Downstream CAR Profile:
Default VLAN ID (1-4094):
Packets Downstream Mode with VLAN Tag:
Max. MAC Addresses Learned by Ethernet Ports (1-255):
Service Type
S-VLAN
S-Priority Policy
S-Priority
C-VLAN
Add
OK
Cancel
Add VLAN Switch
Switch C-VLAN 1001 to VLAN 100.
Service Type:
S-VLAN (0-4095):
S-Priority Policy:
S-Priority (0-7):
C-VLAN (0-4095):
untagged
C-Priority (0-7):
C-Encap:
TLS Switch:
OPEN
OK
Cancel

4. **Configure an MEF IP traffic profile.**

   The profile name is ftth_hsi, CIR is 4 Mbit/s, and the priority is 0. Traffic is scheduled based on the priority specified in the profile.

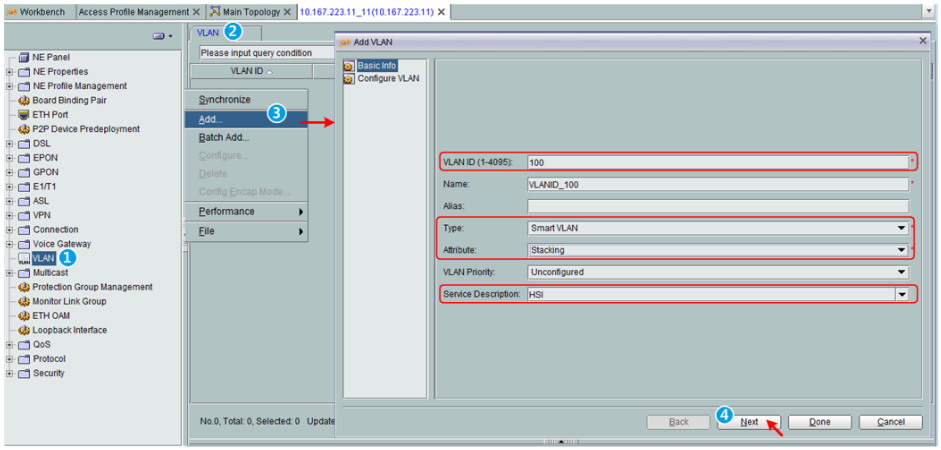


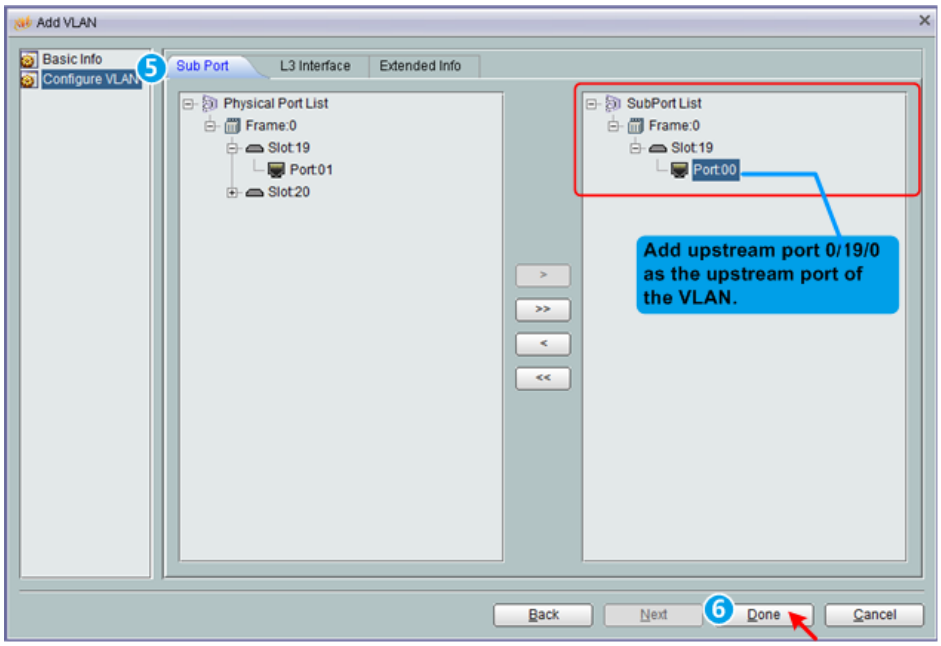


5. **Configure a service VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   A service VLAN is the VLAN used for the Internet service.



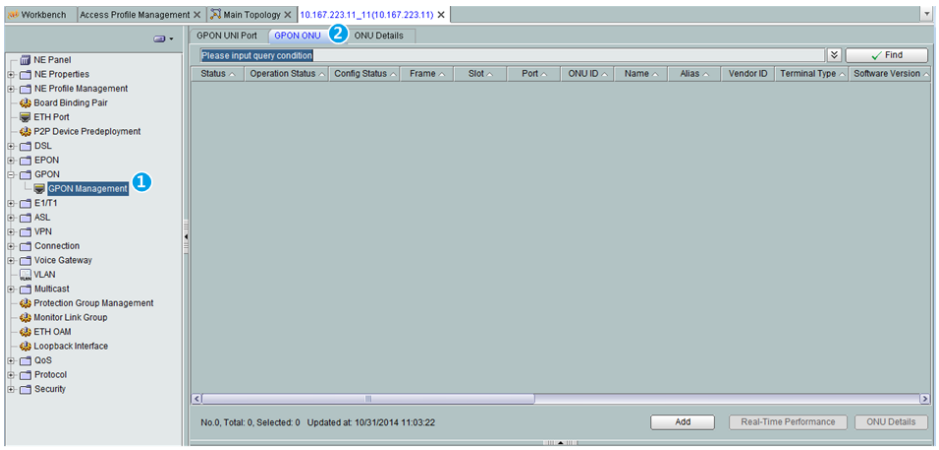


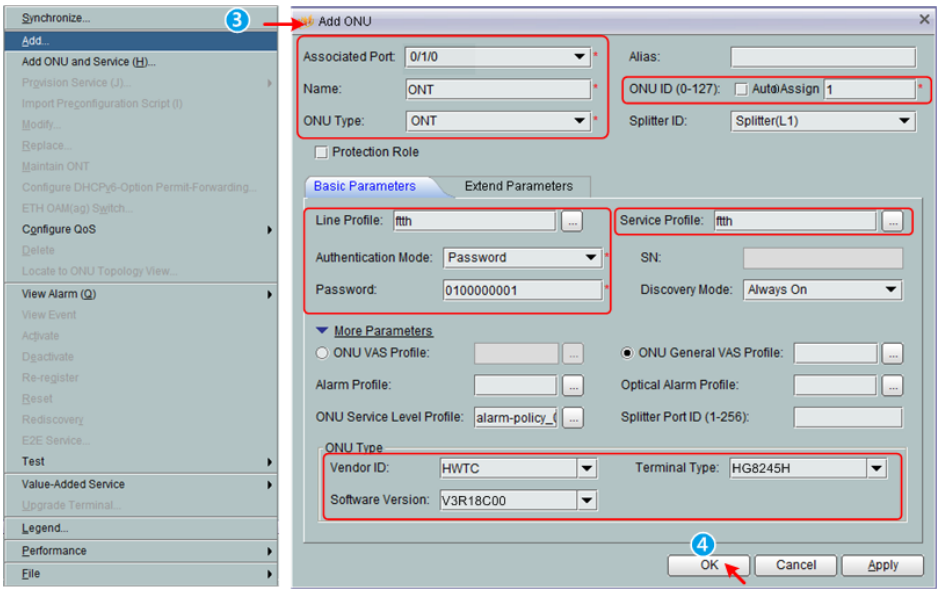
- **Provision services.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

  The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



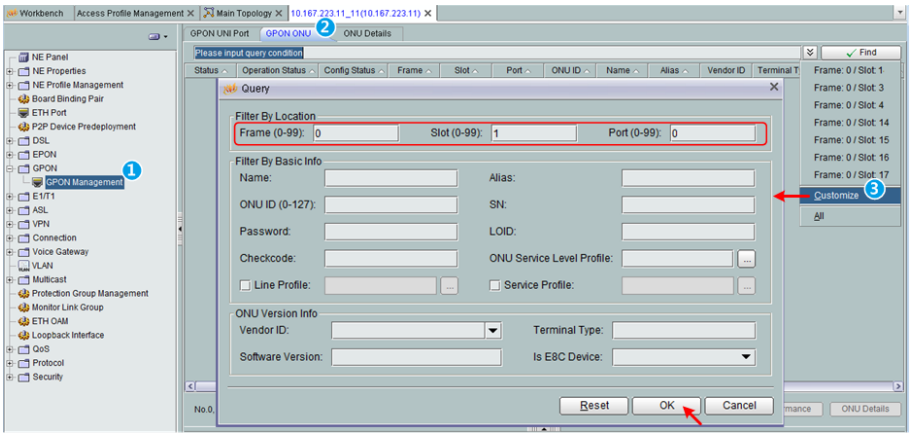


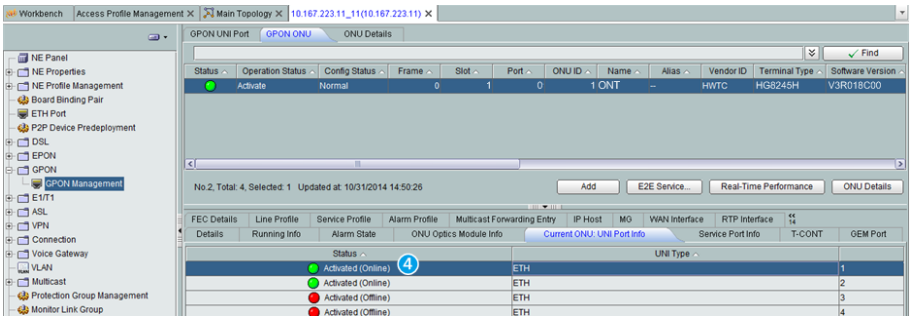
NOTE

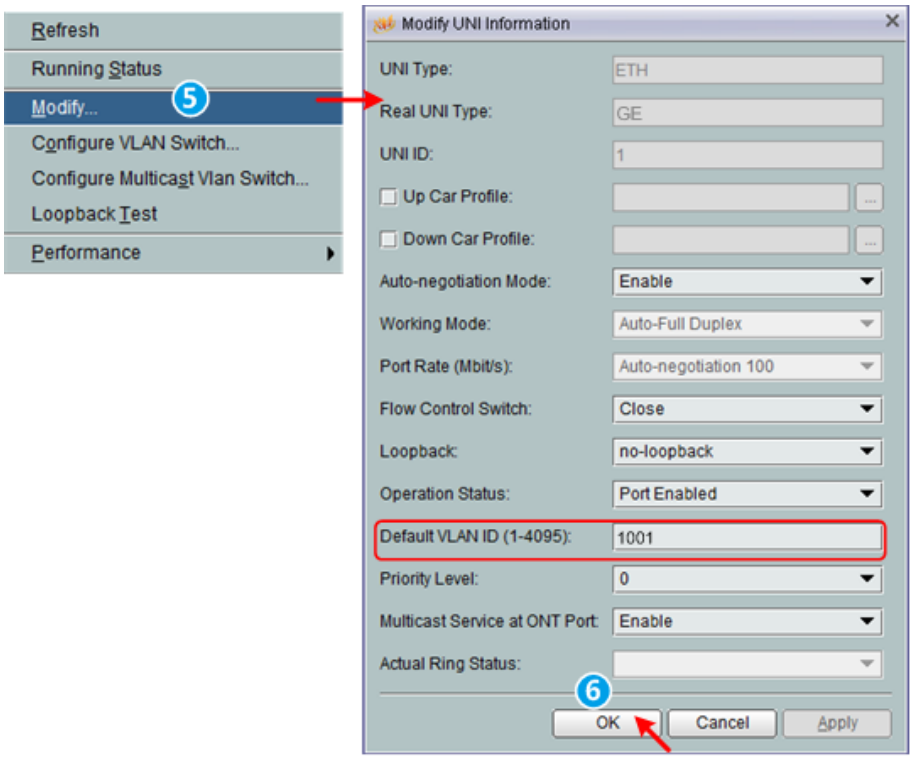
HG8245H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

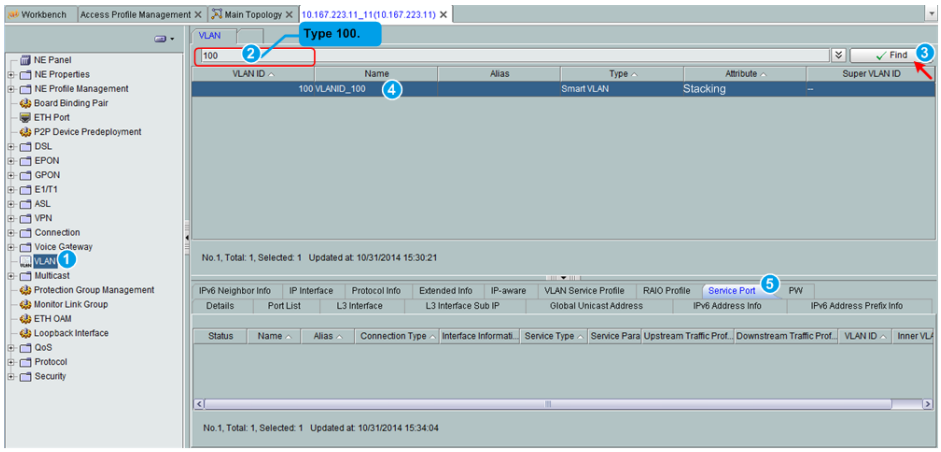
b. **Configure an ETH port of the GPON ONU.**

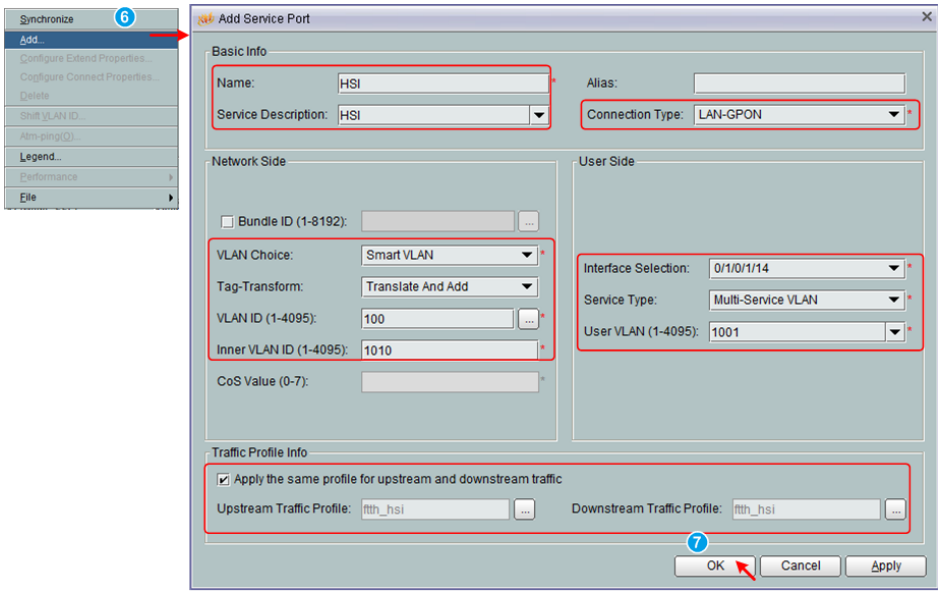






c. **Add a service virtual port on the OLT side.**





Result

Check whether the user successfully gains access to the Internet through dialup on the PC.

1. The LAN1 port of the ONT is connected to the Ethernet port of the PC properly.
2. Dial up on the PC using the PPPoE dialup software.
3. The user gains access to the Internet on the PC after the dialup is successful.

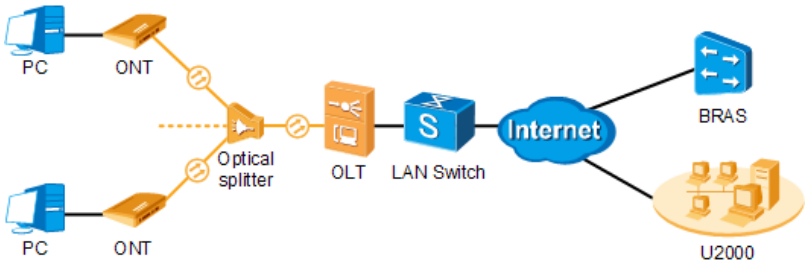
3.3.1.1.2 Configuring the GPON FTTH Layer 3 Internet Access Service on the NMS

This topic describes how to configure the high-speed Internet service when an ONT is connected to an OLT through a GPON port.

Networking

- Users' PCs are connected to the ONT using the LAN ports. IP addresses of users' PCs are allocated by the DHCP IP address pool on the ONT. PPPoE auto dialup is performed on the ONT.
- The ONT is connected to the GPBC card of the OLT through an optical fiber.
- The broadband remote access server (BRAS) provides broadband user access and functions of authentication and accounting.

Figure 3-3 Configuring the GPON FTTH Internet service



Data Plan

Table 3-7 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS ports: Adaptive ● Number of ETH ports: Adaptive ● Number of CATV ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1
VLAN Plan	Double-tagged VLAN ● S-VLAN ID: 100 ● S-VLAN type: Smart ● S-VLAN attribute: Stacking ● C-VLAN ID: 1001 ● C'VLAN ID: 1010 **NOTE** VLAN translation policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.
ONT value-added services (Layer 3 routing)	Profile name: ONT-HSI WAN VLAN ID: 1001 Service type: INTERNET Connection type: Routed Addressing type: PPPoE (User Name: iadtest@pppoe, Password: iadtest) Priority: 0 NAT function: enable Bound port: LAN1 (LAN1 is a Layer 3 LAN)

Procedure

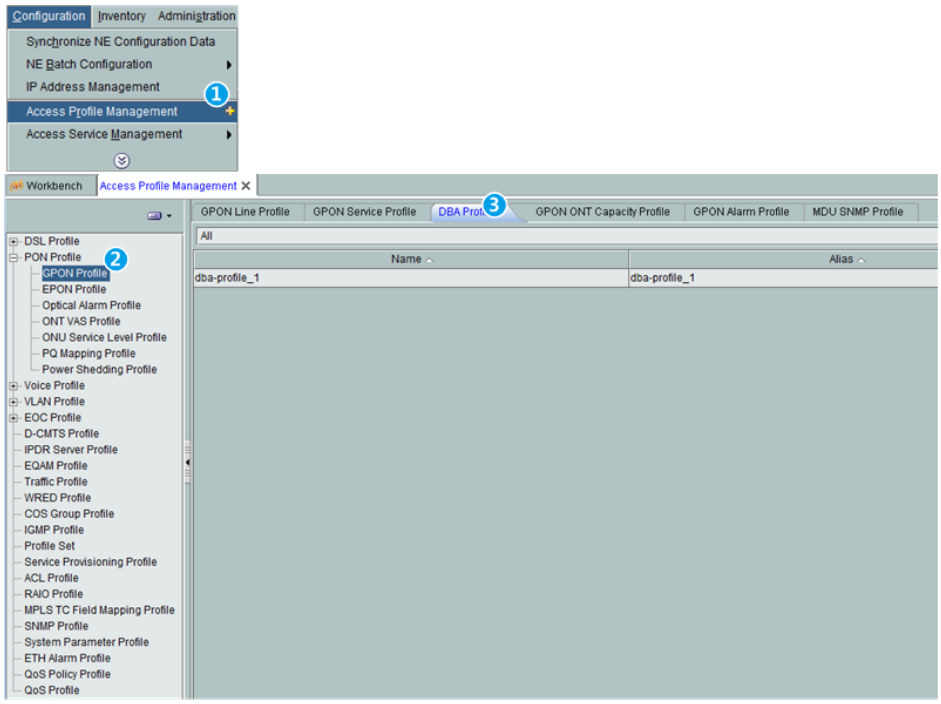
- Implement pre-configurations.

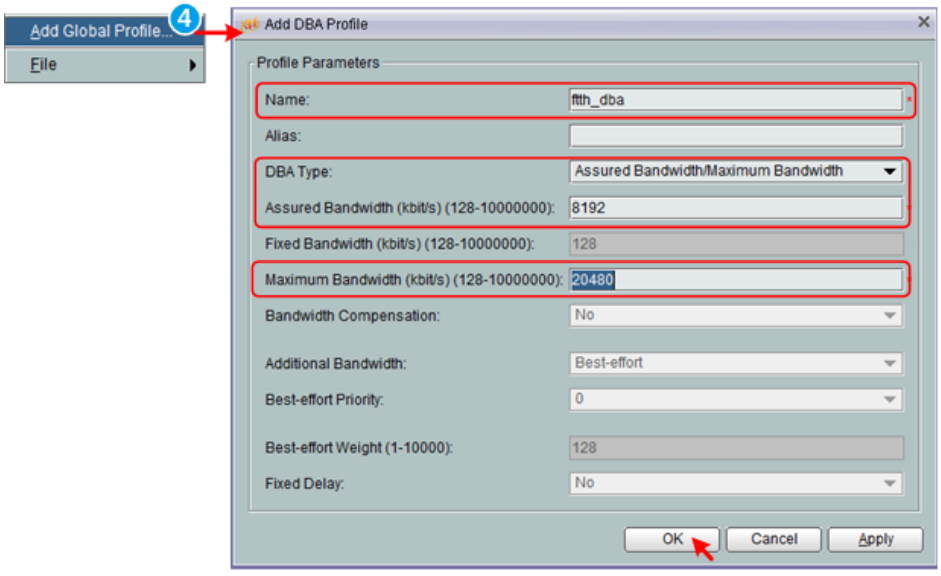
NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

1. **Configure a DBA profile.**

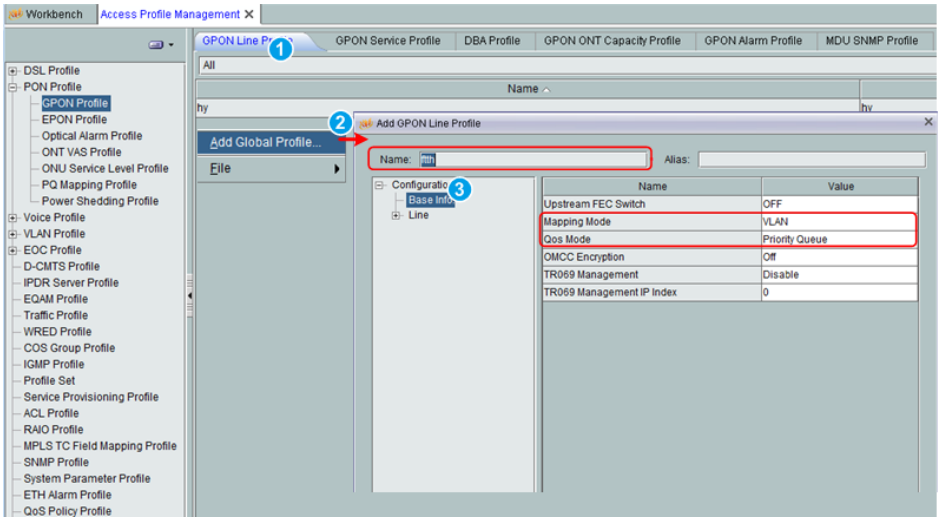


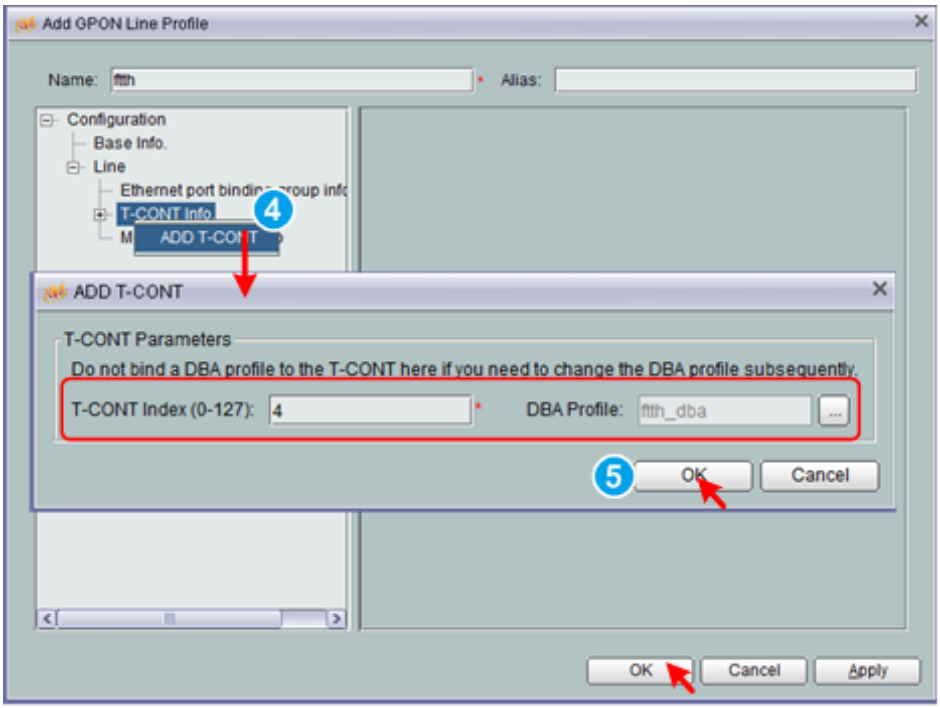


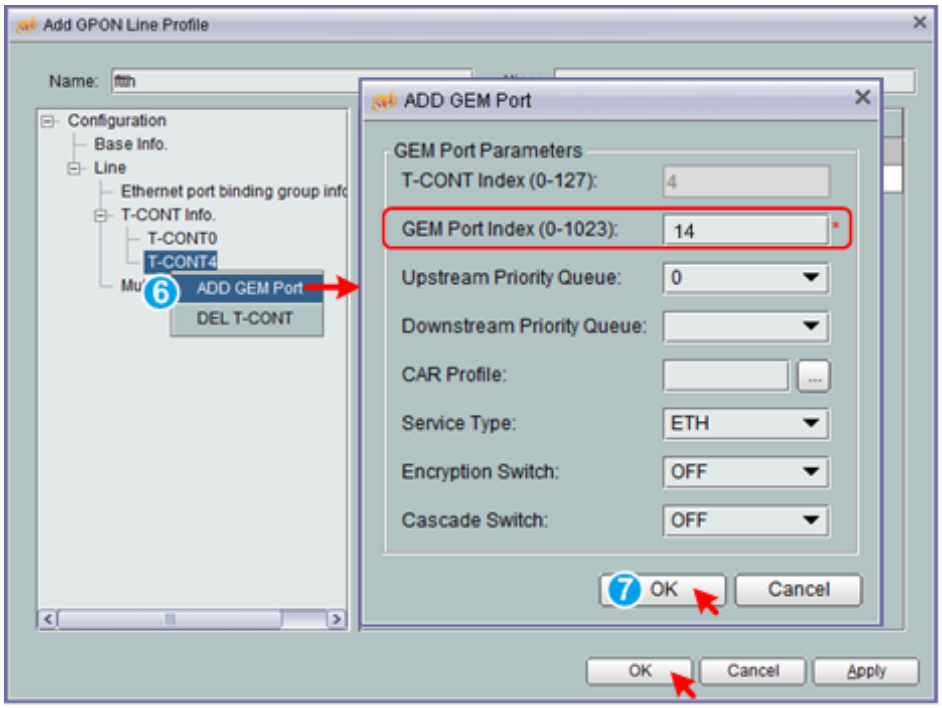
1. **Configure a line profile.**

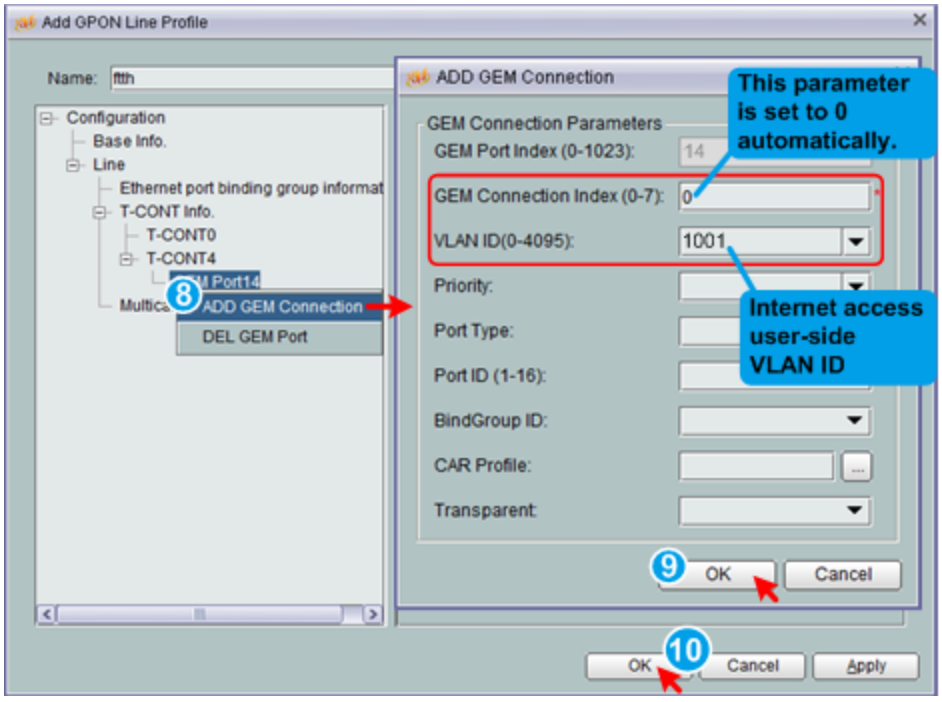
In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 14. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.



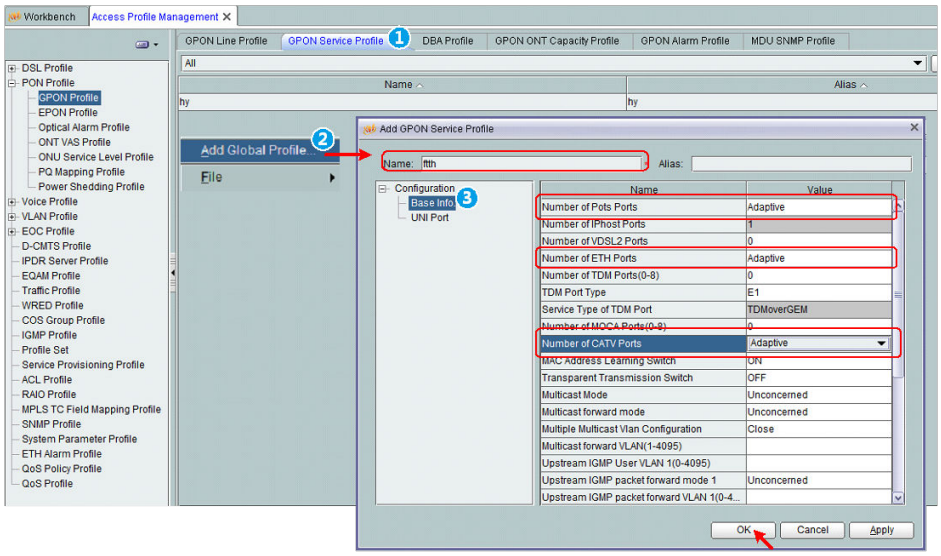






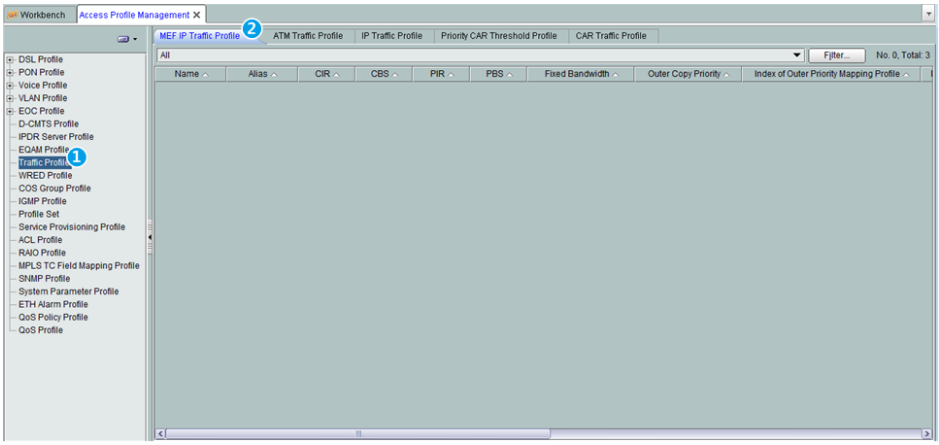
2. **Configure a service profile.**

   Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability.



3. **Configure an MEF IP traffic profile.**

   The profile name is ftth_hsi, CIR is 4 Mbit/s, and the priority is 0. Traffic is scheduled based on the priority specified in the profile.

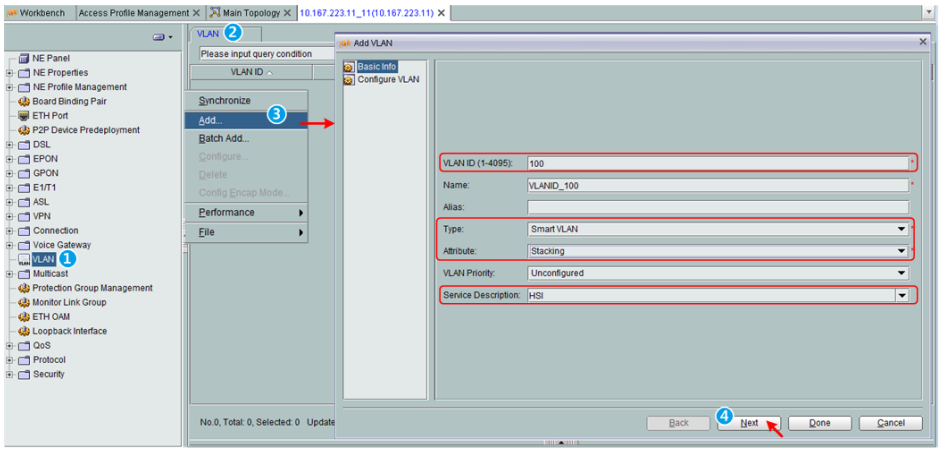


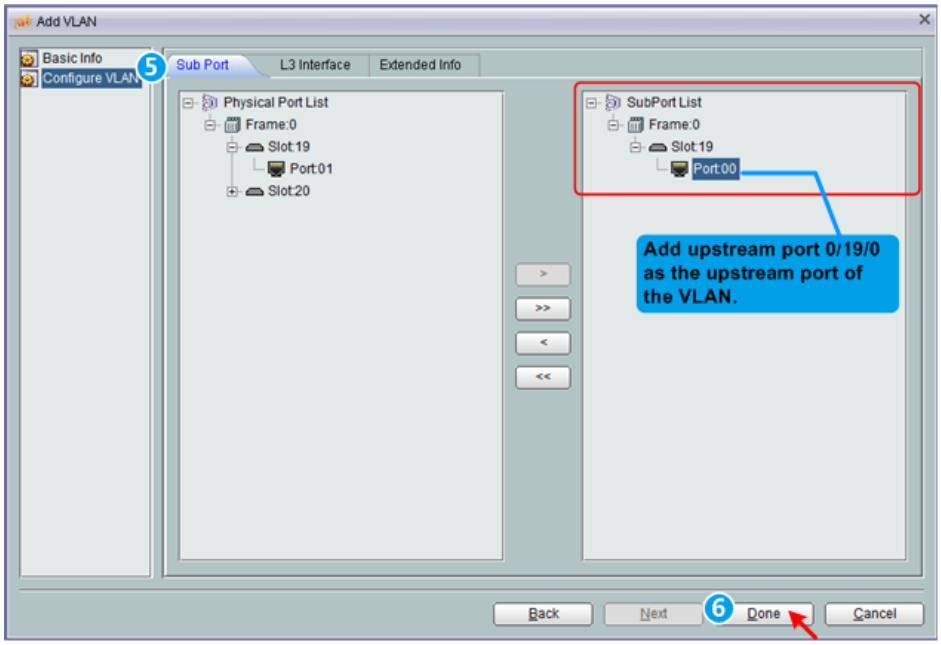
4. **Configure a service VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the

Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

A service VLAN is the VLAN used for the Internet service.

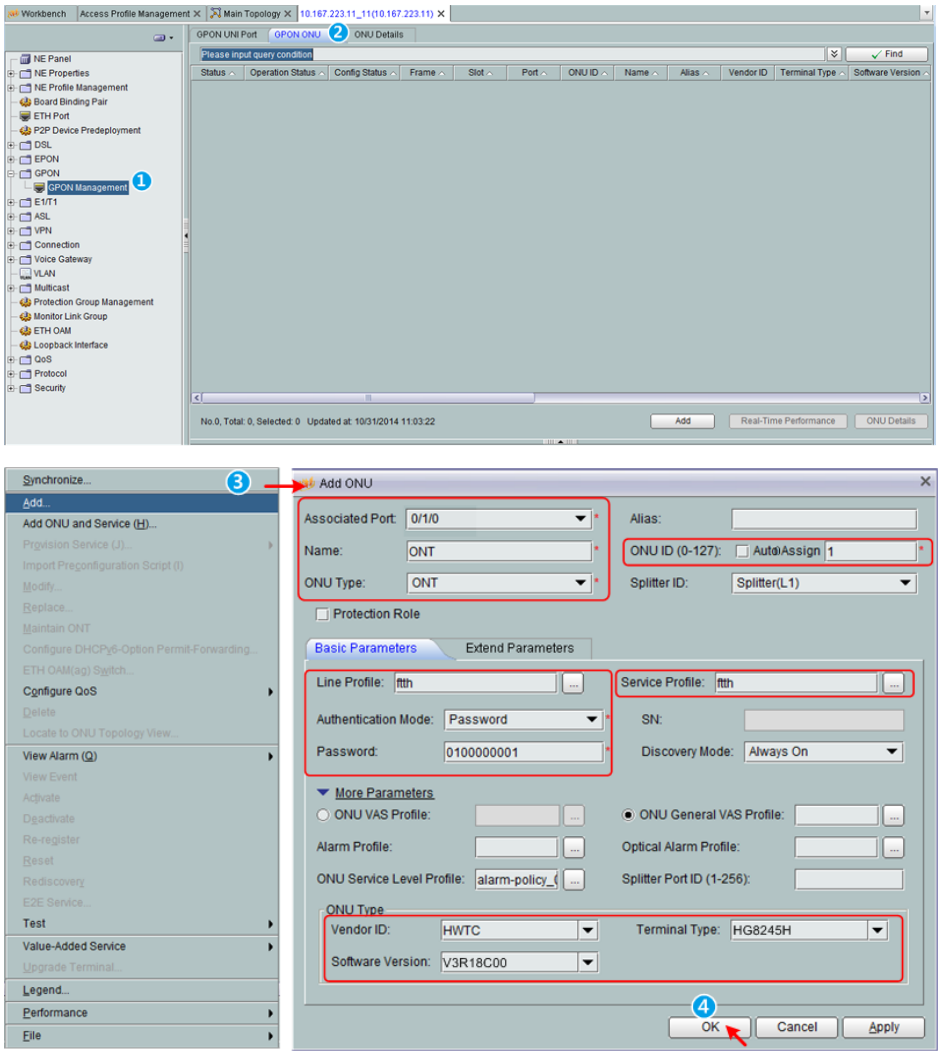




- **Provision services.**

  a. **Add an ONT.**

  The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.

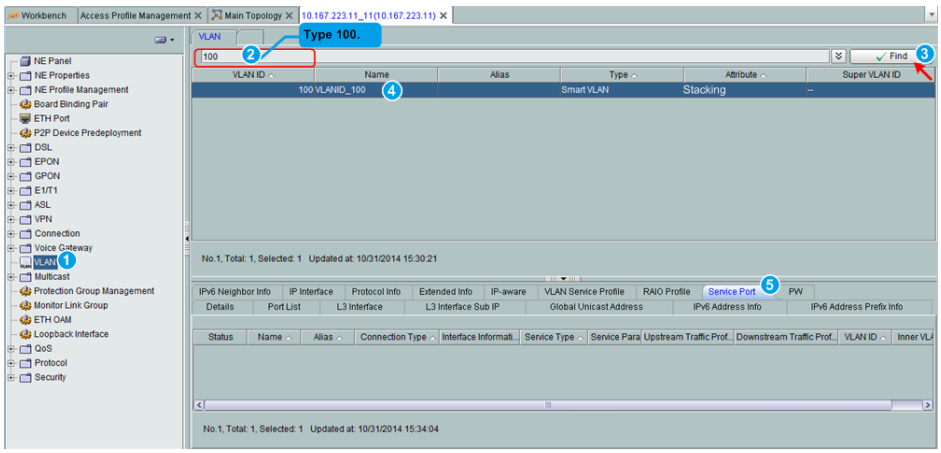


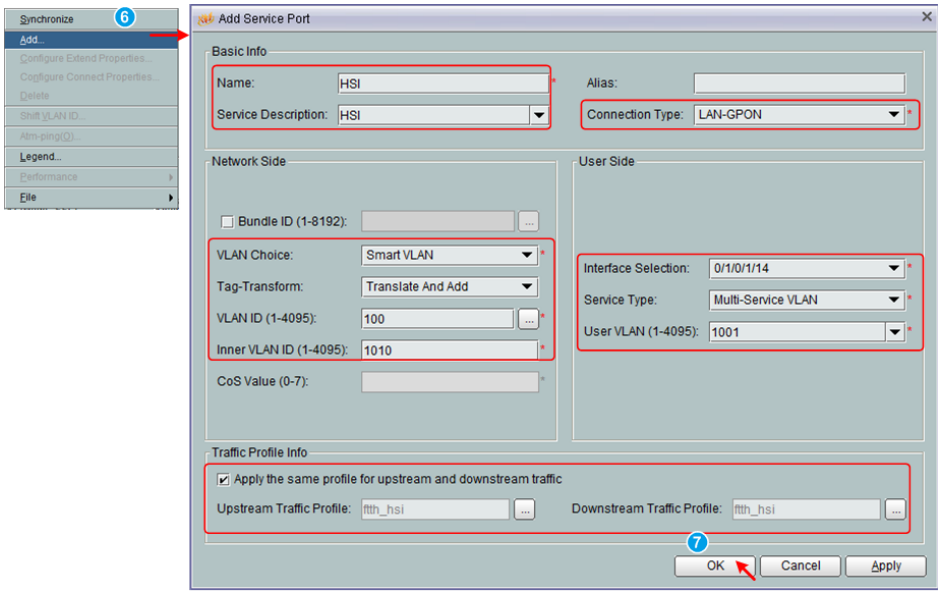
NOTE

HG8245H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

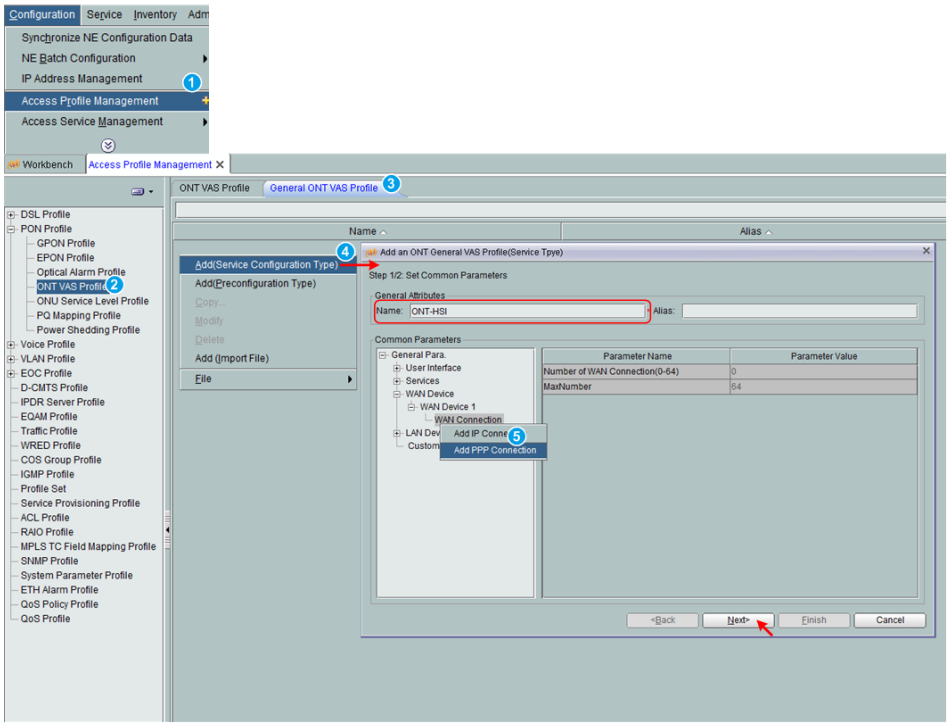
The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

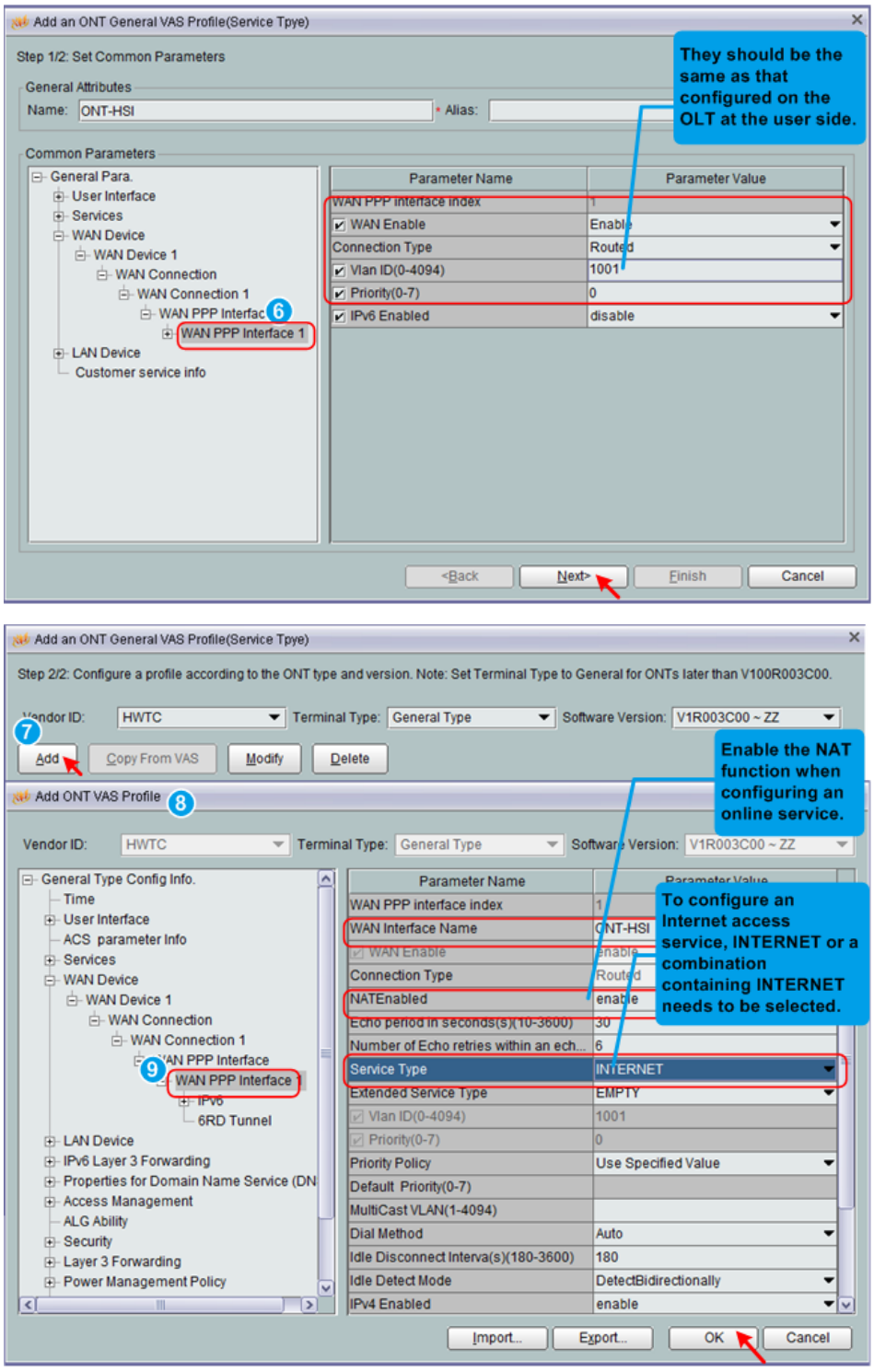
b. **Add a service virtual port on the OLT side.**

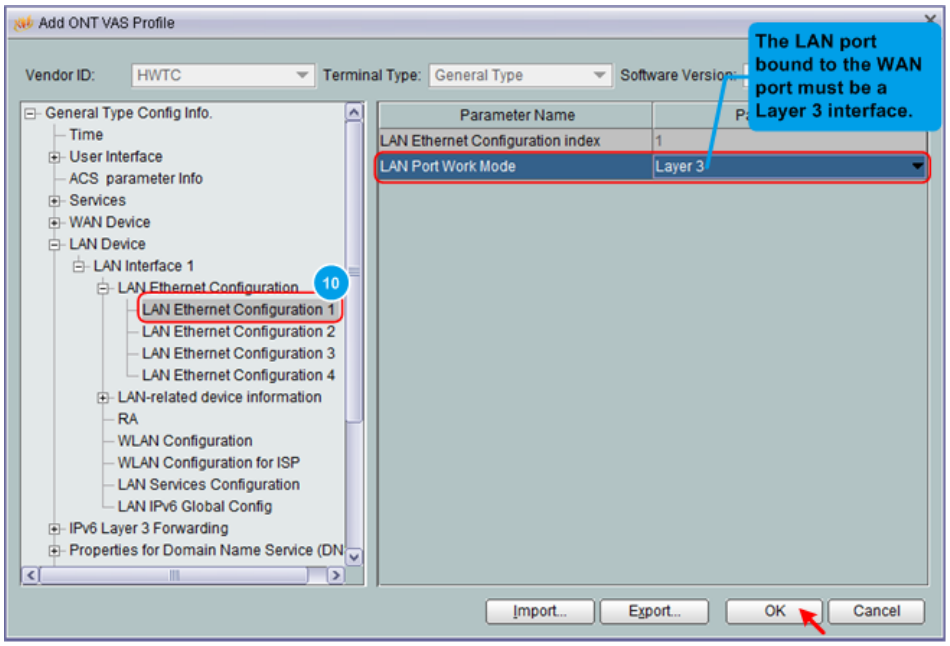


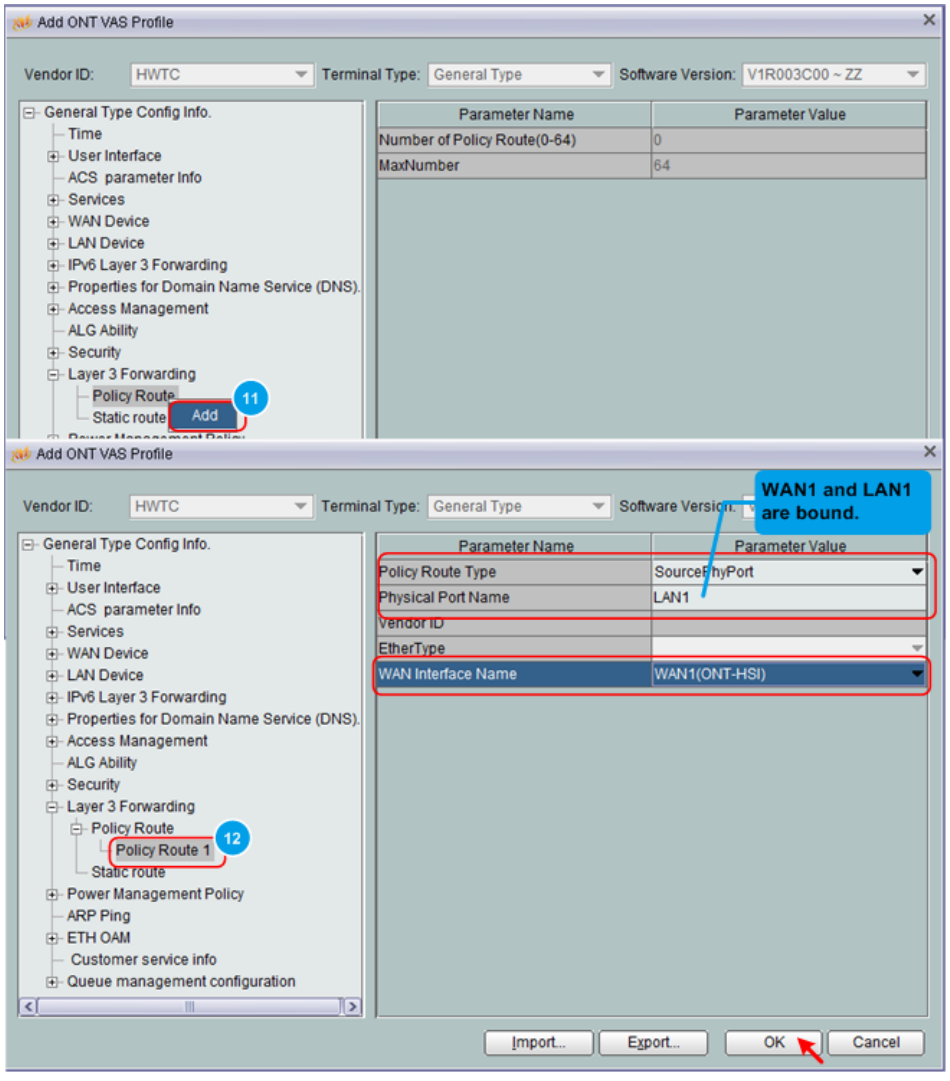


c. **Add a general VAS configuration profile for the ONT.**




Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
They should be the same as that configured on the OLT at the user side.
General Attributes
Name: ONT-HSI
Alias:
Common Parameters
General Para.
User Interface
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interfac
WAN PPP Interface 1
LAN Device
Customer service info
Parameter Name
Parameter Value
WAN PPP interface index
WAN Enable
Enable
Connection Type
Routed
Vlan ID(0-4094)
1001
Priority(0-7)
0
IPv6 Enabled
disable
<Back
Next>
Finish
Cancel
6
Add an ONT General VAS Profile(Service Tpye)
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
7
Add
Copy From VAS
Modify
Delete
Enable the NAT function when configuring an online service.
Add ONT VAS Profile
8
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interface
9
WAN PPP Interface
IPv6
6RD Tunnel
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DN
Access Management
ALG Ability
Security
Layer 3 Forwarding
Power Management Policy
Parameter Name
WAN PPP interface index
WAN Interface Name
ONT-HSI
WAN Enable
Connection Type
Routed
NATEnabled
enable
Echo period in seconds(s)(10-3600)
30
Number of Echo retries within an ech...
6
Service Type
INTERNET
Extended Service Type
EMPTY
Vlan ID(0-4094)
1001
Priority(0-7)
0
Priority Policy
Use Specified Value
Default Priority(0-7)
MultiCast VLAN(1-4094)
Dial Method
Auto
Idle Disconnect Interva(s)(180-3600)
180
Idle Detect Mode
DetectBidirectionally
IPv4 Enabled
enable
To configure an Internet access service, INTERNET or a combination containing INTERNET needs to be selected.
Import...
Export...
OK
Cancel

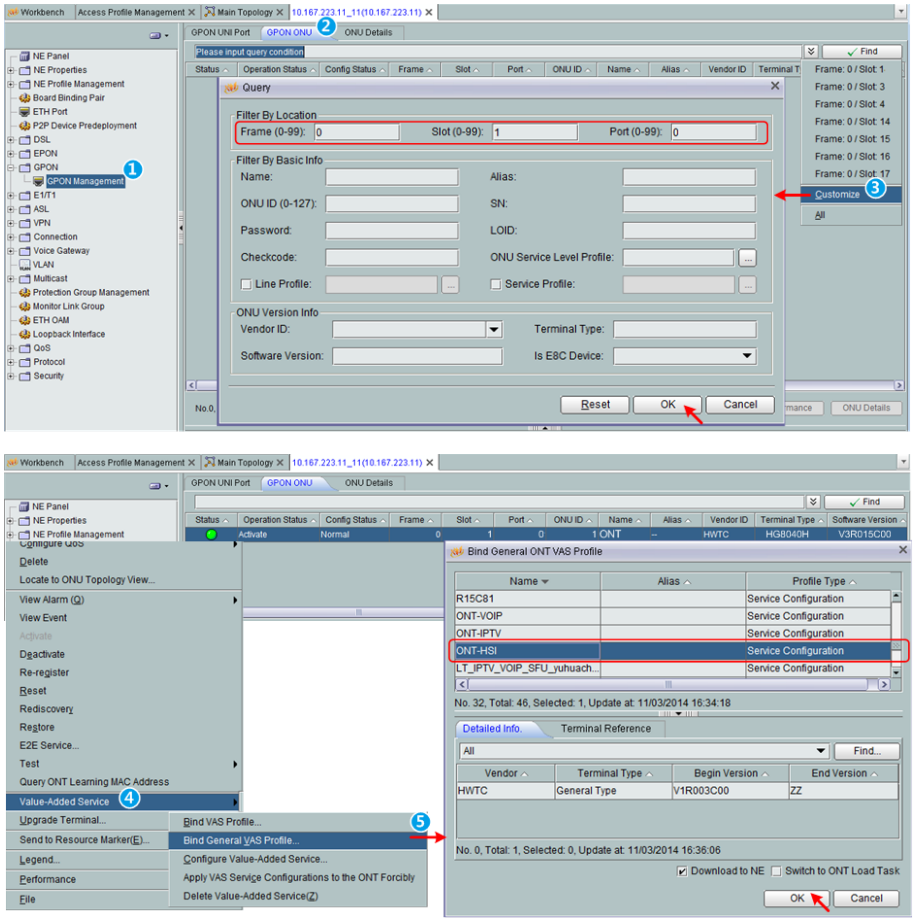

Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version:
The LAN port bound to the WAN port must be a Layer 3 interface.
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
LAN Interface 1
LAN Ethernet Configuration
10
LAN Ethernet Configuration 1
LAN Ethernet Configuration 2
LAN Ethernet Configuration 3
LAN Ethernet Configuration 4
LAN-related device information
RA
WLAN Configuration
WLAN Configuration for ISP
LAN Services Configuration
LAN IPv6 Global Config
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DN
Parameter Name
LAN Ethernet Configuration index
1
LAN Port Work Mode
Layer 3
Import...
Export...
OK
Cancel


Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DNS)
Access Management
ALG Ability
Security
Layer 3 Forwarding
Policy Route
Static route
Add
11
Parameter Name
Parameter Value
Number of Policy Route(0-64)
0
MaxNumber
64
Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version:
WAN1 and LAN1 are bound.
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DNS)
Access Management
ALG Ability
Security
Layer 3 Forwarding
Policy Route
Policy Route 1
12
Static route
Power Management Policy
ARP Ping
ETH OAM
Customer service info
Queue management configuration
Parameter Name
Parameter Value
Policy Route Type
SourcePhyPort
Physical Port Name
LAN1
Vendor ID
EtherType
WAN Interface Name
WAN1(ONT-HSI)
Import...
Export...
OK
Cancel

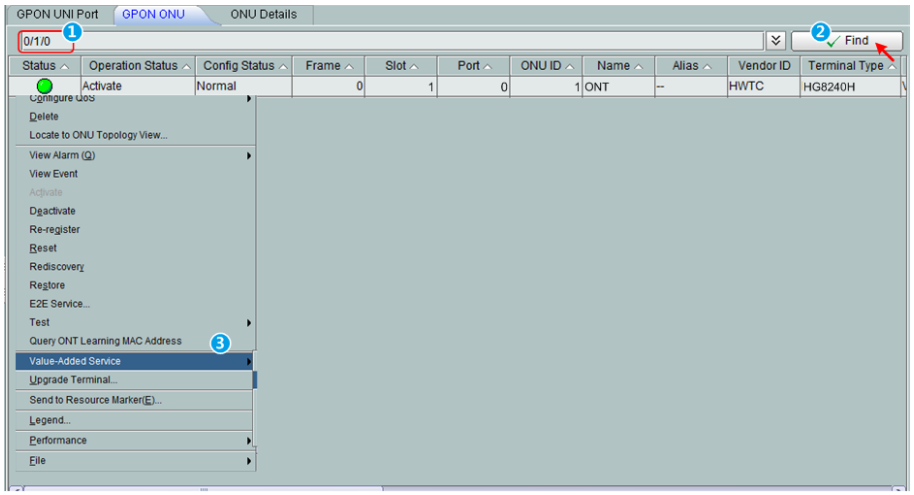
NOTE

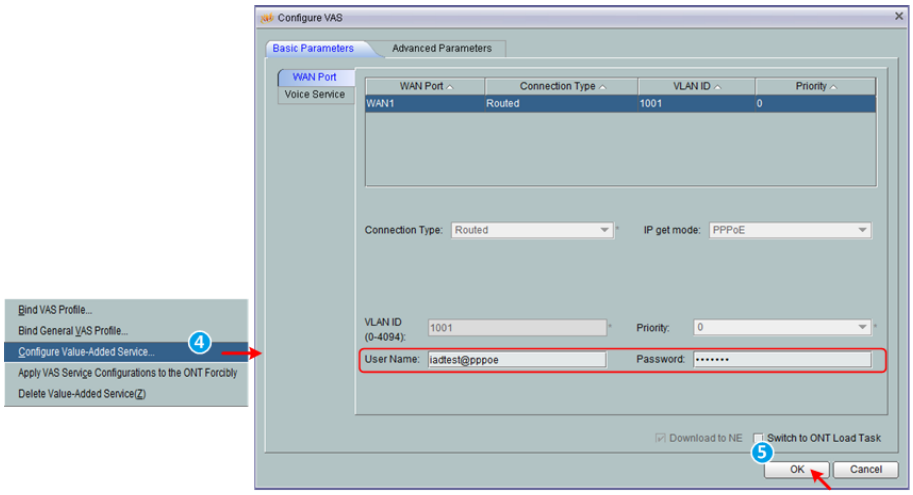
To bind a WAN port to multiple LAN ports, set **Physical Port Name** to **LAN1,...,LANx**. For example, to bind WAN 1 to LAN 1 and LAN 2, set **Physical Port Name** to **LAN1, LAN2**.

d. **Bind a general VAS profile.**



e. **Configure the ONT value-added service.**





NOTE

The **User Name** and **Password** must be the same as those configured on the BRAS.

Result

Check whether the user successfully gains access to the Internet through dialup on the PC.

1. The LAN1 port of the ONT is connected to the Ethernet port of the PC properly.
2. After the PC is configured to obtain its IP addresses automatically, the PC can obtain an IP address allocated by the ONT using DHCP.
3. After automatic PPPoE dialup is performed successfully on the ONT, users can access the Internet.

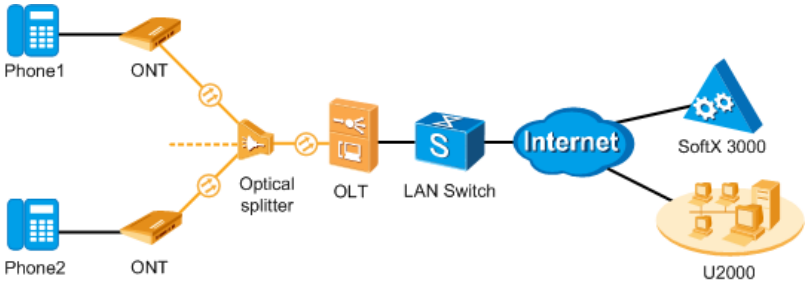
3.3.1.1.3 Configuring the GPON FTTH Voice Service (H.248 Protocol) on the NMS

This topic describes how to configure the voice service when an ONT is connected to an OLT through a GPON port.

Networking

- The phones connected to different ONTs can communicate with each other.
- The ONT obtains an IP address in Dynamic Host Configuration Protocol (DHCP) mode.

Figure 3-4 Configuring the GPON FTTH voice service (H.248 protocol)



Data Plan

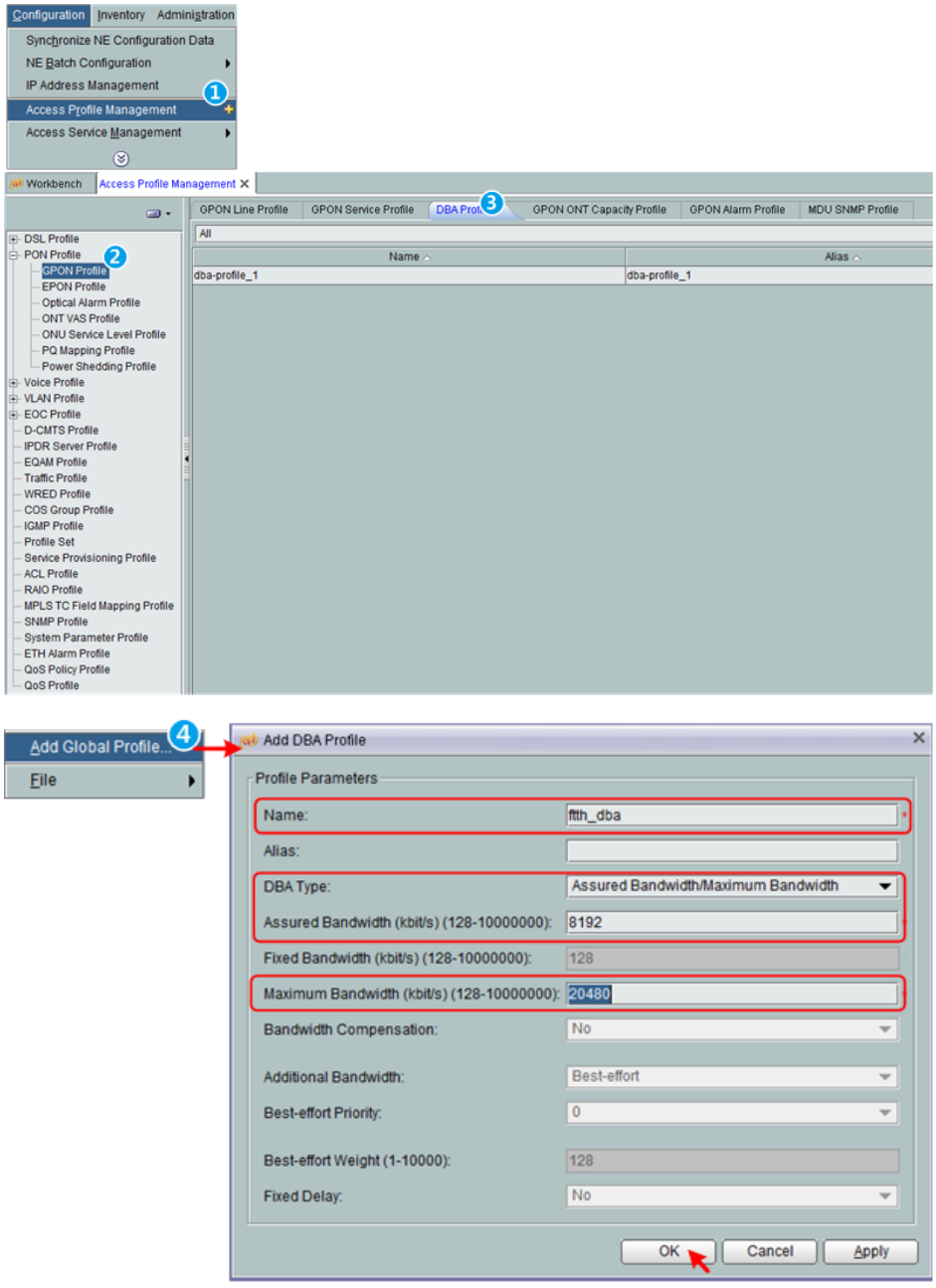
Table 3-8 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for voice services: 12
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1
VLAN plan	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: smart ● S-VLAN attribute: common ● C-VLAN=S-VLAN **NOTE** VLAN translation policy: ● ONT: uses the same VLAN configurations and adds C-VLAN tags to packets. All ONTs use the same C-VLAN. ● OLT: transparently transmits VLAN (C-VLAN is the same as the planned S-VLAN).
ONT value-added services	Profile Name: ONT-VoIP WAN VLAN ID: 300 Service Type: VoIP Connection Type: Routed Priority: 5 Signaling Protocol: H.248 IP address of the MGC server: 10.10.100.10/24 Port ID of the MGC server: 2944 MID Format: Domain name MG Domain name: 0100000001 TID: A0 and A1

Procedure

- **Implement pre-configurations.**

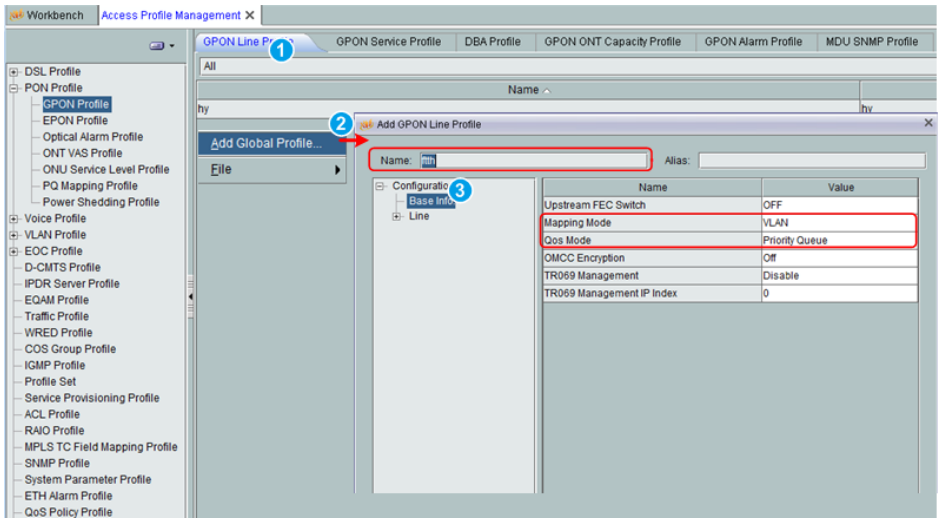
  a. **Configure a DBA profile.**

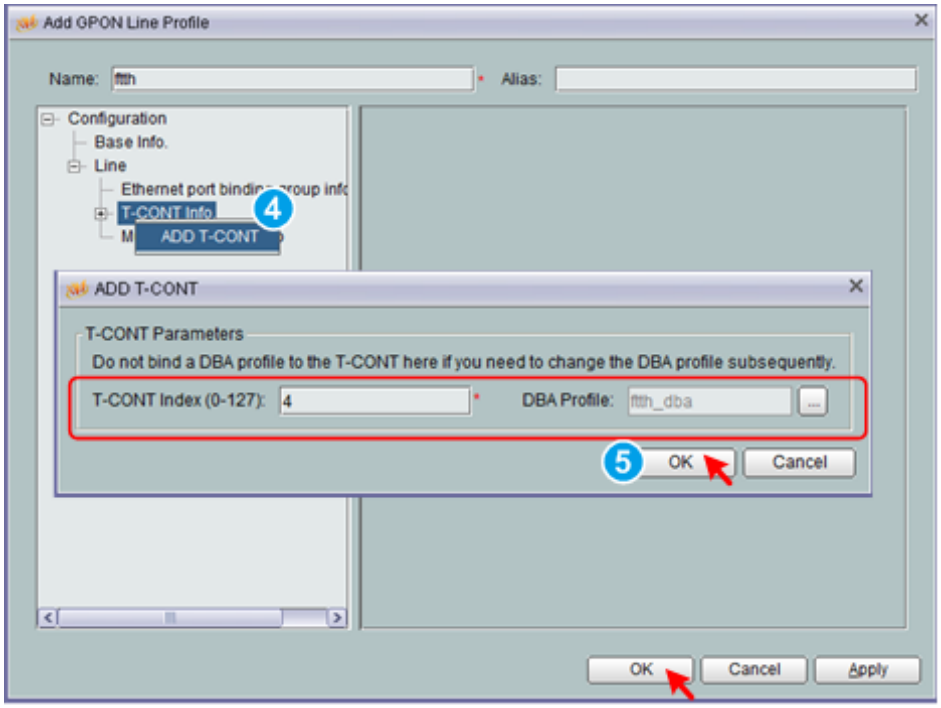


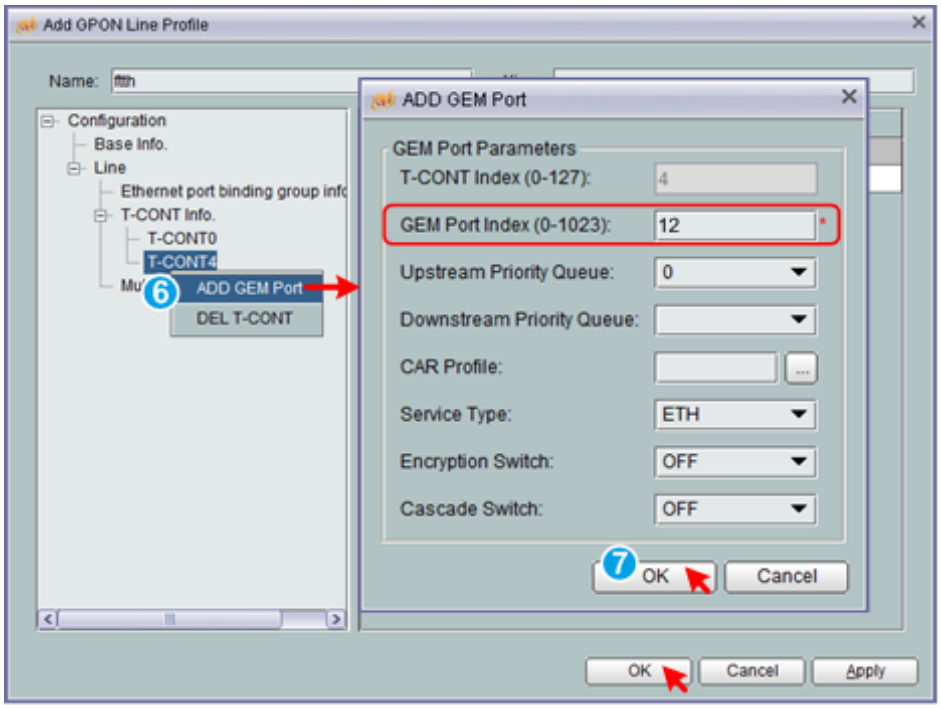
  b. **Configure a line profile.**

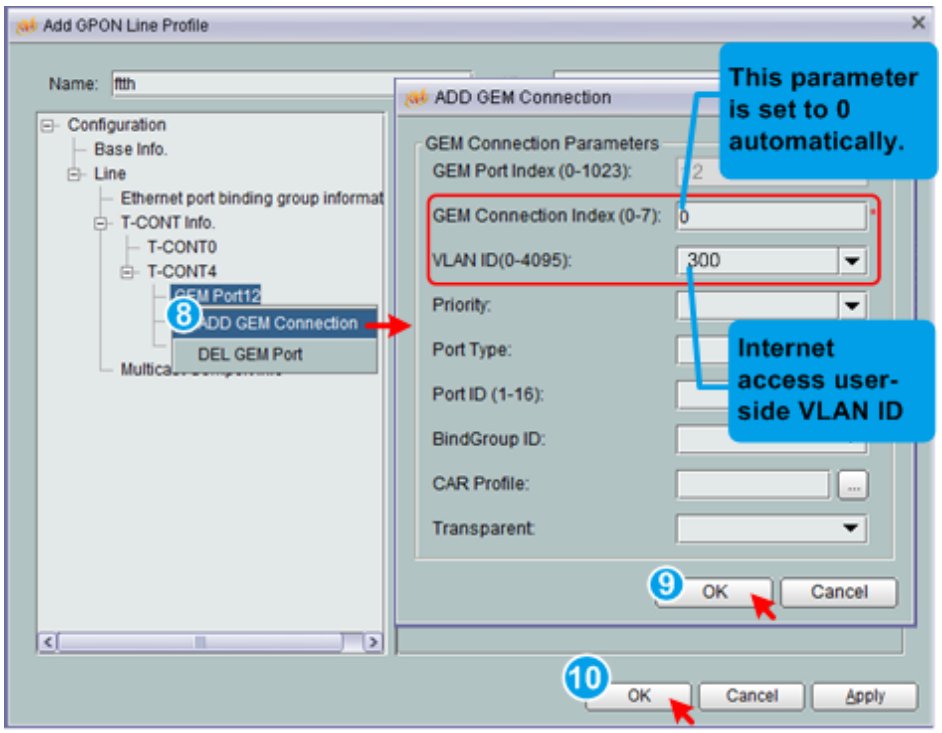
  In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

  In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 12. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.


Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
Add Global Profile...
File
Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
Name
Value
Upstream FEC Switch
OFF
Mapping Mode
VLAN
Qos Mode
Priority Queue
OMCC Encryption
Off
TR069 Management
Disable
TR069 Management IP Index
0
1
2
3

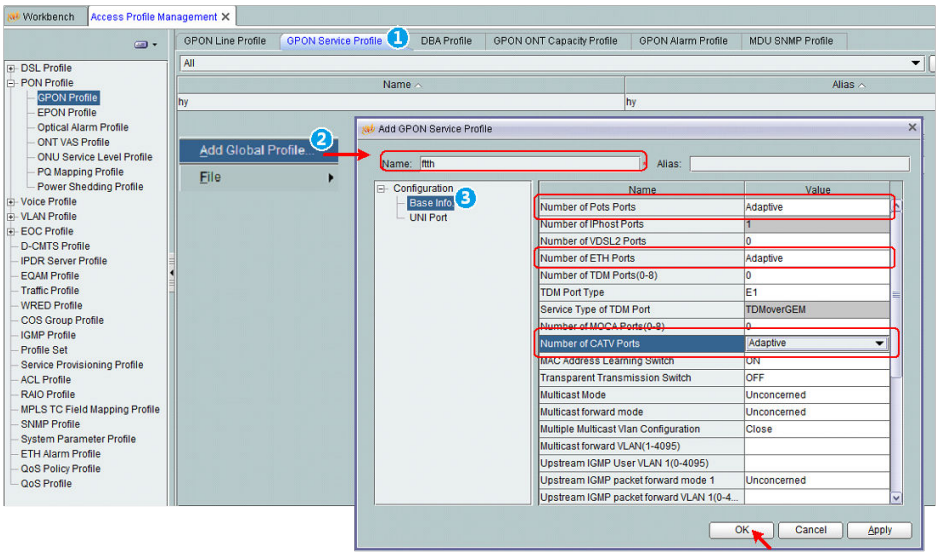

Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
T-CONT Info
ADD T-CONT
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127):
DBA Profile:
5
OK
Cancel
OK
Cancel
Apply





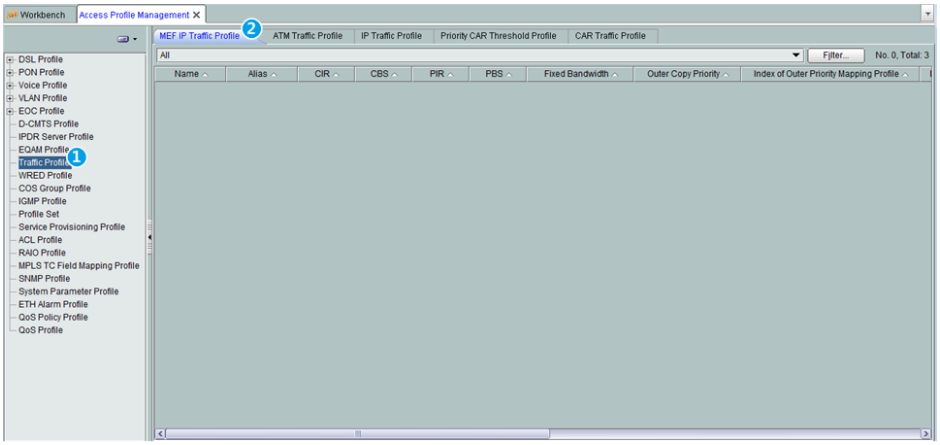
c. **Configure a service profile.**

Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability.



d. **Configure an MEF IP traffic profile.**

The profile name is ftth_voip, upstream/downstream traffic rate is not limited, and the priority is 5. Traffic is scheduled based on the priority specified in the profile.

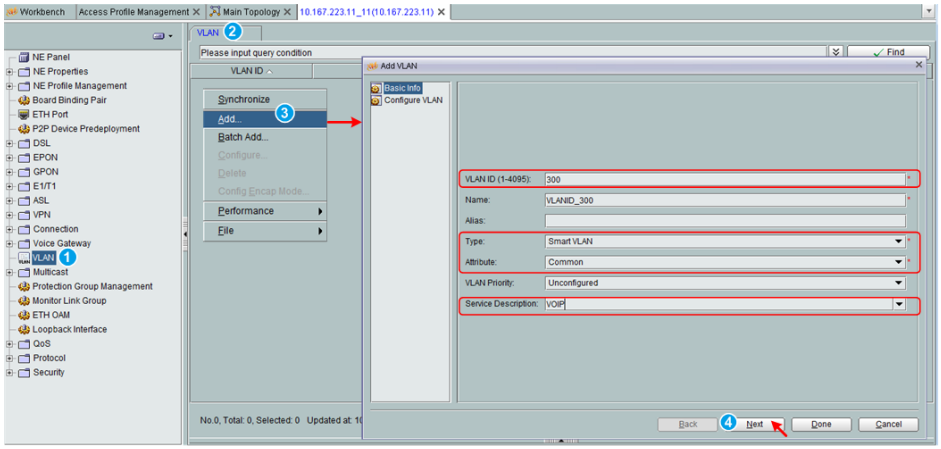


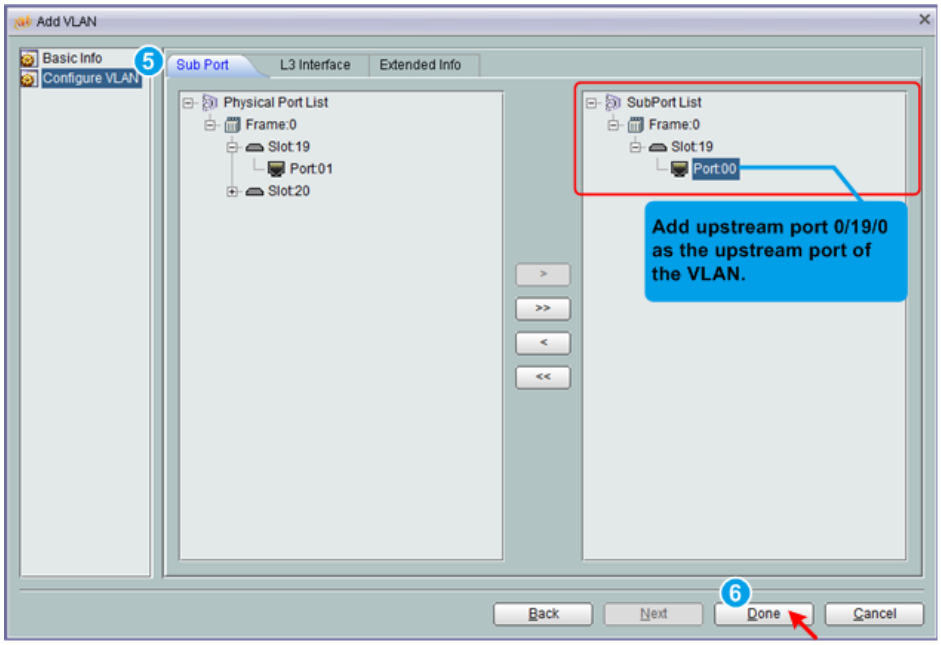
e. **Configure an S-VLAN on the OLT side.**

The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as

follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

The S-VLAN is used for the voice service.

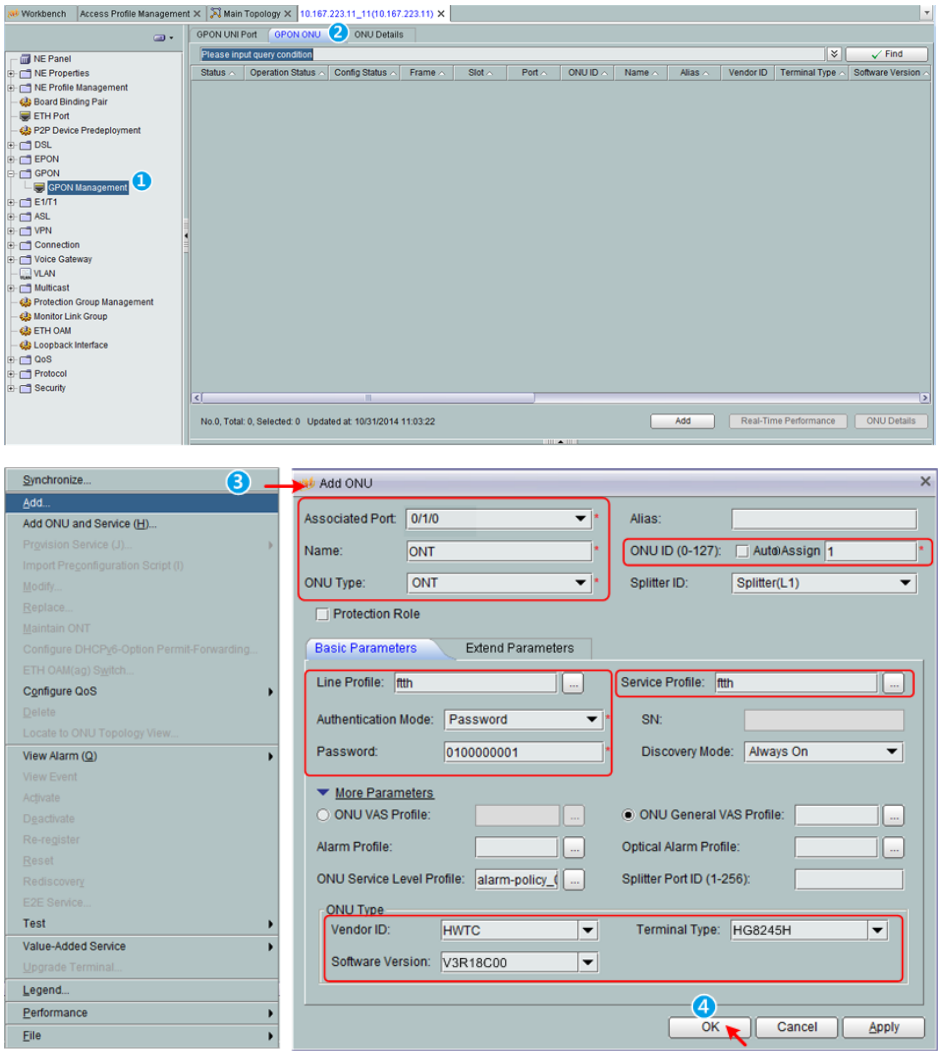




- **Provision services.**

  a. **Add an ONT.**

  The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.

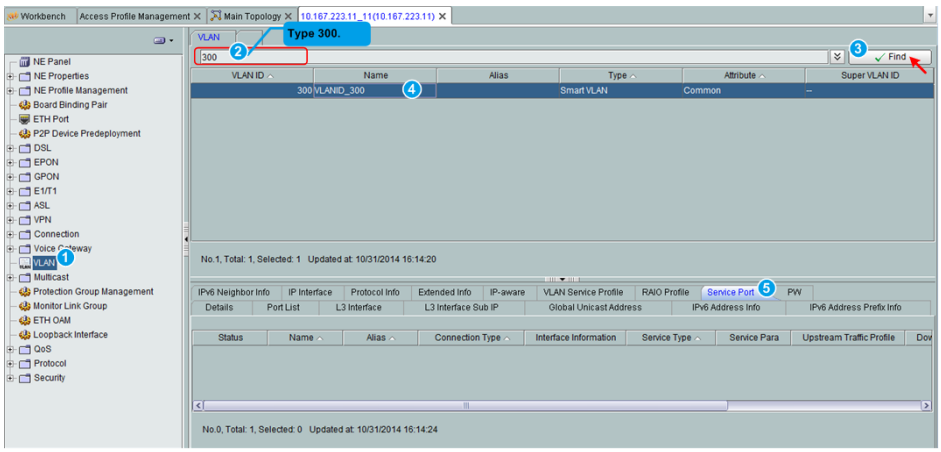


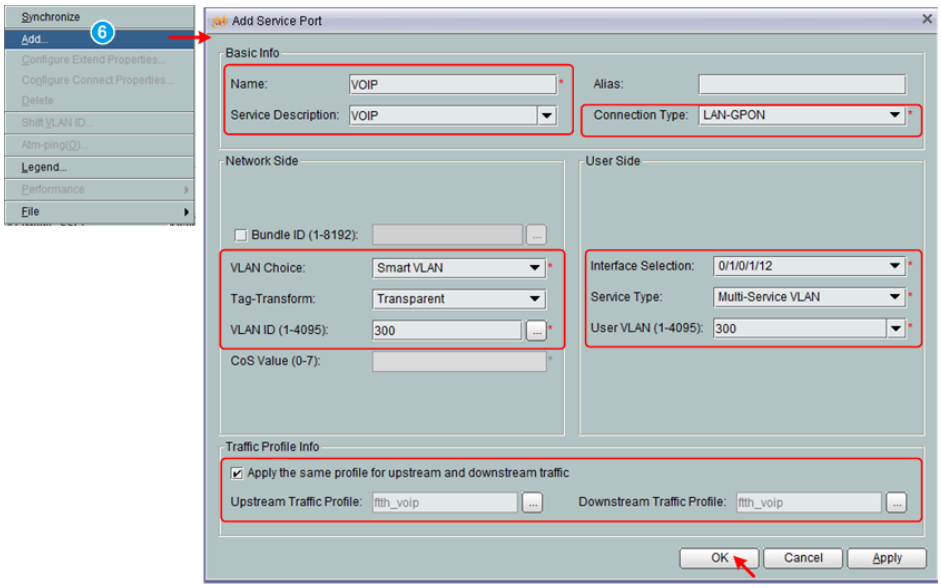
NOTE

HG8245H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

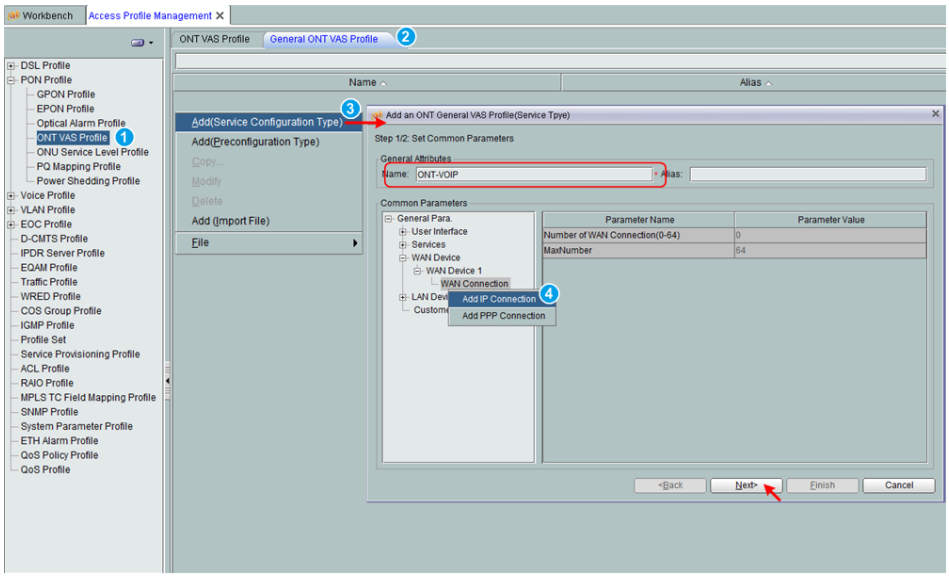
The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

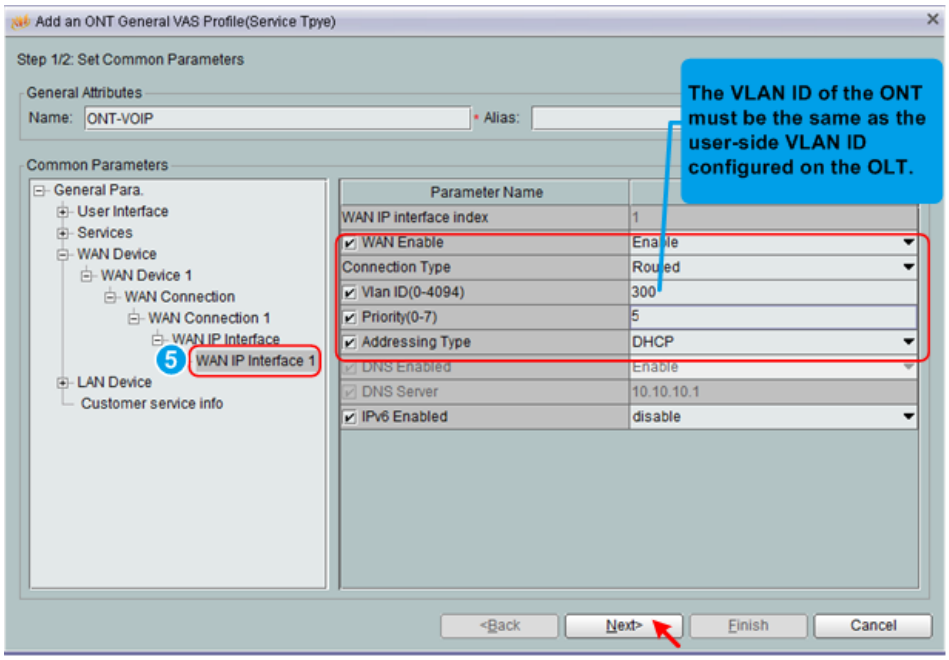
b. **Add a service port on the OLT side.**

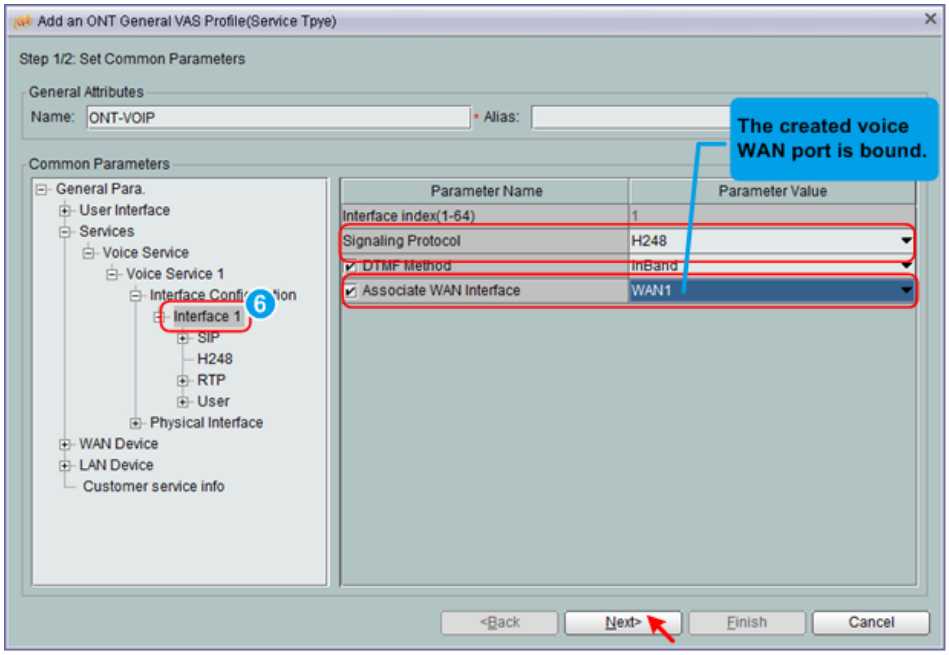


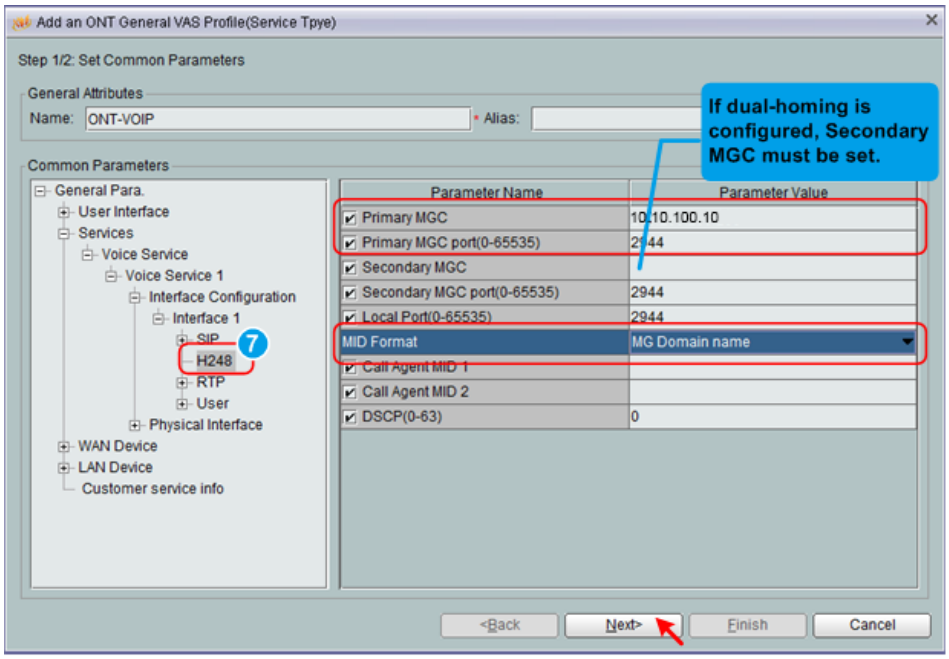


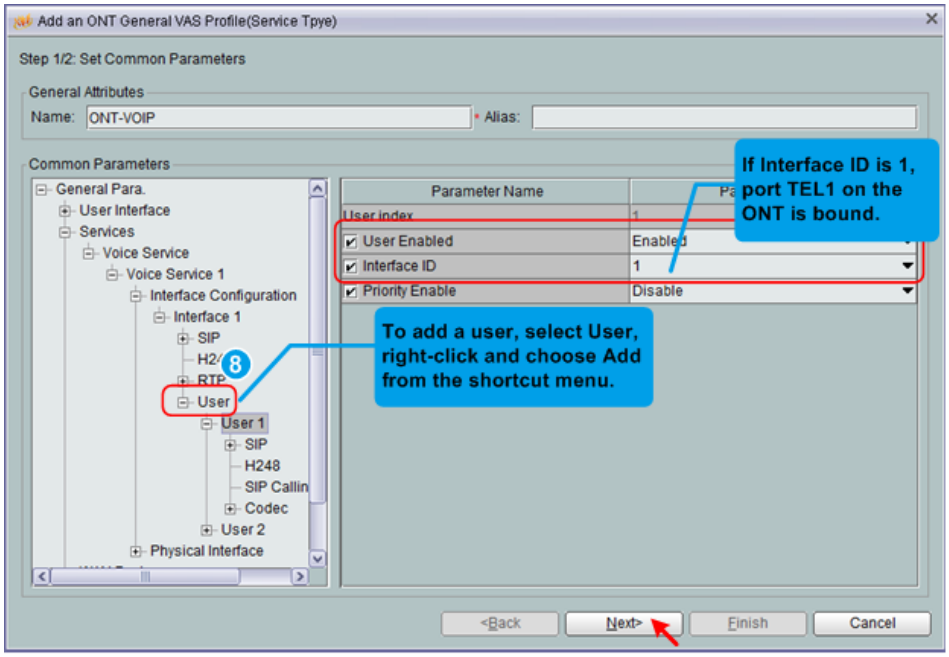
c. **Configure and bind a general value-added service (VAS) profile for the ONT.**

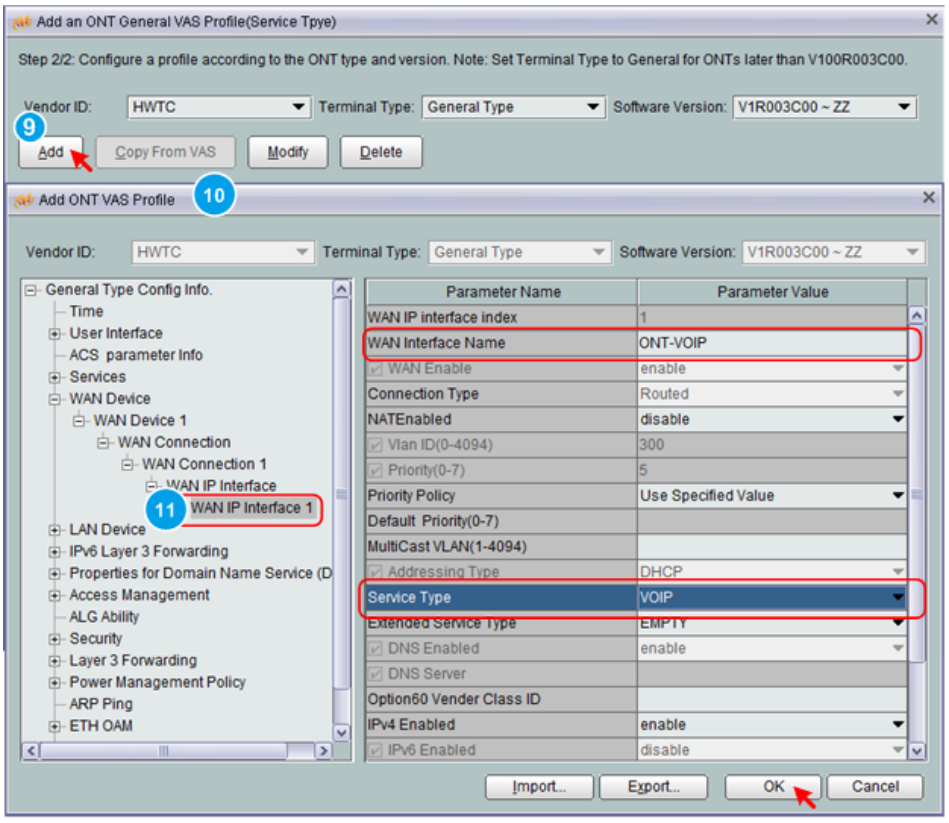



Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN IP Interface
5
WAN IP Interface 1
LAN Device
Customer service info
Parameter Name
WAN IP interface index
WAN Enable
Connection Type
Vlan ID(0-4094)
Priority(0-7)
Addressing Type
DNS Enabled
DNS Server
IPv6 Enabled
1
Enable
Routed
300
5
DHCP
Enable
10.10.10.1
disable
The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.
<Back
Next>
Finish
Cancel


Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
Voice Service
Voice Service 1
Interface Confi ion
6
Interface 1
SIP
H248
RTP
User
Physical Interface
WAN Device
LAN Device
Customer service info
Parameter Name
Parameter Value
Interface index(1-64)
Signaling Protocol
DTMF Method
Associate WAN Interface
1
H248
inBand
WAN1
The created voice WAN port is bound.
<Back
Next>
Finish
Cancel



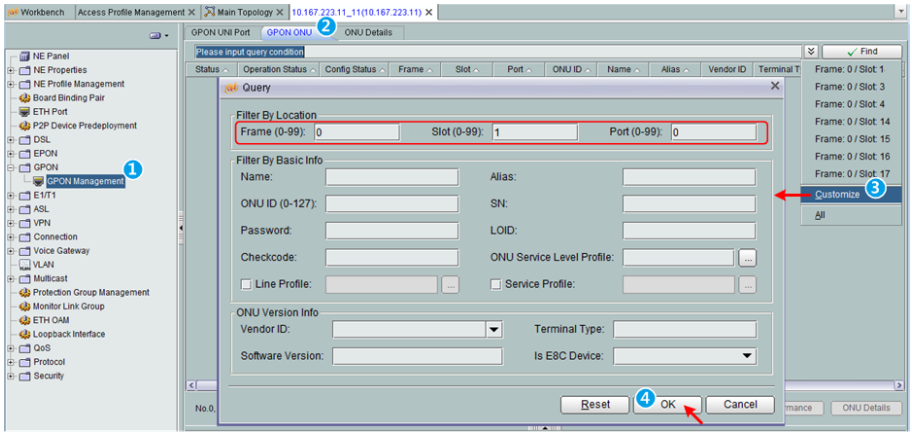


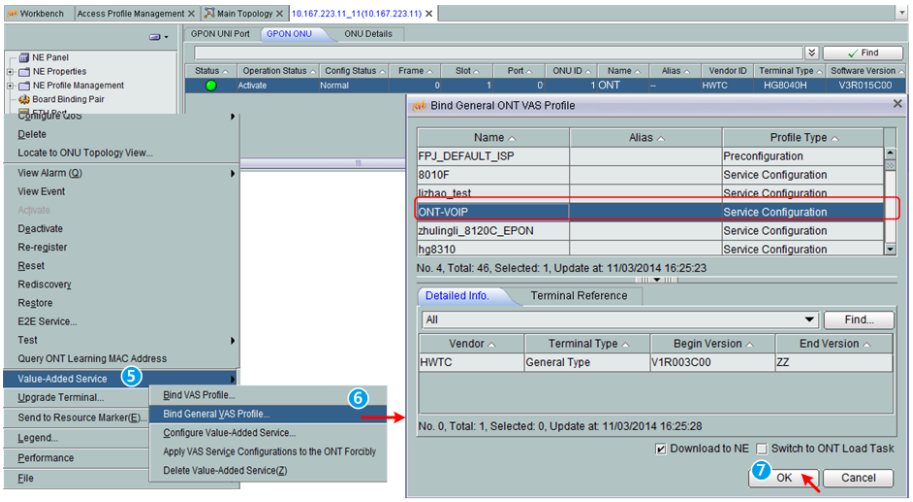


NOTE

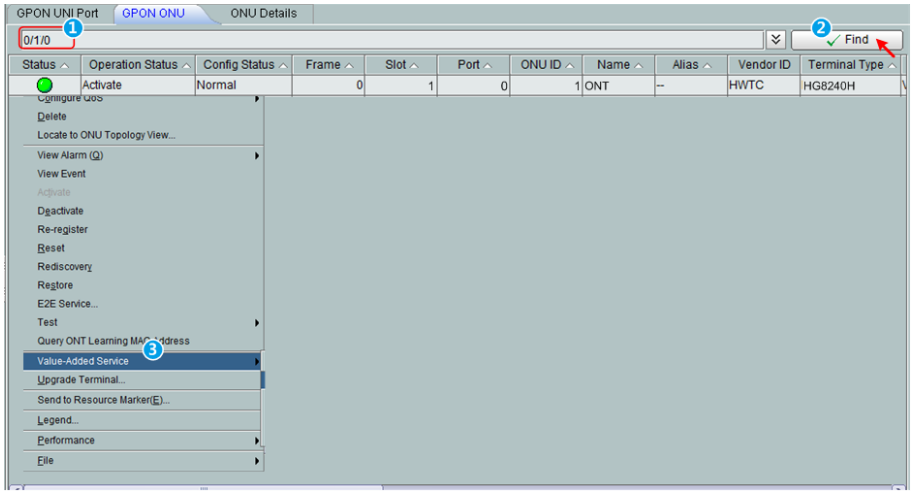
If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default. Create a WAN port named **WAN-RTP** on the ONT, and set this WAN port to a media WAN port. Specifically, choose **Interface 1** > **RTP** and set **Associate WAN Interface** to **WAN2**.

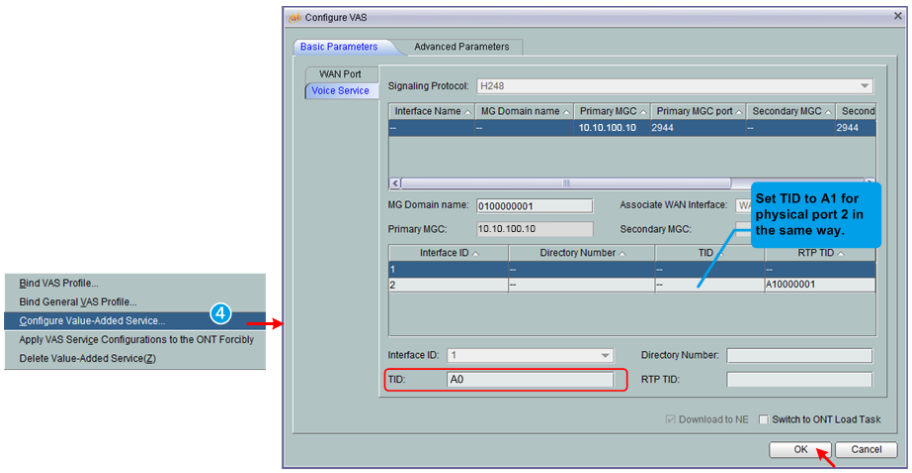
d. **Bind a general VAS profile.**





e. **Configure the ONT VAS service.**





NOTE

Domain Name is ONT's domain name registered with the MGC. It is globally unique. **MG Domain Name** in this example is ONT's password.

Pay attention to the RTP TID configuration when the ONT is interconnected with a softswitch of other vendors. The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.

Do not configure **Directory Number**.

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

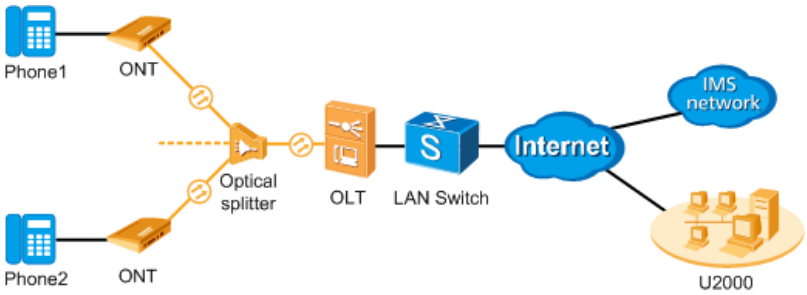
3.3.1.1.4 Configuring the GPON FTTH Voice Service (SIP Protocol) on the NMS

This topic describes how to configure the voice service when an ONT is connected to an OLT through a GPON port.

Networking

- The phones connected to different ONTs can communicate with each other.
- The ONT obtains an IP address in Dynamic Host Configuration Protocol (DHCP) mode.

Figure 3-5 Configuring the GPON FTTH voice service (SIP protocol)



Data Plan

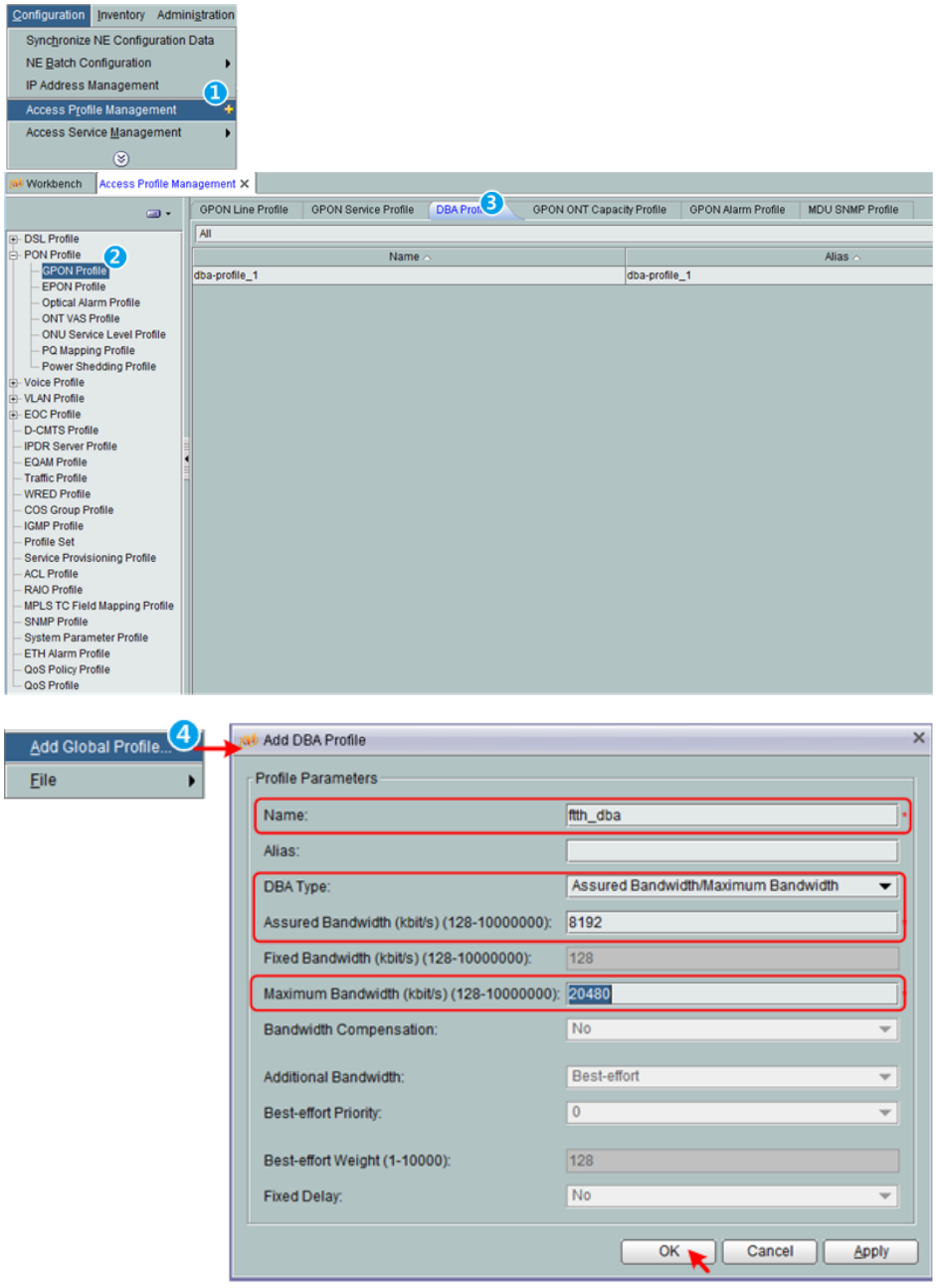
Table 3-9 Data plan

Item	Data
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for voice services: 12
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1
VLAN Plan	Single VLAN tag ● S-VLAN ID: 300 ● S-VLAN type: Smart ● S-VLAN attribute: Common ● C-VLAN=S-VLAN **NOTE** VLAN translation policy: ● ONT: uses the same VLAN configurations and adds C-VLAN tags to packets. All ONTs use the same C-VLAN. ● OLT: transparently transmits VLAN (C-VLAN is the same as the planned S-VLAN).
ONT value-added services	Profile Name: ONT-VoIP WAN VLAN ID: 300 Service Type: VoIP Connection Type: Routed Priority: 5 IP address of the SIP server: 10.10.100.10/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010; Auth User Name is +8675577730010@huawei.com; Auth Password is iadtest1 User phone number 2: 77730020; Auth User Name is +8675577730020@huawei.com; Auth Password is iadtest2

Procedure

- **Implement pre-configurations.**

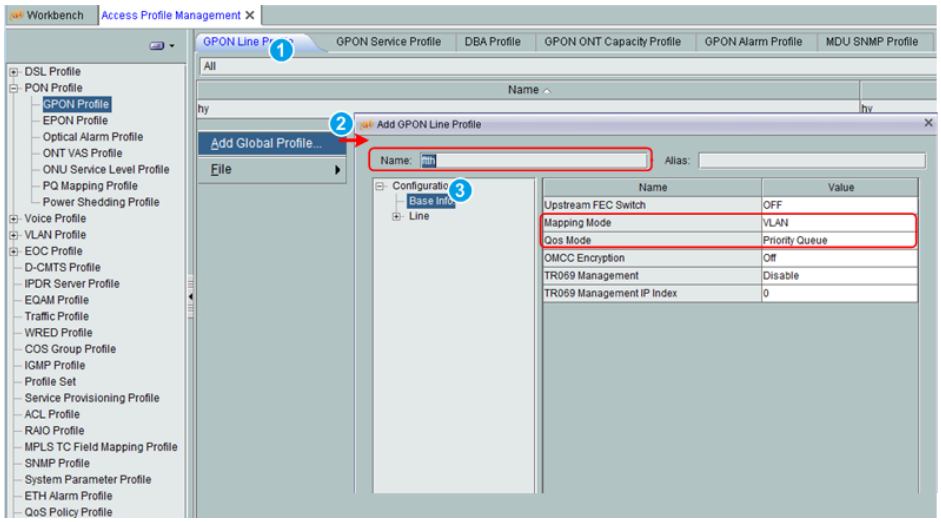
  a. **Configure a DBA profile.**

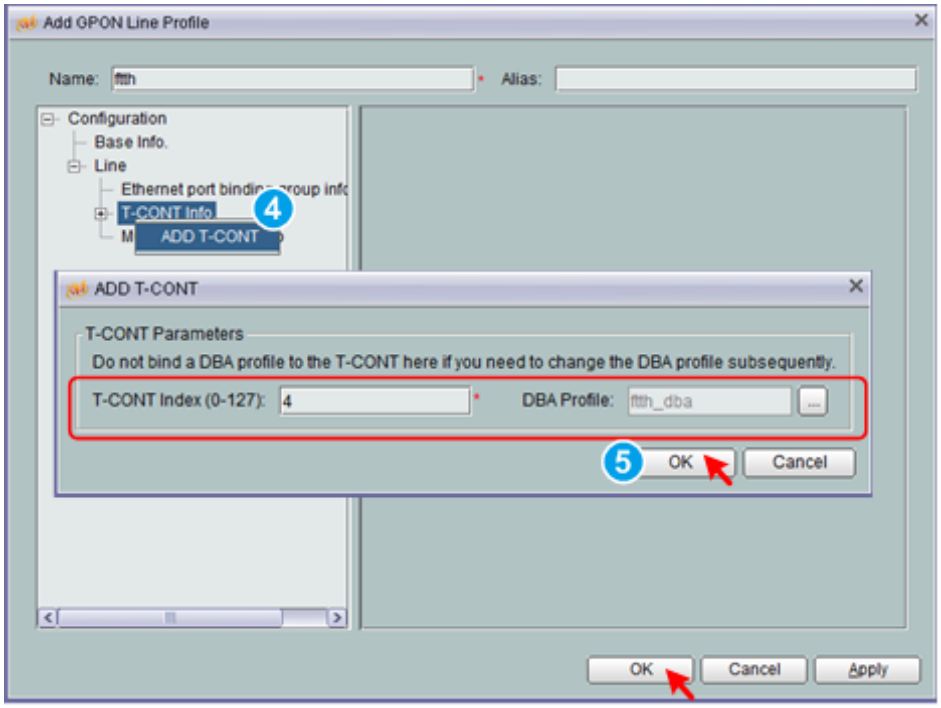


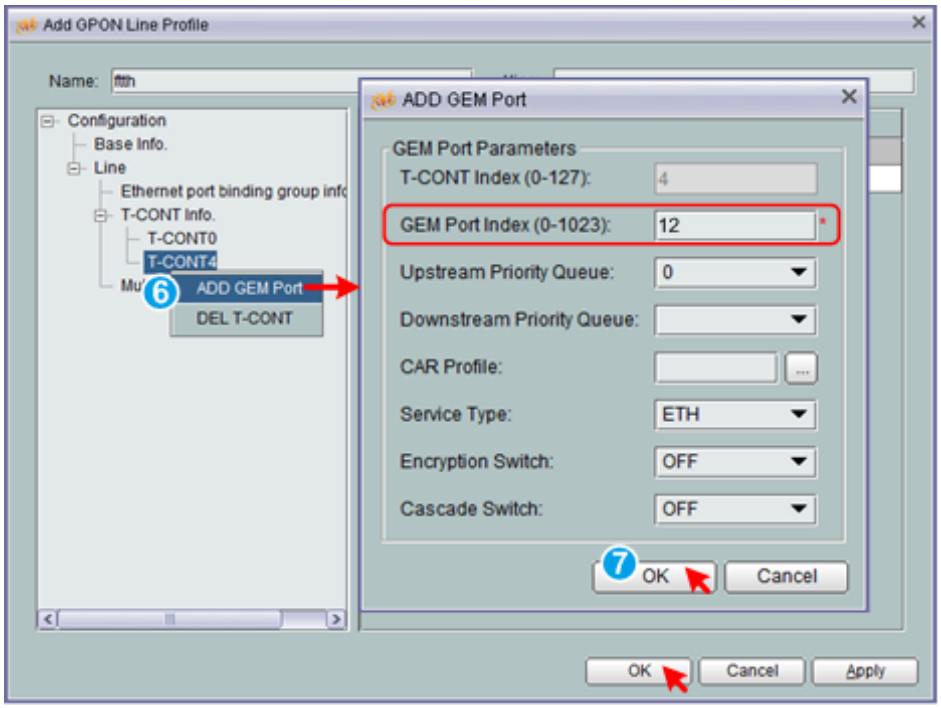
  b. **Configure a line profile.**

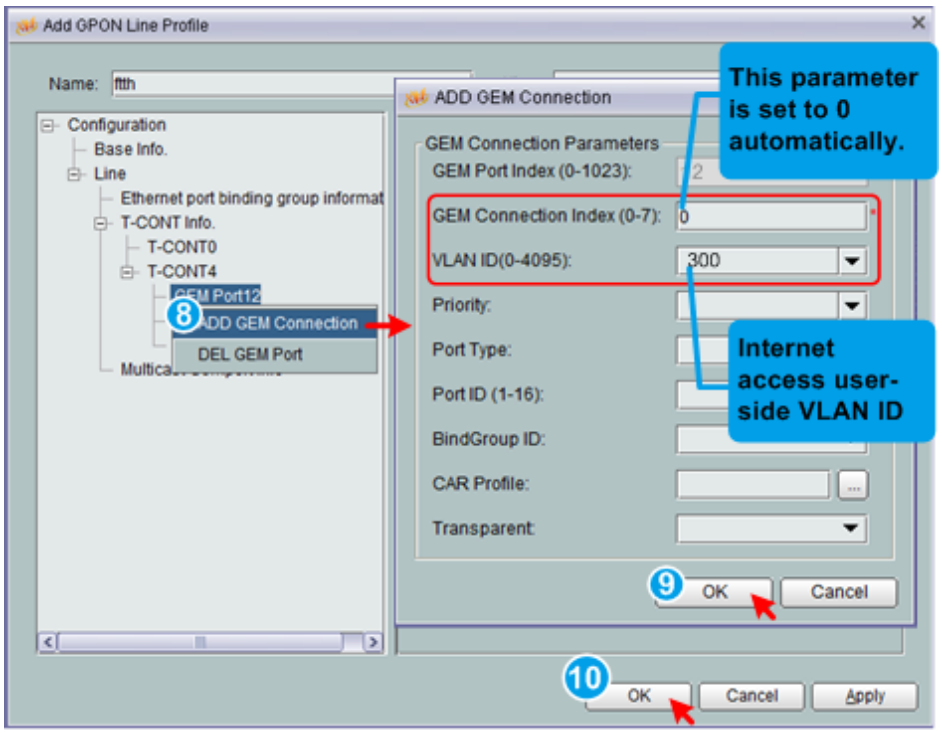
  In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

  In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 12. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.


Workbench
Access Profile Management
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
Add Global Profile...
File
Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
Name
Value
Upstream FEC Switch
OFF
Mapping Mode
VLAN
Qos Mode
Priority Queue
OMCC Encryption
Off
TR069 Management
Disable
TR069 Management IP Index
0

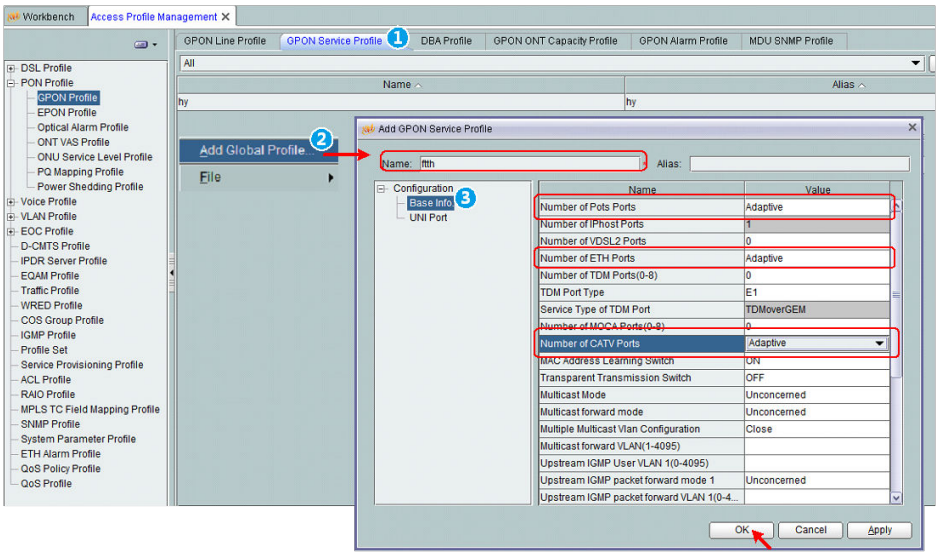

Add GPON Line Profile
Name:
Alias:
Configuration
Base Info.
Line
T-CONT Info
ADD T-CONT
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127):
4
DBA Profile:
OK
Cancel
OK
Cancel
Apply





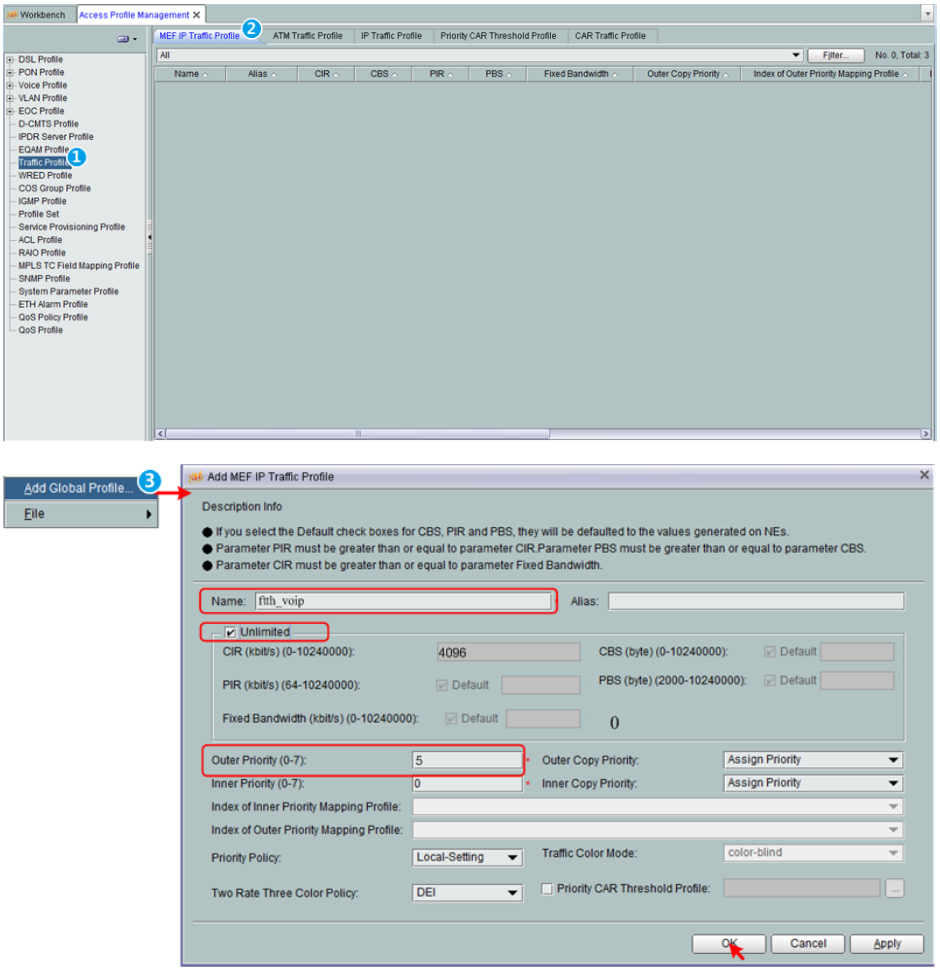
c. **Configure a service profile.**

Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability.



d. **Configure an MEF IP traffic profile.**

The profile name is ftth_voip, upstream/downstream traffic rate is not limited, and the priority is 5. Traffic is scheduled based on the priority specified in the profile.

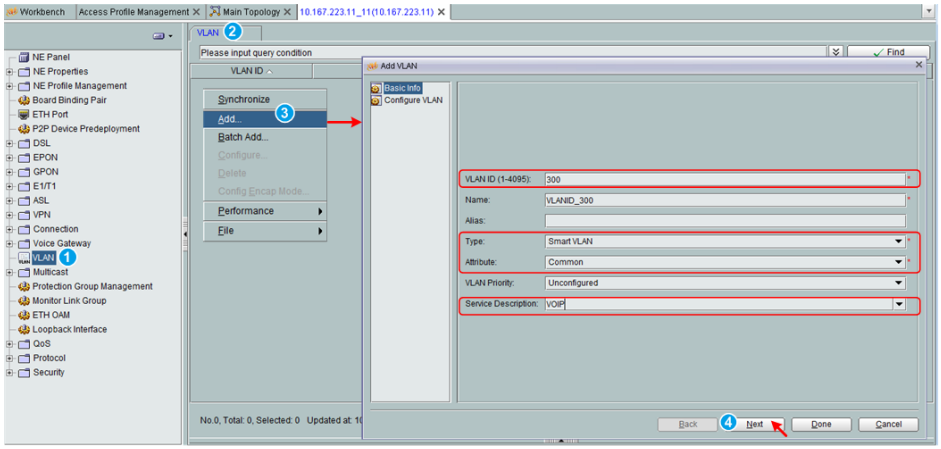


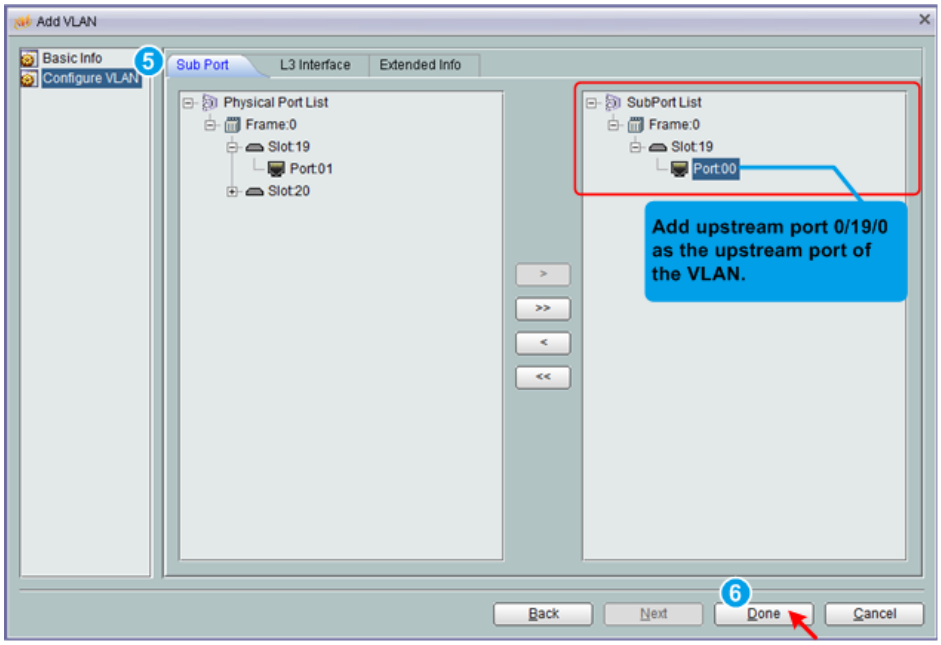
e. **Configure an S-VLAN on the OLT side.**

The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as

follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

The S-VLAN is used for the voice service.

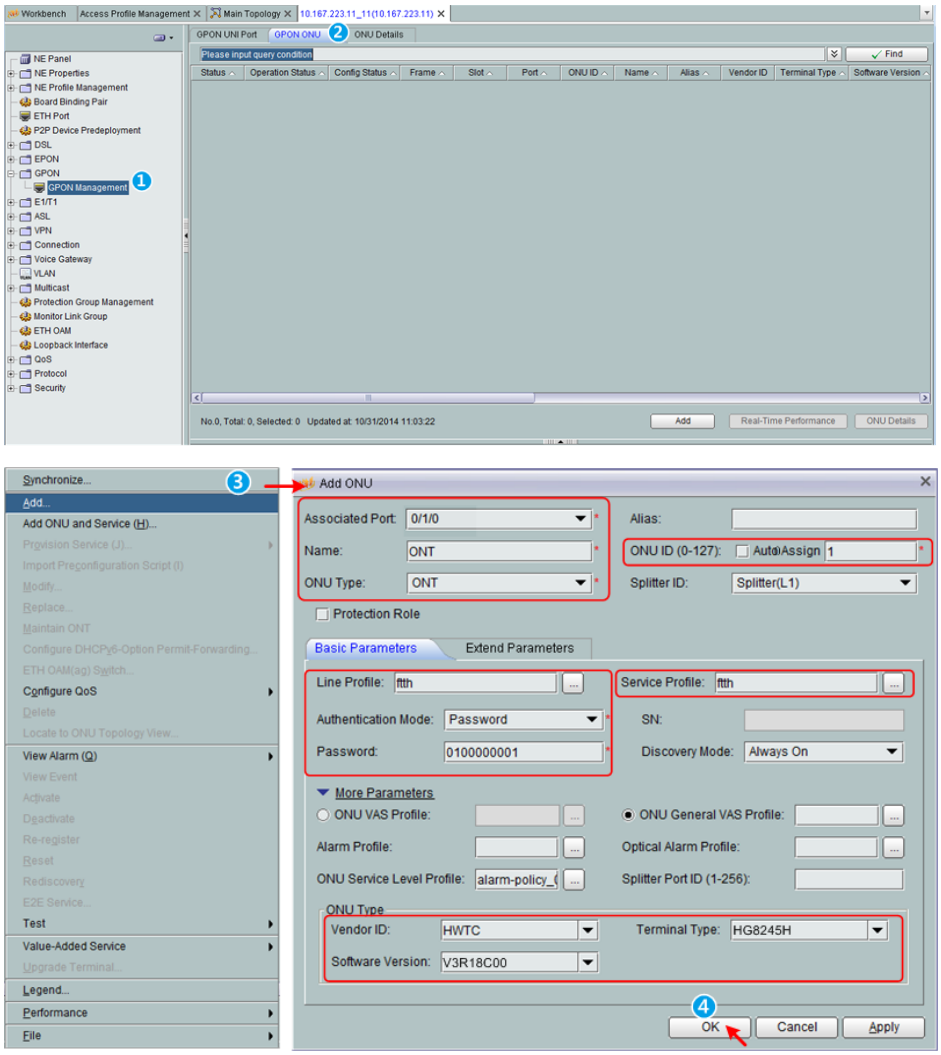




- **Provision services.**

  a. **Add an ONT.**

  The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.

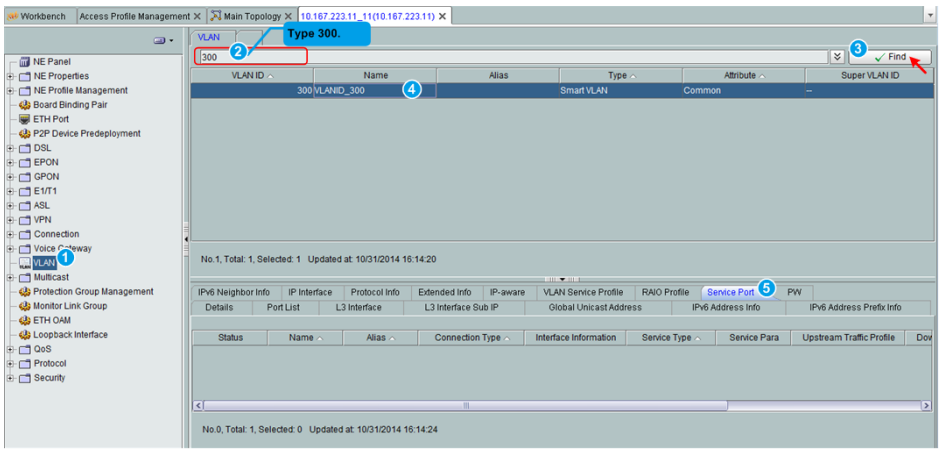


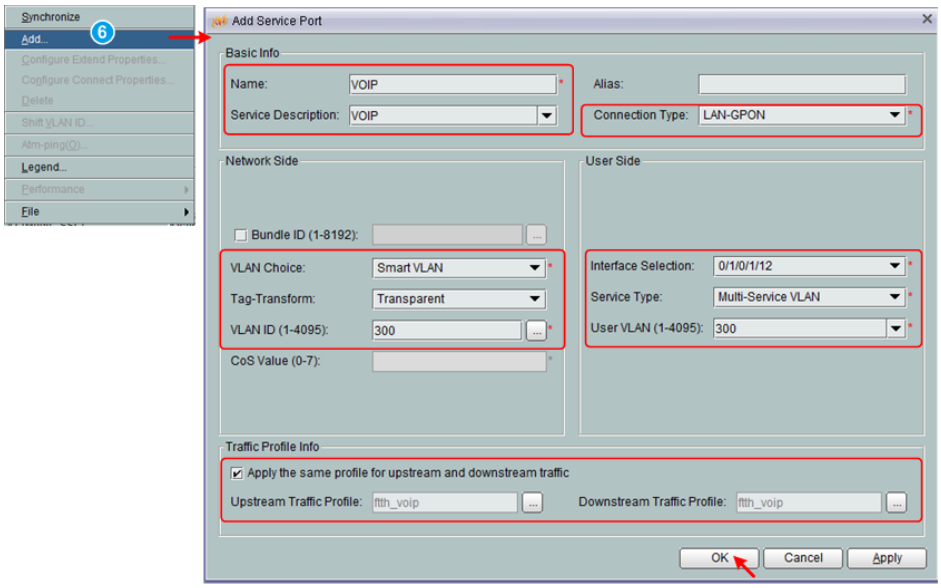
NOTE

HG8245H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

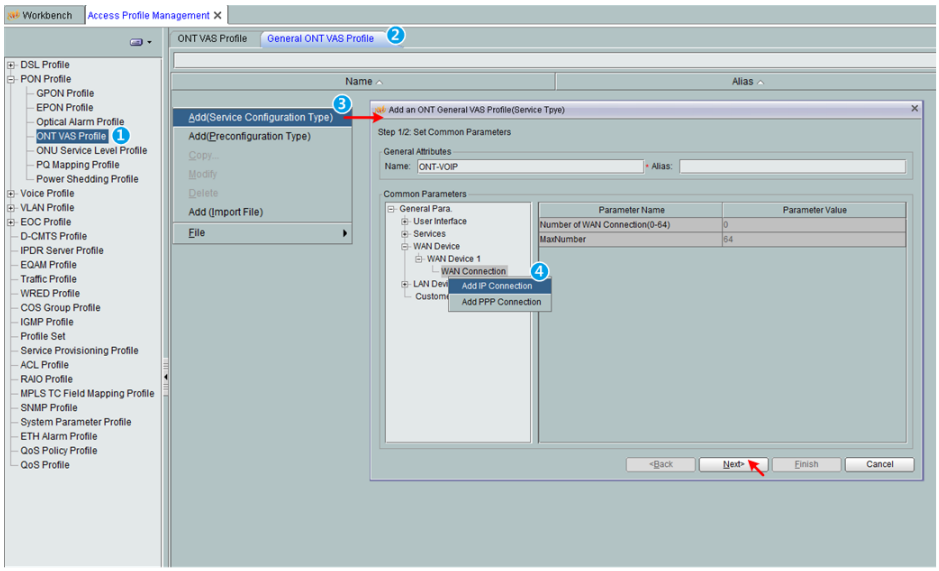
The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

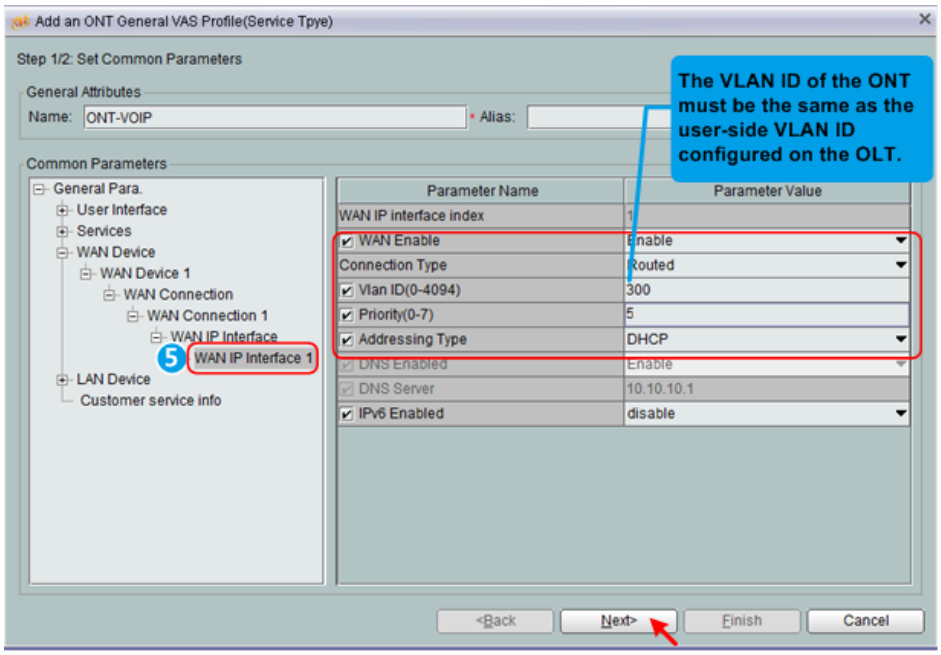
b. **Add a service port on the OLT side.**

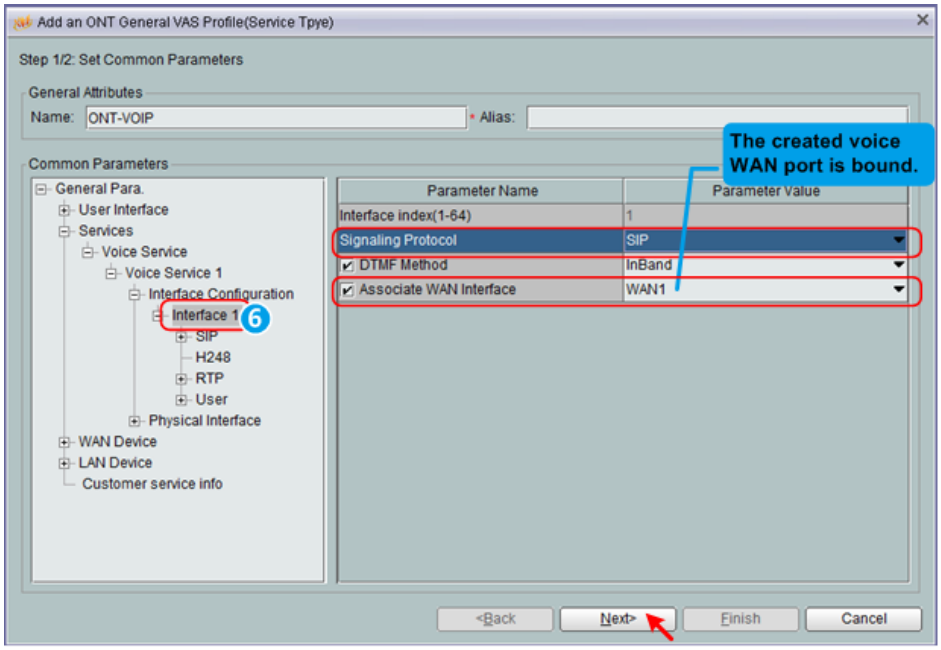


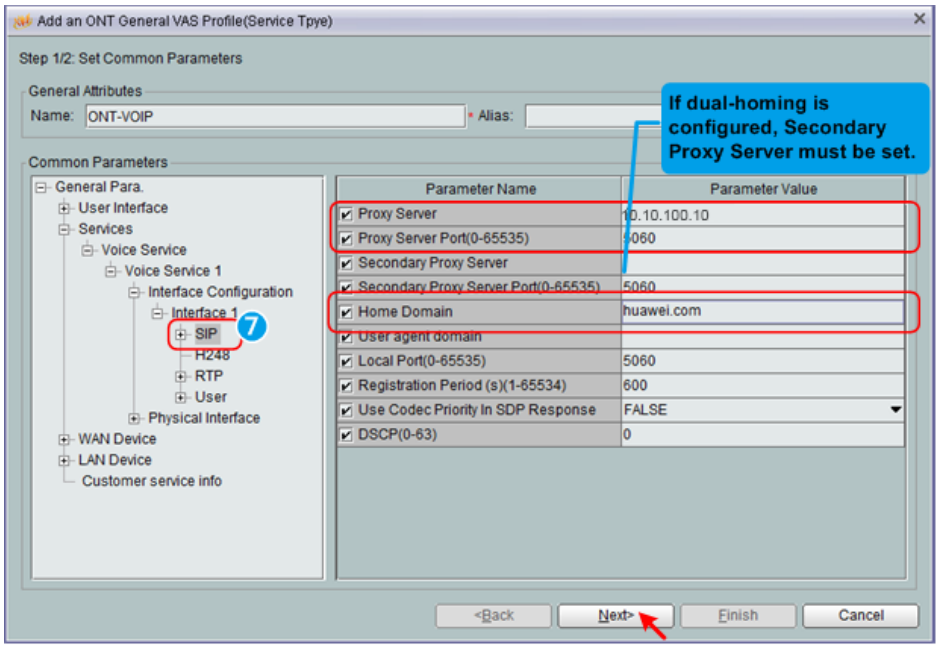


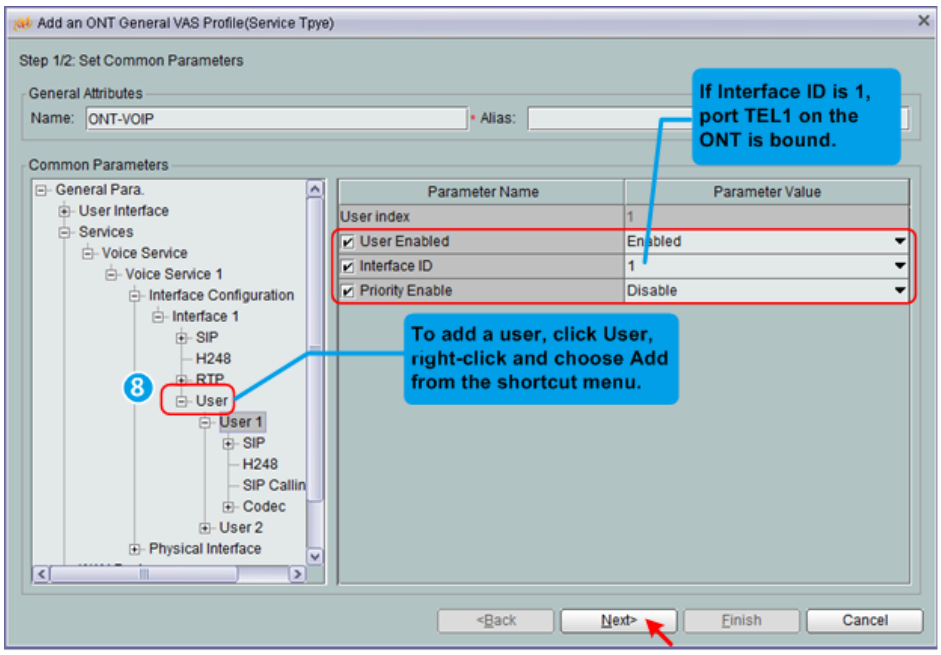
c. **Configure a general VAS profile for the ONT.**

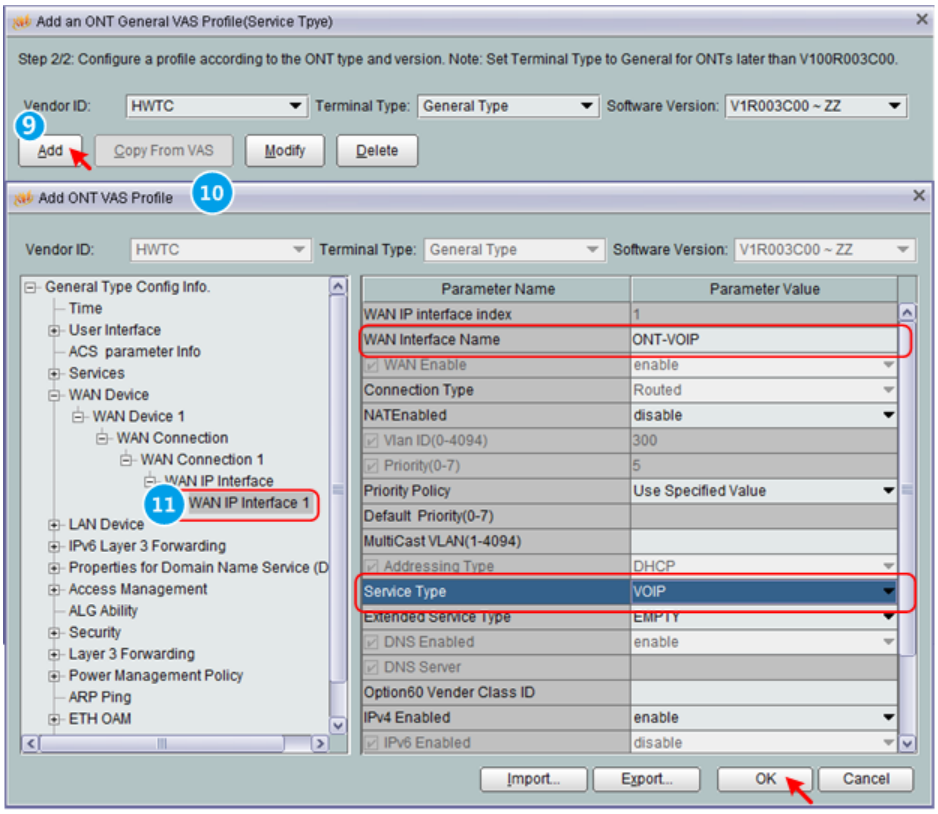




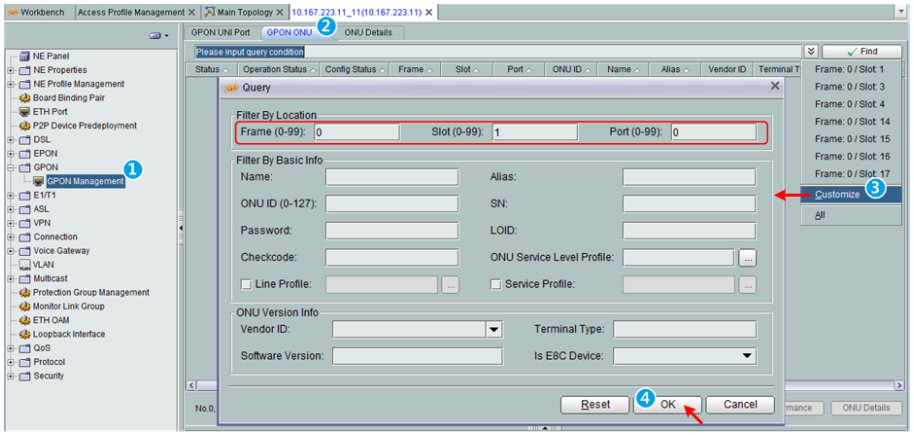


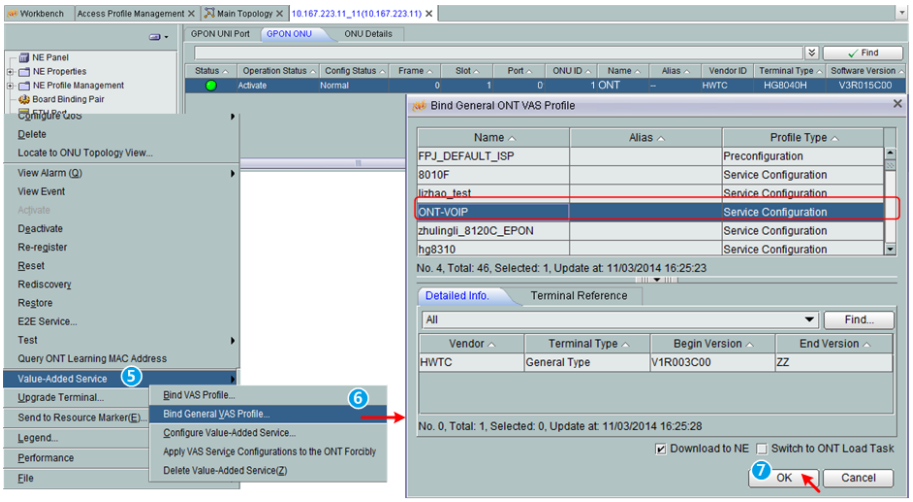

Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
Voice Service
Voice Service 1
Interface Configuration
Interface 1
SIP
H248
RTP
User
Physical Interface
WAN Device
LAN Device
Customer service info
Parameter Name
Parameter Value
Proxy Server
10.10.100.10
Proxy Server Port(0-65535)
5060
Secondary Proxy Server
Secondary Proxy Server Port(0-65535)
5060
Home Domain
huawei.com
User agent domain
Local Port(0-65535)
5060
Registration Period (s)(1-65534)
600
Use Codec Priority In SDP Response
FALSE
DSCP(0-63)
0
If dual-homing is configured, Secondary Proxy Server must be set.
7
<Back
Next>
Finish
Cancel


Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-VOIP
Alias:
Common Parameters
General Para.
User Interface
Services
Voice Service
Voice Service 1
Interface Configuration
Interface 1
SIP
H248
RTP
User
User 1
SIP
H248
SIP Callin
Codec
User 2
Physical Interface
Parameter Name
Parameter Value
User index
1
User Enabled
Enabled
Interface ID
1
Priority Enable
Disable
If Interface ID is 1, port TEL1 on the ONT is bound.
To add a user, click User, right-click and choose Add from the shortcut menu.
8
<Back
Next>
Finish
Cancel

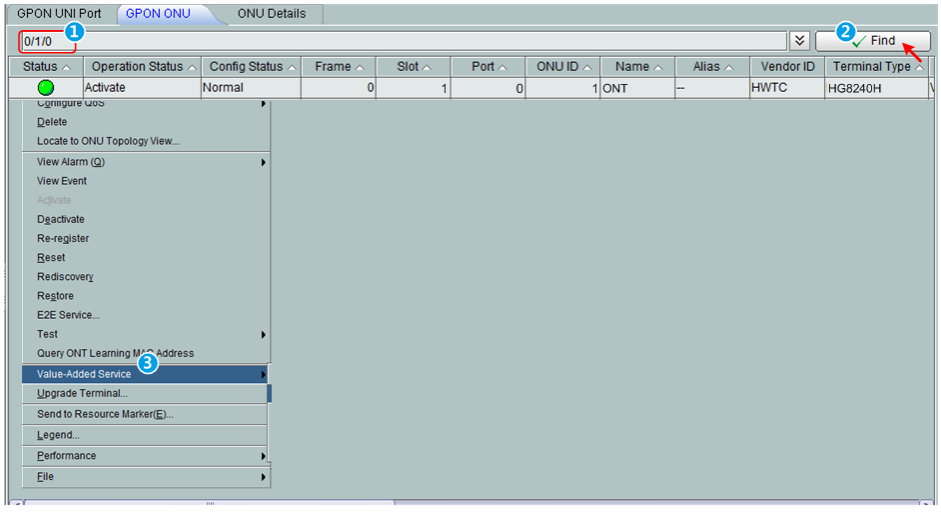


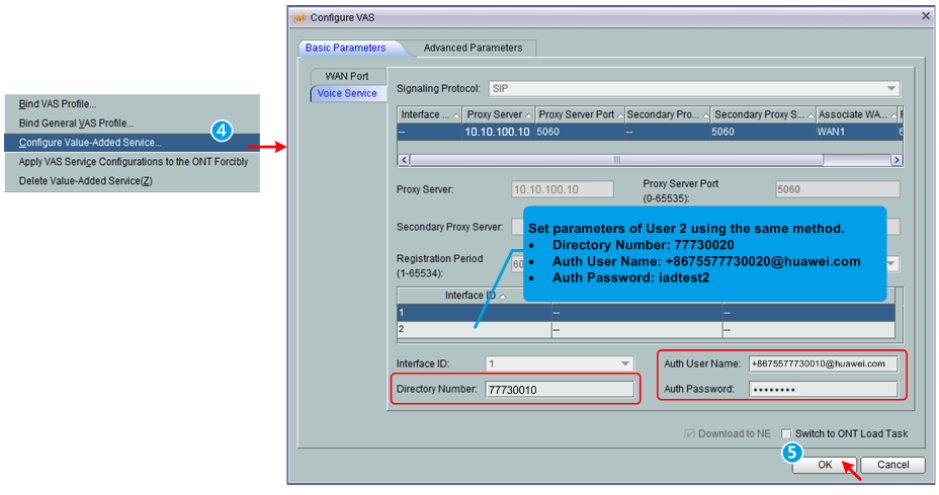
d. **Bind a general VAS profile.**





e. **Configure the ONT VAS service.**





NOTE

The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

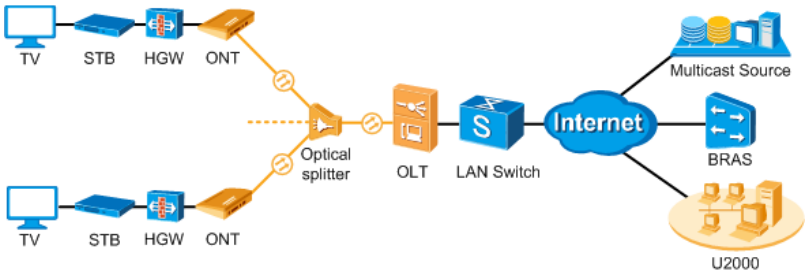
3.3.1.1.5 Configuring the GPON FTTH Layer 2 Multicast Service on the NMS

This topic describes how to configure the multicast service when an ONT is connected to an OLT through a GPON port.

Networking

- The ONT is connected to the OLT in Layer 2 mode.
- The OLT uses IGMP proxy, which is a Layer 2 multicast protocol.
- The IGMP version of the multicast VLAN is IGMPv2.
- The multicast programs are obtained in the dynamic mode.

Figure 3-6 Configuring the GPON FTTH multicast service



Data Plan

Table 3-10 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA Type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for video services: 13

Item	Data
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1 ID of the port on the ONT that is connected to the PC: 2
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode
VLAN Plan	● S-VLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: Smart ● VLAN attribute: Common **NOTE** VLAN translation policy: ● ONT: transparently transmits the MVLAN of the HGW. Multicast packets are duplicated downstream with MVLAN unchanged. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.

Procedure

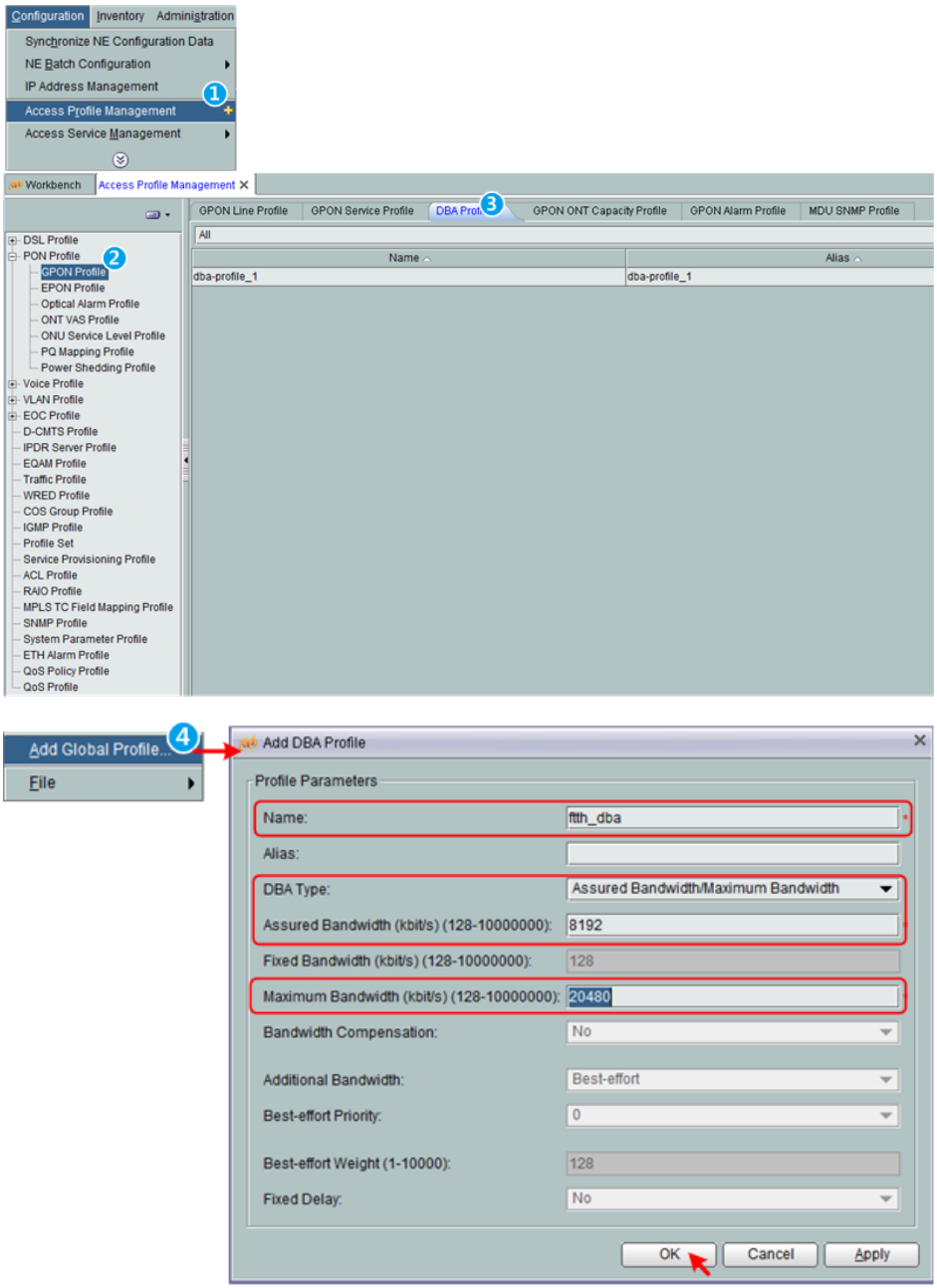
- **Implement pre-configurations.**

NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

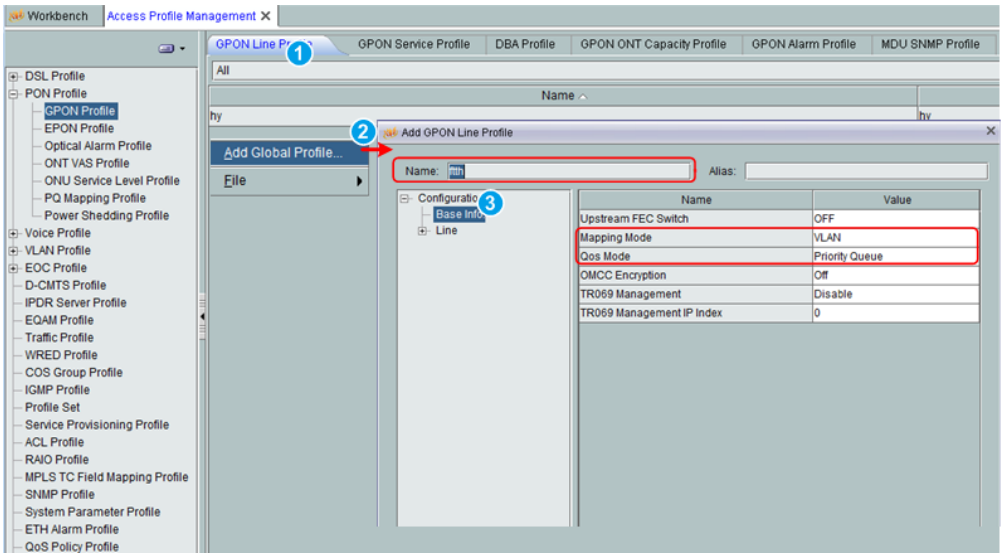
1. **Configure a DBA profile.**

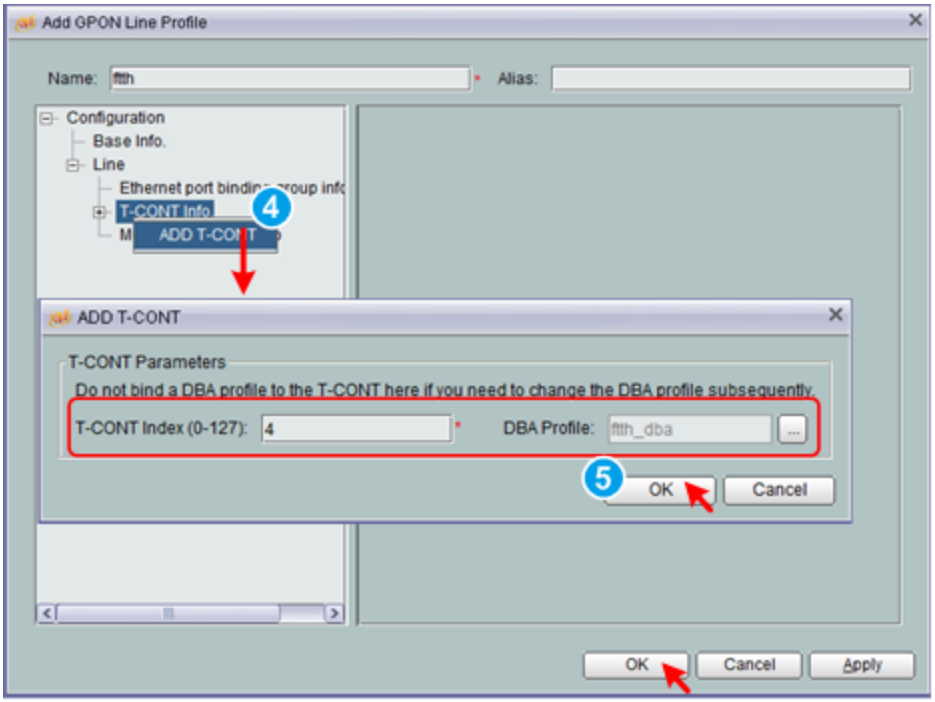


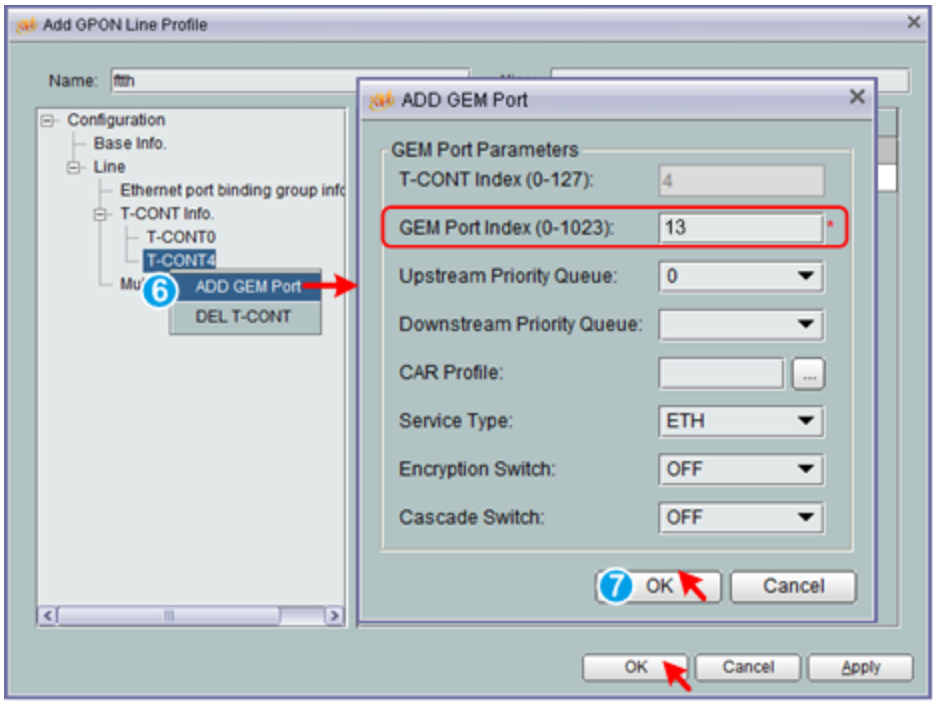
2. **Configure a line profile.**

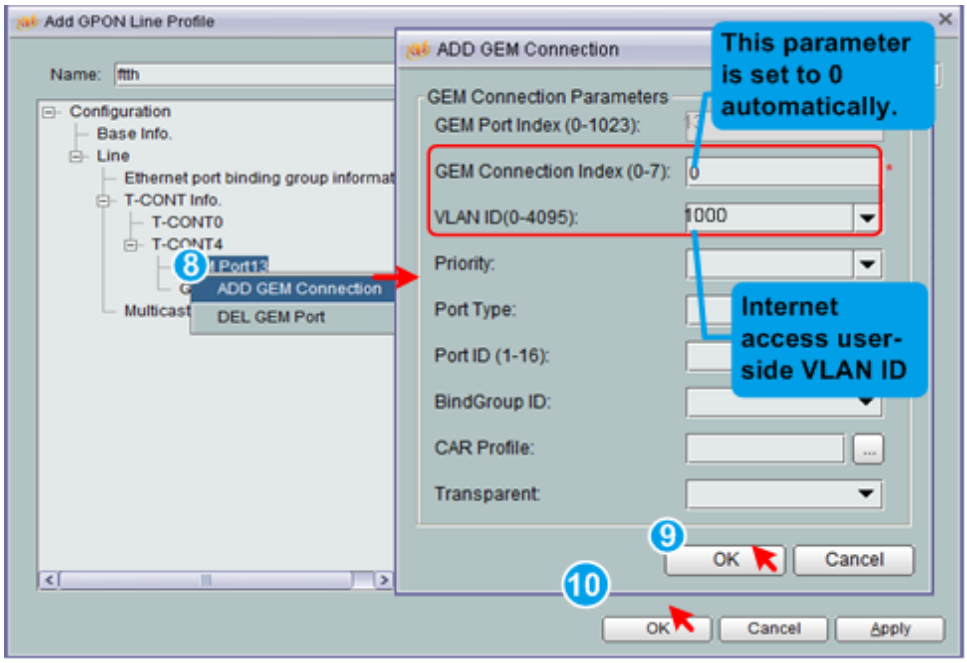
   In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

   In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 13. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.


Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
Add Global Profile...
File
Add GPON Line Profile
Name: ftth
Alias:
Configuration
Base Info.
Line
Name
Value
Upstream FEC Switch
OFF
Mapping Mode
VLAN
Qos Mode
Priority Queue
OMCC Encryption
Off
TR069 Management
Disable
TR069 Management IP Index
0
1
2
3

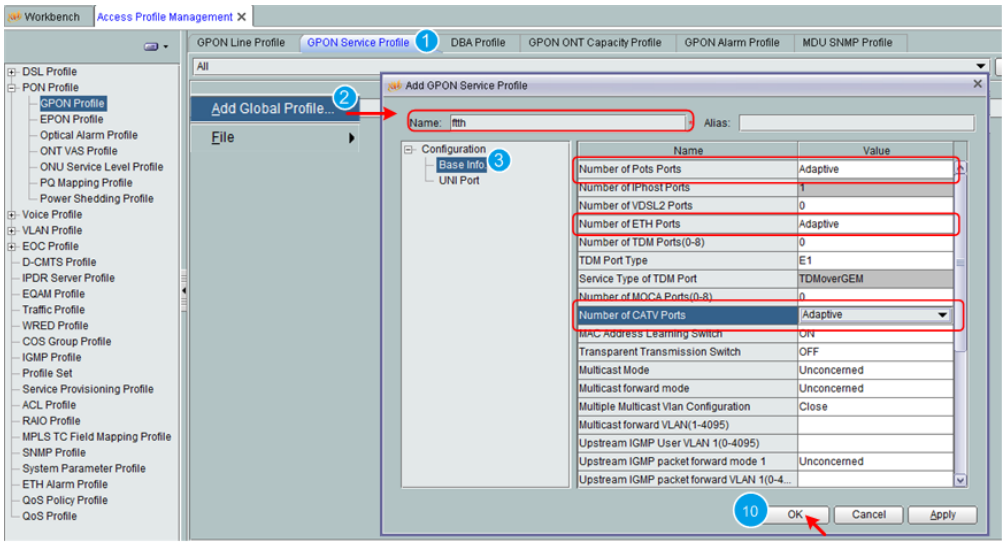

Add GPON Line Profile
Name: ftth
Alias:
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info
ADD T-CONT
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127): 4
DBA Profile: ftth_dba
5
OK
Cancel
OK
Cancel
Apply

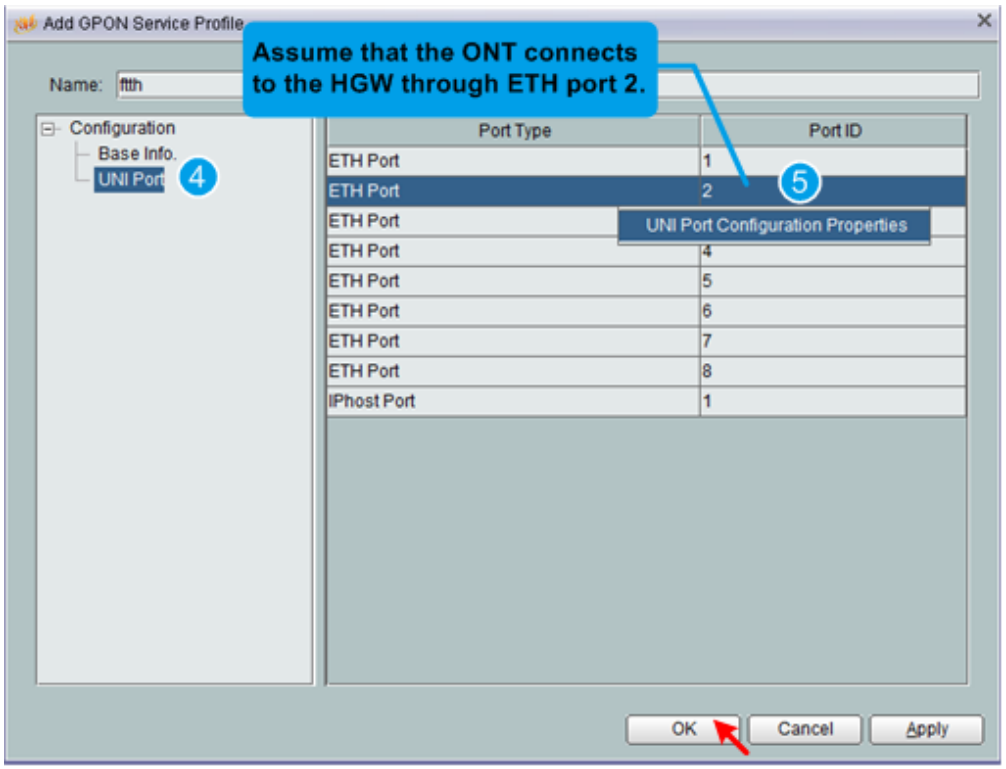


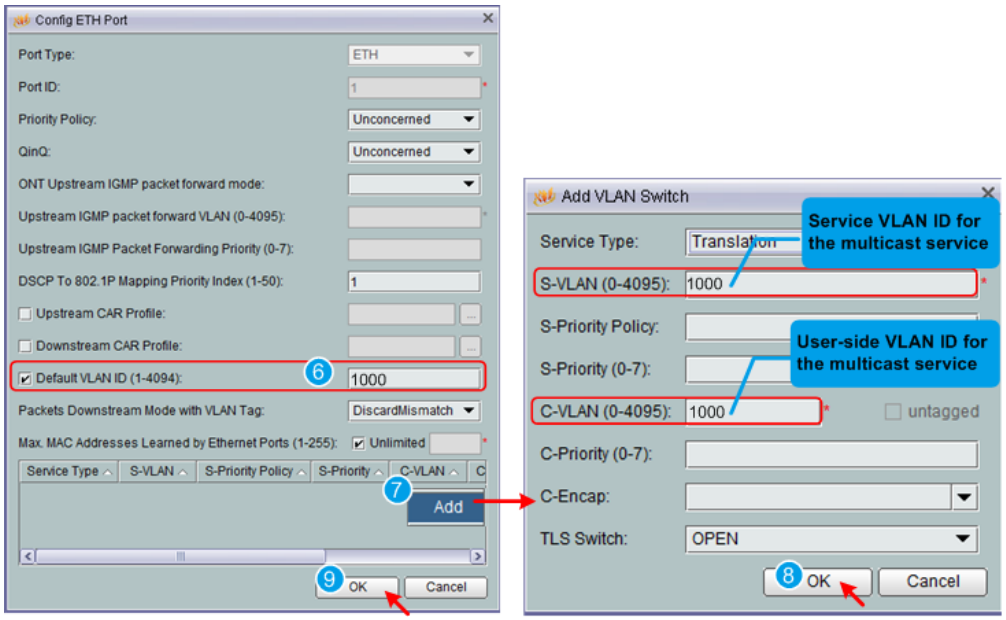


3. **Configure a service profile.**

   Configure a VLAN translation policy for the ONT ETH port. Assume that the ONT connects to the HGW through ETH port 2. Configure a VLAN translation policy to make the ONT transparently transmit the MVLAN of the HGW in the upstream direction, and replicate multicast packets with the MVLAN unchanged in the downstream direction.

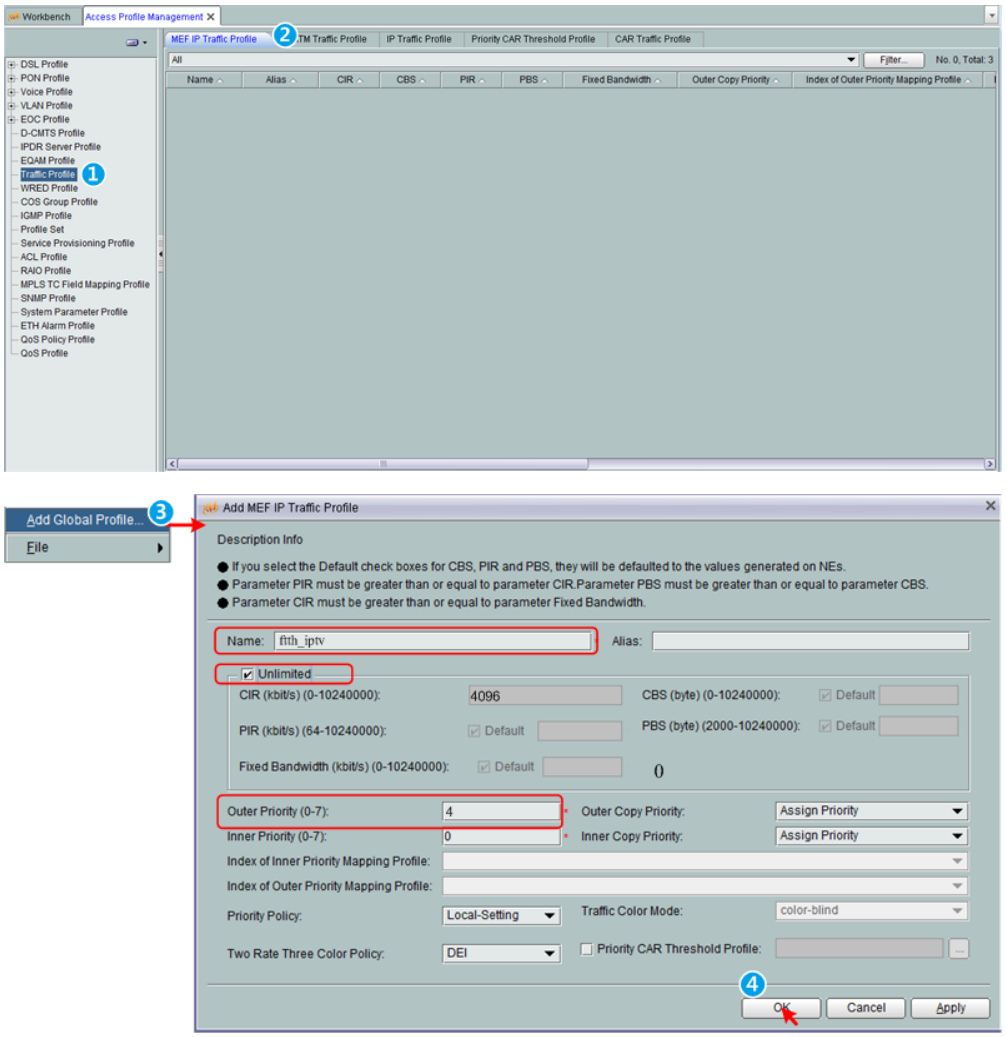

Workbench
Access Profile Management
GPON Line Profile
GPON Service Profile
DBA Profile
GPON ONT Capacity Profile
GPON Alarm Profile
MDU SNMP Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
QoS Profile
Add Global Profile...
File
Add GPON Service Profile
Name: ftth
Alias:
Configuration
Base Info
UNI Port
Name
Value
Number of Pots Ports
Adaptive
Number of IPhost Ports
1
Number of VDSL2 Ports
0
Number of ETH Ports
Adaptive
Number of TDM Ports(0-8)
0
TDM Port Type
E1
Service Type of TDM Port
TDMoverGEM
Number of MOCA Ports(0-8)
0
Number of CATV Ports
Adaptive
Transparent Transmission Switch
OFF
Multicast Mode
Unconcerned
Multicast forward mode
Unconcerned
Multiple Multicast Vlan Configuration
Close
Multicast forward VLAN(1-4095)
Upstream IGMP User VLAN 1(0-4095)
Upstream IGMP packet forward mode 1
Unconcerned
OK
Cancel
Apply


Add GPON Service Profile
Assume that the ONT connects to the HGW through ETH port 2.
Name: ftth
Configuration
Base Info.
UNI Port
Port Type
Port ID
ETH Port 1
ETH Port 2
ETH Port 3
ETH Port 4
ETH Port 5
ETH Port 6
ETH Port 7
ETH Port 8
IPhost Port 1
UNI Port Configuration Properties
OK
Cancel
Apply



4. **Configure an MEF IP traffic profile.**

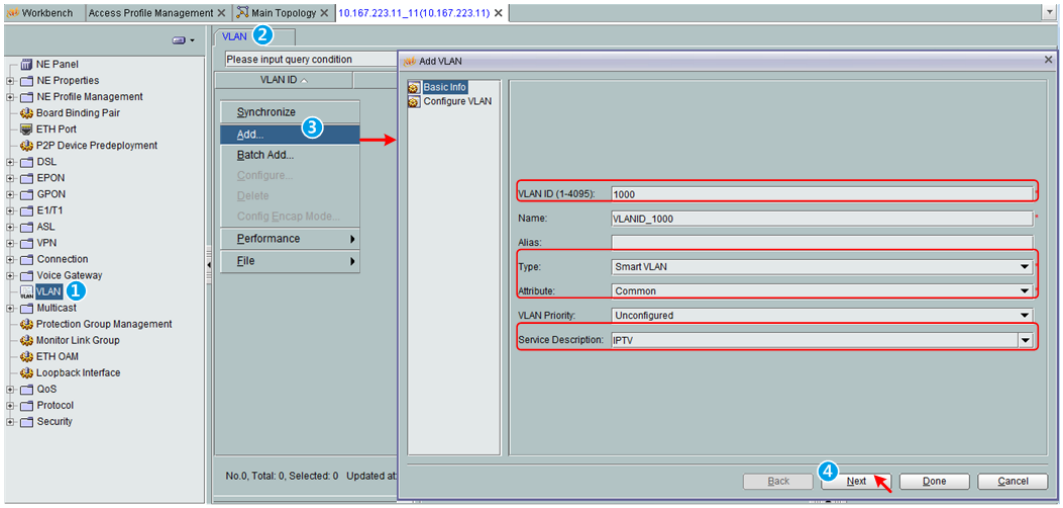
   The profile name is ftth_iptv, CIR is off, priority is 4, and priority-based scheduling policy is Local-Setting. Traffic is scheduled based on the priority specified in the profile.

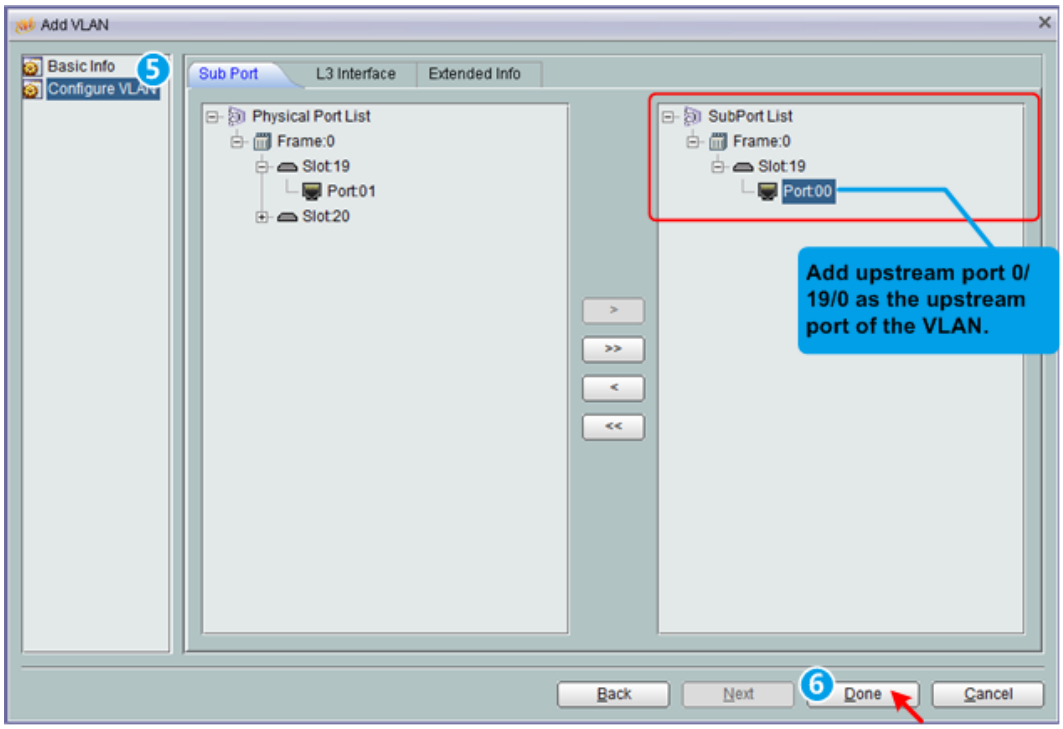


5. **Configure an S-VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   The S-VLAN is used for the multicast service.



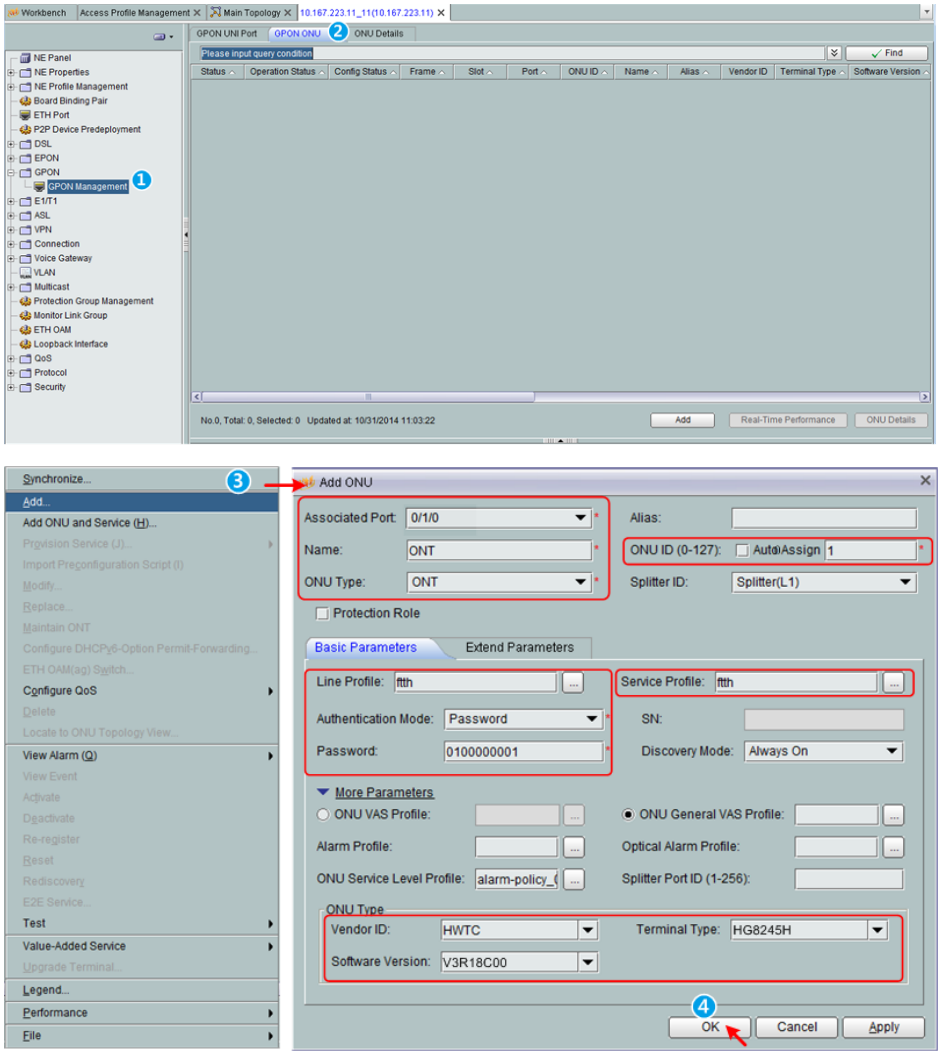


- **Provision services.**

  The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

  a. **Add an ONT.**

The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.

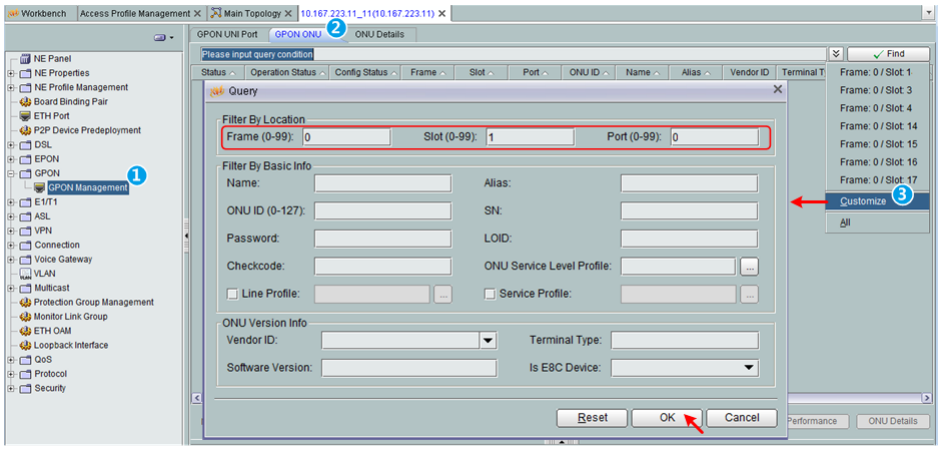


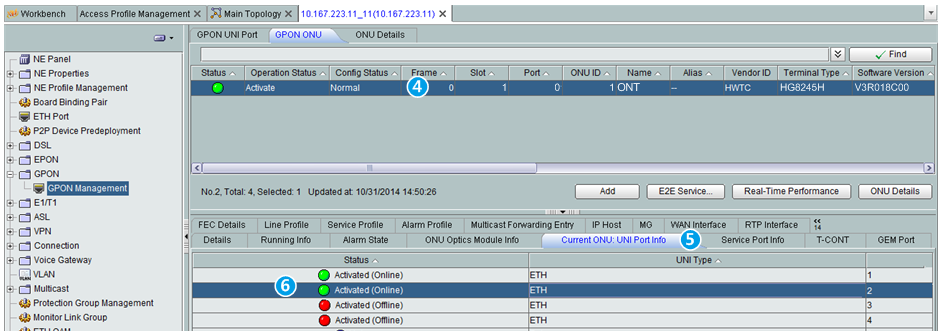
NOTE

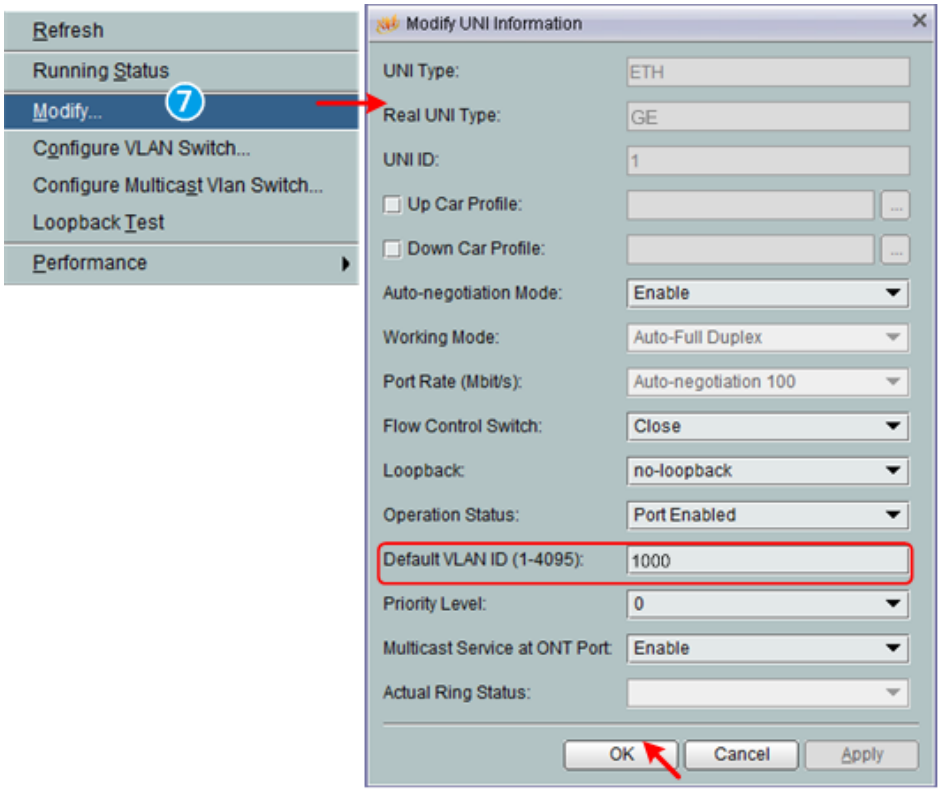
HG8245H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

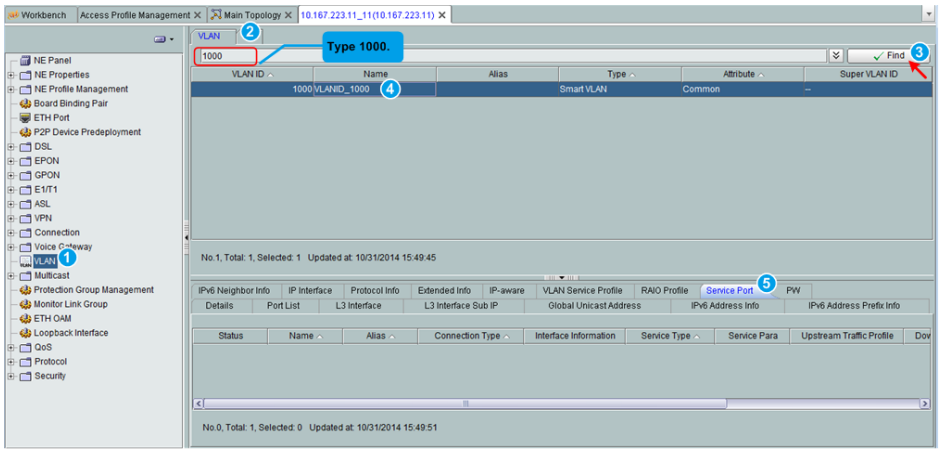
b. **Configure Ethernet port attributes and service channels of a GPON ONU.**

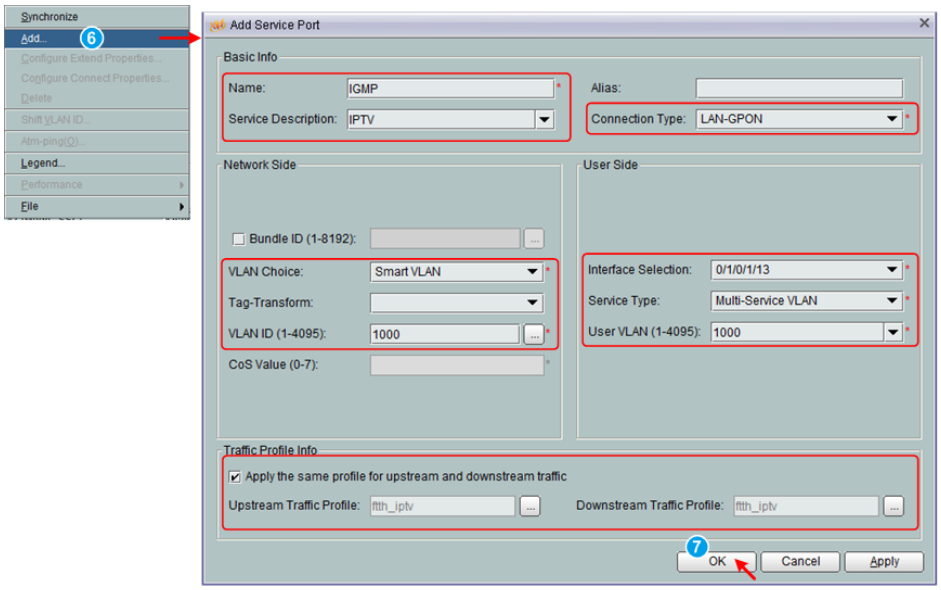




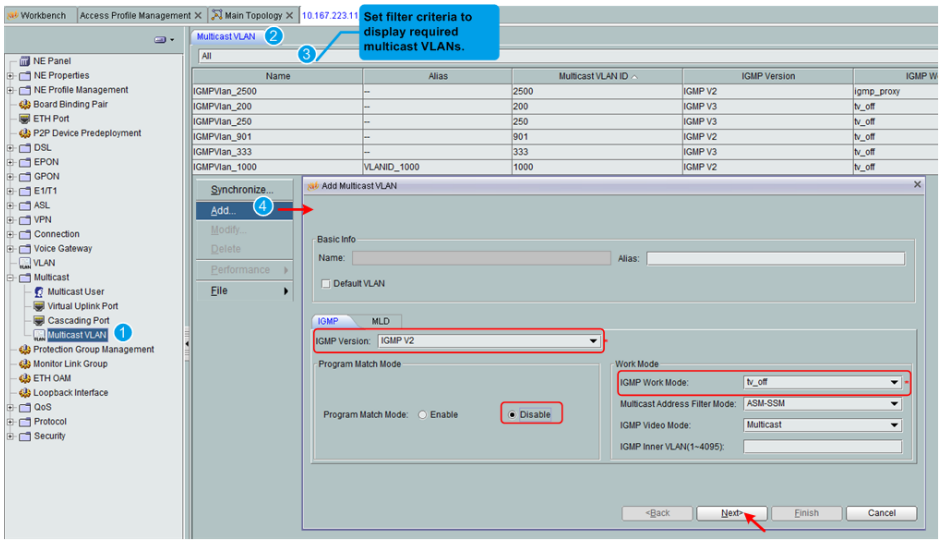


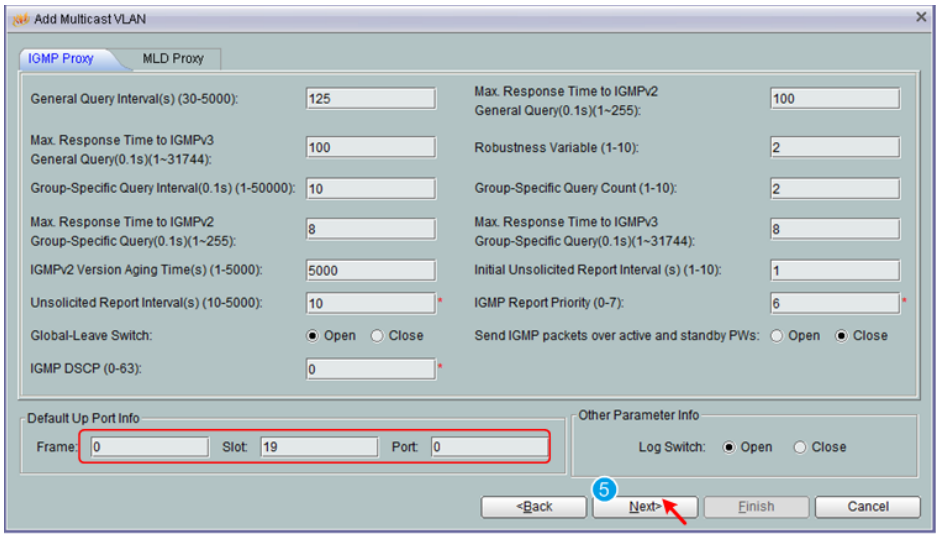
c. **Add a service virtual port on the OLT side.**

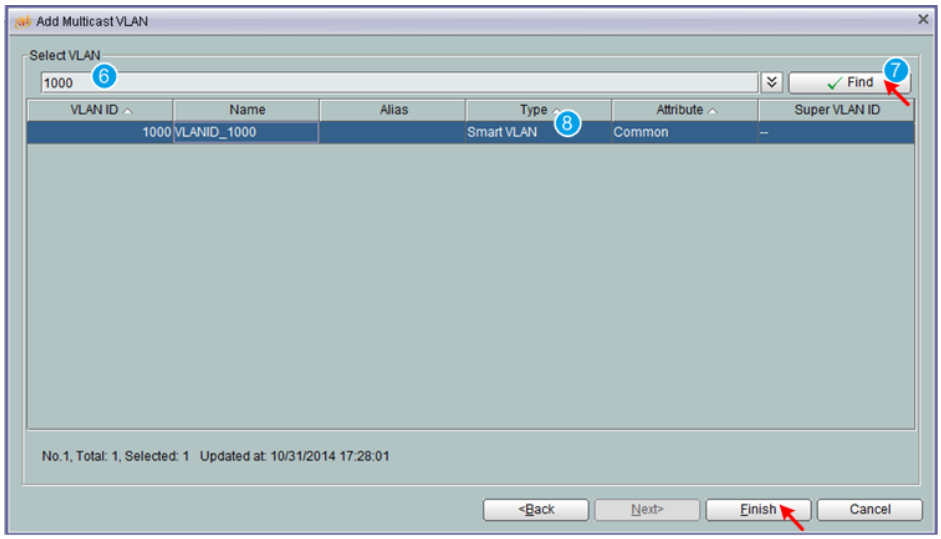




d. **Add a multicast VLAN on the OLT side.**







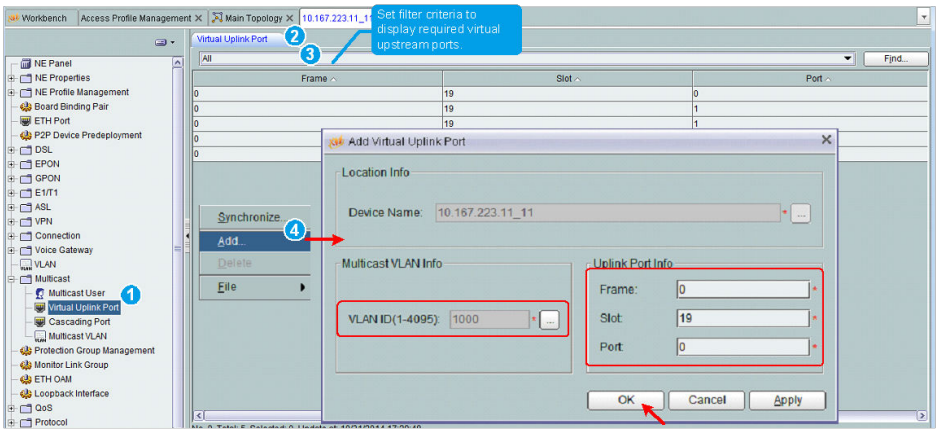
NOTE

Program match mode can be set when **IGMP Work Mode** is **tv_off**. The values of **Program match mode** are as follows:

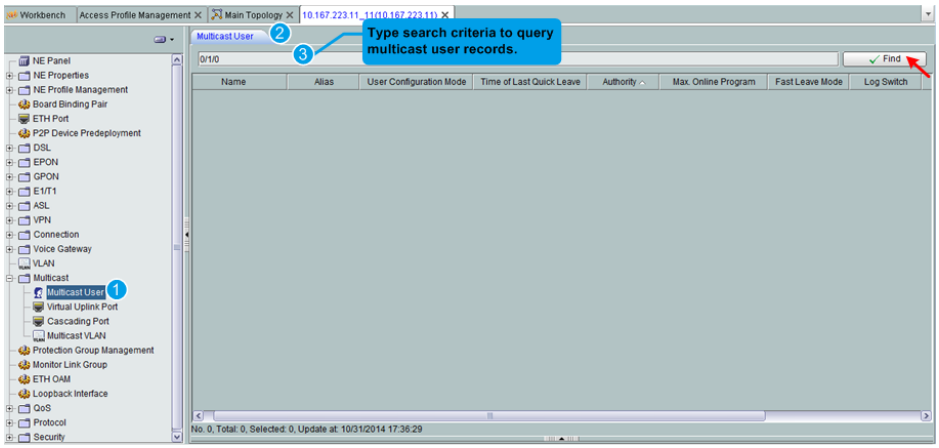
- Enable: Multicast programs are configured statically. Dynamic program generation is not supported.
- Disable: Multicast programs are dynamically generated. Static program configuration is not supported.

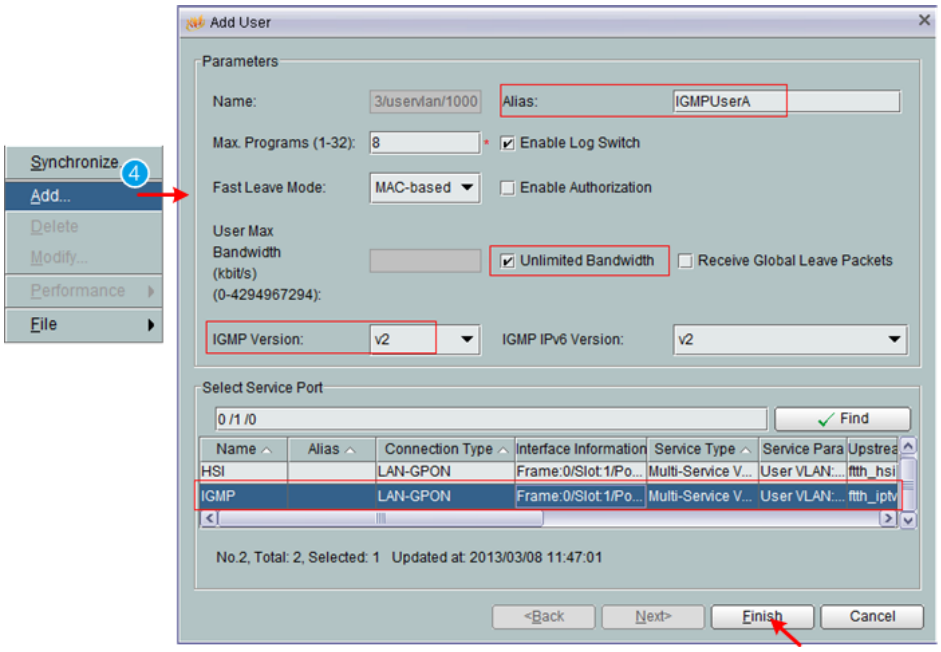
After Configuration, **IGMP Work Mode** should be set to **Proxy** again, otherwise IGMP work abnormally.

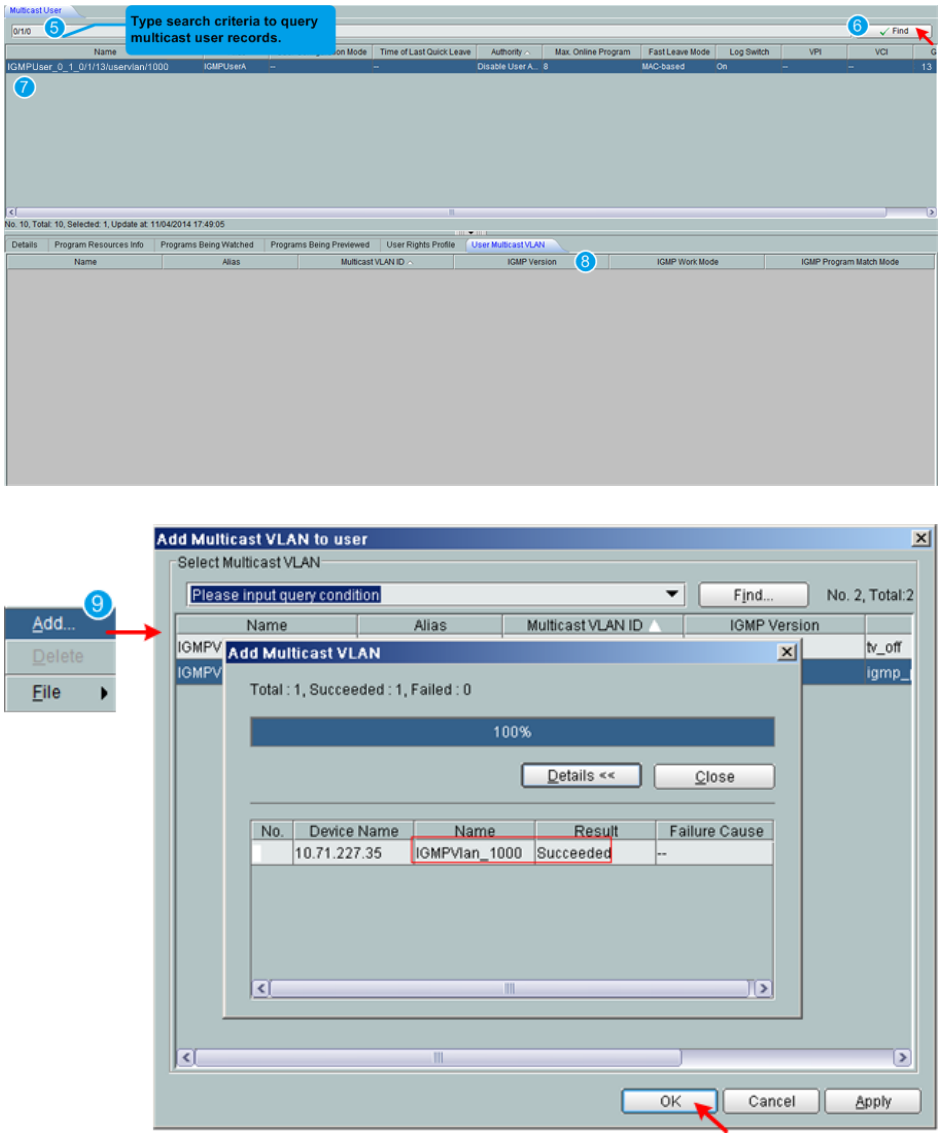
e. **Add a virtual multicast upstream port on the OLT side.**



f. **Configure a multicast user on the OLT side.**







Result

The user can watch programs on TV.

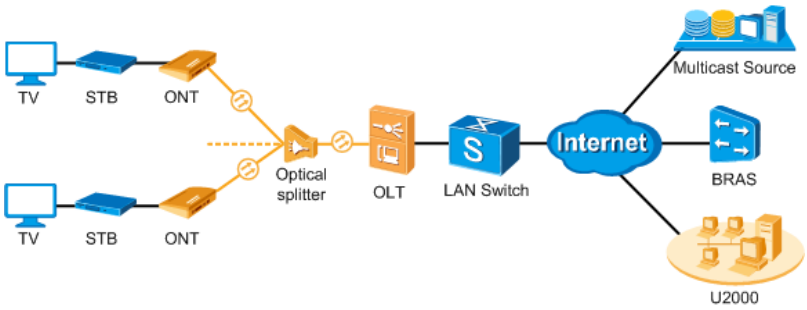
3.3.1.1.6 Configuring the GPON FTTH Layer 3 Bridge Multicast Service on the NMS

This topic describes how to configure the multicast service when an ONT is connected to an OLT through a GPON port.

Networking

- The ONT is connected to the OLT in Layer 3 bridge mode.
- The ONT uses the IGMP snooping multicast protocol.
- The OLT uses IGMP proxy, which is a Layer 2 multicast protocol.
- The IGMP version of the multicast VLAN is IGMPv2.
- Multicast programs are obtained dynamically.

Figure 3-7 Configuring the GPON FTTH multicast service



Data Plan

Table 3-11 Data plan

Item	Data
DBA profile	Name: ftth_dba DBA Type: Assured Bandwidth/Maximum Bandwidth Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for video services: 13
ONT service profile	Profile name: ftth ONT port capability set: ● Number of POTS Ports: Adaptive ● Number of ETH Ports: Adaptive ● Number of CATV Ports: Adaptive
Network topology data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1 ID of the port on the ONT that is connected to the PC: 2
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Item	Data
VLAN Plan	● S-VLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: Smart ● VLAN attribute: Common **NOTE** VLAN translation policy: ● ONT: duplicates multicast packets based on user ports and MVLANs are stripped off downstream. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
ONT value-added services (Layer 3 bridge)	Profile Name: ONT-IPTV WAN VLAN ID: 1000 Priority: 4 Service Type: IPTV Connection Type: Bridged Bound port: LAN2 (LAN2 is a Layer 3 LAN)

Procedure

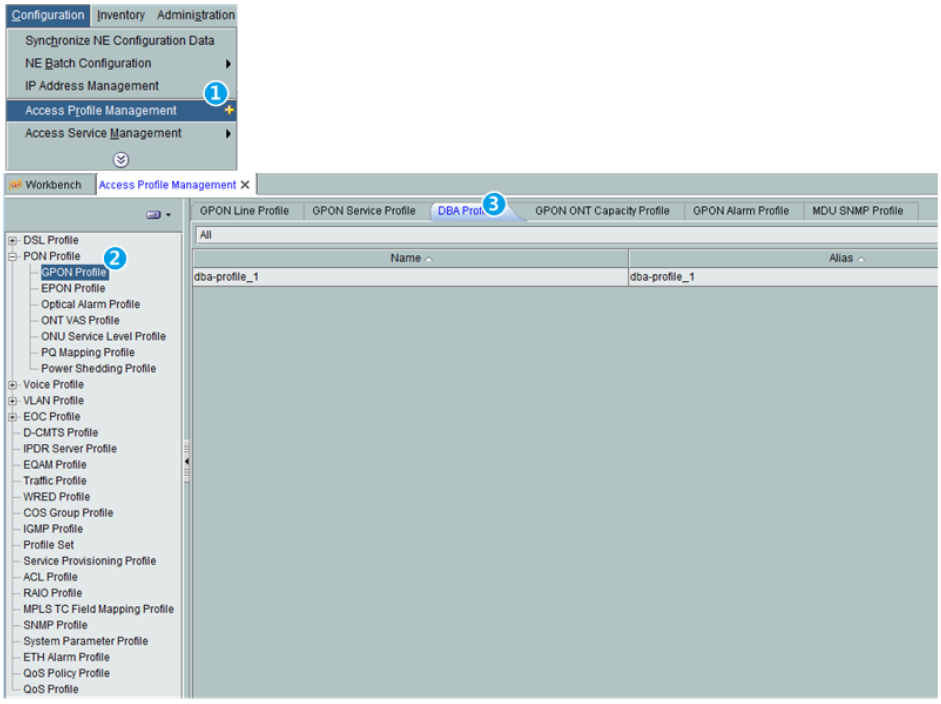
- Implement pre-configurations.

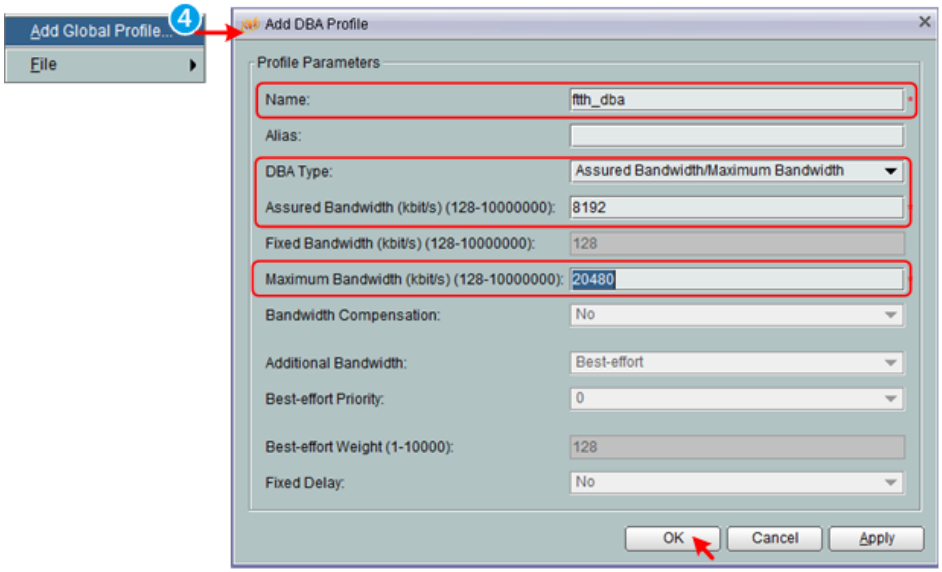
NOTE

After all profiles are configured, perform the following steps to issue them to the device:

- In the information list, right-click the record and choose **Download to NE** from the shortcut menu.
- In the dialog box that is displayed, select the required NE(s), and click **OK**.

1. **Configure a DBA profile.**

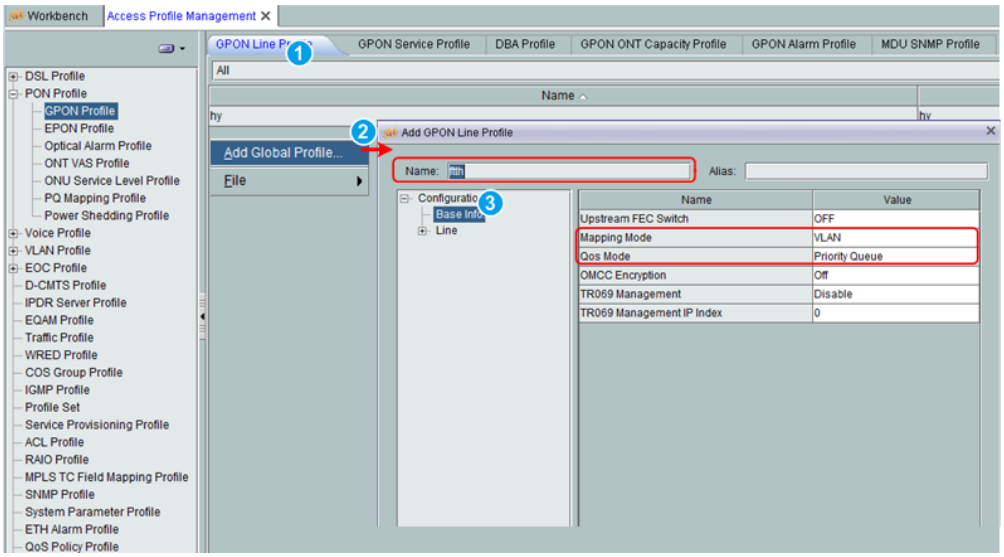


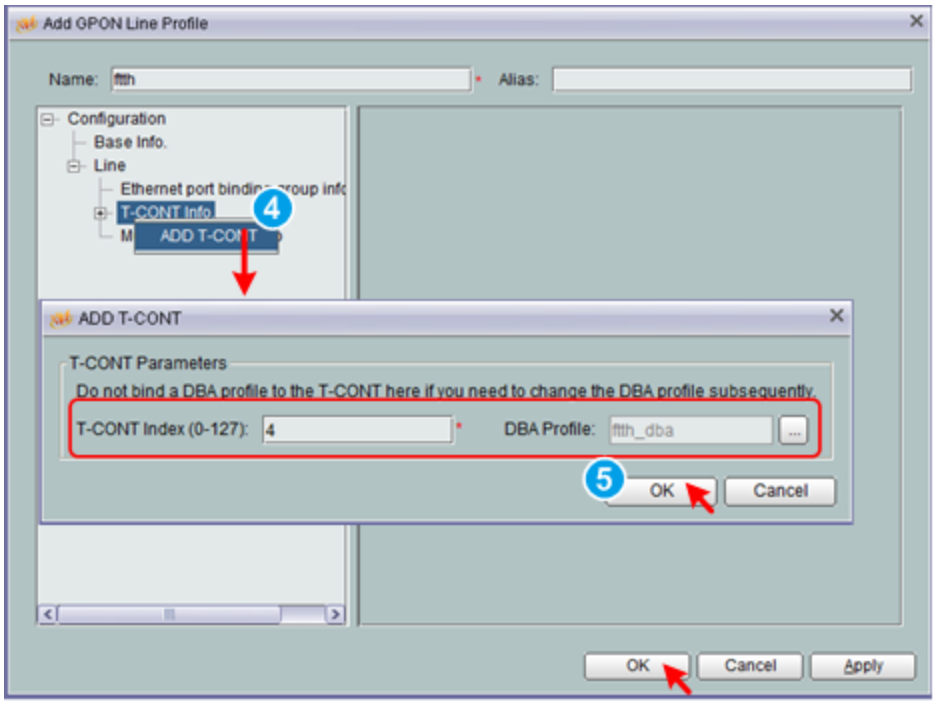


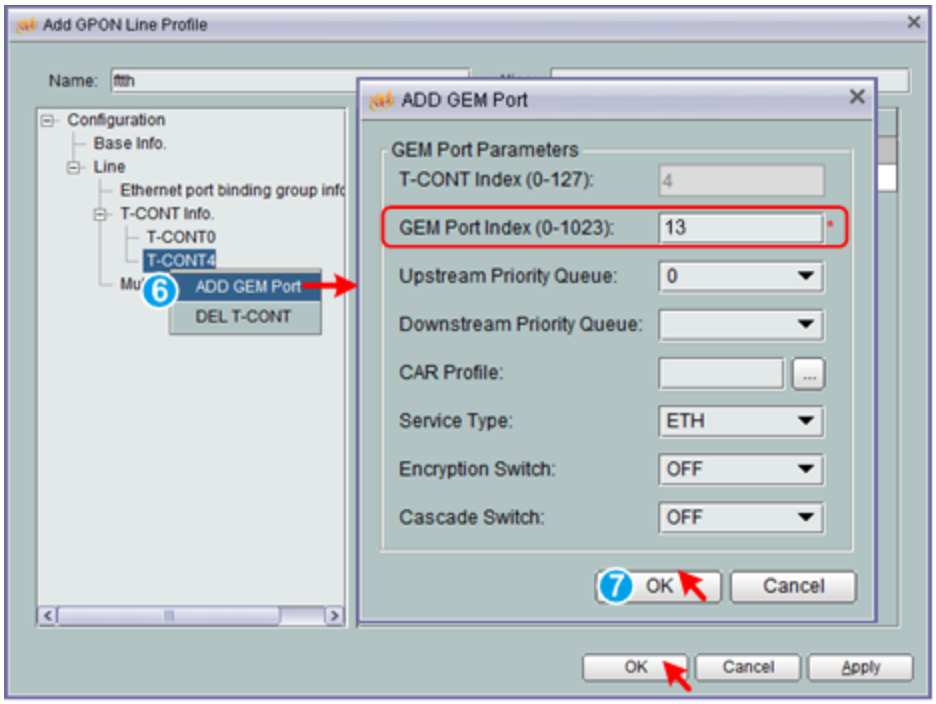
2. **Configure a line profile.**

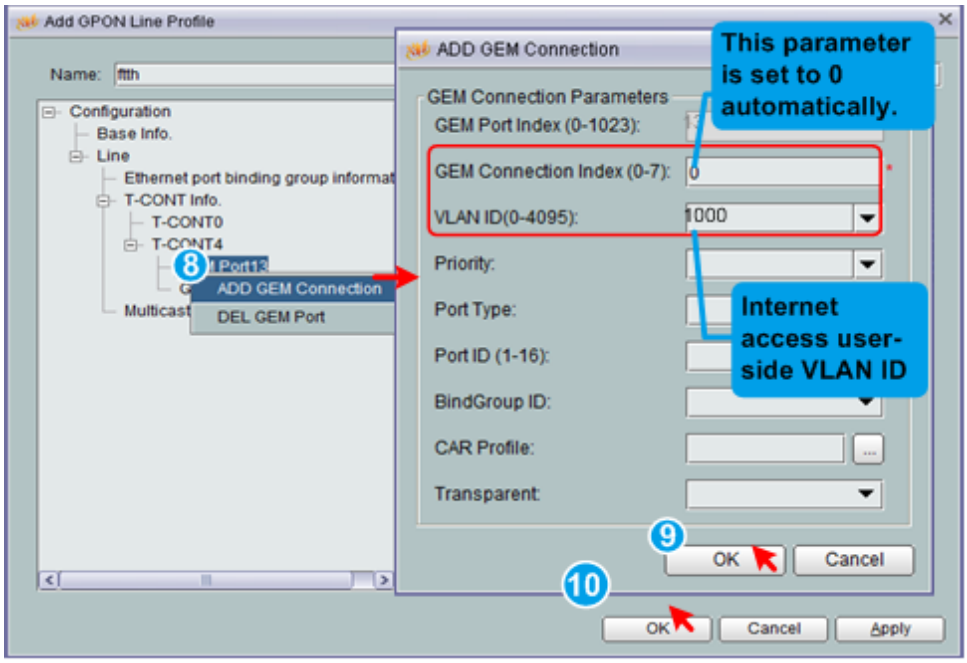
   In a line profile, a GEM port can be bound to up to eight service streams. In a GEM port, different GEM connections need to be set up for different service streams.

   In this example, the mapping between GEM ports and ONT-side services is implemented through VLANs, and the service streams of each service are mapped to GEM port 13. In addition, different GEM connections are set up for the management VLAN and the VLANs for the Internet, voice, and multicast services.



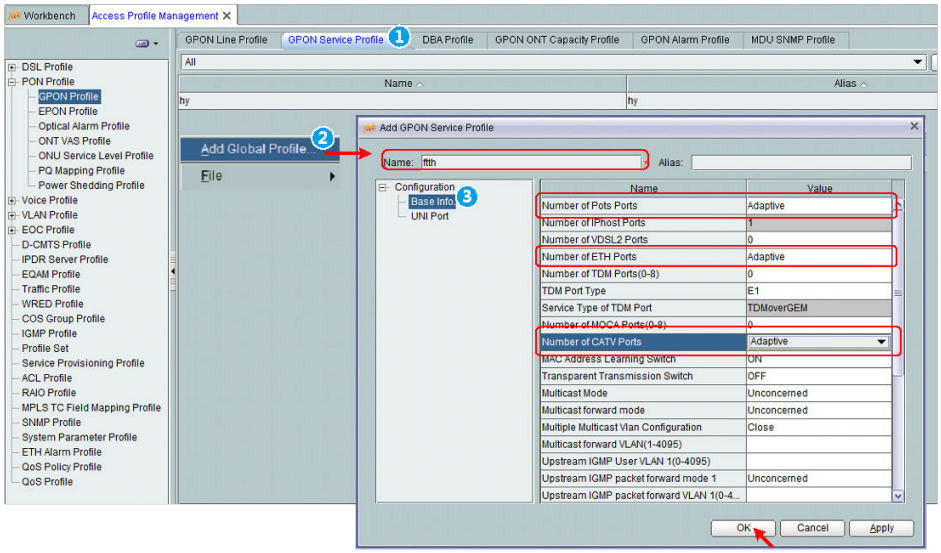

Add GPON Line Profile
Name: ftth
Alias:
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info.
ADD T-CONT
4
ADD T-CONT
T-CONT Parameters
Do not bind a DBA profile to the T-CONT here if you need to change the DBA profile subsequently.
T-CONT Index (0-127): 4
DBA Profile: ftth_dba
5
OK
Cancel
OK
Cancel
Apply


Add GPON Line Profile
Name: ftth
Configuration
Base Info.
Line
Ethernet port binding group info
T-CONT Info.
T-CONT0
T-CONT4
6
ADD GEM Port
DEL T-CONT
ADD GEM Port
GEM Port Parameters
T-CONT Index (0-127): 4
GEM Port Index (0-1023): 13
Upstream Priority Queue: 0
Downstream Priority Queue:
CAR Profile:
Service Type: ETH
Encryption Switch: OFF
Cascade Switch: OFF
7
OK
Cancel
OK
Cancel
Apply



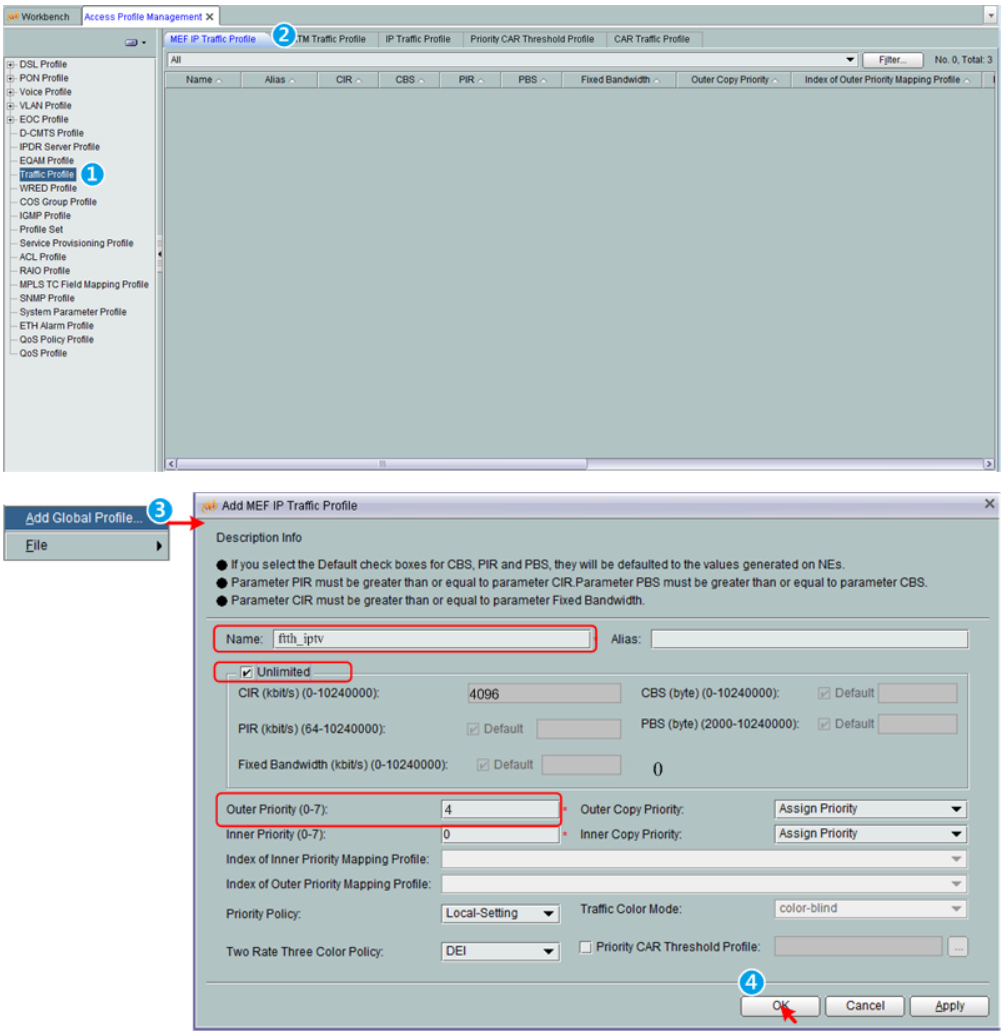
3. **Configure a service profile.**

   Set the port capability set to adaptive. Then, the system adapts the port capability set of an online ONT to its actual capability.



4. **Configure an MEF IP traffic profile.**

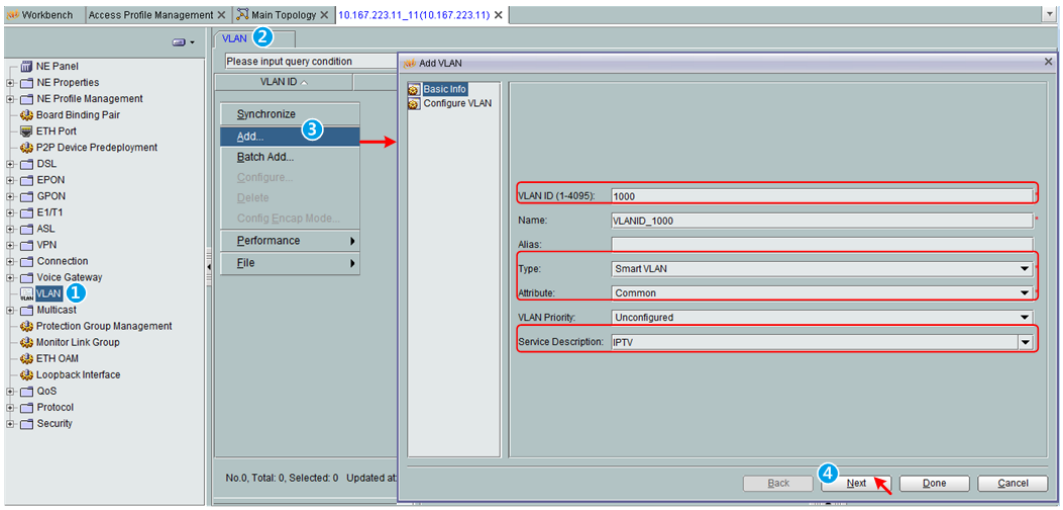
   The profile name is ftth_iptv, CIR is off, priority is 4, and priority-based scheduling policy is Local-Setting. Traffic is scheduled based on the priority specified in the profile.

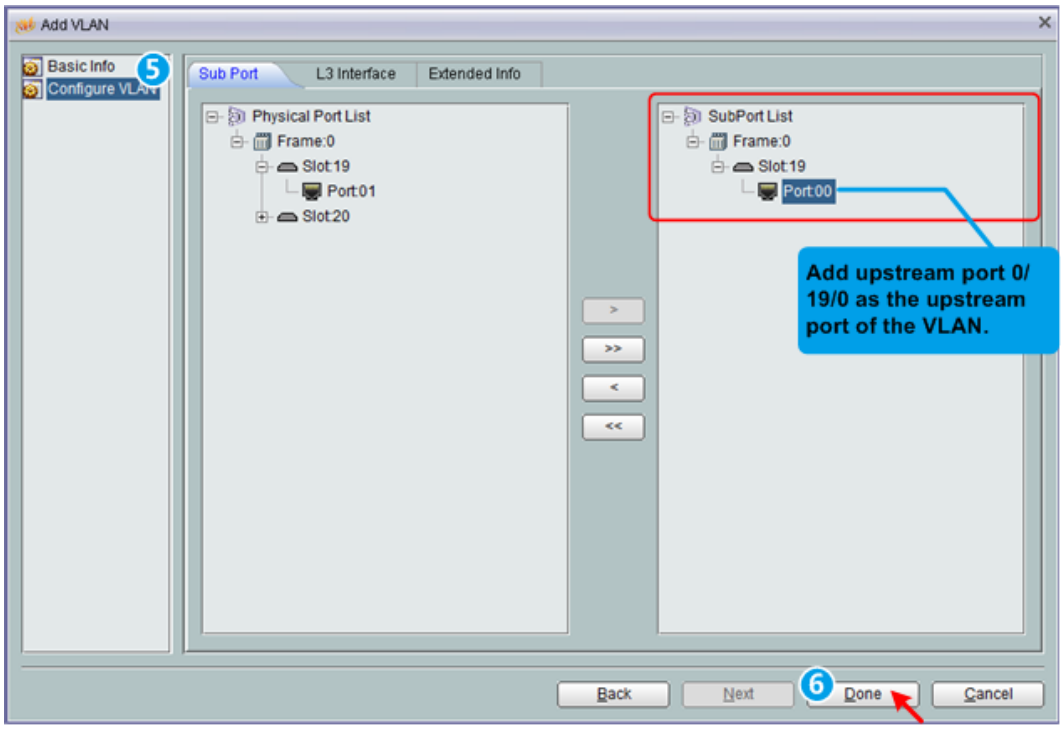


5. **Configure an S-VLAN on the OLT side.**

   The prerequisite for performing operations in the navigation tree is to navigate to the NE Explorer of the OLT. To navigate to the NE Explorer of the OLT, do as follows: In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.

   The S-VLAN is used for the multicast service.

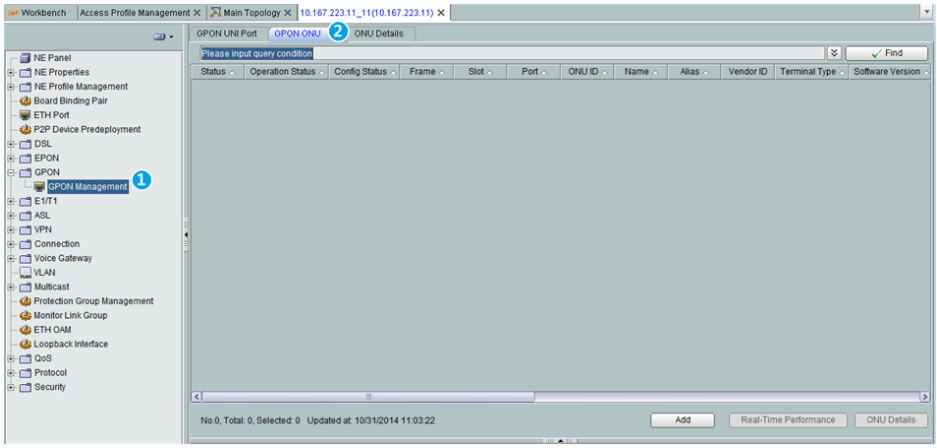


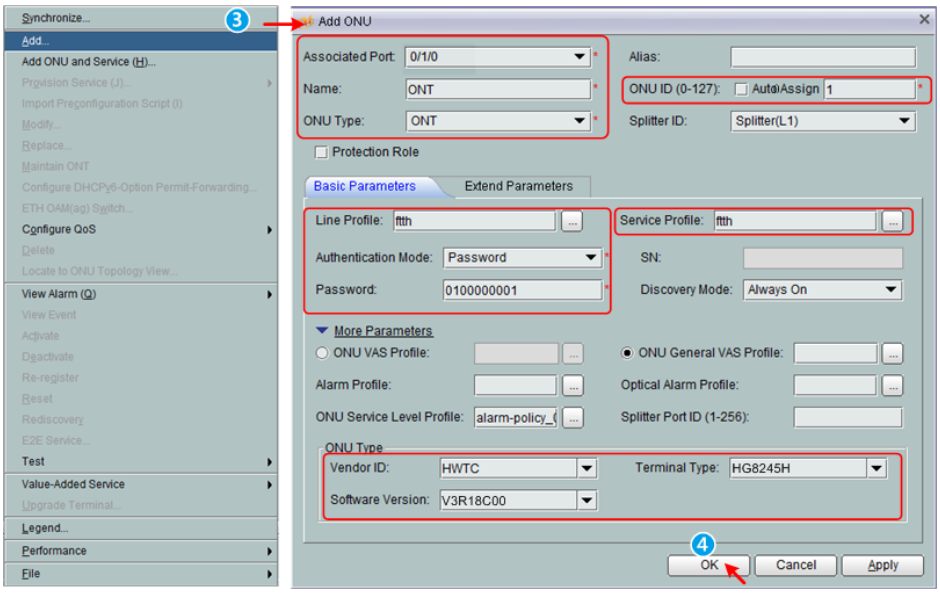


- **Provision services.**

  a. **Add an ONT.**

  The ONT connects to the GPON port 0/1/0 is ONT 1. The serial number of the ONT is 32303131D659FD40, password is 0100000001, discovery mode for password authentication is Always On, management mode is OMCI, bound ONT line profile name is ftth, and the ONT service profile name is ftth.



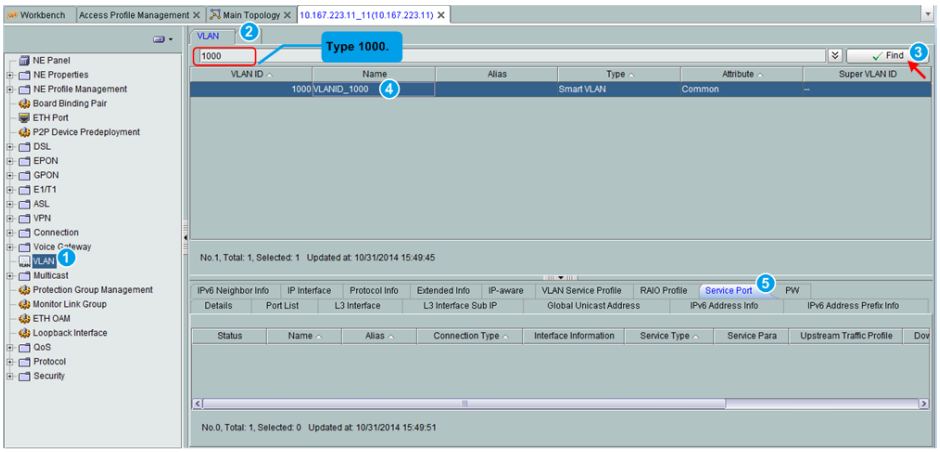


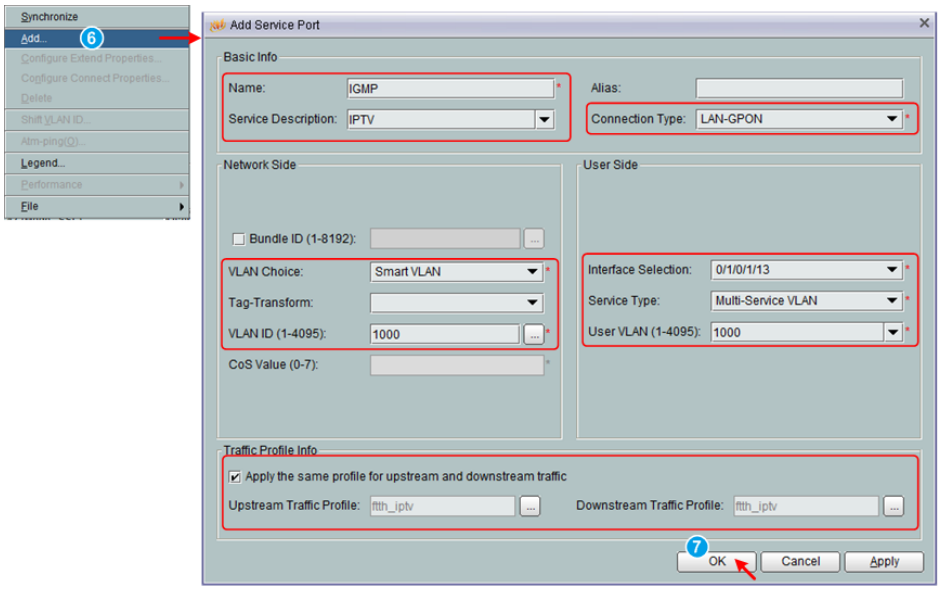
NOTE

HG8245H is used as an example. For other ONTs, set **Terminal Type** based on practical conditions.

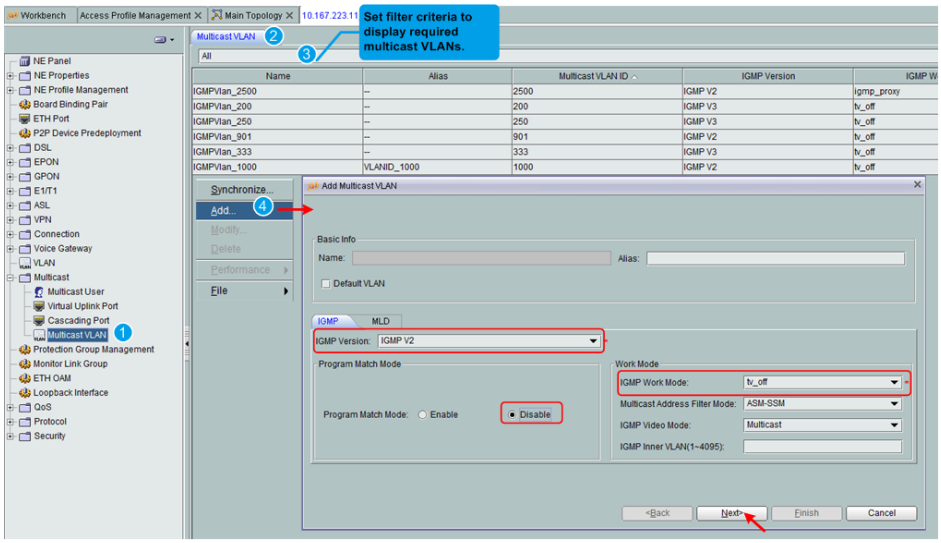
The ONT software version is the same (V300R019C00&V500R019C00) for the SIP protocol and H.248 protocol.

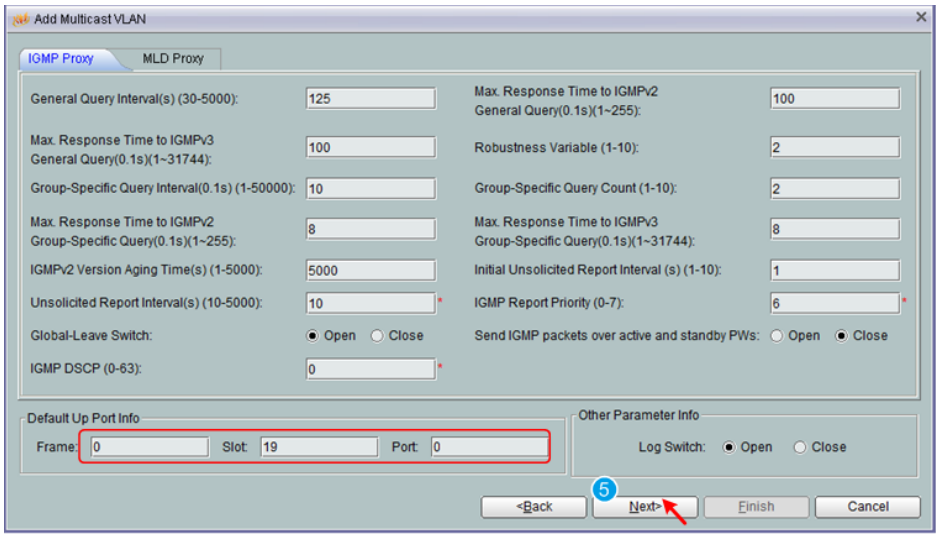
b. **Add a service virtual port on the OLT side.**

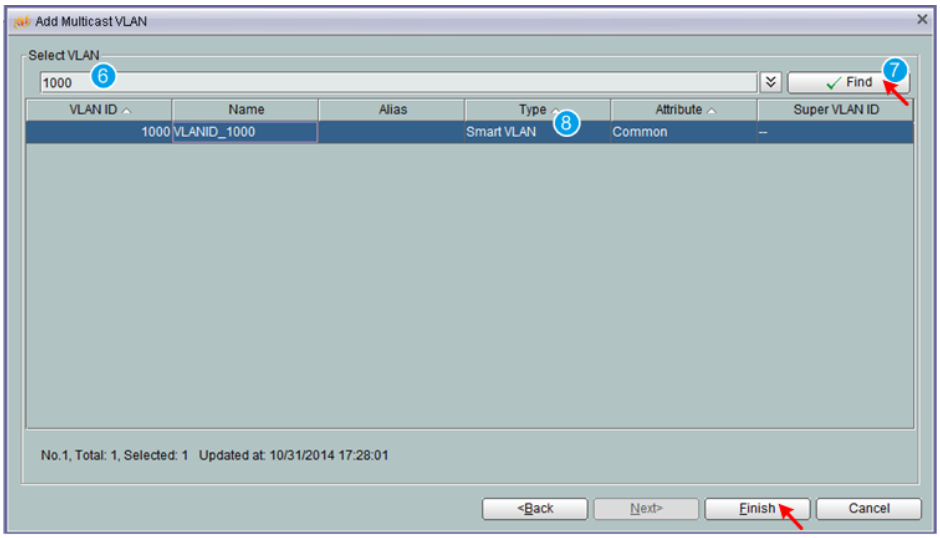




c. **Add a multicast VLAN on the OLT side.**







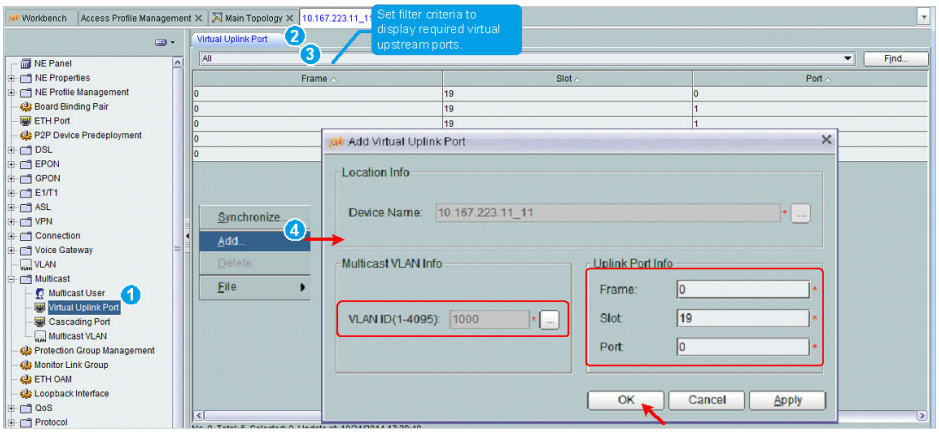
NOTE

Program match mode can be set when **IGMP Work Mode** is **tv_off**. The values of **Program match mode** are as follows:

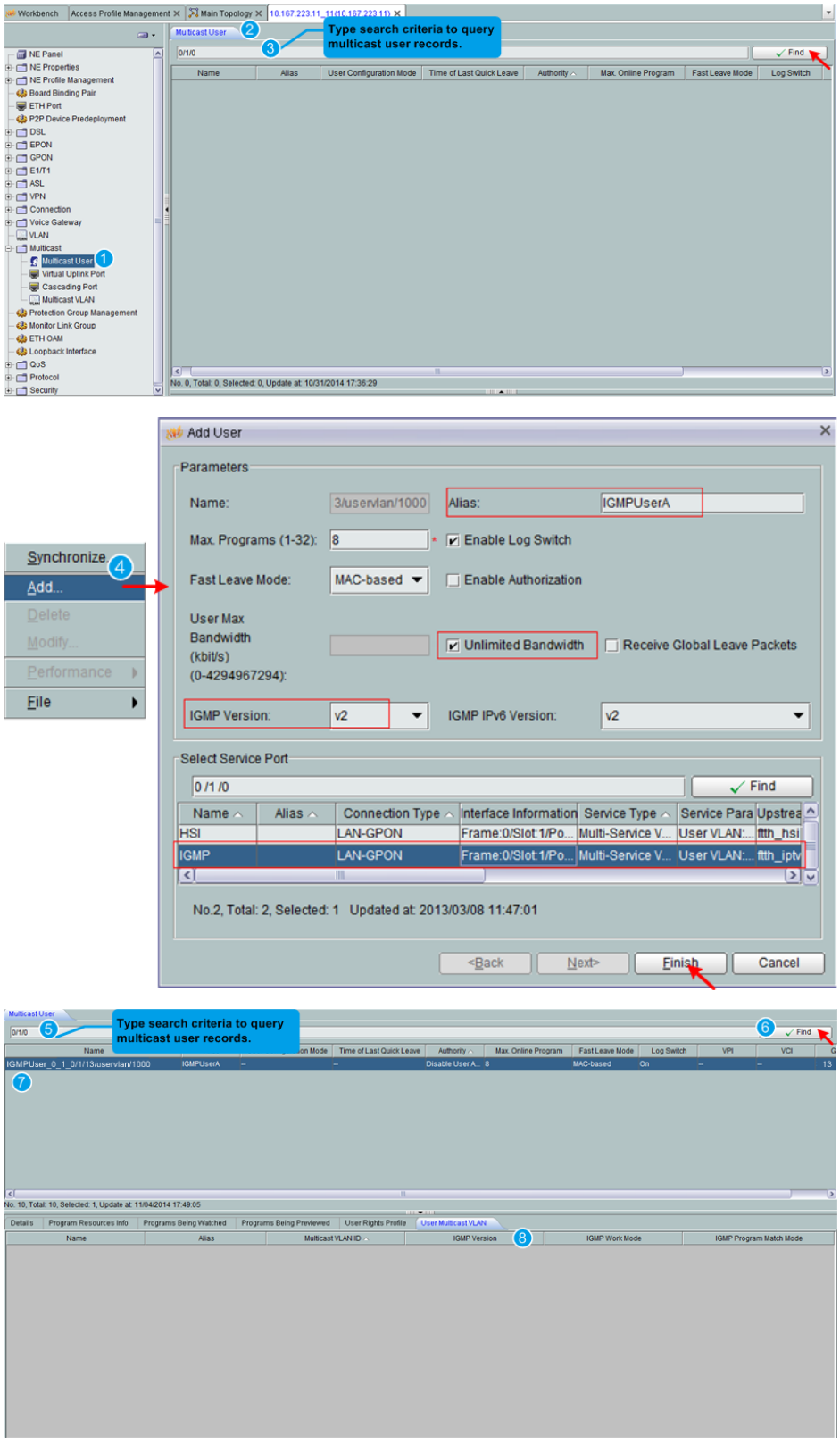
- Enable: Multicast programs are configured statically. Dynamic program generation is not supported.
- Disable: Multicast programs are dynamically generated. Static program configuration is not supported.

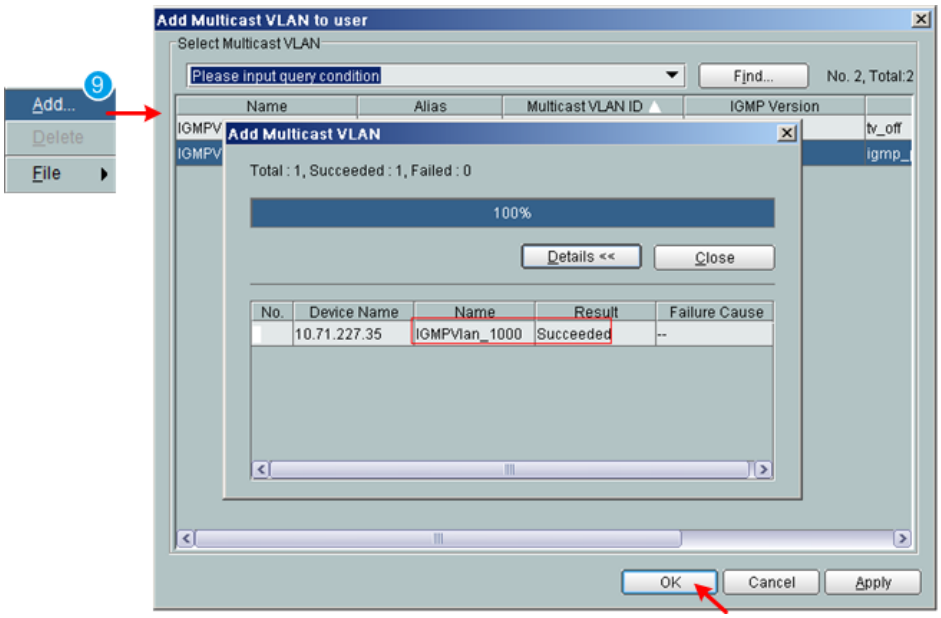
After Configuration, **IGMP Work Mode** should be set to **Proxy** again, otherwise IGMP work abnormally.

d. **Add a virtual multicast upstream port on the OLT side.**

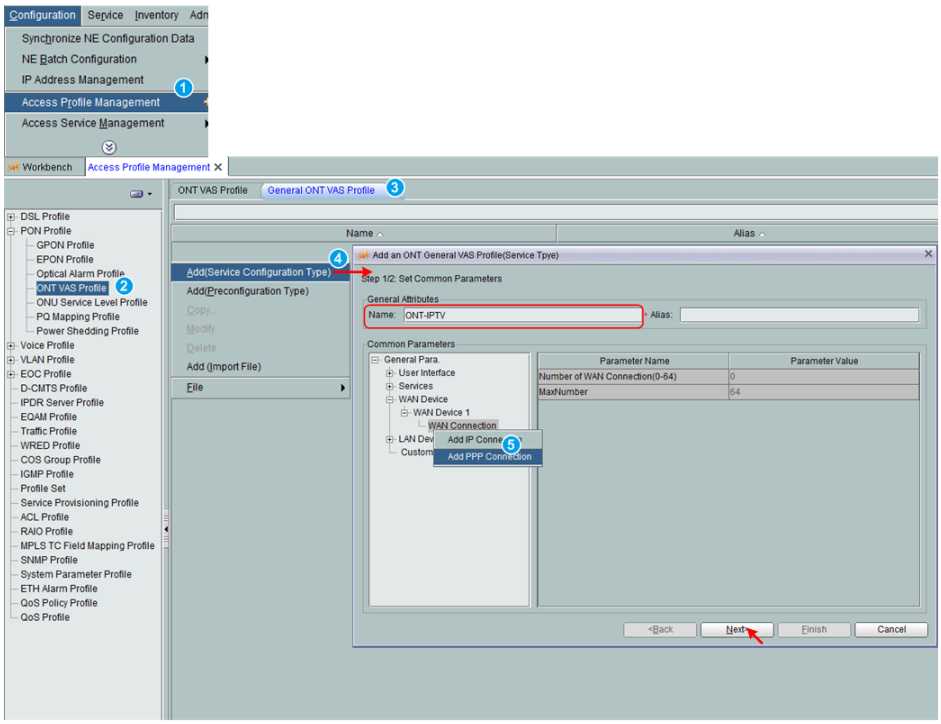


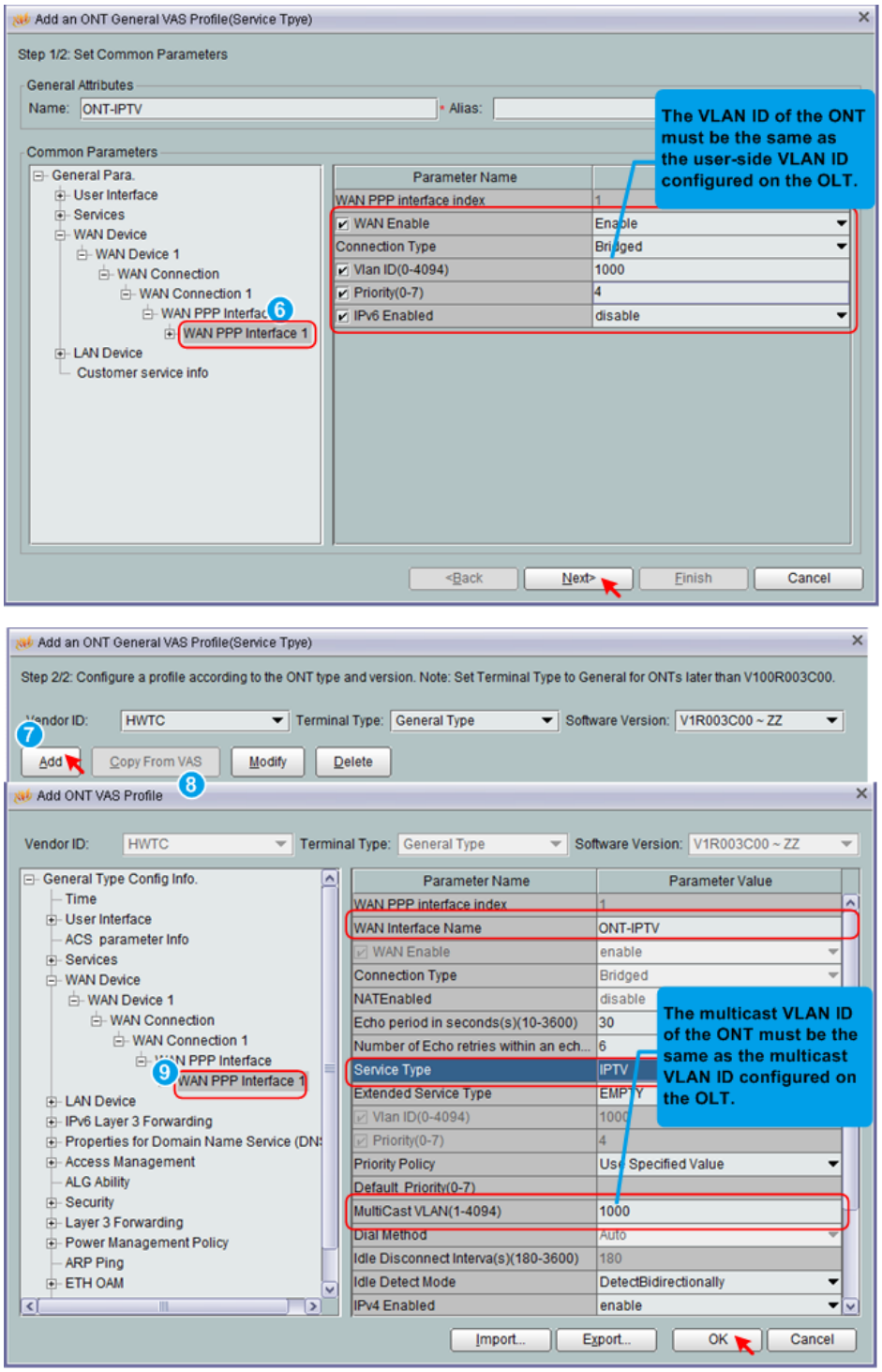
e. **Configure a multicast user on the OLT side.**

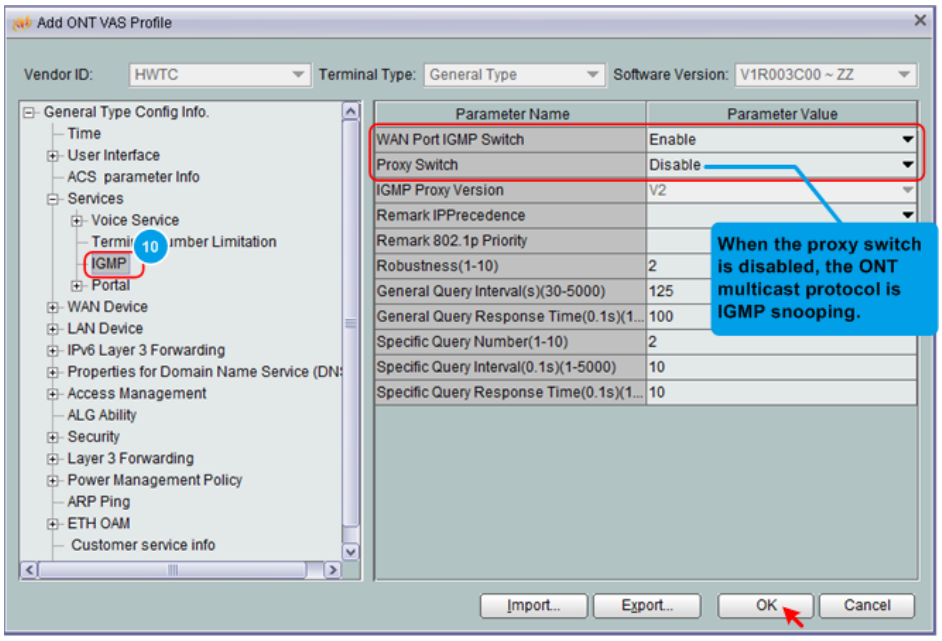

Type search criteria to query multicast user records.
Multicast User
Virtual Uplink Port
Cascading Port
Multicast VLAN
Synchronize
Add...
Delete
Modify...
Performance
File
Add User
Parameters
Name:
3/uservlan/1000
Alias:
IGMPUserA
Max. Programs (1-32):
8
Enable Log Switch
Fast Leave Mode:
MAC-based
Enable Authorization
User Max Bandwidth (kbit/s) (0-4294967294):
Unlimited Bandwidth
Receive Global Leave Packets
IGMP Version:
v2
IGMP IPv6 Version:
v2
Select Service Port
0 /1 /0
Find
Name
Alias
Connection Type
Interface Information
Service Type
Service Para
HSI
LAN-GPON
Frame:0/Slot:1/Po...
Multi-Service V...
User VLAN:...
ftth_hsi
IGMP
LAN-GPON
Frame:0/Slot:1/Po...
Multi-Service V...
User VLAN:...
ftth_iptv
No.2, Total: 2, Selected: 1 Updated at: 2013/03/08 11:47:01
<Back
Next>
Finish
Cancel
Type search criteria to query multicast user records.
Details
Program Resources Info
Programs Being Watched
Programs Being Previewed
User Rights Profile
User Multicast VLAN
Name
Alias
Multicast VLAN ID
IGMP Version
IGMP Work Mode
IGMP Program Match Mode

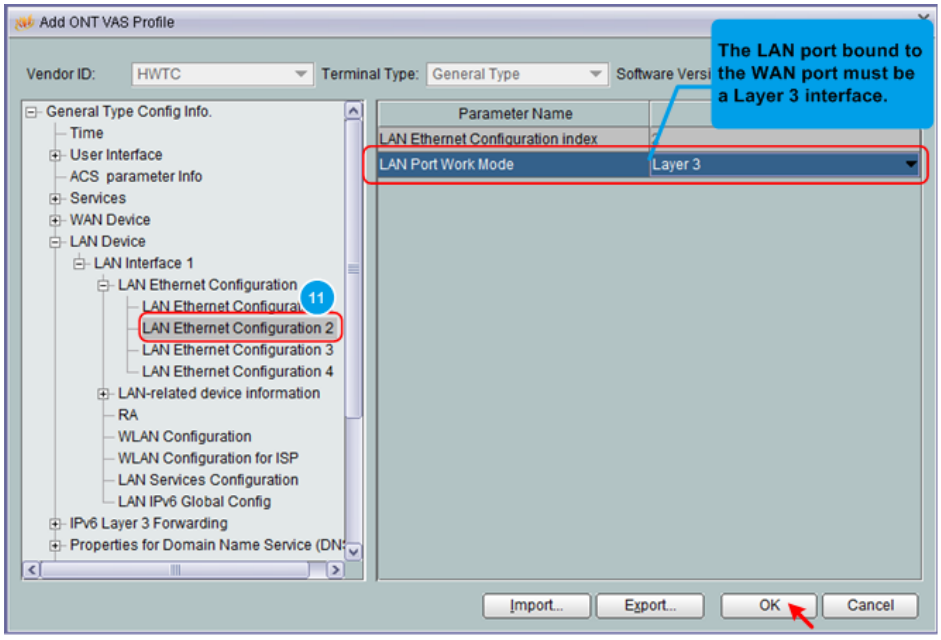


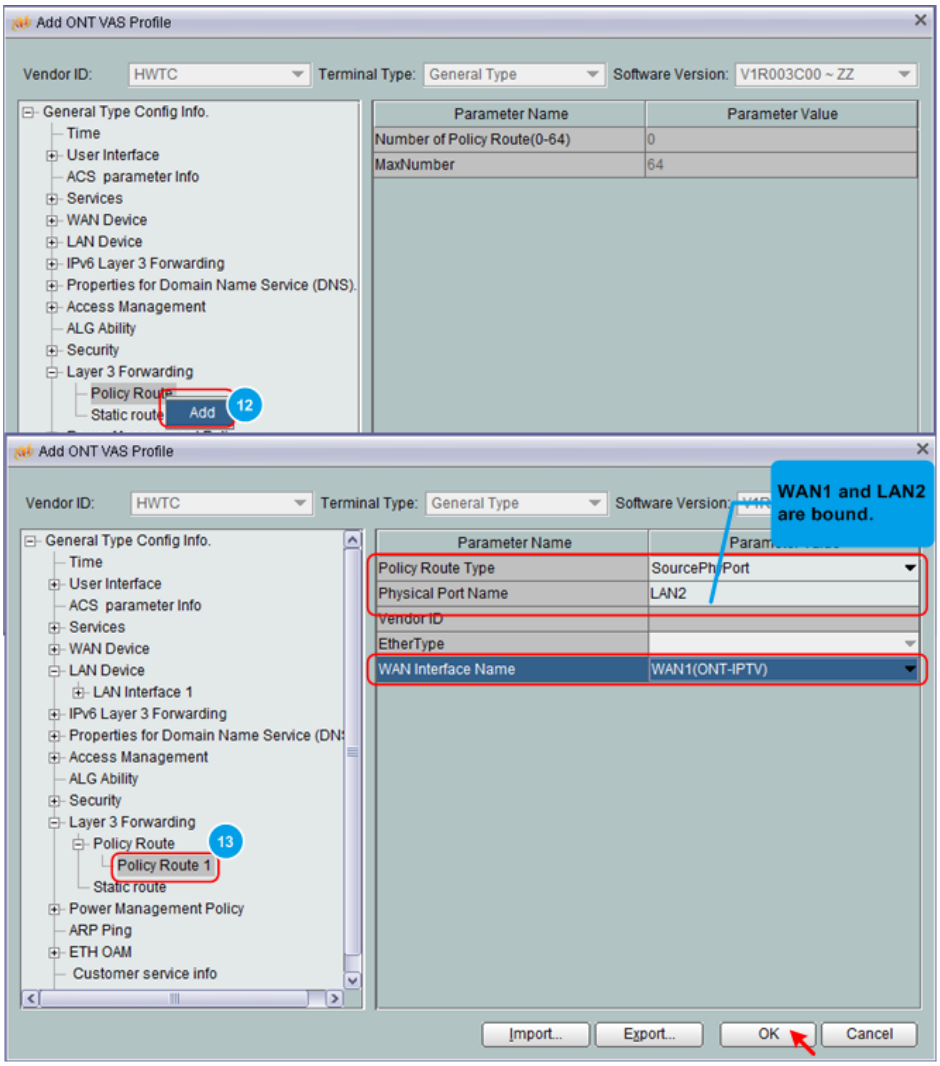
f. **Configure a general VAS profile for the ONT.**




Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-IPTV
Alias:
Common Parameters
General Para.
User Interface
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interface
WAN PPP Interface 1
LAN Device
Customer service info
Parameter Name
WAN PPP interface index
WAN Enable
Connection Type
Vlan ID(0-4094)
Priority(0-7)
IPv6 Enabled
Enable
Bridged
1000
4
disable
The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT.
6
<Back
Next>
Finish
Cancel
Add an ONT General VAS Profile(Service Tpye)
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
7
Add
Copy From VAS
8
Modify
Delete
Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interface
9
WAN PPP Interface 1
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DN
Access Management
ALG Ability
Security
Layer 3 Forwarding
Power Management Policy
ARP Ping
ETH OAM
Parameter Name
Parameter Value
WAN PPP interface index
WAN Interface Name
ONT-IPTV
WAN Enable
enable
Connection Type
Bridged
NATEnabled
disable
Echo period in seconds(s)(10-3600)
30
Number of Echo retries within an ech...
6
Service Type
IPTV
Extended Service Type
EMPTY
Vlan ID(0-4094)
1000
Priority(0-7)
4
Priority Policy
Use Specified Value
Default Priority(0-7)
MultiCast VLAN(1-4094)
1000
Dial Method
Auto
Idle Disconnect Interva(s)(180-3600)
180
Idle Detect Mode
DetectBidirectionally
IPv4 Enabled
enable
The multicast VLAN ID of the ONT must be the same as the multicast VLAN ID configured on the OLT.
Import...
Export...
OK
Cancel


Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
Voice Service
IGMP
Portal
WAN Device
LAN Device
IPv6 Layer 3 Forwarding
Access Management
ALG Ability
Security
Layer 3 Forwarding
Power Management Policy
ARP Ping
ETH OAM
Customer service info
10
Parameter Name
Parameter Value
WAN Port IGMP Switch
Enable
Proxy Switch
Disable
IGMP Proxy Version
V2
Remark IPPrecedence
Remark 802.1p Priority
Robustness(1-10)
2
General Query Interval(s)(30-5000)
125
General Query Response Time(0.1s)(1...
100
Specific Query Number(1-10)
2
Specific Query Interval(0.1s)(1-5000)
10
Specific Query Response Time(0.1s)(1...
10
When the proxy switch is disabled, the ONT multicast protocol is IGMP snooping.
Import...
Export...
OK
Cancel

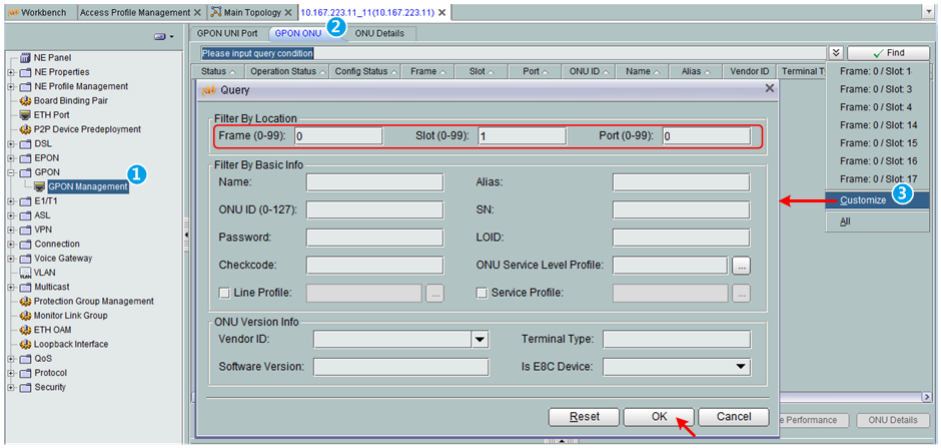

Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
LAN Interface 1
LAN Ethernet Configuration
LAN Ethernet Configuration 2
LAN Ethernet Configuration 3
LAN Ethernet Configuration 4
LAN-related device information
RA
WLAN Configuration
WLAN Configuration for ISP
LAN Services Configuration
LAN IPv6 Global Config
IPv6 Layer 3 Forwarding
11
Parameter Name
LAN Ethernet Configuration index
LAN Port Work Mode
Layer 3
The LAN port bound to the WAN port must be a Layer 3 interface.
Import...
Export...
OK
Cancel

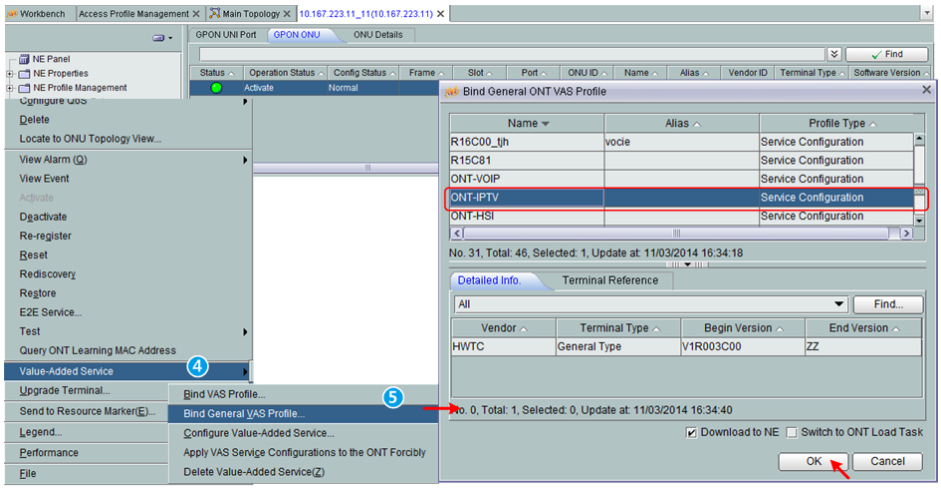


NOTE

To bind a WAN port to multiple LAN ports, set **Physical Port Name** to **LAN1,...,LANx**. For example, to bind WAN 1 to LAN 1 and LAN 2, set **Physical Port Name** to **LAN1, LAN2**.

g. Bind a general VAS profile.





Result

The user can watch programs on TV.

3.3.2 Configuration by Using OLT Commands

This topic describes how to configure the Internet access service, VoIP service and IPTV service by using OLT commands.

3.3.2.1 Gateway ONT Network Scenario (GPON and 10G GPON Access)

This topic describes how to configure Internet access service, voice service, BTV service and VoD service when gateway ONT are used to build an FTTH network.

The FTTH GPON and 10G GPON access have the same configuration procedure. ONT web pages for configuring them have differences; however, they have the same configuration parameters. The following uses GPON ONT configuration as an example. For differences on web pages, see the related ONT manuals.

3.3.2.1.1 Service Requirements and Application Scenario

Service Requirements

Optical fibers are connected to users' home and triple play services are required. The following provides detailed service requirements:

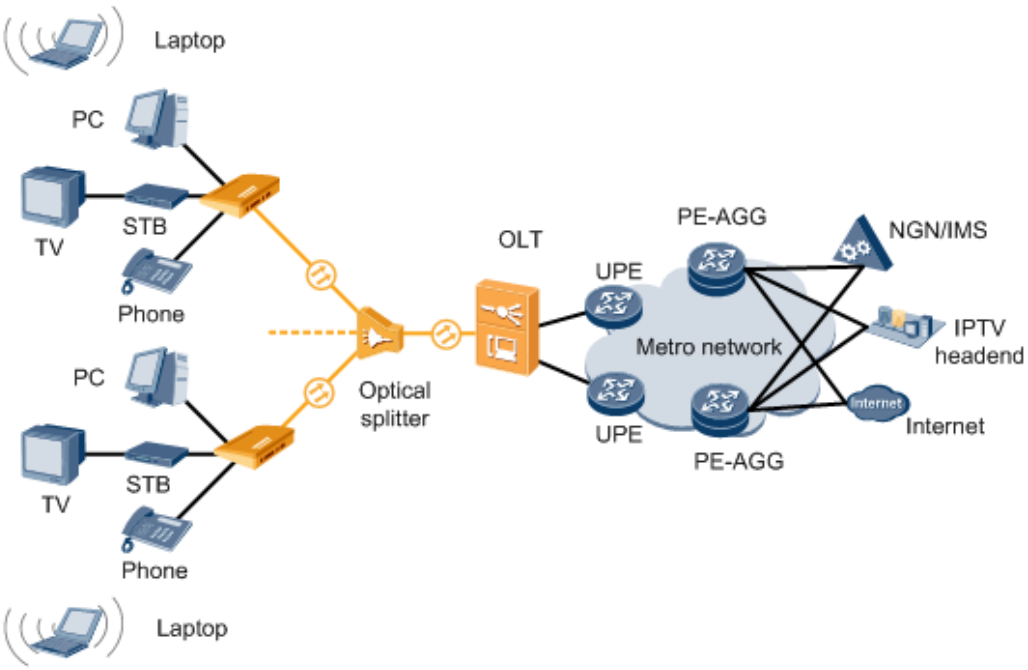
- Internet access of multiple PCs in a home is supported.
- Access of multiple telephones in a home is supported.
- IPTV programs can be previewed and watched using STBs.
- Service expansibility is supported and different services do not affect each other.
- Service security is ensured.
  - Internet and Wi-Fi access services are protected against unauthorized access, user account theft or borrowing, MAC/IP spoofing, and malicious attack.
  - Voice and IPTV services are protected against MAC/IP spoofing, malicious attack, and traffic flooding attack.
- Service faults are easy to locate and services are easy to maintain.

Application Scenario

As shown in **Figure 3-8**, the ONT integrating an IAD provides Internet, Wi-Fi, VoIP, and IPTV services to users.

The HGW ONT facilitates interconnection of home devices by providing Layer 3 services, such as Point-to-Point Protocol over Ethernet (PPPoE)/DHCP dialup, network address translation (NAT), and Internet Group Management Protocol (IGMP) snooping. This scenario provides fine-grained management channels and service control, and mainly applies to Layer 3 networking.

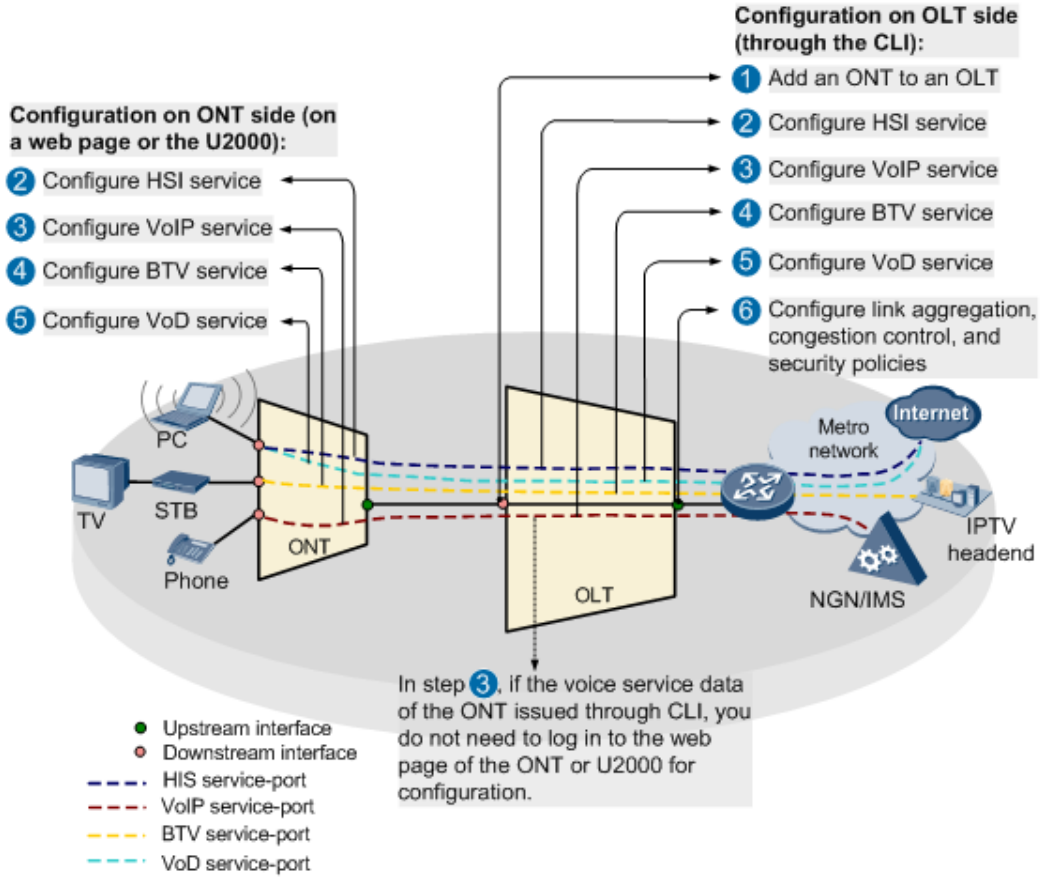
Figure 3-8 HGW ONT



3.3.2.1.2 Configuration Process

Figure 3-9 shows the configuration roadmap in fiber to the home (FTTH) networking using a gateway optical network terminal (ONT).

Figure 3-9 Configuration roadmap in FTTH networking using a gateway ONT



The following table describes the configuration steps.

Item	Step	Description
Optical line terminal (OLT)	Adding an ONT to an OLT	Services can be configured for an ONT only after the ONT is successfully added to an OLT.
OLT ONT U2000	Configuring the Internet Access Service (on a Web Page or the U2000)	None
	Configuring the Wi-Fi Access Service (on a Web Page)	None

<table>
<tr><th>Item</th><th colspan="2">Step</th><th>Description</th></tr>
<tr><td rowspan="5"></td><td rowspan="4">Configure the VoIP service.</td><td>Configuring the H.248-based Voice Service (on a Web Page or the U2000)</td><td rowspan="4">NOTE
● The H.248 and Session Initiation Protocol (SIP) protocols are mutually exclusive for the VoIP service. Either of them is configured at a time.
● The voice service can be configured through command line interface (CLI) on an OLT, web page, or U2000. Select a configuration mode based on site requirements.
  ● OLT CLI: This mode can be used for site deployment or the U2000 has not been deployed.
  ● Web page: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for site deployment.
  ● U2000: This mode can be used to configure voice parameters after the service channel has been configured through the OLT CLI. It can be used for service provisioning in batches.</td></tr>
<tr><td>Configuring the H.248-based Voice Service (Through the CLI)</td></tr>
<tr><td>Configuring the SIP-based Voice Service (on a Web Page or the U2000)</td></tr>
<tr><td>Configuring the SIP-based Voice Service (Through the CLI)</td></tr>
<tr><td rowspan="2">Configure the IPTV service.</td><td>Configuring the BTV Service (on the Web Page)</td><td rowspan="2">IPTV services include the BTV and VoD services that are different in configuration procedures and need to be configured separately.</td></tr>
<tr><td>Configuring the VoD Service (on the Web Page)</td></tr>
<tr><td>OLT</td><td colspan="2">Configuring Link Aggregation, Congestion Control, and Security Policies</td><td>The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.</td></tr>
<tr><td>OLT</td><td colspan="2">Verifying Services</td><td>The OLT provides remote verification methods including ONT PPPoE/DHCP dialup emulation and call emulation for configuration and commissioning engineers to verify services remotely after service configuration, avoiding a second on-site operation.</td></tr>
</table>

3.3.2.1.3 Adding an ONT to an OLT

Services can be configured for an ONT only after the ONT is successfully added to an OLT.

Data Plan

Item	Data
DBA profile	Profile name: ftth_dba_mngt ● Profile type: Type1 ● Fixed bandwidth: 1 Mbit/s Profile name: ftth_dba_hsi ● Profile type: Type4 ● Maximum bandwidth: 32 Mbit/s Profile name: ftth_dba_voip ● Profile type: Type2 ● Assured bandwidth: 1 Mbit/s Profile name: ftth_dba_iptv ● Profile type: Type2 ● Assured bandwidth: 1 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID for management services: 4 T-CONT ID for voice services: 5 T-CONT ID for video services: 6 T-CONT ID for Internet access services: 7 GEM port ID for management services: 11 GEM port ID for voice services: 12 GEM port ID for video services: 13 GEM port ID for Internet access services: 14
ONT service profile	Profile name: ftth ONT port capability set: adaptive
Network topology data	PON port: 0/1/0 ONT IDs: 1 and 2

Procedure

Step 1 Configure GPON ONT profiles.

GPON ONT profiles include the DBA profile, line profile, service profile, and alarm profile.

- DBA profile: A DBA profile describes the GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth utilization.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the traffic stream, and the mapping between the GEM port and the ONT-side service.

- Service profile: A service profile provides the service configuration channel for the ONT that is managed by using optical network terminal management and control interface (OMCI).
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONT lines. When a statistical value reaches the threshold, the host is notified and an alarm is reported to the log host and the NMS.

1. Configure a DBA profile.

   Run the **display dba-profile** command to query the existing DBA profiles in the system. If the existing DBA profiles in the system cannot meet the requirements, run the **dba-profile add** command to add a DBA profile.

   ```
   huawei(config)#dba-profile add profile-name ftth_dba_mngt type1 fix 1024
   huawei(config)#dba-profile add profile-name ftth_dba_voip type2 assure 1024
   huawei(config)#dba-profile add profile-name ftth_dba_iptv type2 assure 1024
   huawei(config)#dba-profile add profile-name ftth_dba_hsi type4 max 32768
   ```

   NOTE

   Select a DBA profile of the proper bandwidth type and configure proper bandwidth according to the service types and total user count of the ONT. Note that the sum of the fixed bandwidth and the assured bandwidth must not be greater than the total bandwidth of the PON port.

2. Configure an ONT line profile.

   Create a GPON ONT line profile, named **ftth**, and bind it to the DBA profile.

   ```
   huawei(config)#ont-lineprofile gpon profile-name ftth
   huawei(config-gpon-lineprofile-1)#tcont 4 dba-profile-name ftth_dba_mngt
   huawei(config-gpon-lineprofile-1)#tcont 5 dba-profile-name ftth_dba_voip
   huawei(config-gpon-lineprofile-1)#tcont 6 dba-profile-name ftth_dba_iptv
   huawei(config-gpon-lineprofile-1)#tcont 7 dba-profile-name ftth_dba_hsi
   ```

   Create different GEM ports according to different service types, in which

   - GEM port 11 is used to carry management services.
   - GEM port 12 is used to carry voice services.
   - GEM port 13 is used to carry video services.
   - GEM port 14 is used to carry Internet access services.

   ```
   huawei(config-gpon-lineprofile-1)#gem add 11 eth tcont 4
   huawei(config-gpon-lineprofile-1)#gem add 12 eth tcont 5
   huawei(config-gpon-lineprofile-1)#gem add 13 eth tcont 6
   huawei(config-gpon-lineprofile-1)#gem add 14 eth tcont 7
   ```

   NOTE

   1. To change the default QoS mode, run the **qos-mode** command to set the QoS mode to **gem-car** or **flow-car**, and run the **gem add** command to set the index of the traffic profile bound to the GEM port.
   2. When the QoS mode is priority-queue (PQ), the default queue priority is 0; when the QoS mode is flow-car or gem-car, traffic profile 6 is bound to the GEM port by default (no rate limitation).

   After the configurations are complete, run the **commit** command to apply the parameters settings.

   ```
   huawei(config-gpon-lineprofile-1)#commit
   huawei(config-gpon-lineprofile-1)#quit
   ```

3. Configure an ONT service profile.

   Create a GPON ONT service profile, named **ftth**. Configure the capability set of the ETH port, POTS port and CATV POTS to **adaptive**. Then the system automatically adapts to the ONT according to the actual capability of the online ONT.


```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#ont-port eth adaptive pots adaptive catv
adaptive
```

After the configurations are complete, run the **commit** command to apply the parameters setting.

```
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. (Optional) Add an alarm profile.
   - The default GPON alarm profile 1 is used. The alarm thresholds for the default alarm profile are 0, which indicates that no alarm is generated.
   - In this example, the default alarm profile is used, and therefore the configuration of the alarm profile is not required.
   - Run the **gpon alarm-profile add** command to configure a GPON alarm profile, which is used for monitoring the performance of an activated ONT line.

Step 2 Add an ONT.

The procedures for configuring GPON, XG-PON, and XGS-PON services are the same. The difference lies in this step. Here, the GPON service is used as an example. When configuring XG-PON and XGS-PON services, you need to configure the ONT network-side interface type parameter (ont-type) in the **ont add** and **ont confirm** commands. Select a value based on the actual ONT capability or service data plan, for example, 10g/2.5g.

Connect two ONTs to GPON port 0/1/0. Set the ONT IDs to **1** and **2**, SNs to **3230313126595540** and **6877687714852901**, passwords to **0100000001** and **0100000002**, discovery mode for password authentication to **once-on**, and management mode to **OMCI**. Bind the two ONTs to ONT line profile **ftth** and ONT service profile **ftth**.

There are two methods of adding an ONT: add an ONT offline and confirm an automatically discovered ONT.

- Add ONTs offline.

  If the password of an ONT is known, run the **ont add** command to add an ONT offline.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont add 0 1 password-auth 0100000001 once-on no-
aging omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont add 0 2 password-auth 0100000002 once-on no-
aging omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```

- Confirm automatically discovered ONTs.

  If the password or SN of an ONT is unknown, run the **port** *portid* **ont-auto-find** command in GPON mode to enable the ONT auto-discovery function of the GPON port. Then, run the **ont confirm** command to confirm the ONT.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/1)#display ont autofind 0
  //After this command is executed, the information about all ONTs connected
to the GPON port through optical splitters is displayed.

huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 3230313126595540
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 2 sn-auth 6877687714852901
omci ont-lineprofile-name
 ftth ont-srvprofile-name ftth
```


NOTE

If multiple ONTs of the same type bound to the same line profile or service profile are connected to the same port, you can bulk add ONTs by bulk confirming automatically discovered ONTs to make configuration easier and more efficient. To do so, the preceding command can be modified as follows:

```
huawei(config-if-gpon-0/1)#ont confirm 0 all sn-auth omci ont-lineprofile-
name ftth
ont-srvprofile-name ftth
```

- (Optional) Bind the alarm profile to the ONT.

  The default profile 1 is used in this example.

```
huawei(config-if-gpon-0/1)#ont alarm-profile 0 1 profile-id 1
huawei(config-if-gpon-0/1)#ont alarm-profile 0 2 profile-id 1
```

Step 3 Check ONT status.

After an ONT is added, run the **display ont info** command to query the current status of the ONT. Ensure that **Config flag** of the ONT is **active**, **Run State** is **online**, **Config state** is **normal**, and **Match state** is **match**.

```
huawei(config-if-gpon-0/1)#display ont info 0 1
  ------------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  Control flag         : active    //Indicates that the ONT is
activated.
  Run state            : online    //Indicates that the ONT goes online
successfully.
  Config state         : normal    //Indicates that the configuration state of
the ONT is normal.
  Match state          : match     //Indicates that the capability profile bound
to the ONT is consistent with the actual capability of the ONT.
...//The rest of the response information is omitted.
```

When **Config state** is **failed**, **Run state** is **offline**, or **Match state** is **mismatch**:

- If **Control flag** is **deactivated**, run the **ont active** command in GPON mode to activate the ONU.
- If **Run state** is **offline**, a physical line may be broken or the optical module may be damaged. Check the line and the optical module.
- If **Config state** is **failed**, the configured ONU capability exceeds the actual ONU capability. In this case, run the **display ont failed-configuration** command in the diagnose mode to check the failed configuration item and the failure cause. Then, rectify the fault accordingly.

----End

3.3.2.1.4 Configuring the Internet Access Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with high-speed Internet access services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configurations, see the configuration guide.
- The ONT has been added to the OLT. For details, see **3.3.2.1.3 Adding an ONT to an OLT**.

- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 14
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● CVLAN ID: 1001 ● C'-VLAN ID: 1010-1011 VLAN translation policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the profile ID to ftth_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

     ```
     huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0 priority-policy local-setting
     ```

  b. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 1001 is mapped to GEM port 14 in the ONT line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  c. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 100.

```
huawei(config)#vlan 100 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100 0/9 0
```

d. Create service flows.

Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001, and use traffic profile ftth_hsi.

```
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add
inner-vlan 1010 inbound traffic-table name ftth_hsi outbound traffic-table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-service
user-vlan 1001 tag-transform translate-and-add
inner-vlan 1011 inbound traffic-table name ftth_hsi outbound traffic-table name ftth_hsi
```

e. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the Web page.

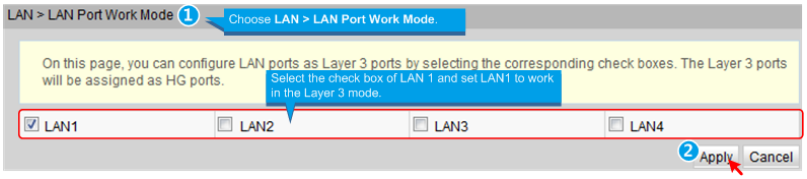
a. Log in to the Web configuration page.

i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

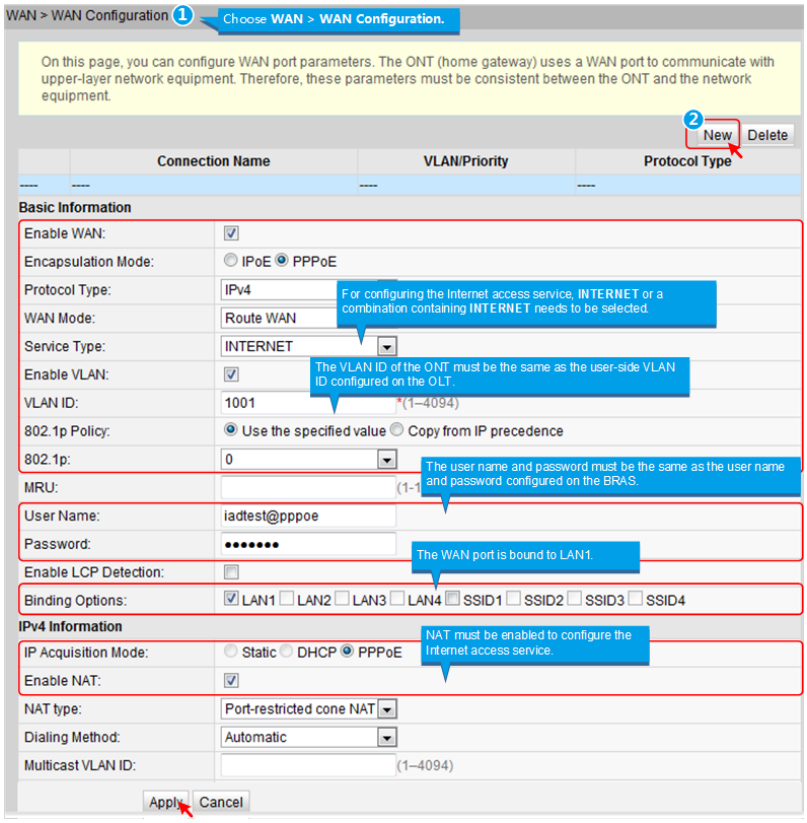
ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

b. Configure the working mode of a LAN port.

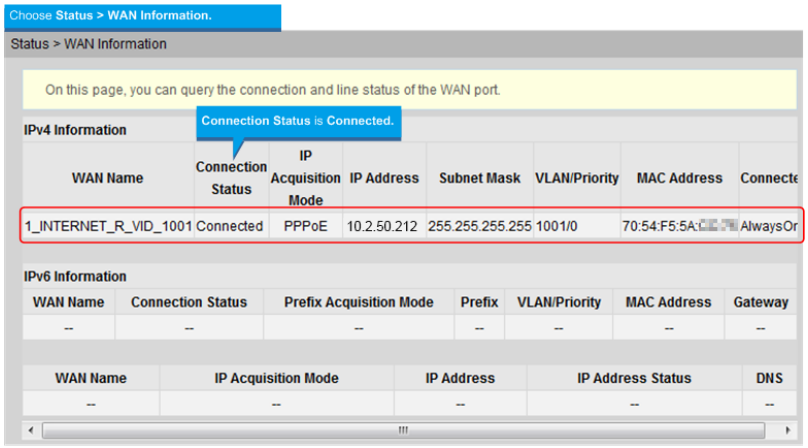
The LAN port bound to the WAN port must work in the Layer 3 mode. Therefore, set the working mode to Layer 3 for the LAN port connected to the PC.



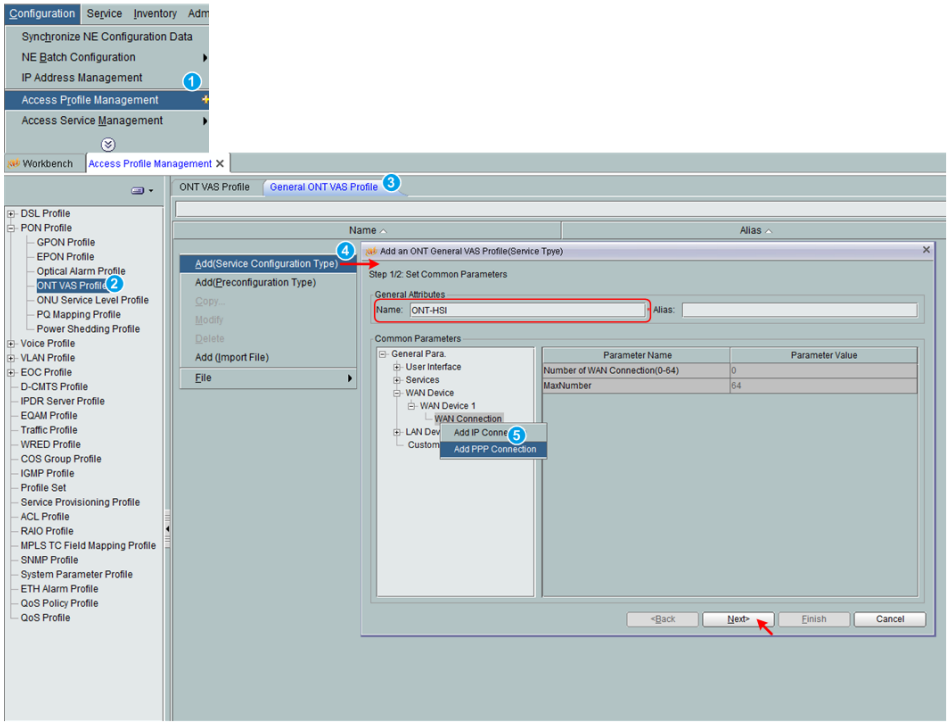
c. Configure parameters of a WAN port.



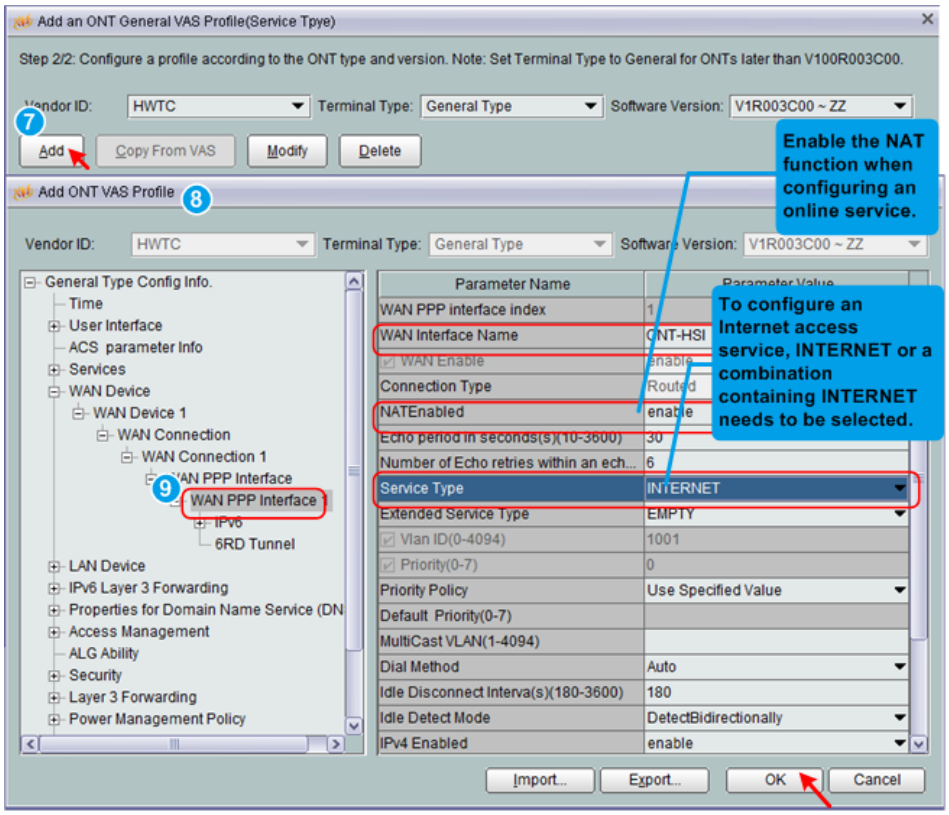
d. Check the ONT connection status.

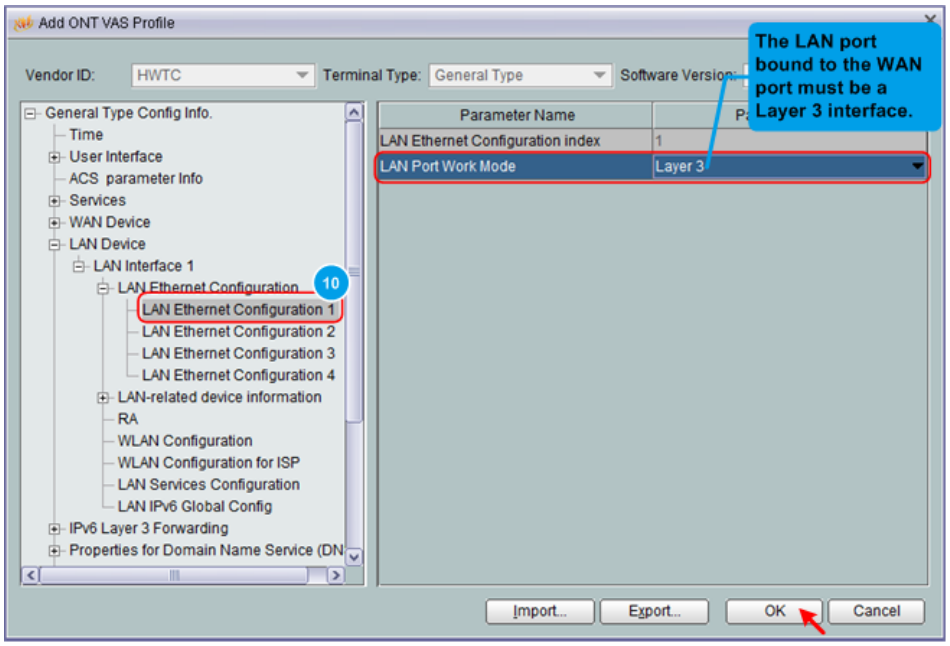


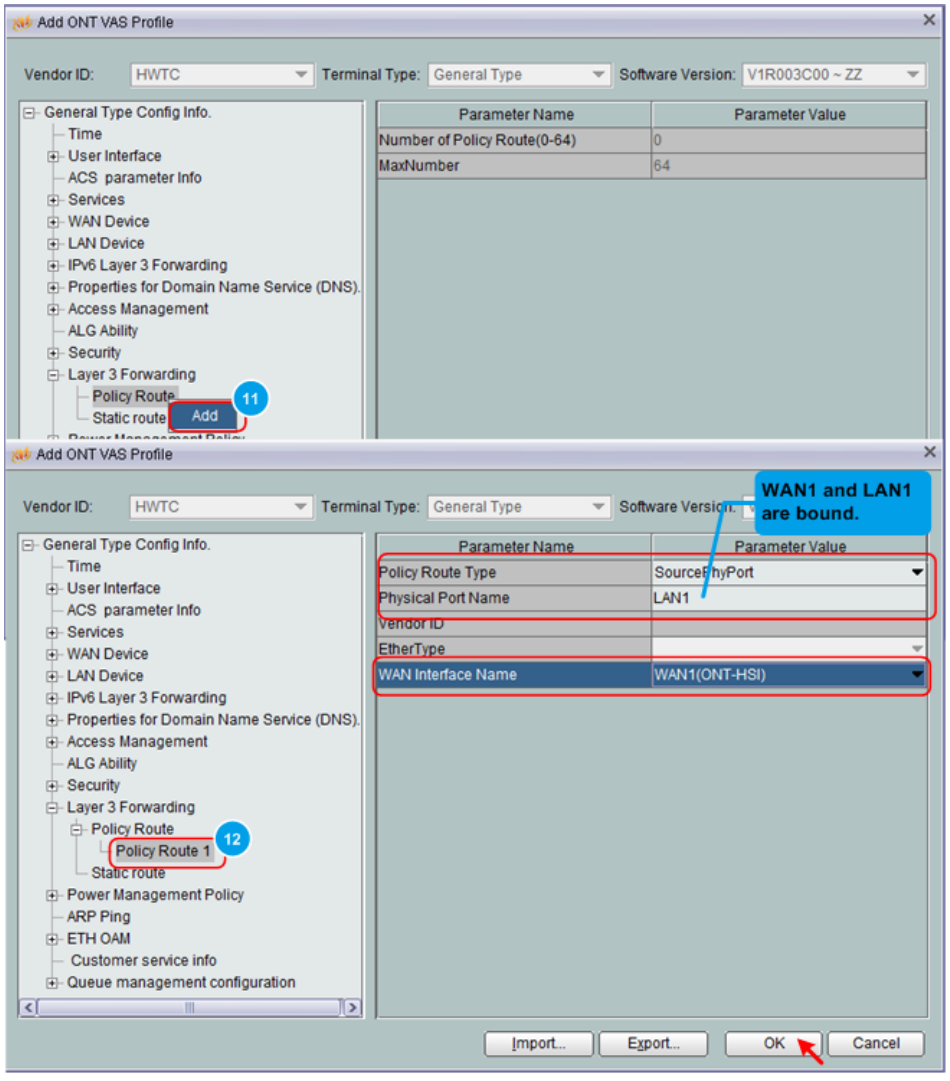
- Configure the ONT on the U2000.
  a. **Add a general VAS configuration profile for the ONT.**


Configuration
Service
Inventory
Synchronize NE Configuration Data
NE Batch Configuration
IP Address Management
Access Profile Management
Access Service Management
Workbench
Access Profile Management
ONT VAS Profile
General ONT VAS Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
QoS Profile
Name
Alias
Add(Service Configuration Type)
Add(Preconfiguration Type)
Copy
Modify
Delete
Add (Import File)
File
Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-HSI
Alias:
Common Parameters
General Para.
User Interface
Services
WAN Device
WAN Device 1
WAN Connection
Add IP Connection
Add PPP Connection
Parameter Name
Parameter Value
Number of WAN Connection(0-64)
MaxNumber
<Back
Next>
Finish
Cancel

353


Add an ONT General VAS Profile(Service Tpye)
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
Add
Copy From VAS
Modify
Delete
Add ONT VAS Profile
Enable the NAT function when configuring an online service.
To configure an Internet access service, INTERNET or a combination containing INTERNET needs to be selected.
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interface
IPv6
6RD Tunnel
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DN
Access Management
ALG Ability
Security
Layer 3 Forwarding
Power Management Policy
Parameter Name
WAN PPP interface index
WAN Interface Name
WAN Enable
Connection Type
NATEnabled
Echo period in seconds(s)(10-3600)
Number of Echo retries within an ech...
Service Type
Extended Service Type
Vlan ID(0-4094)
Priority(0-7)
Priority Policy
Default Priority(0-7)
MultiCast VLAN(1-4094)
Dial Method
Idle Disconnect Interva(s)(180-3600)
Idle Detect Mode
IPv4 Enabled
ONT-HSI
Routed
enable
30
6
INTERNET
EMPTY
1001
0
Use Specified Value
Auto
180
DetectBidirectionally
enable
Import...
Export...
OK
Cancel

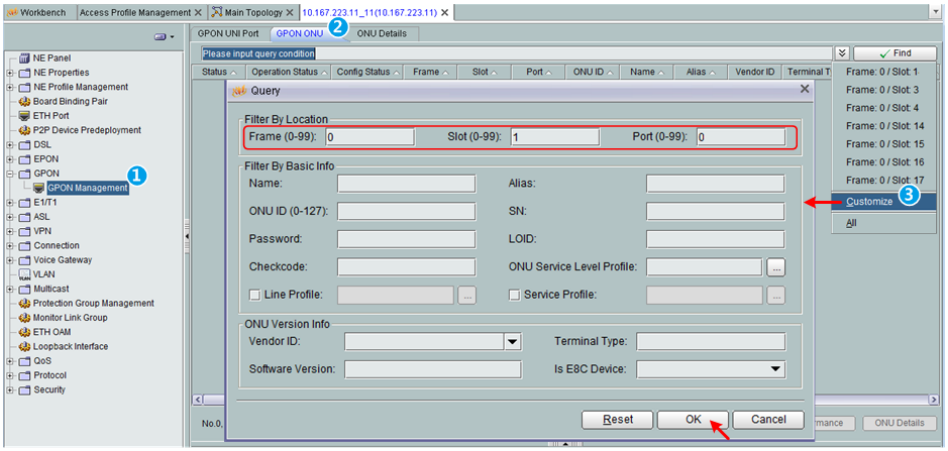

Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version:
The LAN port bound to the WAN port must be a Layer 3 interface.
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
LAN Interface 1
LAN Ethernet Configuration
LAN Ethernet Configuration 1
LAN Ethernet Configuration 2
LAN Ethernet Configuration 3
LAN Ethernet Configuration 4
LAN-related device information
RA
WLAN Configuration
WLAN Configuration for ISP
LAN Services Configuration
LAN IPv6 Global Config
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DN
10
Parameter Name
LAN Ethernet Configuration index
1
LAN Port Work Mode
Layer 3
Import...
Export...
OK
Cancel


Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DNS)
Access Management
ALG Ability
Security
Layer 3 Forwarding
Policy Route
Static route
Add
11
Parameter Name
Parameter Value
Number of Policy Route(0-64)
0
MaxNumber
64
Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version:
WAN1 and LAN1 are bound.
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DNS)
Access Management
ALG Ability
Security
Layer 3 Forwarding
Policy Route
Policy Route 1
Static route
Power Management Policy
ARP Ping
ETH OAM
Customer service info
Queue management configuration
12
Parameter Name
Parameter Value
Policy Route Type
SourcePhyPort
Physical Port Name
LAN1
Vendor ID
EtherType
WAN Interface Name
WAN1(ONT-HSI)
Import...
Export...
OK
Cancel

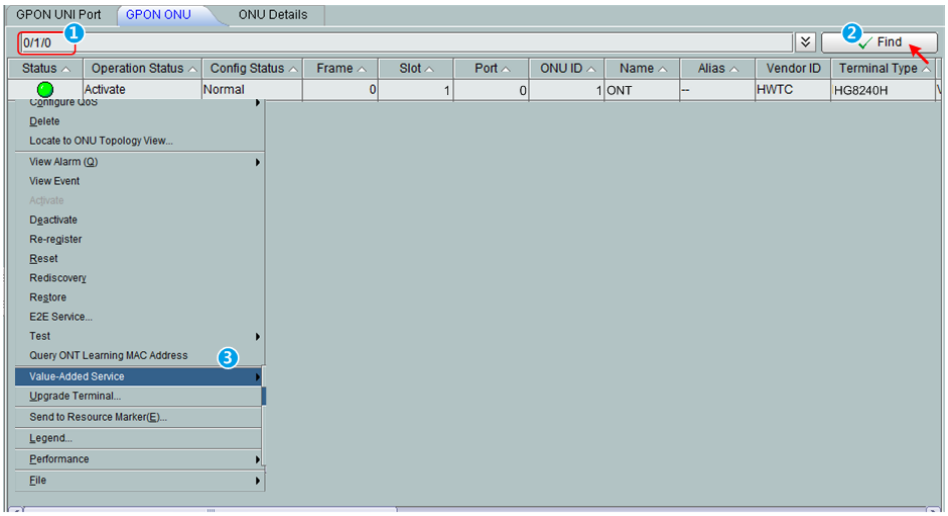
NOTE

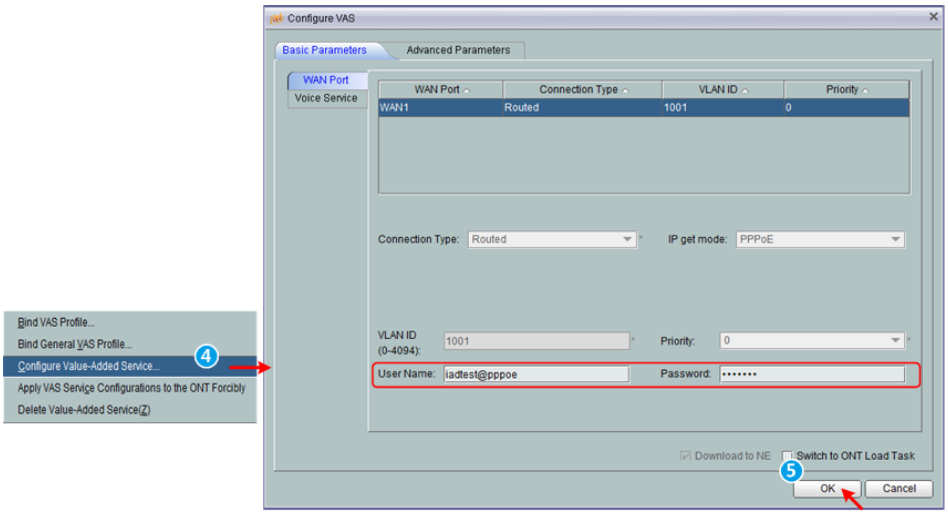
To bind a WAN port to multiple LAN ports, set **Physical Port Name** to **LAN1,...,LANx**. For example, to bind WAN 1 to LAN 1 and LAN 2, set **Physical Port Name** to **LAN1, LAN2**.

b. **Bind a general VAS profile.**



c. **Configure the ONT value-added service.**





NOTE

The **User Name** and **Password** must be the same as those configured on the BRAS.

----End

3.3.2.1.5 Configuring the Wi-Fi Access Service (on a Web Page)

The OLT is connected to the remote ONT through a GPON port to provide users with high-speed Internet Wi-Fi services.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configurations, see the configuration guide.
- The ONT has been added to the OLT. For details, see Adding an ONT to an OLT.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 14

Item	Data
VLAN Plan	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● CVLAN ID: 1001 ● C'-VLAN ID: 1010-1011 VLAN translation policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the profile ID to ftth_hsi, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

     ```
     huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0
     priority-policy local-setting
     ```

  b. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 1001 is mapped to GEM port 14 in the ONT line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  c. Create a service VLAN and add an upstream port to it.

     Add upstream port 0/9/0 to VLAN 100.

     ```
     huawei(config)#vlan 100 smart
     huawei(config)#vlan attrib 100 stacking
     huawei(config)#port vlan 100 0/9 0
     ```

  d. Create service flows.

     Set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001, and use traffic profile ftth_hsi.

     ```
     huawei(config)#service-port vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
     service
     ```



```
user-vlan 1001 tag-transform translate-and-add
inner-vlan 1010 inbound traffic-table name ftth_hsi outbound traffic-
table name ftth_hsi
huawei(config)#service-port vlan 100 gpon 0/1/0 ont 2 gemport 14 multi-
service
user-vlan 1001 tag-transform translate-and-add
inner-vlan 1011 inbound traffic-table name ftth_hsi outbound traffic-
table name ftth_hsi
```

e. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the Web page.

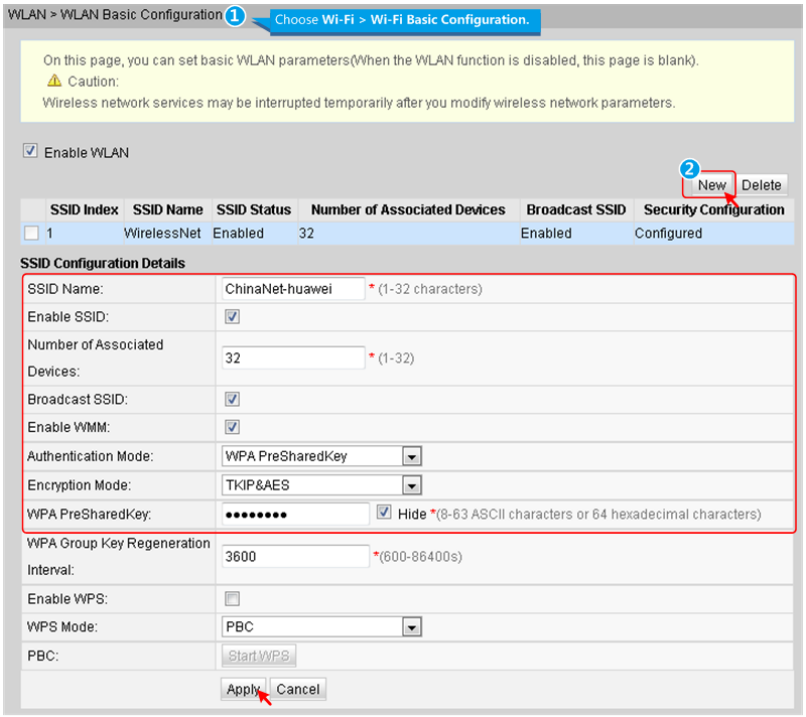
  Layer 3 bridge Wi-Fi service

  a. Log in to the Web configuration page.

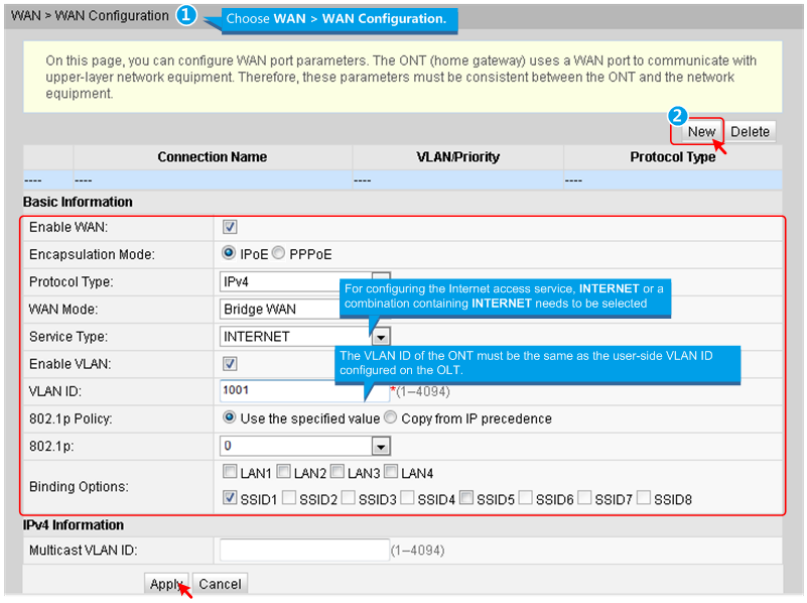
     i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

     ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

  b. Configure the Wi-Fi parameters.



  c. Configure the parameters of the Layer 3 bridge WAN port.

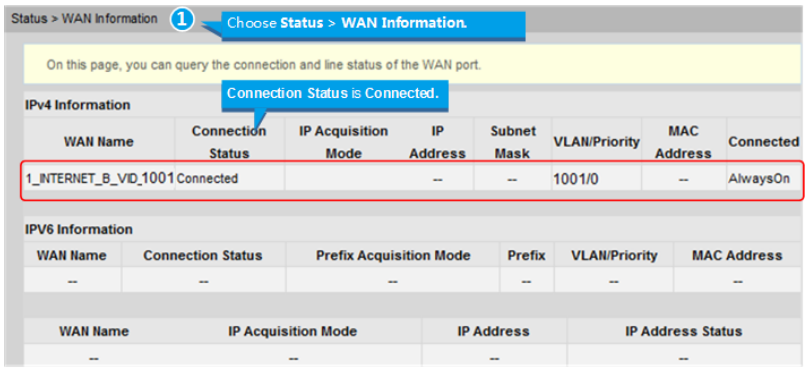


NOTE

When you use Wi-Fi access service in the IPoE mode, you need to enable the DHCP relay function. For procedure details, see DHCP Server Configuration.

d. Check the ONT connection status.

In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Connection Status** is **Connected**.



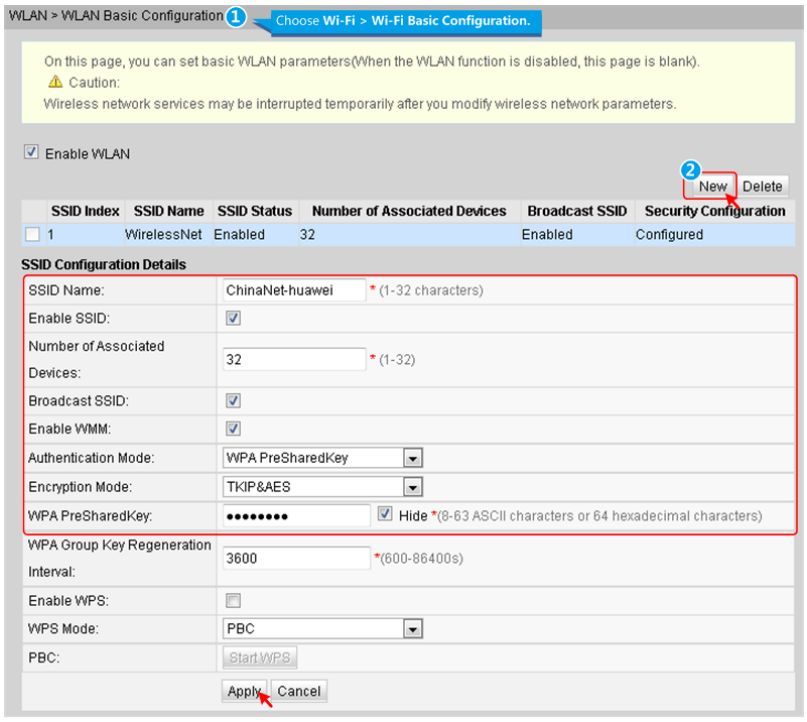
Layer 3 route Wi-Fi service

a. Log in to the Web configuration page.

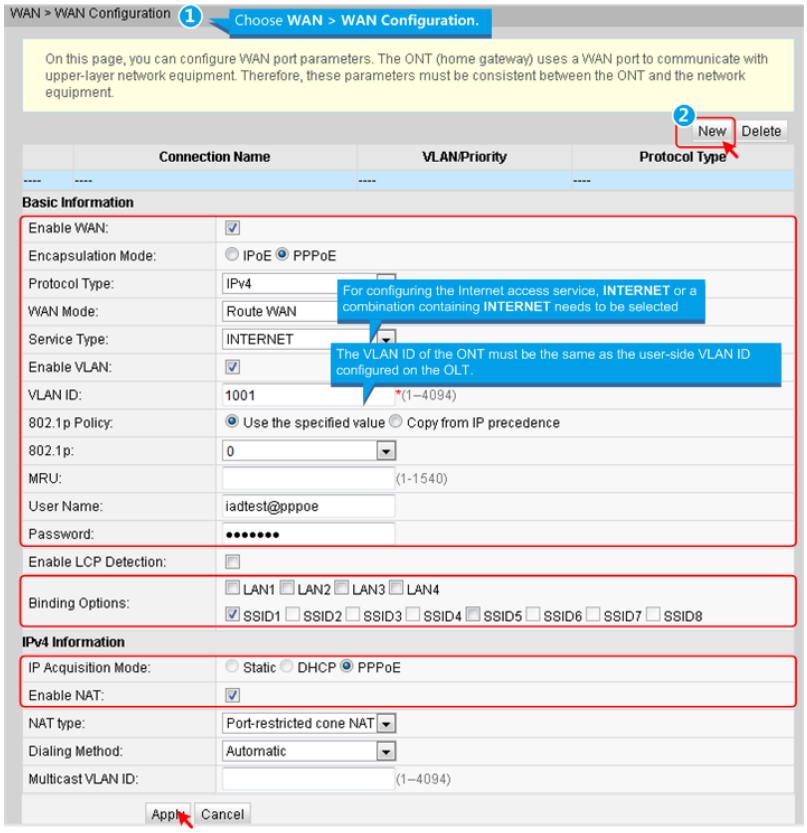
i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

b. Configure the Wi-Fi parameters.

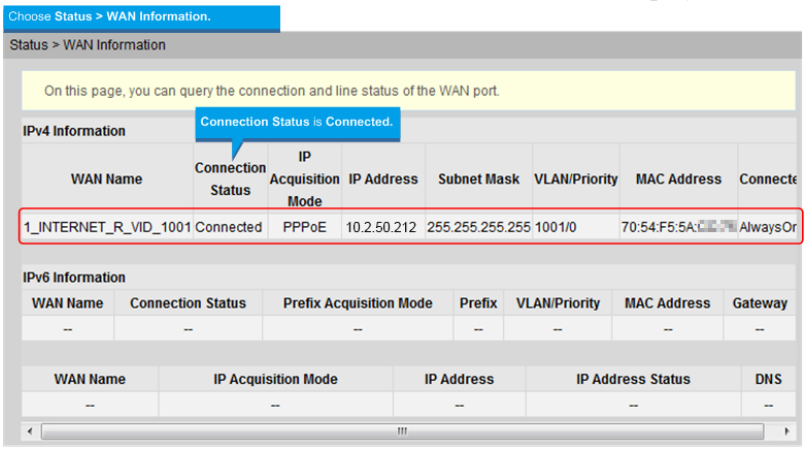


c. Configure the parameters of the Layer 3 route WAN port.



d. Check the ONT connection status.

In the navigation tree, choose **Status** > **WAN Information**. In the right pane, **Connection Status** is **Connected** and the obtained IP address is displayed at **IP Address**.



----End

Result

- Layer 3 bridge Wi-Fi service: SSID radio signals can be searched on the Wi-Fi terminal. After the user enter the authentication key and pass the authentication, the user can access the Internet.
- Layer 3 route Wi-Fi service: SSID radio signals can be searched on the Wi-Fi terminal. After the user enter the authentication key and pass the authentication, the Wi-Fi terminal can obtain the IP address allocated by the DHCP IP address pool on the ONT. After the PPPoE dialup is successfully performed on the ONT, the user can access the Internet.

NOTE

The security mode and encryption configured on a Wi-Fi terminal must be the same as those of an ONT. If you cannot find the following encryption modes: TKIP&AES, and AES. The reason may lie in an old Wi-Fi driver version. If so, replace the old version with a new one.

3.3.2.1.6 Configuring the H.248-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see **3.3.2.1.3 Adding an ONT to an OLT**.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Context

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
Voice parameter	IP address of the MGC server: 10.10.100.10/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     ```
     huawei(config)#traffic table ip name ftth_voip cir off priority 5
     priority-policy
      local-setting
     ```

  b. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

  c. Create a service VLAN and add an upstream port to it.

     Add upstream port 0/9/0 to VLAN 200.


```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/9 0
```

d. Create service flows.

Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name ftth_voip
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name ftth_voip
```

e. Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#arp proxy enable
huawei(config-if-vlanif200)#quit
```

f. Save the data.

```
huawei(config)#save
```

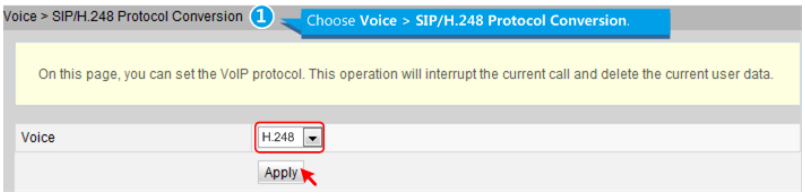
- Configure the ONT on the Web page.

a. Log in to the Web configuration page.

i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

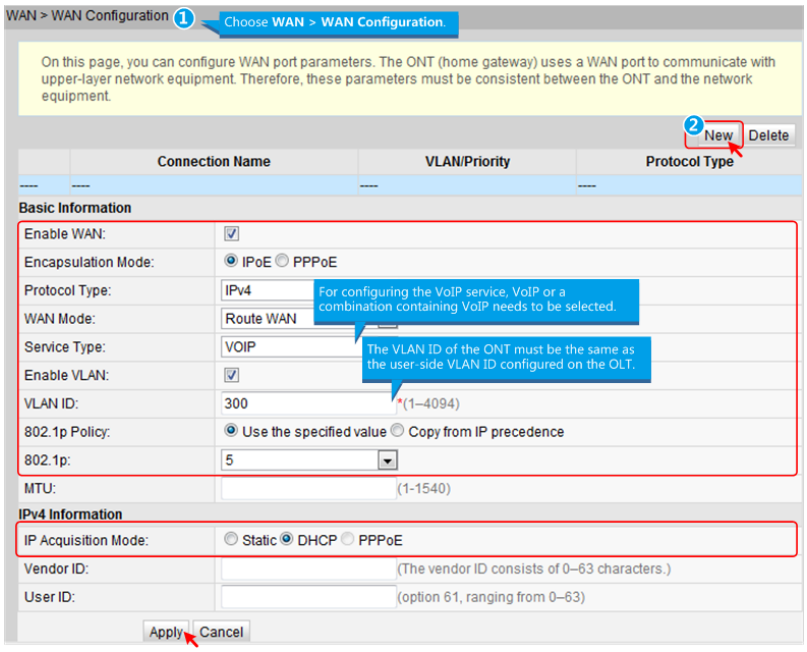
b. Configure the voice protocol.



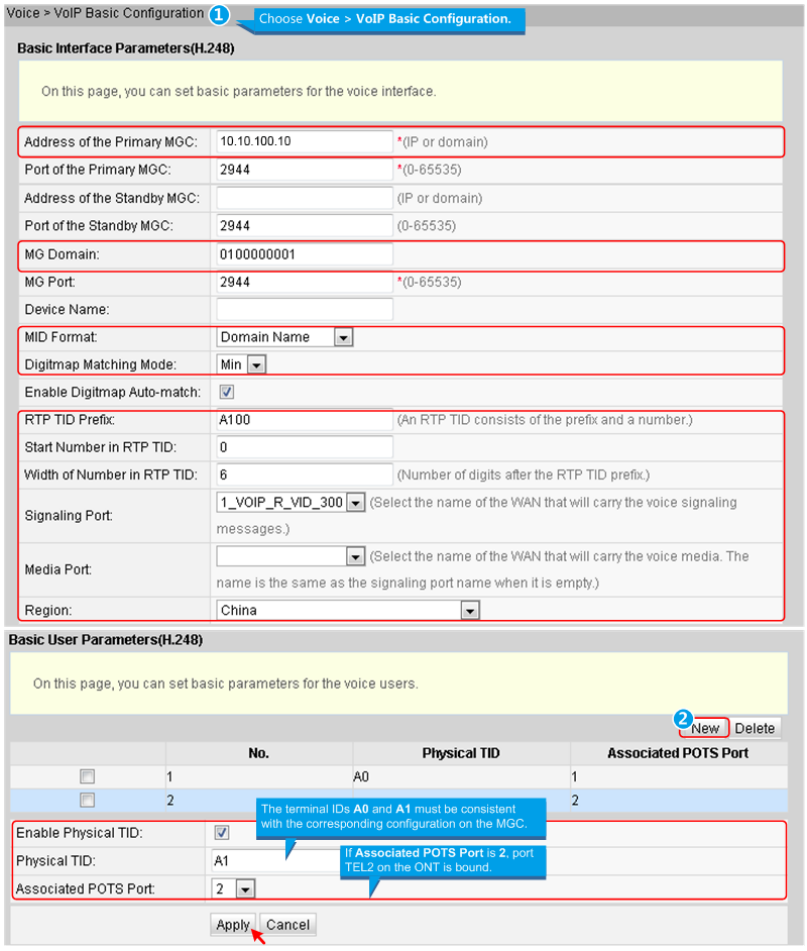
NOTE

The default voice protocol is SIP. Therefore, change the voice protocol first.

c. Configure parameters for the voice WAN interface.



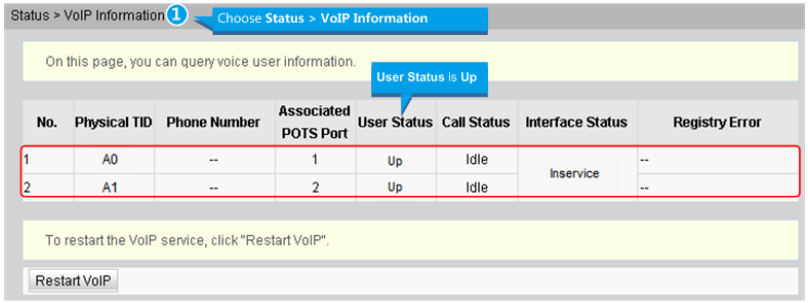
d. Configure parameters for the H.248-based voice interface.



NOTE

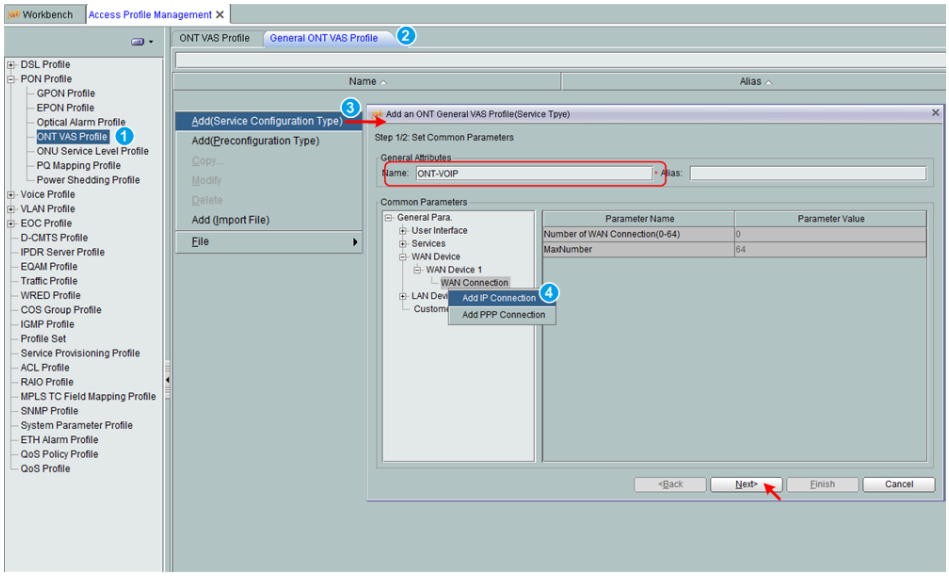
- The parameters of the H.248-based voice interface must be consistent with the corresponding configuration on the media gateway controller (MGC).
- If dual-homing is configured, **Address of the Standby MGC** must be configured.
- **MID Format** can be set to **Domain Name**, **IP**, or **Device Name**. If **MID Format** is set to **Domain Name** or **Device Name**, the setting must be consistent with the corresponding configuration on the MGC.
- **MG Domain** is ONT's domain name registered with the MGC. It is globally unique. **MG Domain** in this example is ONT's password.
- If **Media Port** is empty, the parameter value is the same as **Signaling Port**. The media streams are not isolated from signaling streams. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.
- When the ONT is interconnected with a third-party softswitch, check **RTP TID Prefix**, **Start Number of RTP TID**, and **Width of RTP TID Number**.

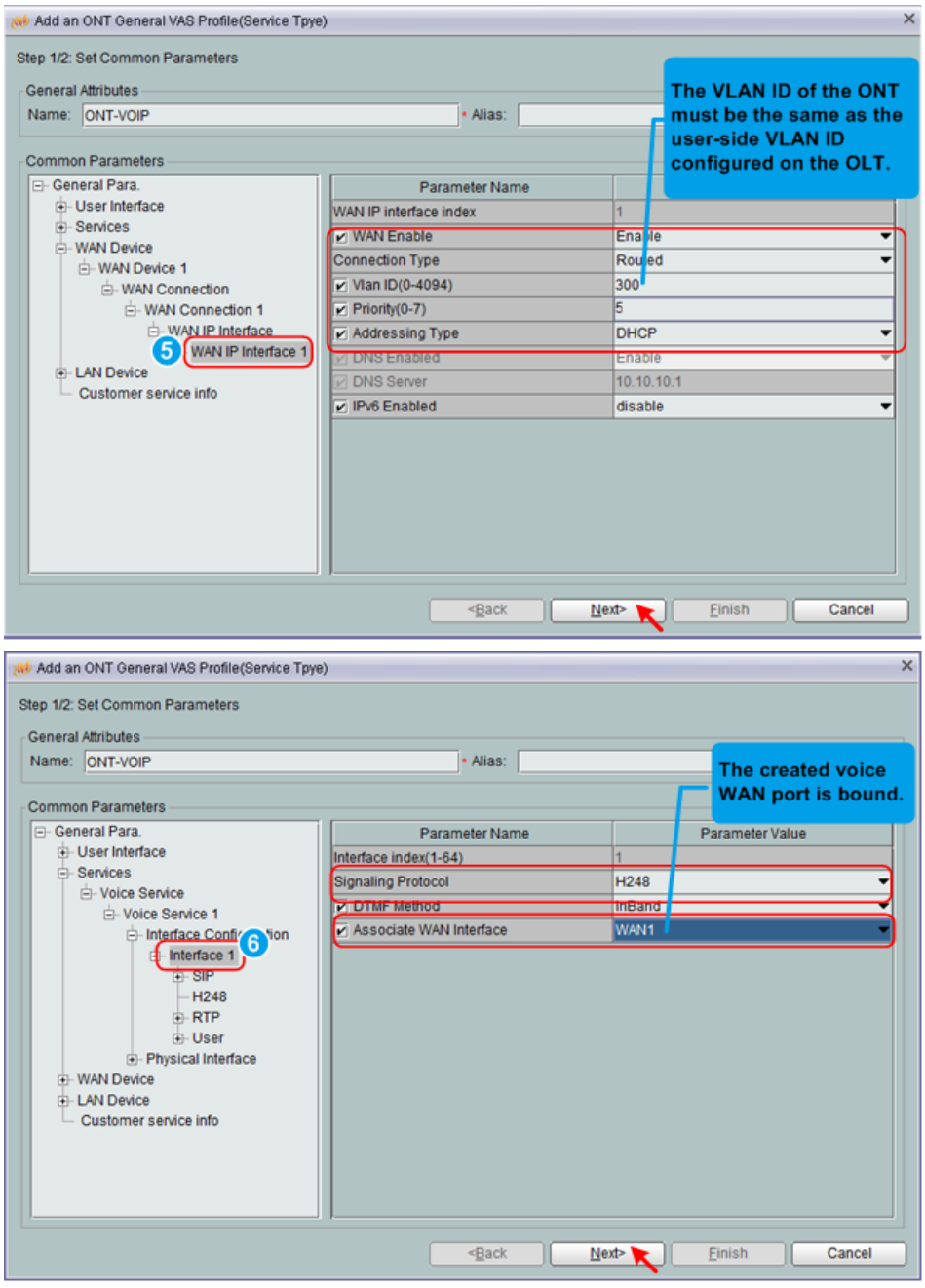
e. Check the registration status of the voice user.

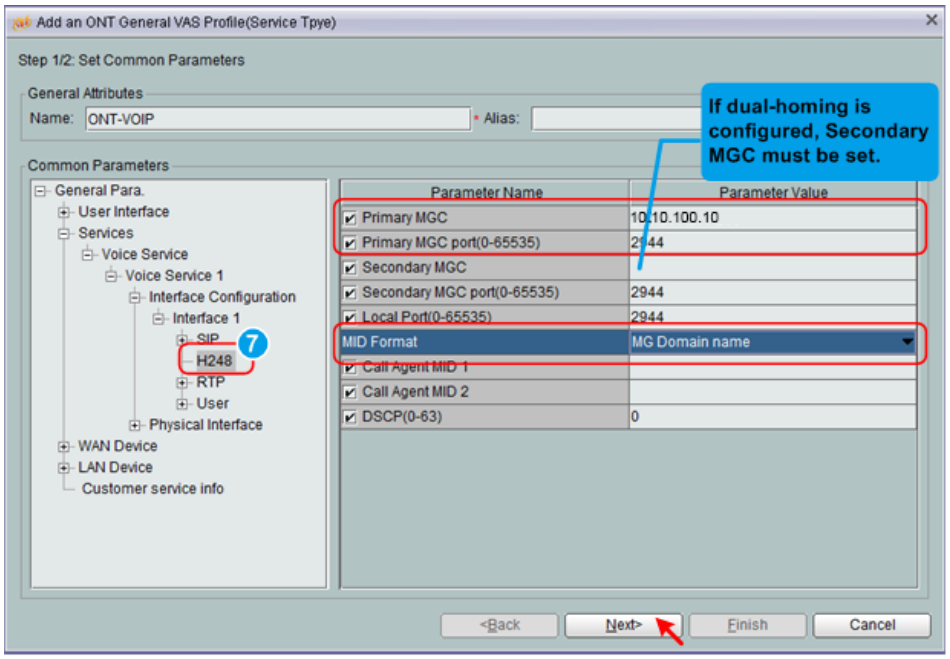


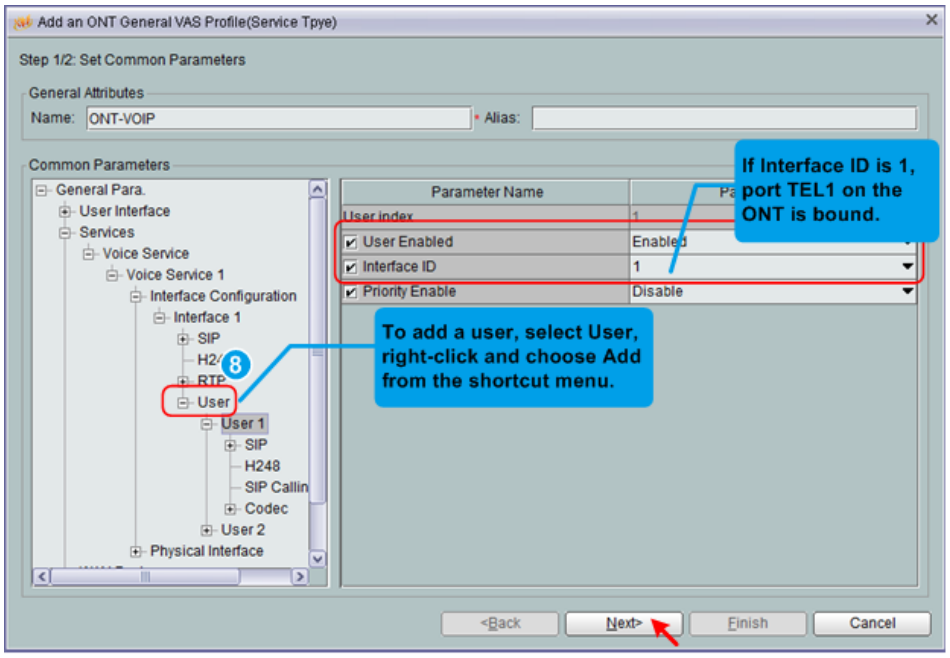
- Configure the ONT on the U2000.

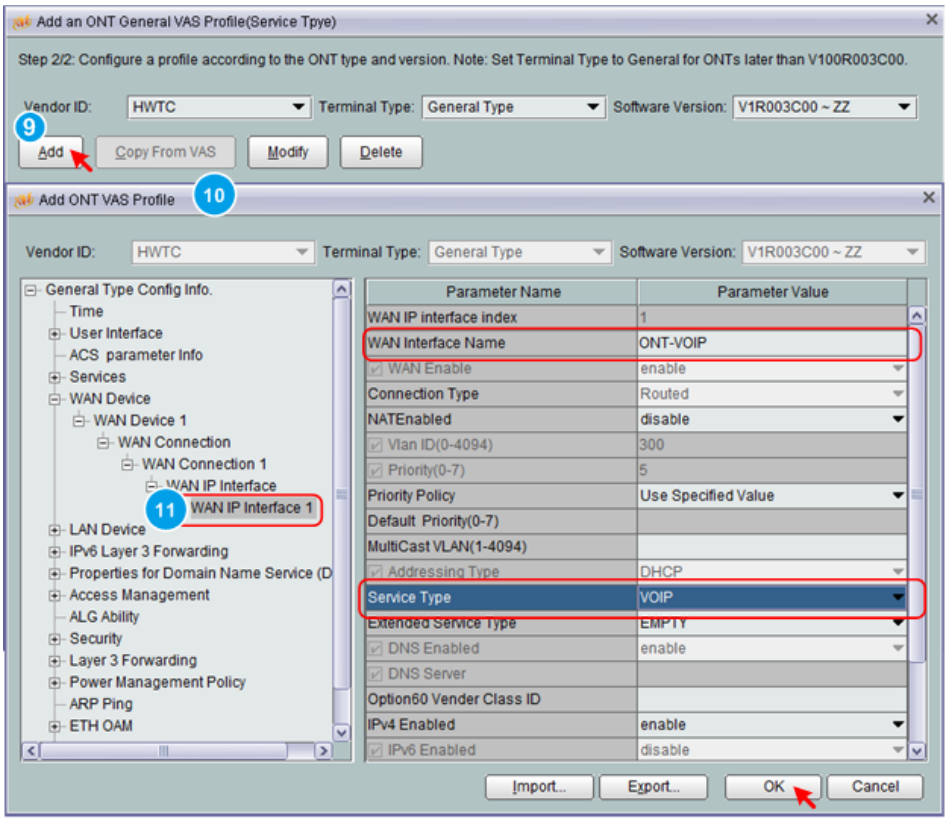
a. **Configure and bind a general value-added service (VAS) profile for the ONT.**







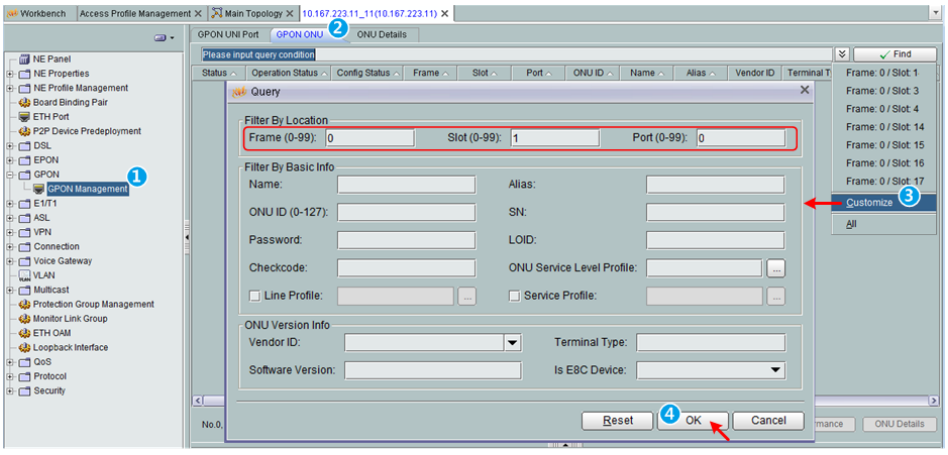


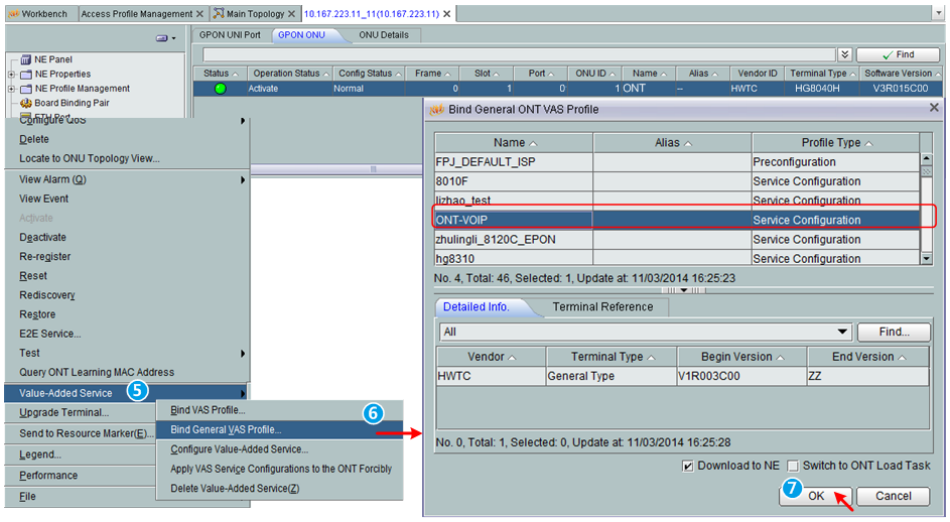


NOTE

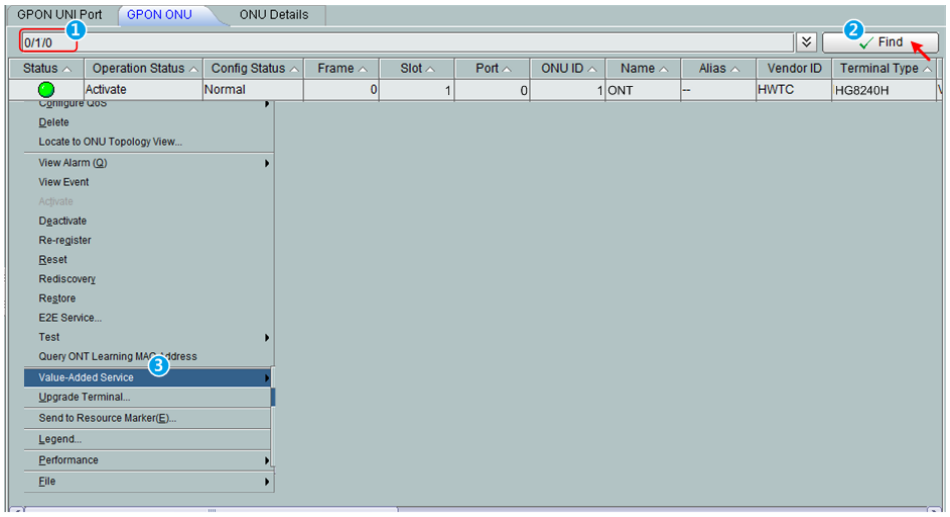
If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default. Create a WAN port named **WAN-RTP** on the ONT, and set this WAN port to a media WAN port. Specifically, choose **Interface 1** > **RTP** and set **Associate WAN Interface** to **WAN2**.

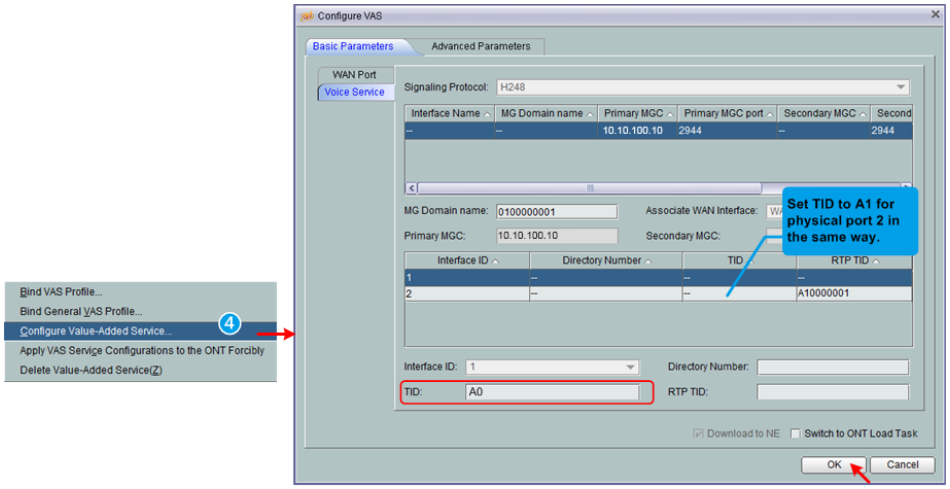
b. **Bind a general VAS profile.**





c. **Configure the ONT VAS service.**





NOTE

Domain Name is ONT's domain name registered with the MGC. It is globally unique. **MG Domain Name** in this example is ONT's password.

Pay attention to the RTP TID configuration when the ONT is interconnected with a softswitch of other vendors. The terminal IDs **A0** and **A1** must be consistent with the corresponding configuration on the MGC.

Do not configure **Directory Number**.

----End

3.3.2.1.7 Configuring the H.248-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the H.248-based voice service.

Prerequisites

- The interface data and POTS user configuration data corresponding to the MG interface have been configured on the MGC.
- The OLT has been connected to the MGC. The OLT can ping the IP address of the MGC server successfully.
- The ONT has been added to the OLT. For details, see Adding an ONT to an OLT.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports H.248. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Context

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).

Item	Data
Voice parameter	IP address of the MGC server: 10.10.100.10/24 Port ID of the MGC server: 2944 MG Domain: 0100000001 or 0100000002

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/9 0
```

Step 4 Create service flows.

Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
```

Step 5 Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#arp proxy enable
huawei(config-if-vlanif200)#quit
```

Step 6 Configure ONT voice profiles.

ONT voice service configurations include the VoIP service provisioning mode, ONT voice profiles, voice users, and voice-related parameters.

ONT voice profiles include the common MG interface attribute profile, POTS port profile, MGC profile, and voice signal profile.

- Common MG interface attribute profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, Tx gain, Rx gain, and signaling type of a POTS port.
- MGC profile: saves the IP address or domain name of an MGC, protocol port ID of the MGC transport layer to which the MG interface belongs, and DSCP priority of media packets.
- Voice signal profile: saves the ONT signal tone and ringing tone.

Currently, the common MG interface attribute profile, POTS port profile, and MGC profile can be applied to an H.248 interface, and the voice signal profile can be bound to an H.248 interface.

For profiles that can be applied to an H.248 interface, if parameters in those profiles are changed, those profiles must be reapplied to the H.248 interface so that the changed parameters can take effect. For profiles that can be bound to an H.248 interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the H.248 interface and the changed parameters can take effect.

1. Configure the VoIP service provisioning mode.

   Run the **ont voip config-method** command to configure the VoIP service provisioning mode. Run the **display ont info** command to query the mode of issuing VoIP services.

   In this example, the mode is **default**, that is, the VoIP service provisioning mode is depended on the actual service provisioning mode on the ONT. Run this command to select a proper mode if the system supports multiple voice service provisioning modes. The service provisioning modes can be OMCI, FTP, and TR069.

2. Configure and apply an MG interface public attribute profile.

   In this example, the default profile 1 is used.

   a. Configure an MG interface public attribute profile.

      Run the **display ont-mg-attribute-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add a profile.

   b. Apply a common MG interface attribute profile.

      Run the **ont-if-h248 bat-apply** command to apply profiles in batches to H.248 interfaces and run the **if-h248 attribute** command to apply a profile to an H.248 interface or configure customized parameters on an H.248 interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

3. Configure and apply a POTS port profile.

   In this example, the default profile 1 is used.

   a. Configure a POTS port profile.

      Run the **display ont-pots-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a profile.

   b. Apply a POTS port profile.

      Run the **ont-pstnport electric bat-apply** command to apply POTS port profiles in batches and run the **pstnport electric** command to apply a POTS port profile to an

H.248 interface or configure customized parameters on an H.248 interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

4. Configure the voice WAN port of the ONT.

   For ONT 1 and ONT 2, configure the IP address obtaining mode to DHCP, set the management VLAN to VLAN 300, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 300
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 300
```

5. Configure and apply an MGC profile.

   a. Configure and apply an MGC profile.

      Run the **display ont-mgc-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-mgc-profile add** command to add a profile.

      Create MGC profile 2, set the IP address of the MGC to 10.10.100.10, and use default values for other parameters.

```
huawei(config)#ont-mgc-profile add profile-id 2 primary-mgc 10.10.100.10
```

   b. Add an H.248 interface and apply an MGC profile to the interface.

      For ONT 1 and ONT 2, set the MG ID to 1, apply MGC profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

```
huawei(config-if-gpon-0/1)#if-h248 add 0 1 1 mgc-profile profile-id 2
huawei(config-if-gpon-0/1)#if-h248 add 0 2 1 mgc-profile profile-id 2
```

1. Add POTS users.

   For ONT 1 and ONT 2, create a POTS user, set the MG ID to 1 (identical to the MG ID of the H.248 interface), and set the physical terminal port ID to A0 and A1.

```
huawei(config-if-gpon-0/1)#mgpstnuser add 0 1 1 mgid 1 terminalid A0
huawei(config-if-gpon-0/1)#mgpstnuser add 0 2 1 mgid 1 terminalid A1
```

   Run the **display mgpstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 1 1

-----------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A0
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display mgpstnuser attribute 0 2 1

-----------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Terminal ID                 : A1
...//The rest of the response information is omitted.
```

1. Configure and bind the voice signal profile.

   In this example, the default profile 1 is used.

a. Configure the voice signal profile.

Run the **display ont-voipsignal-profile** command to query the existing profiles in the system. If the existing profile in the system does not meet the requirement, run the **ont-voipsignal-profile** command to add a profile.

b. Configure the ONT signal tone.

Run the **display ont-tone** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-tone add** command to add signal tone parameters. The ONT signal tone will not be configured independently in this example.

c. Configure ONT ringing parameters.

Run the **display ont-ring** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-ring add** command to add ringing parameters. The ONT ringing parameter will not be configured independently in this example.

d. Run the **commit** command to save parameters of the voice signal profile to the database.

e. Bind the voice signal profile.

Run the **ont-voipsignal bat-bind** command to bind voice signal profiles in batches or run the **voipsignal** command to bind a voice signal profile to an ONT. If you run these two commands to bind profiles in batches or bind a voice signal profile to an ONT repeatedly, the last configurations take effect.

2. (Optional) Configure the H.248 user codec.

Run the **mgpstnuser codec** command to configure the H.248 user codec. The H.248 user codec will not be configured independently in this example.

3. (Optional) Configure the global VoIP media attributes of the ONT.

Run the **ont-voip-media attribute** command to configure the global VoIP media attributes of the ONT. Before configuration, ensure that the configured media attributes are supported by the corresponding ONT. Otherwise, the ONT configuration will fail. The global VoIP media attributes of the ONT will not be configured independently in this example.

Step 7 Save the data.

```
huawei(config)#save
```

----End

3.3.2.1.8 Configuring the SIP-based Voice Service (on a Web Page or the U2000)

The OLT is connected to the remote ONT through a GPON port to provide users with the IP-based high-quality and low-cost VoIP service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see **3.3.2.1.3 Adding an ONT to an OLT**.

- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
Voice parameter	IP address of the SIP server: 10.10.100.10/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

     Set the profile name to **ftth_voip** and do not limit the upstream and downstream rates. Set the priority to **5** and packets are scheduled according to the priority carried.

     ```
     huawei(config)#traffic table ip name ftth_voip cir off priority 5
     priority-policy
      local-setting
     ```

  b. Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

c. Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/9 0
```

d. Create service flows.

Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-
service
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-
table name ftth_voip
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-
service
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-
table name ftth_voip
```

e. Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#arp proxy enable
huawei(config-if-vlanif200)#quit
```

f. Save the data.

```
huawei(config)#save
```

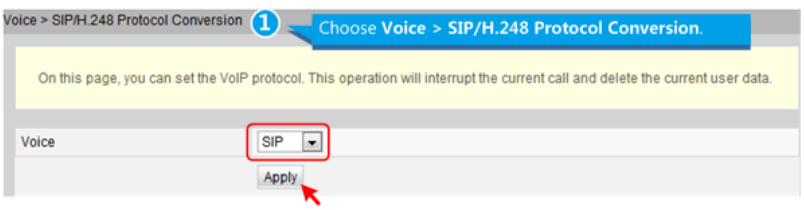
- Configure the ONT on the Web page.

a. Log in to the Web configuration page.

i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

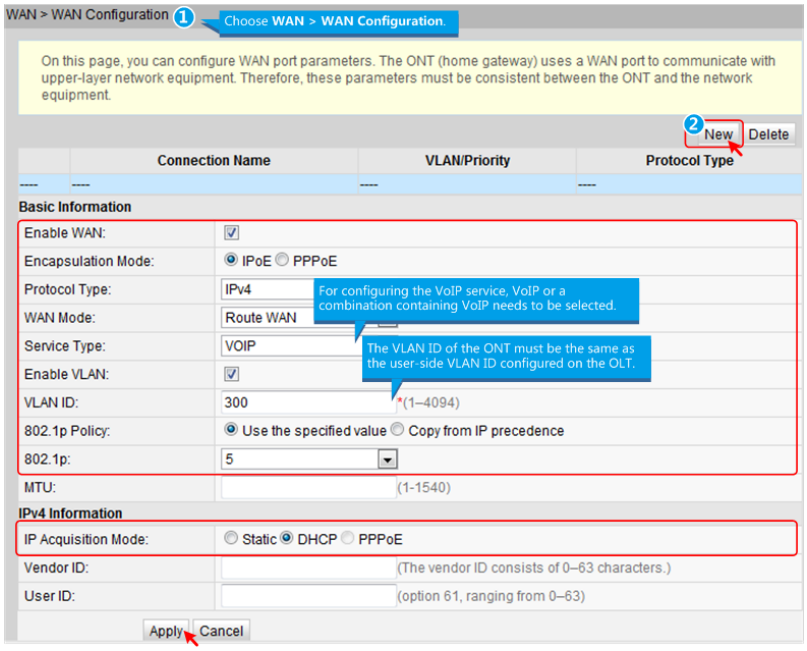
b. **Optional:** Configure the voice protocol.



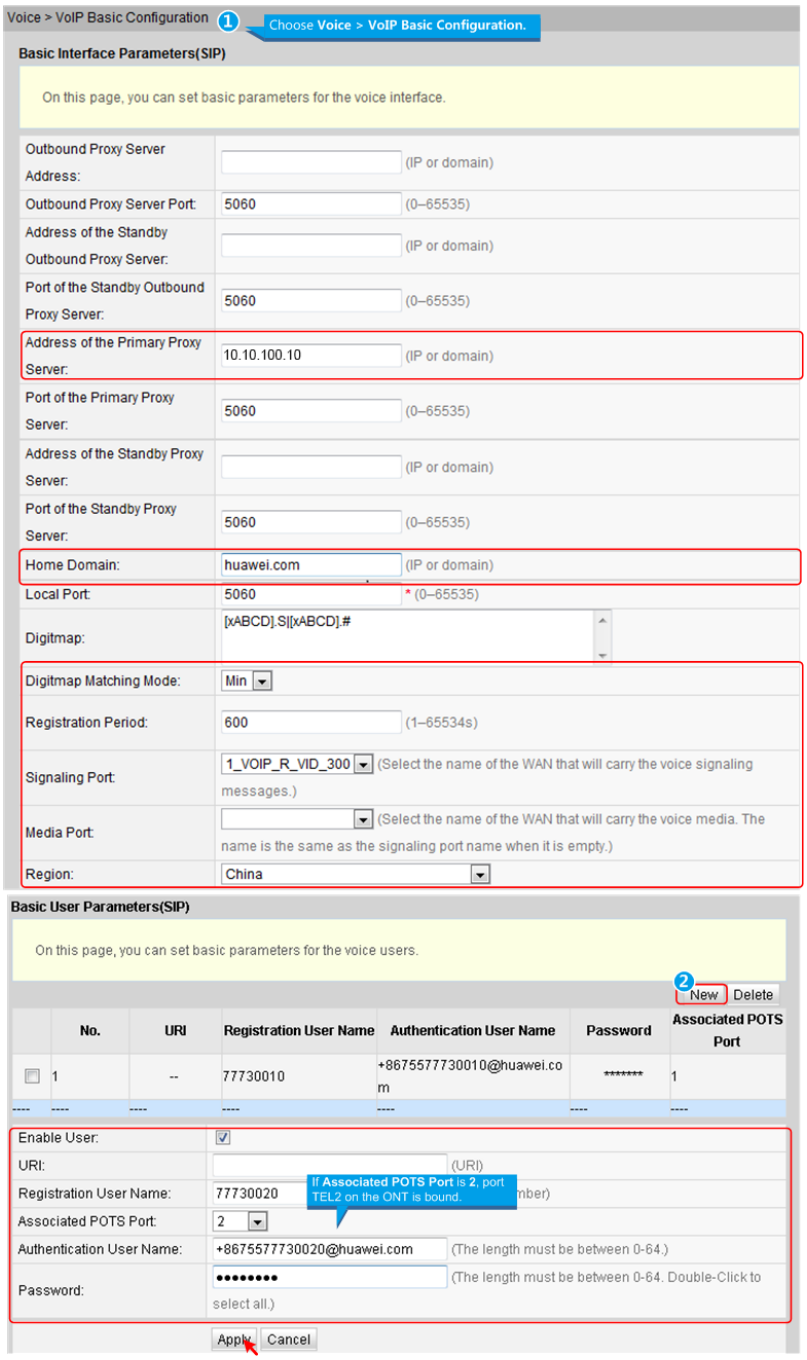
NOTE

The default voice protocol is SIP. If the protocol is not changed, skip this step.

c. Configure parameters for the voice WAN interface.



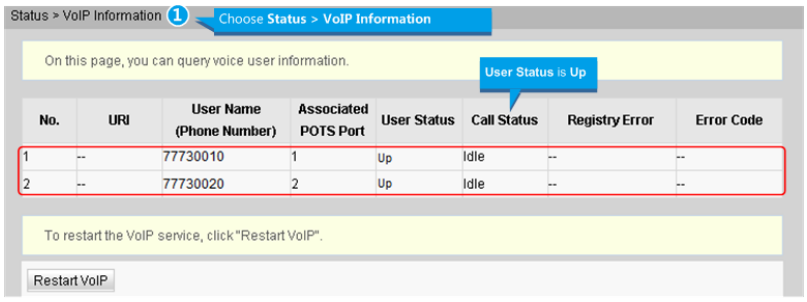
d. Configure parameters for the SIP-based voice interface.



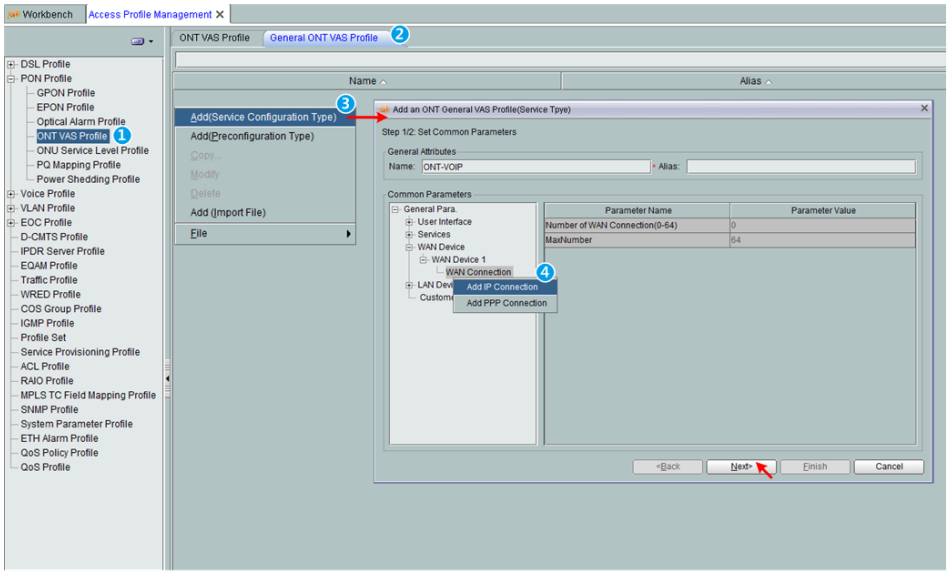
NOTE

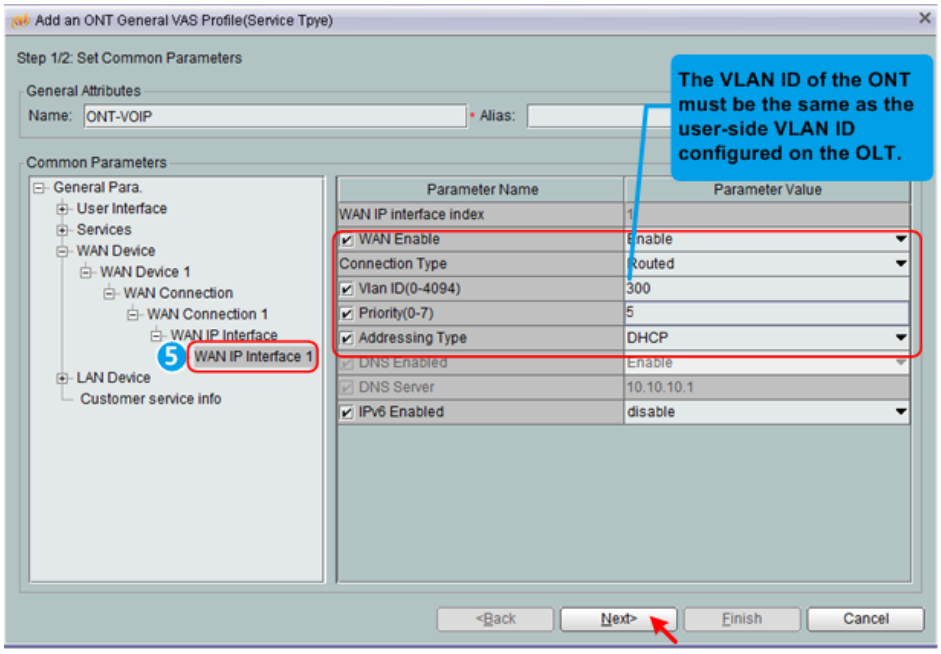
- The parameters of the SIP-based voice interface must be consistent with the corresponding configuration on the softswitch.
- If dual-homing is configured, **Address of the Standby Proxy Server** must be configured.
- If **Signaling Port** is empty, the parameter value is the same as **Media Port**. If the upper-layer network requires isolation of media streams from signaling streams, create different traffic streams for the media streams and signaling streams on the OLT, create different WAN ports on the ONT, and bind the created WAN ports to **Media Port** and **Signaling Port**. When the packet is forwarded from two WAN ports, the configured VLAN is carried by default.

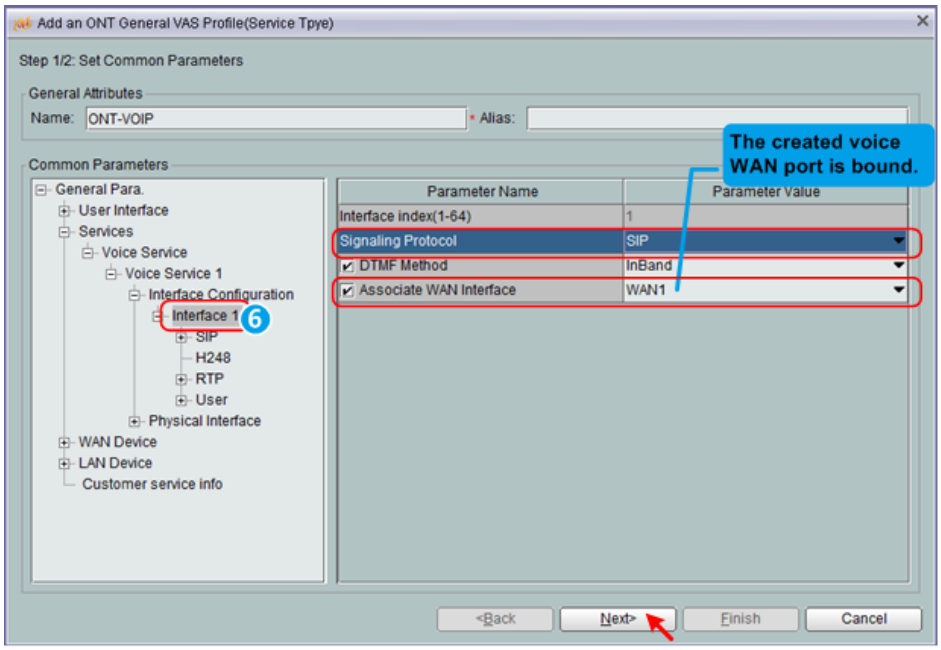
e. Check the registration status of the voice user.

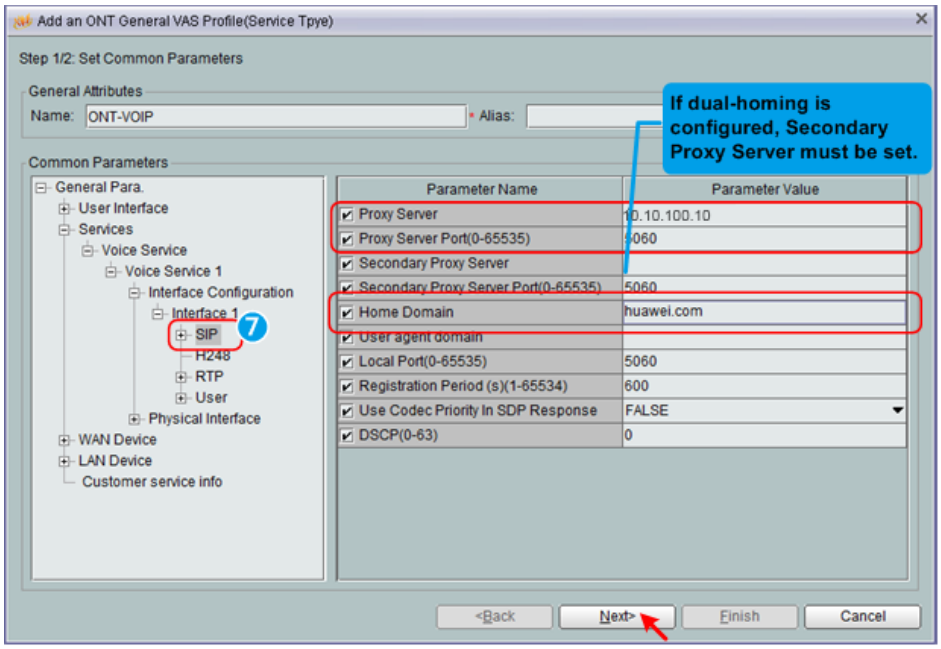


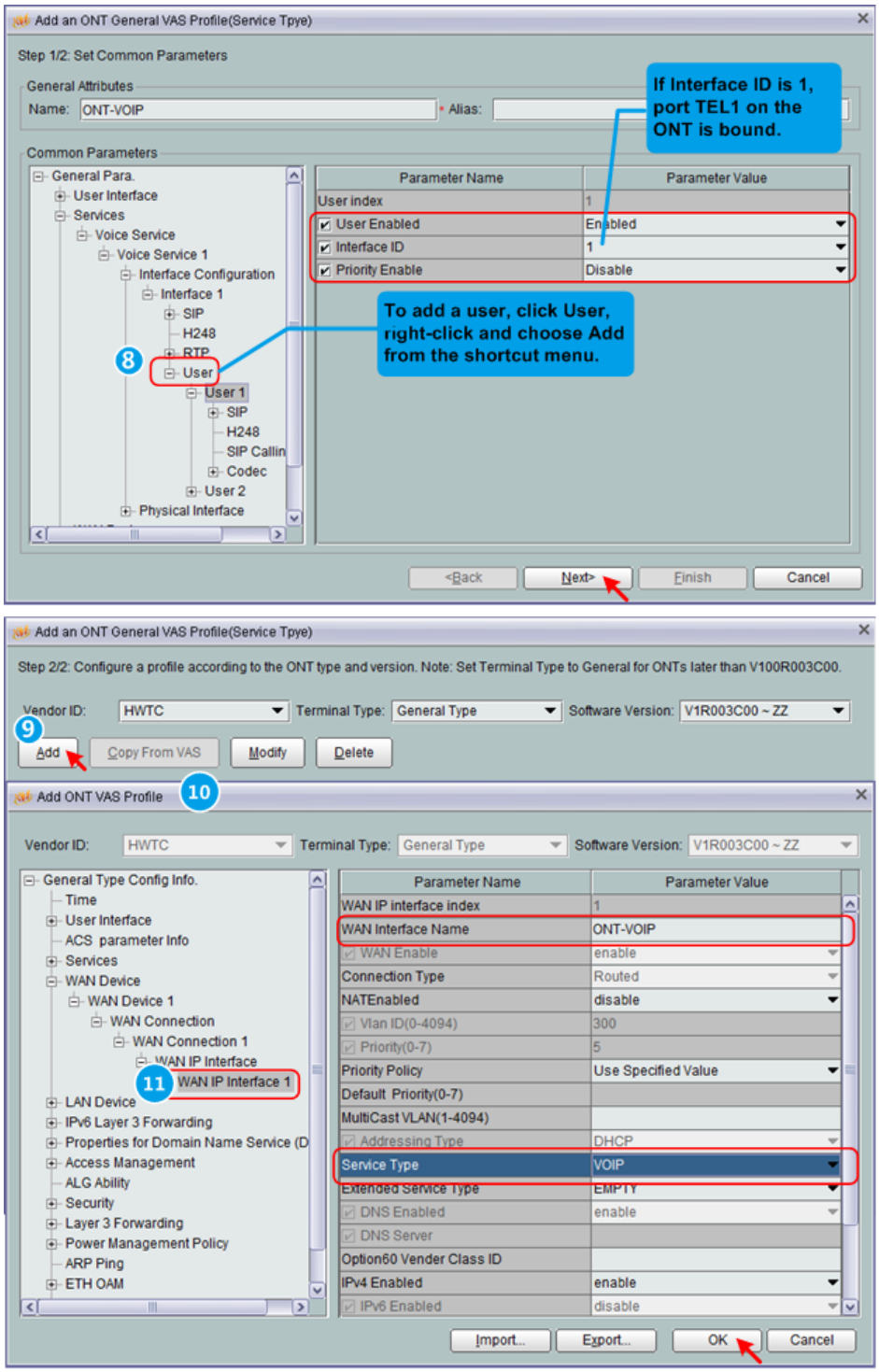
- Configure the ONT on the U2000.
  a. **Configure a general VAS profile for the ONT.**



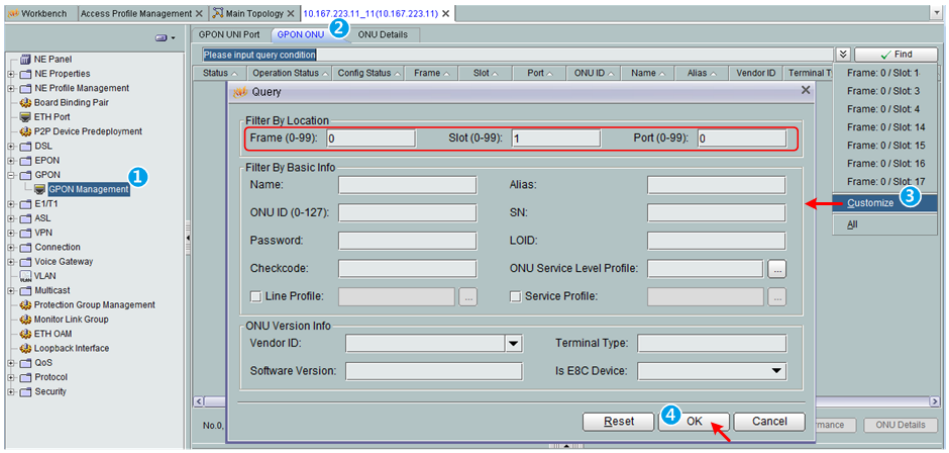


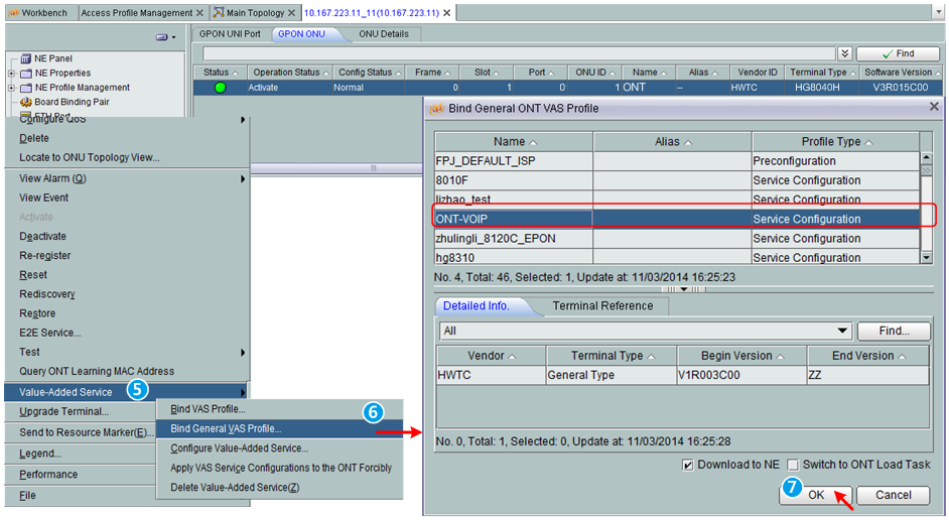




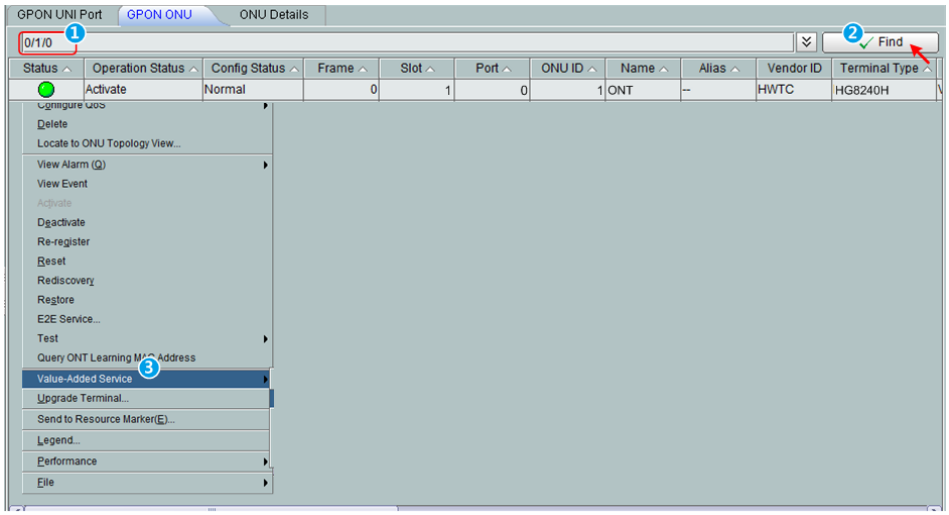


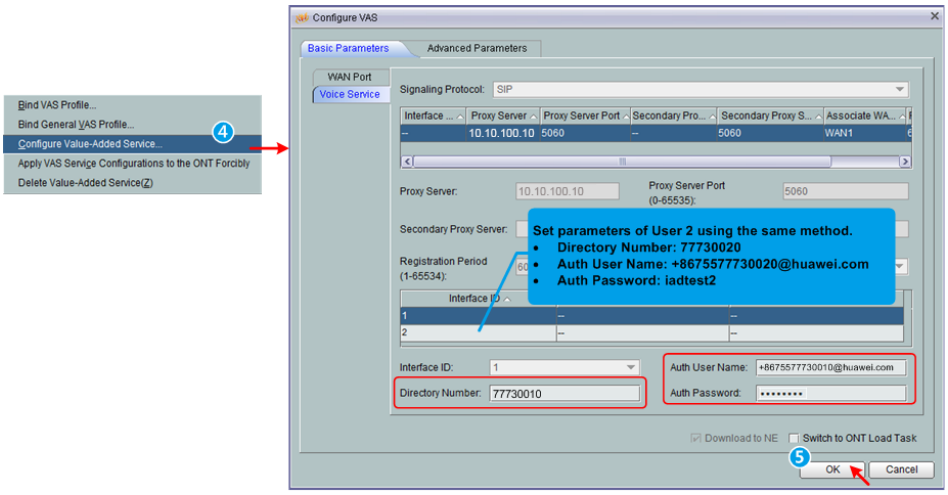
b. **Bind a general VAS profile.**





c. **Configure the ONT VAS service.**





NOTE

The parameters of the SIP-based voice user must be consistent with the corresponding configuration on the softswitch.

----End

3.3.2.1.9 Configuring the SIP-based Voice Service (Through the CLI)

The OLT manages ONTs and applies VoIP configurations to the ONT using the OMCI protocol. This topic describes how to configure the SIP-based voice service.

Prerequisites

- The SIP interface data and POTS user configuration data corresponding to the MG interface have been configured on the SIP server.
- The connection between the OLT and the SIP server is set up. The OLT can ping the IP address of the SIP server successfully.
- The ONT has been added to the OLT. For details, see Adding an ONT to an OLT.
- Different voice services require different ONT software versions. Before the configuration, ensure that the current ONT software version supports SIP. For details, see relevant ONT manuals.
- The Web page and NMS window for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 12

Item	Data
VLAN Plan	Single VLAN tag: ● SVLAN ID: 200 ● SVLAN type: smart ● SVLAN attribute: common ● CVLAN ID: 300 VLAN translation policy: ● ONT: VLANs are configured for the ONTs on the same network in a unified manner, and the ONTs have the same C-VLAN. The ONT adds a C-VLAN tag to packets. ● OLT: translates the VLAN tag (C-VLAN <-> S-VLAN).
Voice parameter	IP address of the SIP server: 10.10.100.10/24 Port ID of the SIP server: 5060 Home domain name: huawei.com User phone number 1: 77730010 User phone number 2: 77730020

Procedure

Step 1 Configure a traffic profile.

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

Step 2 Configure the mapping relationship between a GEM port and a VLAN.

The service flow of user VLAN 300 is mapped to GEM port 12 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 12 2 vlan 300
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

Step 3 Create a service VLAN and add an upstream port to it.

Add upstream port 0/9/0 to VLAN 200.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/9 0
```

Step 4 Create service flows.

Set the service VLAN to 200, GEM port ID to 12, and user VLAN to 300. Use traffic profile **ftth_voip**.

```
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 1 gemport 12 multi-service
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
huawei(config)#service-port vlan 200 gpon 0/1/0 ont 2 gemport 12 multi-service
```



```
user-vlan 300 inbound traffic-table name ftth_voip outbound traffic-table name
ftth_voip
```

Step 5 Enable the ARP proxy function.

Voice media streams for different users of the same SVLAN fail to interchange because the service ports of the smart VLAN are isolated from each other. Therefore, the ARP proxy function needs to be enabled on the OLT.

```
huawei(config)#arp proxy enable
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#arp proxy enable
huawei(config-if-vlanif200)#quit
```

Step 6 Configure ONT voice profiles.

ONT voice service configurations include the VoIP service provisioning mode, ONT voice profiles, voice users, and voice-related parameters.

ONT voice profiles include the common MG interface attribute profile, POTS port profile, SIP service profile, SIP agent profile, digitmap profile, and voice signal profile.

- Common MG interface attribute profile: saves common attributes of an ONT voice interface, including the fax mode, fax/modem negotiation mode, and priority of the coding and decoding mode.
- POTS port profile: saves physical attributes of a POTS port on an ONT, including the impedance, Tx gain, Rx gain, and signaling type of a POTS port.
- SIP service data profile: saves the data information about the ONT voice service, including the rights of call waiting (CW), three-way calling (3WC), call transfer (CT), and call hold (CH).
- SIP agent profile: saves the SIP agent information about an ONT, including the IP address and domain name of the SIP agent server and attributes of media packets and signaling packets.
- Digitmap profile: saves the digitmap information about an ONT, including the timeout time of the digitmap timer and the digitmap format.
- Voice signal profile: saves the ONT signal tone and ringing tone.

Currently, the common MG interface attribute profile, POTS port profile, SIP service profile, and SIP agent profile can be applied to an SIP interface, and the digitmap profile and voice signal profile can be bound to an SIP interface.

For profiles that can be applied to an SIP interface, if parameters in those profiles are changed, those profiles must be reapplied to the SIP interface so that the changed parameters can take effect. For profiles that can be bound to an SIP interface, if parameters in those profiles are changed, those profiles do not need to be rebound to the SIP interface and the changed parameters can take effect.

1. Configure the VoIP service provisioning mode.

   Run the **ont voip config-method** command to configure the VoIP service provisioning mode. Run the **display ont info** command to query the mode of issuing VoIP services.

   In this example, the mode is **default**, that is, the VoIP service provisioning mode is depended on the actual service provisioning mode on the ONT. Run this command to select a proper mode if the system supports multiple voice service provisioning modes. The service provisioning modes can be OMCI, FTP, and TR069.

2. Configure and apply an MG interface public attribute profile.

In this example, the default profile 1 is used.

a. Configure an MG interface public attribute profile.

Run the **display ont-mg-attribute-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-mg-attribute-profile add** command to add a profile.

b. Apply a common MG interface attribute profile.

Run the **ont-if-sip bat-apply** command to apply profiles in batches to SIP interfaces and run the **if-sip attribute** command to apply a profile to an SIP interface or configure customized parameters on an SIP interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

3. Configure and apply a POTS port profile.

In this example, the default profile 1 is used.

a. Configure a POTS port profile.

Run the **display ont-pots-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-pots-profile add** command to add a profile.

b. Apply a POTS port profile.

Run the **ont-pstnport electric bat-apply** command to apply POTS port profiles in batches and run the **pstnport electric** command to apply a POTS port profile to an SIP interface or configure customized parameters on an SIP interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

4. Configure the voice WAN port of the ONT.

For ONT 1 and ONT 2, configure the IP address obtaining mode to DHCP, set the management VLAN to VLAN 300, and use default values for other parameters.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont ipconfig 0 1 dhcp vlan 300
huawei(config-if-gpon-0/1)#ont ipconfig 0 2 dhcp vlan 300
```

5. Configure and apply an SIP agent profile.

a. Configure an SIP agent profile.

Run the **display ont-sipagent-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-sipagent-profile add** command to add a profile.

Create SIP agent profile 2, set the IP address of the SIP server to 10.10.100.10, and use default values for other parameters.

```
huawei(config)#ont-sipagent-profile add profile-id 2 proxy-server
10.10.100.10
```

b. Add an SIP interface and apply an SIP agent profile to the interface.

For ONT 1 and ONT 2, set the MG ID to 1, apply SIP agent profile 2 to ONT 1 and ONT 2, and use default values for other parameters.

```
huawei(config-if-gpon-0/1)#if-sip add 0 1 1 sipagent-profile profile-id 2
huawei(config-if-gpon-0/1)#if-sip add 0 2 1 sipagent-profile profile-id 2
```

6. Add POTS users.

For ONT 1 and ONT 2, set the MG ID to 1 (identical to the MG ID of the added SIP interface), create two POTS users named huawei1 and huawei2, set passwords to user1

and user2, set their phone numbers to 77730010 and 77730020 and use default values for other parameters.

```
huawei(config-if-gpon-0/1)#sippstnuser add 0 1 1 mgid 1 username huawei1
telno 77730010
huawei(config-if-gpon-0/1)#sippstnuser add 0 2 1 mgid 1 username huawei2
telno 77730020
```

Run the **display sippstnuser attribute** command to check whether the configuration of the POTS user is properly set.

```
huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 1 1

-------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 1
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730010
  User name                   : huawei1
  Password                    : user1
...//The rest of the response information is omitted.

huawei(config-if-gpon-0/1)#display sippstnuser attribute 0 2 1

-------------------------------------------------------------------------------
  F/S/P                       : 0/1/0
  ONT ID                      : 2
  Port ID                     : 1

  MG ID                       : 1
  Telephone NO.               : 77730020
  User name                   : huawei2
  Password                    : user2
...//The rest of the response information is omitted.
```

1. Configure and apply an SIP service profile.

   In this example, the default profile 1 is used.

   a. Configure an SIP service profile.

      Run the **display ont-siprightflag-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-siprightflag-profile add** command to add a profile.

   b. Apply an SIP service profile.

      Run the **ont-sippstnuser bat-apply from** command to apply profiles in batches to SIP interfaces and run the **sippstnuser rightflag** command to apply a profile to a SIP interface or configure customized parameters on a SIP interface. If you run these two commands to apply profiles in batches or configure customized parameters repeatedly, the last configurations take effect.

2. Configure and bind a digitmap profile.

   In this example, the default profile 1 is used.

   a. Configure a digitmap profile.

      Run the **display ont-digitmap-profile** command to query the existing profile in the system. If the existing profile in the system does not meet the requirements, run the **ont-digitmap-profile add** command to add a profile.

   b. Bind a digitmap profile.

      Run the **ont-sippstnuser bat-bind from** command to apply profiles in batches to SIP interfaces, or run the **sippstnuser digitmap** command to bind a profile to an

SIP interface. If you use these two commands to bind the profile to SIP ports repeatedly, the last configurations take effect.

3. Configure and bind the voice signal profile.

   In this example, the default profile 1 is used.

   a. Configure the voice signal profile.

      Run the **display ont-voipsignal-profile** command to query the existing profiles in the system. If the existing profile in the system does not meet the requirement, run the **ont-voipsignal-profile** command to add a profile.

   b. Configure the ONT signal tone.

      Run the **display ont-tone** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-tone add** command to add signal tone parameters. The ONT signal tone will not be configured independently in this example.

   c. Configure ONT ringing parameters.

      Run the **display ont-ring** command to query the existing configuration in the system. If the existing configuration in the system does not meet the requirement, run the **ont-ring add** command to add ringing parameters. The ONT ringing parameter will not be configured independently in this example.

   d. Run the **commit** command to save parameters of the voice signal profile to the database.

   e. Bind the voice signal profile.

      Run the **ont-voipsignal bat-bind** command to bind voice signal profiles in batches or run the **voipsignal** command to bind a voice signal profile to an ONT. If you run these two commands to bind profiles in batches or bind a voice signal profile to an ONT repeatedly, the last configurations take effect.

4. (Optional) Configure the SIP user codec.

   Run the **sippstnuser codec** command to configure the SIP user codec. The SIP user codec will not be configured independently in this example.

5. (Optional) Configure the global VoIP media attributes of the ONT.

   Run the **ont-voip-media attribute** command to configure the global VoIP media attributes of the ONT. Before configuration, ensure that the configured media attributes are supported by the corresponding ONT. Otherwise, the ONT configuration will fail. The global VoIP media attributes of the ONT will not be configured independently in this example.

Step 7 Save the data.

```
huawei(config)#save
```

----End

3.3.2.1.10 Configuring the BTV Service (on a Web Page)

The OLT is connected to the remote gateway ONT through a GPON port to provide users with the bridge WAN multicast service.

Prerequisites

- The OLT has been connected to the BRAS and the multicast source.

- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **3.3.2.1.3 Adding an ONT to an OLT**.
- The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Table 3-12 Data plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● MVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONT: duplicates multicast packets based on user ports and MVLANs are stripped off downstream. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.
Multicast service data	Multicast protocol: IGMP proxy Multicast version: IGMPv2 Multicast program: dynamic obtaining mode

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Set the profile name to ftth_iptv. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

NOTE

Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

```
huawei(config)#traffic table ip name ftth_iptv cir off priority 4 priority-
policy local-setting
```

2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 1000 is mapped to GEM port 13 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1000
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the Ethernet port on the ONT and the multicast forwarding mode.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000. Configure the multicast forwarding mode is untagged.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#multicast-forward untag
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/9/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/9 0
```

5. Create service flows.

   Set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile ftth_iptv.

```
huawei(config)#service-port 1 vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service
user-vlan 1000 inbound traffic-table name ftth_iptv outbound traffic-table
name ftth_iptv
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service
user-vlan 1000 inbound traffic-table name ftth_iptv outbound traffic-table
name ftth_iptv
```

6. Create an MVLAN and configure the IGMP version.

   Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

7. Configure a program library.

   Set the mode for obtaining multicast programs to dynamic.

   NOTE

   You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
```



```
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

8. Set the IGMP mode.

   Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

9. (Optional) Configure the IGMP upstream port.

   In this example, the IGMP upstream port uses default value default.

   Run the **display igmp config global** command to query the IGMP upstream port mode. If this mode does not meet the requirement, run the **igmp uplink-port-mode** command to configure it.

10. Configure multicast users.

    Add service ports 1 and 2 as multicast users.

```
huawei(config-mvlan1000)#btv
huawei(config-btv)#igmp user add service-port 1
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 1
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

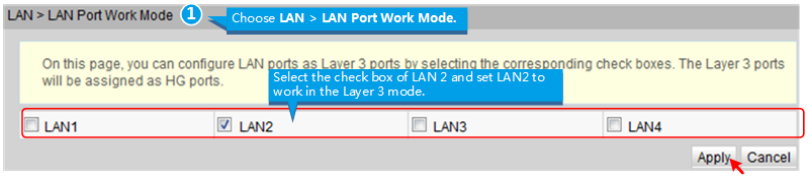
11. Save the data.

```
huawei(config)#save
```

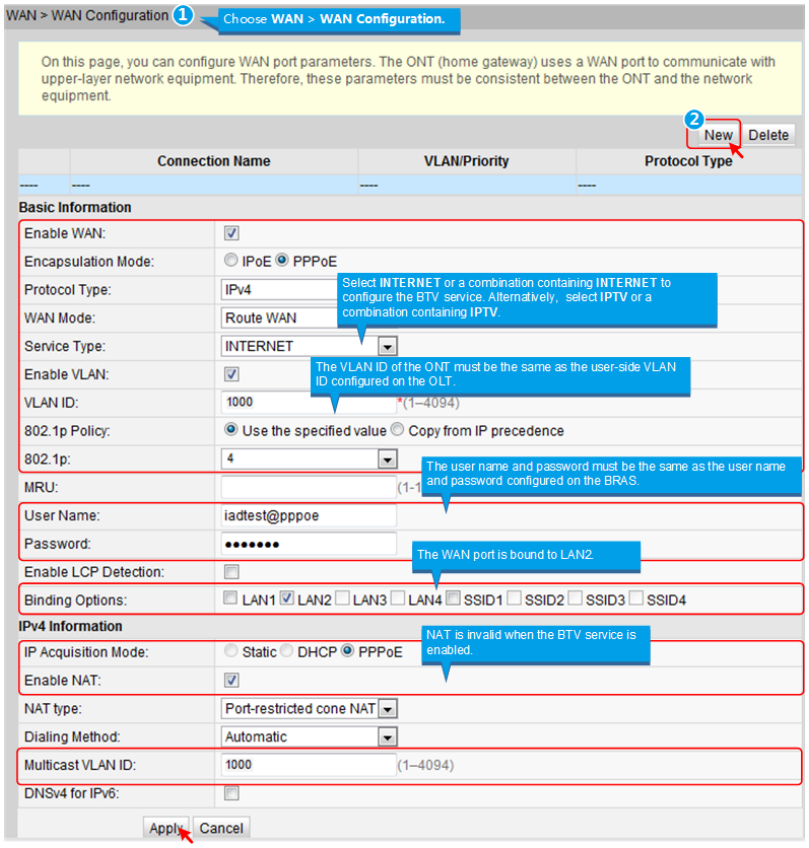
Step 2 Configure the ONT on the Web page.

1. Configure the working mode of a LAN port.

   The LAN port bound to the WAN port must work in the Layer 3 mode. Therefore, set the working mode to Layer 3 for the LAN port connected to the PC.



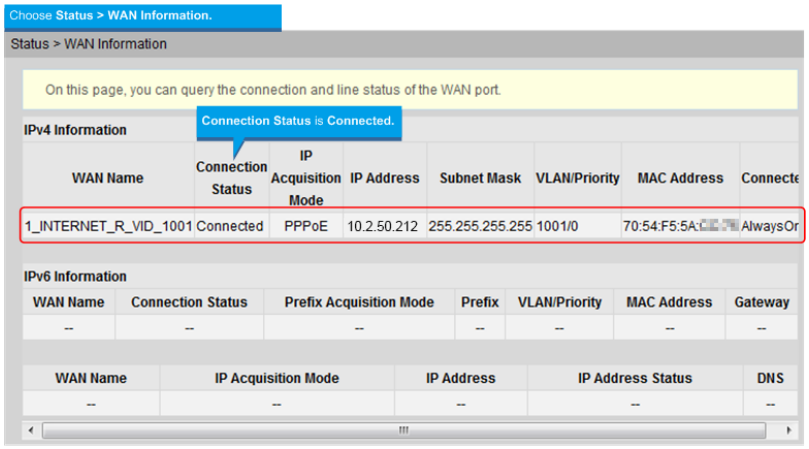
2. Configure parameters of a WAN port.



NOTE

If **Service Type** is set to IPTV or a type containing IPTV, this WAN port does not need to be bound to a LAN port.

3. Check the ONT connection status.



----End

3.3.2.1.11 Configuring the VoD Service (on a Web Page)

The OLT is connected to the remote gateway ONT through a GPON port to provide users with the VoD service.

Prerequisites

- The iTMS has configured the IPTV WAN ports on the ONT.
- The OLT has been connected to the BRAS and the program source.
- The VLAN of the LAN switch port connected to the OLT is the same as the upstream VLAN of the OLT.
- The ONT has been added to the OLT. For details, see **3.3.2.1.3 Adding an ONT to an OLT**.
- The Web page for configuring ONT varies with ONT versions, but the parameter configuration is the same. For details, see relevant ONT manuals.

Data Plan

Item	Data
ONT line profile	Profile name: ftth GEM port ID: 13
Traffic profile	ID: 8 802.1p priority: 4 CIR: off (unlimited) Priority-based scheduling policy: local-setting
VLAN Plan	Single VLAN tag: ● SVLAN ID: 1000 ● VLAN type: smart ● VLAN attribute: common ● CVLAN: 2001 VLAN translation policy: ● The ONT adds CVLAN tags (configured on the iTMS) to packets: untag<->C. ● The OLT implements VLAN translation: C<->S.

Procedure

Step 1 Configure the OLT.

1. Configure a traffic profile.

   Set the profile name to ftth_iptv. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

   NOTE

   Run the **display traffic table ip** command to query the existing traffic profiles in the system. If the existing traffic profiles in the system do not meet the requirements, run the **traffic table ip** command to add a traffic profile.

   ```
   huawei(config)#traffic table ip name ftth_iptv cir off priority 4 priority-policy local-setting
   ```


2. Configure the mapping relationship between a GEM port and a VLAN.

   The service flow of user VLAN 1000 is mapped to GEM port 13 in the ONT line profile.

```
huawei(config)#ont-lineprofile gpon profile-name ftth
huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1000
huawei(config-gpon-lineprofile-1)#commit
huawei(config-gpon-lineprofile-1)#quit
```

3. Configure the VLAN of the Ethernet port on the ONT.

   If the ONT is connected to the STB through Ethernet port 2, add Ethernet port 2 to VLAN 1000.

```
huawei(config)#ont-srvprofile gpon profile-name ftth
huawei(config-gpon-srvprofile-1)#port vlan eth 2 1000
huawei(config-gpon-srvprofile-1)#commit
huawei(config-gpon-srvprofile-1)#quit
```

4. Create a service VLAN and add an upstream port to it.

   Add upstream port 0/9/0 to VLAN 1000.

```
huawei(config)#vlan 1000 smart
huawei(config)#port vlan 1000 0/9 0
```

5. Create service flows.

   Create service flows. Set the S-VLAN to 1000, GEM port ID to 13, and C-VLAN to 2001, and use traffic profile ftth_iptv. Set the VLAN translation policy to Translate. The C-VLAN 2001 of the ONT is translated to S-VLAN 1000.

```
huawei(config)#service-port vlan 1000 gpon 0/1/0 ont 1 gemport 13 multi-
service user-vlan 2001
tag-transform translate inbound traffic-table name ftth_iptv outbound traffic-
table name ftth_iptv
huawei(config)#service-port vlan 1000 gpon 0/1/0 ont 2 gemport 13 multi-
service user-vlan 2001
tag-transform translate inbound traffic-table name ftth_iptv outbound traffic-
table name ftth_iptv
```

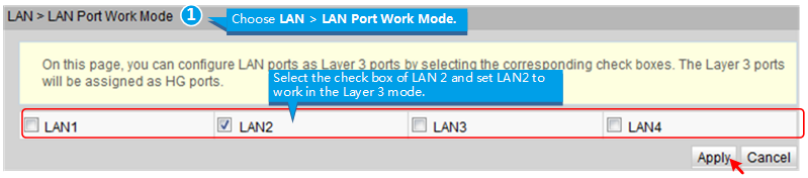
6. Save the data.

```
huawei(config)#save
```

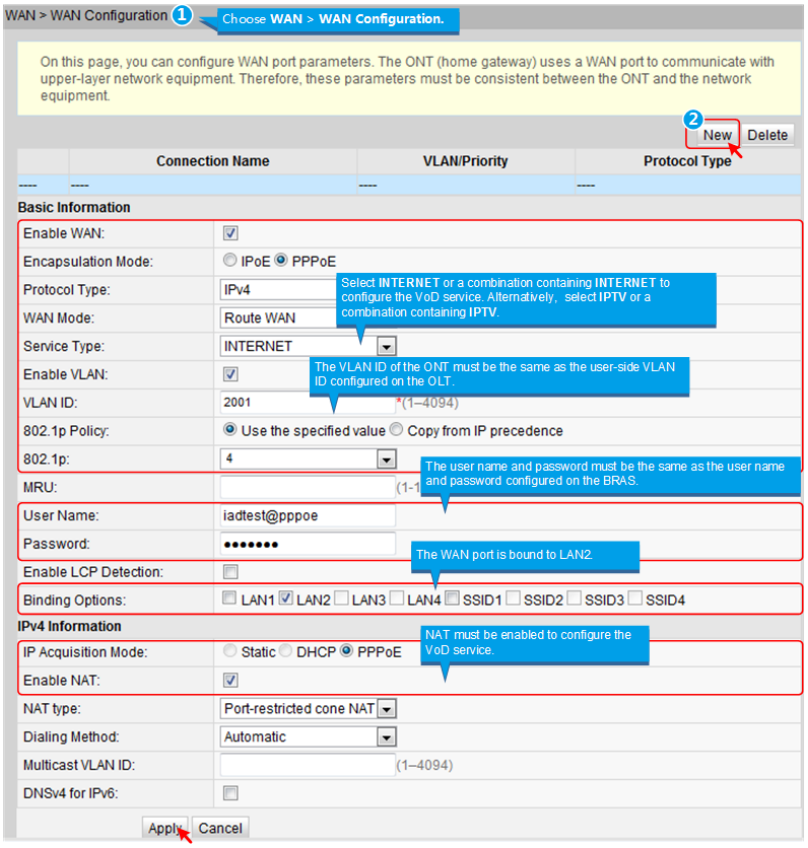
Step 2 Configure the ONT on the Web page.

1. Configure the working mode of a LAN port.

   The LAN port bound to the WAN port must work in the Layer 3 mode. Therefore, set the working mode to Layer 3 for the LAN port connected to the PC.



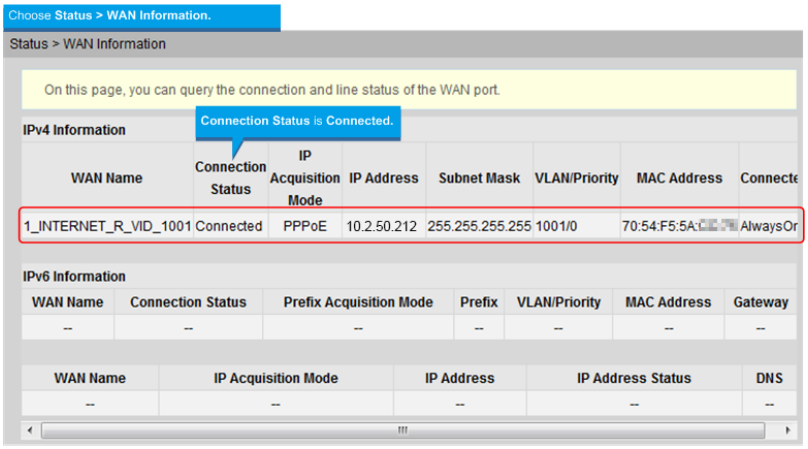
2. Configure parameters of a WAN port.



NOTE

If **Service Type** is set to IPTV or a type containing IPTV, this WAN port does not need to be bound to a LAN port.

3. Check the ONT connection status.



----End

3.3.2.1.12 Configuring the CATV Service

The OLT is connected to the remote ONT through a GPON port to provide users with the CATV service.

Prerequisites

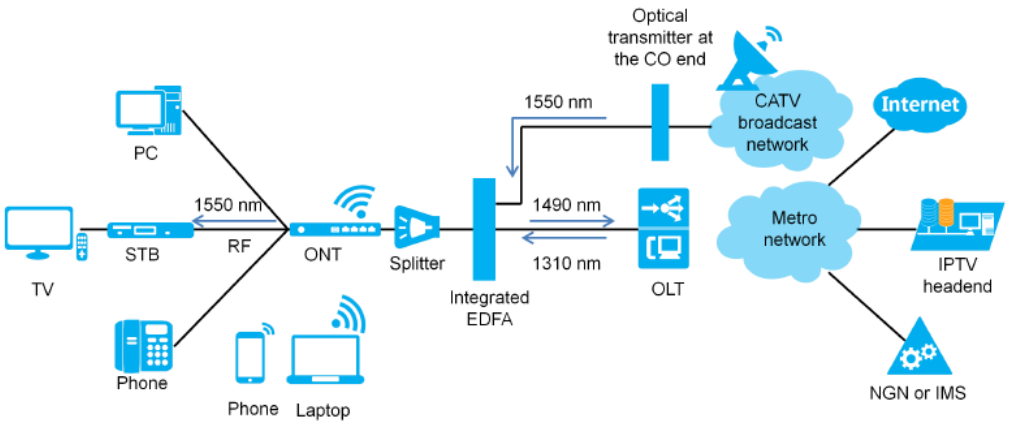
- The ONT is added to the OLT. For details, see Adding an ONT to an OLT.
- The ONT supports the CATV function.

Context

The optical transmitter at the CO end converts CATV signals to 1550 nm optical signals. After being amplified by the built-in optical amplifier inside the EDFA integrated device, the built-in WDM1r module multiplexes the 1550 nm optical signals and data optical signals for transmission. The CATV receiver on the user side or the ONT supporting CATV reception then restore 1550 nm optical signals to CATV video signals, as shown in the following figure.

NOTE

As shown in the figure, the EDFA is an integrated device supporting amplifying and multiplexing, which integrates optical amplifiers and WDM1r modules.



On the OLT side, enable ONT CATV (which is enabled by default). On the ONT side, no other configurations are required.

Procedure

Step 1 (Optional) Enable ONT CATV.

The port is enabled by default.

```
huawei(config)#ont port attribute catv default-operational-state on
```

----End

3.3.2.1.13 Configuring Any Port Any Service (on the Web Page)

The OLT can connect a remote ONT through the GPON interface. This topic describes how to configure the function of any port any service.

Prerequisites

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configuration, see the configuration guide.

- The ONT has been added to the OLT. For details, see **3.3.2.1.3 Adding an ONT to an OLT**.
- The VLAN of the LAN switch port connected to the OLT is consistent with the upstream VLAN of the OLT.

Data Plan

Item	Service Type	Data
ONT line profile	Internet access	Profile name: ftth T-CONT ID: 4 GEM port ID for Internet access service: 14
	Multicast service	Profile name: ftth T-CONT ID: 4 Multicast access service: 13
Traffic profile	Internet access	● Profile name: ftth_hsi ● 802.1p priority: 0 ● Upstream and downstream bandwidth: 4 Mbit/s ● Priority-based scheduling policy: local-setting
	Multicast service	● ID: 8 ● 802.1p priority: 4 ● CIR: off (unlimited) ● Priority-based scheduling policy: local-setting
VLAN Plan	Internet access	Double-tagged VLAN: ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● CVLAN ID: 1001 ● C'-VLAN ID: 1010-1011 VLAN Translation Policy: ● ONT: ONTs configure the VLAN and add the same C-VLAN tag to packets. All ONTs are in the same C-VLAN. ● OLT: The OLT performs VLAN translation: C<->S+C'. The C'-VLAN of every ONT differs from each other.

Item	Service Type	Data
	Multicast service	Single VLAN tag: ● SVLAN ID: 1000 ● MVLAN ID: 1000 ● CVLAN ID:1000 ● VLAN type: smart ● VLAN attribute: common VLAN translation policy: ● ONT: duplicates multicast packets based on user ports and MVLANs are stripped off downstream. ● OLT: duplicates multicast packets based on PON ports with MVLAN unchanged.

Procedure

- Configure the OLT.
  a. Configure a traffic profile.

     Run the **display traffic table ip** command to query existing traffic profiles in the system. If the traffic profiles existing in the system do not meet the requirements, you need to run the **traffic table ip** command to add a traffic profile.

     Set the name to ftth_hsi for the traffic profile of the Internet access service, the CIR to 4 Mbit/s, and the priority to 0. In addition, configure the scheduling mode so that packets are scheduled according to their priorities.

     ```
     huawei(config)#traffic table ip name ftth_hsi cir 4096 priority 0
     priority-policy local-setting
     ```

     Configure traffic profile 8 for the multicast service. Set the CIR to off (unlimited), priority to 4, and priority-based scheduling policy to local-setting (that is, queues are scheduled based on the priority specified in the profile).

     ```
     huawei(config)#traffic table ip index 8 cir off priority 4 priority-
     policy local-setting
     ```

  b. Configure the mapping relationship between a GEM port and a VLAN.

     The service flow of user VLAN 1001 is mapped to GEM port 14 in the ONT line profile. Map the service flows of user VLAN 1000 to the GEM port with index 13.

     ```
     huawei(config)#ont-lineprofile gpon profile-name ftth
     huawei(config-gpon-lineprofile-1)#gem mapping 14 0 vlan 1001
     huawei(config-gpon-lineprofile-1)#gem mapping 13 4 vlan 1000
     huawei(config-gpon-lineprofile-1)#commit
     huawei(config-gpon-lineprofile-1)#quit
     ```

     NOTE

     Do not configure the port VLAN or native VLAN of an ONT port.

  c. Create a service VLAN and add an upstream port to it.

     Add upstream port 0/9/0 to VLAN 100 and 1000.


```
huawei(config)#vlan 100,1000 smart
huawei(config)#vlan attrib 100 stacking
huawei(config)#port vlan 100,1000 0/9/0 0
```

d. Create service flows.

For the Internet access service, set the service VLAN to 100, GEM port ID to 14, and user VLAN to 1001. Use traffic profile ftth_hsi.

```
huawei(config)#service-port 1 vlan 100 gpon 0/1/0 ont 1 gemport 14 multi-
service
user-vlan 1001 tag-transform translate-and-add inner-vlan 1010 inbound
traffic-table name
ftth_hsi outbound traffic-table name ftth_hsi
```

For the multicast service, set the service VLAN to 1000, GEM port ID to 13, and user VLAN to 1000, and use traffic profile 8.

```
huawei(config)#service-port 2 vlan 1000 gpon 0/1/0 ont 1 gemport 13
multi-service
 user-vlan 1000 rx-cttr 8 tx-cttr 8
```

e. Create an MVLAN and configure the IGMP version.

Set the IGMP version for the MVLAN to IGMPv2.

```
huawei(config)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp version v2
  This operation will delete all IPv4 programs with source IP addresses
in the
current multicast VLAN
  Are you sure to change current IGMP version? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

f. Configure a program library.

Set the mode for obtaining multicast programs to dynamic.

NOTE

You can set the mode for obtaining multicast programs to dynamic only when the IGMP mode is off.

```
huawei(config-mvlan1000)#igmp mode off
  Are you sure to close IGMP? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully

huawei(config-mvlan1000)#igmp match mode disable
  Command has been executed successfully
```

(Optional) Set the address range for the dynamic programs. If you need to limit the address range of dynamic programs, perform this operation. For example, set the address range of dynamic programs to 224.1.1.1-224.1.1.100.

```
huawei(config-mvlan1000)#igmp match group ip 224.1.1.1 to-ip 224.1.1.100
```

g. Set the IGMP mode.

Select the IGMP proxy mode.

```
huawei(config-mvlan1000)#igmp mode proxy
  Are you sure to change IGMP mode? (y/n)[n]:y
  Command is being executed. Please wait...
  Command has been executed successfully
```

h. (Optional) Configure the IGMP upstream port.

In this example, the IGMP upstream port uses default value default.

Run the **display igmp config global** command to query the IGMP upstream port mode. If this mode does not meet the requirement, run the **igmp uplink-port-mode** command to configure it.

i. Configure multicast users.

Add service port 2 as multicast users.

```
huawei(config-btv)#igmp user add service-port 2
huawei(config-btv)#multicast-vlan 1000
huawei(config-mvlan1000)#igmp multicast-vlan member service-port 2
huawei(config-mvlan1000)#quit
```

j. Save the data.

```
huawei(config)#save
```

- Configure the ONT on the web page.

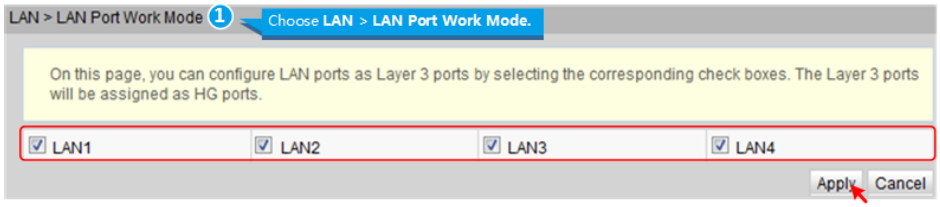
a. Log in to the Web configuration page.

i. Configure the IP address of the PC network adapter to be in the same network segment with the IP address of the local maintenance Ethernet port on the ONT.

ii. Open the Web browser, and enter the IP address (https with high priority is recommended) of the local maintenance Ethernet port on the ONT. In the login window that is displayed, enter the user name and password of the administrator. After the password is authenticated, the web configuration window is displayed.

b. Configure the working mode of a LAN port.

The function of any port any service requires that all LAN ports work in Layer 3 mode. Set LAN ports to Layer 3 mode.

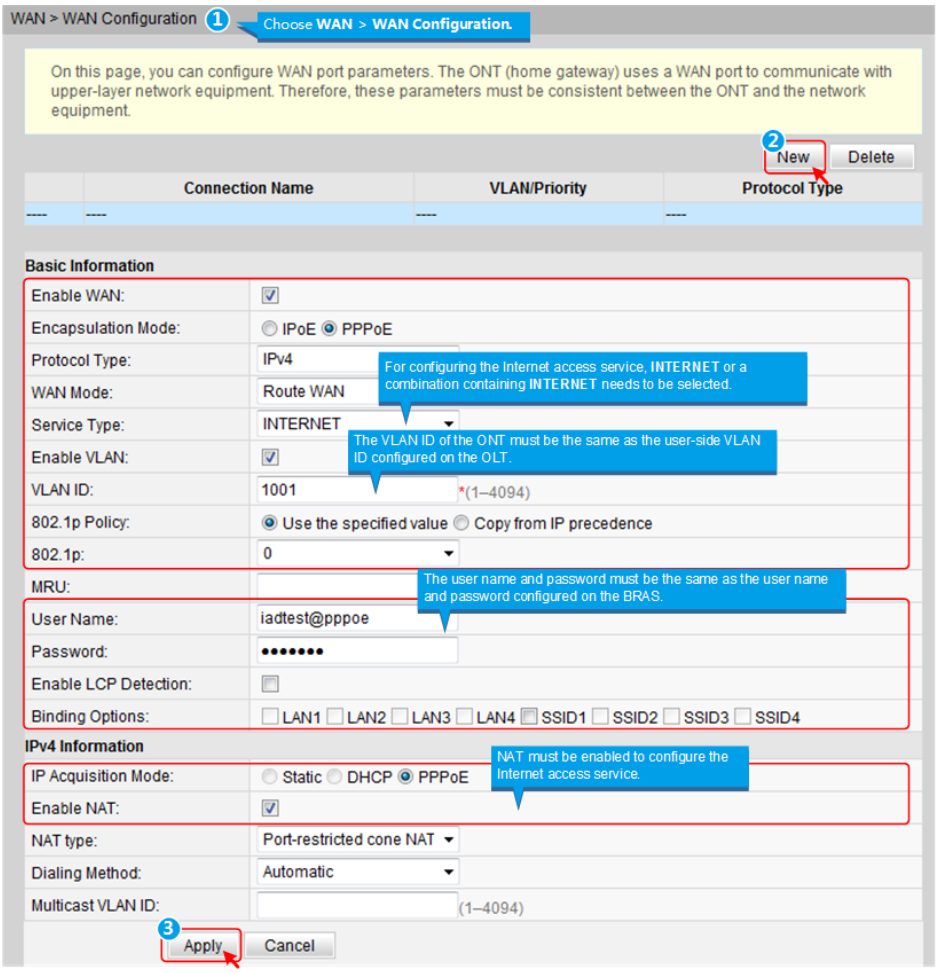


c. Configure parameters of a WAN port.

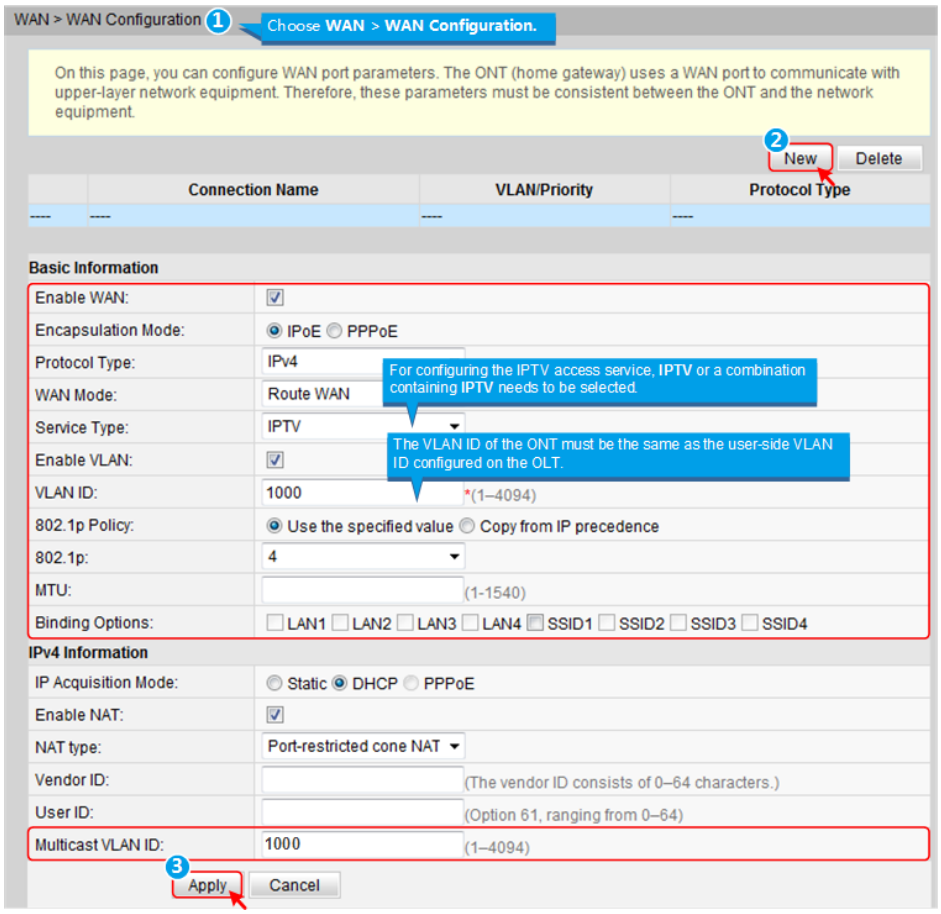
NOTE

Do not bind WAN ports and LAN ports during the configuration of any port any service.

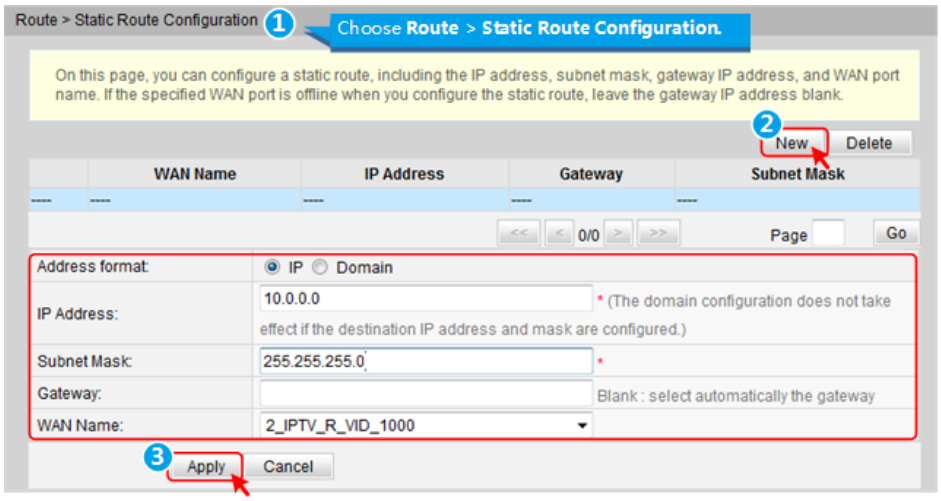
WAN configuration for the Internet access service



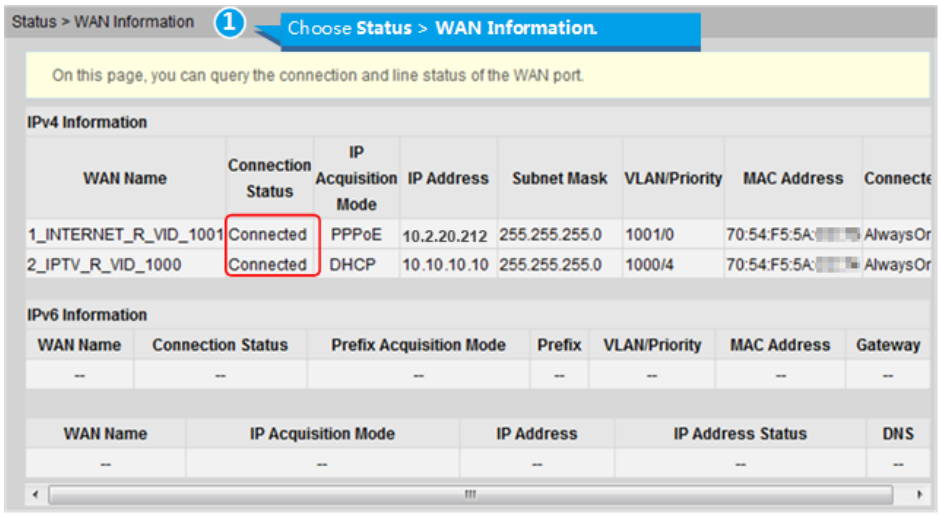
WAN configuration for the multicast service



d. Configure a static route for the multicast service.



e. Check the ONT connection status.



----End

Result

The ONT can connect to the Internet access service or Multicast service through any LAN port.

3.3.2.1.14 Configuring Link Aggregation, Congestion Control, and Security Policies

The global configuration of link aggregation and queue scheduling based on priorities ensures service reliability. The global configuration of security policies ensures service security.

Context

Link aggregation provides a higher bandwidth and uplink reliability for optical line terminals (OLTs) by aggregating multiple uplink Ethernet ports to one link aggregation group (LAG).

Congestion control places the packets to be sent from a port into multiple queues that are marked with different priorities. Then, the packets are sent based on queue priorities.

Security policies ensure system, user, and service security.

NOTE

Enable a service security function based on the service type. For details, see **3.2.6 Principle of Security Data Plan**.

Procedure

- Configure link aggregation.

  The following configurations are used as an example to configure link aggregation:

  - Uplink ports 0/9/0 and 0/9/1 are added to a LAG.
  - The two ports send packets upstream based on the packets' source MAC addresses.
  - The LAG works in Link Aggregation Control Protocol (LACP) static aggregation mode.

  ```
  huawei(config)#link-aggregation 0/9 0-1 ingress workmode lacp-static
  ```

- Configure queue scheduling.

According to quality of service (QoS) planning principles, all packets are scheduled in strict priority (SP) mode and mapped to queues according to the packets' priorities. For details about QoS planning principles, see **3.2.2 Principle of QoS Planning**.

```
huawei(config)#queue-scheduler strict-priority
huawei(config)#cos-queue-map cos0 0 cos4 4 cos5 5 cos6 6
```

- Configure system security.
  - Enable deny of service (DoS) anti-attack on the OLT.
    i. Run the **security anti-dos enable** command to globally enable DoS anti-attack.
    ii. Run the **security anti-dos control-packet policy** command to configure a protocol packet processing policy that will be used when a DoS attack occurs.
    iii. Run the **security anti-dos control-packet rate** command to configure the threshold for the rate of sending protocol packets to the CPU.
  - Enable IP address anti-attack on the OLT.
    Run the **security anti-ipattack enable** command to enable IP address anti-attack.
- Configure user security.
  - Enable MAC address anti-flapping on the OLT.
    Run the **security anti-macduplicate enable** command to enable MAC address anti-flapping.
  - Enable MAC address anti-spoofing on the OLT.
    i. In global config mode, run the **security anti-macspoofing enable** command to globally enable MAC address anti-spoofing.
    ii. Enable MAC address anti-spoofing at VLAN level in global config mode or service profile mode:
      1) In global config mode, run the **security anti-macspoofing vlan** command to enable MAC address anti-spoofing.
      2) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
      3) Perform the following operations to enable MAC address anti-spoofing in VLAN service profile mode:
        1) Run the **security anti-macspoofing enable** command to enable MAC address anti-spoofing at VLAN level.
        2) Run the **commit** command to make the profile configuration take effect.
        3) Run the **quit** command to quit the VLAN service profile mode.
        4) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    iii. (Optional) Run the **security anti-macspoofing max-mac-count** command to set the maximum number of MAC addresses that can be bound to a service flow.
    iv. (Optional) Run the **security anti-macspoofing exclude** command to configure the types of packets for which MAC address anti-spoofing does not take effect, such as Internet Group Management Protocol (IGMP) packets.
  - Enable IP address anti-spoofing on the OLT.
    IP address anti-spoofing can be enabled or disabled at three levels: global, VLAN, and service port levels. This function takes effect only after it is enabled at the three

levels. Among the three levels, IP address anti-spoofing is disabled only at the global level by default.

i. In global config mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the global level.

ii. In VLAN service profile mode, run the **security anti-ipspoofing enable** command to enable IP address anti-spoofing at the VLAN level.

iii. Run the **security anti-ipspoofing service-port** *serviceport-id* **enable** command to enable IP address anti-spoofing at the service port level.

- Configure service security.
  - Enable Dynamic Host Configuration Protocol (DHCP) Option 82 on the OLT. This configuration is recommended for the DHCP-based Internet access service.

    i. Enable DHCP Option 82 on the OLT.

    DHCP Option 82 can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four levels. Among the four levels, DHCP Option 82 is disabled only at the global level by default.

    - The global level: In global config mode, run the **dhcp option82** command to enable DHCP Option 82 at the global level.

      When you run this command, select the **enable**, **forward**, or **rebuild** parameter based on site requirements. The three parameters can all enable DHCP Option 82 but provide different packet processing policies on the OLT. For details, see the **dhcp option82** command.
    - The port level: In global config mode, run the **dhcp option82 port** or **dhcp option82 board** command to enable DHCP Option 82 at the port level.
    - The VLAN level:

      1) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.

      2) Run the **dhcp option82 enable** command to enable DHCP Option 82 at the VLAN level.

      3) Run the **commit** command to make the profile configuration take effect.

      4) Run the **quit** command to quit the VLAN service profile mode.

      5) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
    - The service port level: In global config mode, run the **dhcp option82 service-port** command to enable DHCP Option 82 at the service port level.

    ii. On the OLT, run the **dhcp-option82 permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT DHCP packets to carry Option 82 information.
  - Enable Policy Information Transfer Protocol (PITP) on the OLT. This configuration is recommended for the PPPoE-based Internet access service.

    i. Enable PITP on the OLT.

    PITP can be enabled or disabled at four levels: global, port, VLAN, and service port levels. This function takes effect only after it is enabled at the four

levels. Among the four levels, PITP is disabled only at the global level by default.

- The global level: In global config mode, run the **pitp enable pmode**, **pitp forward pmode**, or **pitp rebuild pmode** command to enable PITP at the global level.

  In the preceding commands, the **enable**, **forward**, and **rebuild** parameters can all enable PITP but provide different packet processing policies on the OLT. Select one of them based on site requirements. For details, see the **pitp** command.
- The port level: In global config mode, run the **pitp port** or **pitp board** command to enable PITP at the port level.
- The VLAN level:
  1) In global config mode, run the **vlan service-profile** command to create a VLAN service profile.
  2) Run the **pitp enable** command to enable PITP at the VLAN level.
  3) Run the **commit** command to make the profile configuration take effect.
  4) Run the **quit** command to quit the VLAN service profile mode.
  5) Run the **vlan bind service-profile** command to bind the created VLAN service profile to a VLAN.
- The service port level: In global config mode, run the **pitp service-port** command to enable PITP at the service port level.

ii. On the OLT, run the **pitp permit-forwarding service-port** command with the **enable** parameter selected, to allow ONT PPPoE packets to carry a vendor tag.

----End

3.3.2.1.15 Verifying Services

In the FTTH scenario, ONTs are installed in users' houses which are far away from the central equipment room. ONTs provide remote service verification methods including PPPoE dialup emulation, call emulation, and multicast emulation to facilitate configuration and commissioning engineers to verify services remotely after service configuration.

Prerequisites

ONTs and upper-layer devices have been connected properly. The BRAS and MGC/IMS have been configured.

Background

Remote Service Verification Method	Function	Description
PPPoE dialup emulation	An ONT simulates a PPPoE user terminal software to perform dialup and interact with the BRAS to verify the connectivity between the ONT and BRAS.	● PPPoE dialup emulation requires a service flow which does not belong to a QinQ VLAN. ● A user name, password, and authentication mode must be configured on the BRAS for the PPPoE dialup emulation. ● An ONT supports a maximum of a PPPoE dialup emulation.
Call Emulation	An ONT simulates a voice user to make a call to check whether the voice service data is correctly configured. You can also use the call emulation function to locate a fault when the voice service is faulty.	● An ONT can simulate a caller or callee to communicate with a phone in a call. In this case, only a functional phone is required in the central office where the acceptance personnel is. ● An ONT supports a maximum of a call emulation.
Multicast emulation	This function enables you to simulate a multicast user going online and lead the program stream to an ONT. You can check whether the multicast service is normal by checking the real-time traffic of the multicast program.	Multicast services configured in the dynamic controllable multicast mode do not support this function.

Data plan

Item	Data	Remarks
PPPoE dialup emulation parameters	PPPoE user name: test@huawei Password: test1234	The user name, password, and authentication mode for the emulation test must be configured on the BRAS. The entered user name, password, and authentication mode must be consistent with those configured on the BRAS.
Call emulation parameters	ONT POTS ID: 1	The default values are used. You can run the **display pots emulational configuration** command to check the parameter values.

Item	Data	Remarks
Multicast emulation parameters	Multicast service flow ID: 1 MVLAN: 1000 IP address of the multicast program: 224.1.1.10	-

Procedure

- Verify the Internet access service using PPPoE dialup emulation.
  a. In the xPON board mode, run the **pppoe simulate start** command to start a PPPoE dialup emulation test. The following test uses GPON as an example:

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#pppoe simulate start
{ portid<U><0,7> }:0
{ ontid<U><0,127> }:1
{ eth<K>|untagged<K>|vlanid<U><0,4095> }:eth
{ ont-portid<U><1,8> }:4
{ untagged<K>|vlanid<U><0,4095> }:100
{ priority<U><0,7>|user-name<K> }:user-name
{ username<S><Length 1-64> }:test@huawei
{ user-password<K> }:user-password
{ password<S><Length 1-64> }:test1234
{ authentication-mode<K> }:authentication-mode
{ protocol<E><chap,pap> }:chap

  Command:
          pppoe simulate start 0 1 eth 4 100 user-name test@huawei user-
password
 test authentication-mode chap

huawei(config-if-gpon-0/1)#
  ---------------------------------
  ONT PPPoE Test Result
  ---------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 1
  ONT ETH Port ID      : 4
  ONT Vlan ID          : 100
  Vlan Priority        : -
  Emluator result      : Success
  Session ID           : 18814
  User IP              : 192.168.100.101
  Gateway IP           : 192.168.100.1
  ---------------------------------
```

- Troubleshooting methods for the Internet access service
  a. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the Internet access service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.
     - If a native VLAN is configured for the Ethernet port on the ONT, run the **display ont port attribute** command in the xPON board mode to check whether the native VLAN is correct.
  b. Check the upstream and downstream ports by checking the MAC address learning status.

i. Run the **display mac-address vlan** command to check the MAC address learning status of the Internet service VLAN.
   - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
   - If the downstream port does not learn a MAC address, check whether the ONT is activated, whether the PC is connected to the right port on the ONT, and whether the PC is working properly.

ii. Run the **display ont-learned-mac** command to check whether the ONT connecting to the PON port learned any MAC addresses.

   If not, check whether the ONT properly connects to the PC or home gateway (HGW).

- Verify the voice service using call emulation.

  a. Run the **ont emulational call** command to configure a call emulation test.

```
huawei(config)#test
huawei(config-test)#ont emulational call caller-port 0/1/0 1 1 telno
77730020
{ <cr>|caller-stop-time<K> }:

  Command:
          ont emulational call caller-port 0/1/0 1 1 telno 77730020
```

  b. The ONT outputs the call emulation result after the test is complete.

```
huawei(config-test)#
  ------------------------------------------------------------------
  F/S/P                : 0/1/0
  ONT-ID               : 0
  ONT-POTSID           : 1
  Test type            : caller emulational call test
  Detected number      : 77730020
  Reported number      : 77730020
  Current status       : test end
  Test Result          : success
  ------------------------------------------------------------------
```

- Troubleshooting methods for the voice service.

  a. Check whether configurations are complete on the OLT.
     - Run the **display ont info** command to query the ONT status to check whether the ONT is registered successfully.
     - Run the **display service-port** command to check whether the voice service flow is configured and whether the inner VLAN ID of the service flow is consistent with that in the data plan.

  b. Check the upstream and downstream ports by checking the MAC address learning status.

     Run the **display mac-address vlan** command to check the MAC address learning status of the voice service VLAN.
     - If the upstream port does not learn a MAC address, check the network connections between the upstream port and upper-layer devices and check the configurations of upper-layer devices.
     - If the downstream port does not learn a MAC address, check whether the ONT is activated and whether physical links are normal.
     - If both the upstream and downstream ports can learn the MAC address, record the MAC address of the ONT and log in to the service router (SR) to check whether an IP address is allocated to the MAC address.

c. Check the registration status of the voice service.

- You can run the **display ont port state** command on the OLT to query the call connection status on the POTS port. If **Call State** is **RegisterFail** or **Connecting** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
- If the ONT uses the H.248 protocol, you can run the **display ont mg status** command on the OLT to query the registration status of the MG interface that connects to the ONT. If **MG Status** is **UnRegistered** or **Registering** for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.
- You can query the registration status of the voice service on the ONT web page. If the query result shows that the registration fails or the voice service is in the registering state for a long time, check whether the voice configuration on the MGC/SIP server is consistent with that on the ONT.

- Verify the multicast service using multicast emulation.

a. Run the **igmp static-join** command to simulate a multicast user to order a multicast program.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 1 ip 224.1.1.10 vlan
1000
```

NOTE

If the multicast program is obtained dynamically, **igmp static-join** can be executed successfully only when the range for obtaining the dynamic program is set.

b. Run the **display igmp user** command to query the status of the multicast user.

```
huawei(config-btv)#display igmp user service-port 1
  User                        : 0/1/0/1
  State                       : online
  Authentication              : no-auth
  Quick leave                 : MAC-based
  IGMP flow ID                : 1
  Video flow ID               : 1
  Log switch                  : enable
  Bind profiles               : -
  IGMP version                : IGMP v3
  Current version             : IGMP v3
  Current IGMP IPv6 version   : IGMP IPv6 v2
  Available programs          : 8
  Global leave                : disable
  User max bandwidth          : no-limit
  Used bandwidth(kbps)        : 0
  Used bandwidth
  to max bandwidth(%)         : -
  Total video bandwidth       : -
  Mcast video bandwidth       : -
  Active program list

------------------------------------------------------------------------
--
  Program name     VLAN  IP/MAC           State           Start time

------------------------------------------------------------------------
--
  PROGRAM-5        1000  224.1.1.10       watching        2011-10-29
                                                         16:33:41+08:00

------------------------------------------------------------------------
--
  Total: 1
```


c. Run the **display multicast flow-statistic** command to query the real-time traffic of the multicast program.

```
huawei(config-btv)#display multicast flow-statistic vlan 1000 ip
224.1.1.10
{ <cr>|sourceip<K> }:

  Command:
          display multicast flow-statistic vlan 1000 ip 224.1.1.10
  Command is being executed. Please wait...
  Multicast flow statistic result: 8736(kbps)
```

----End

3.3.3 Configuring the Service by Using U2560

This topic describes how to configure the Internet access service, VoIP service and Wi-Fi service by using U2560.

3.3.3.1 Prerequisites

Before configuring services on the U2560, plan data of the entire network in a unified manner and add the ONT to the U2560.

Before adding the ONT to the U2560, complete pre-configuration on the NMS or using commands to set up Layer 2 service channels. For details, see **Table 3-13**.

Table 3-13 Pre-configuration

Configuration Method	Procedure
On the NMS	GPON ONT: **3.3.1.1.1 Configuring the GPON FTTH Layer 2 Internet Access Service on the NMS**
Using commands	See the following to configure ONTs on the OLT: GPON ONT:**3.3.2.1.3 Adding an ONT to an OLT**, **3.3.2.1.4 Configuring the Internet Access Service (on a Web Page or the U2000)**, **3.3.2.1.5 Configuring the Wi-Fi Access Service (on a Web Page)**, **3.3.2.1.6 Configuring the H.248-based Voice Service (on a Web Page or the U2000)** and **3.3.2.1.8 Configuring the SIP-based Voice Service (on a Web Page or the U2000)**

3.3.3.2 Commissioning Interoperation Between the U2560 and the ONT

To configure and issue ONT services using the U2560, you need to add the ONT on the U2560 so that the U2560 can manage the ONT.

Data Plan

Table 3-14 provides the data plan for commissioning interoperation between the U2560 and the ONT through the web page.

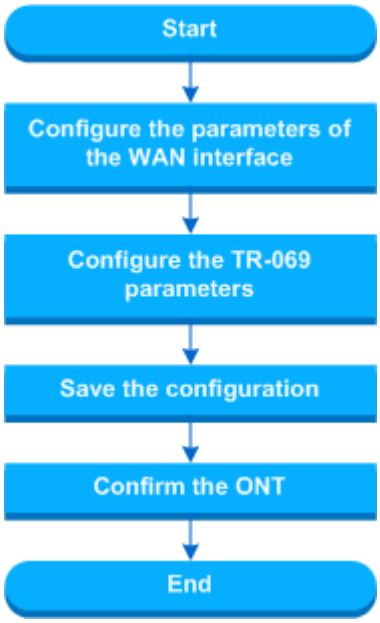
Table 3-14 Data plan for commissioning interoperation between the U2560 and the ONT through the web page

Parameter	Data	Description
Service type of the WAN interface	TR069	When configuring the U2560 management channel, you need to select only TR069 or a combination with TR069. In this example, TR069 is selected.
Connection mode	Route	-
VLAN ID of the WAN interface	50	The VLAN ID of the WAN interface must be the same as the C-VLAN ID configured on the OLT.
Mode of obtaining an IP address	DHCP	There are three modes to obtain an IP address: ● DHCP: Obtain an IP address dynamically. ● Static: Configure an IP address manually. ● PPPoE: Access in the PPPoE dialup mode. In this example, the DHCP mode is configured. You can also select the static or PPPoE mode according to the data plan of the upper-layer network.
ACS URL	http://10.11.11.1:9070	It can be the IP address, port ID, domain name of the ACS server.
Periodical notification interval	43200	It is the default value of the system.
ACS user name	hgw	It is the default value of the system.
ACS password	hgw	It is the default value of the system.
User name of a requested connection	server	It must be the same as that planned on the U2560.
Password of a requested connection	server	It must be the same as that planned on the U2560.

Process

Figure 3-10 shows the flowchart for commissioning interoperation between the U2560 and the ONT through the web page.

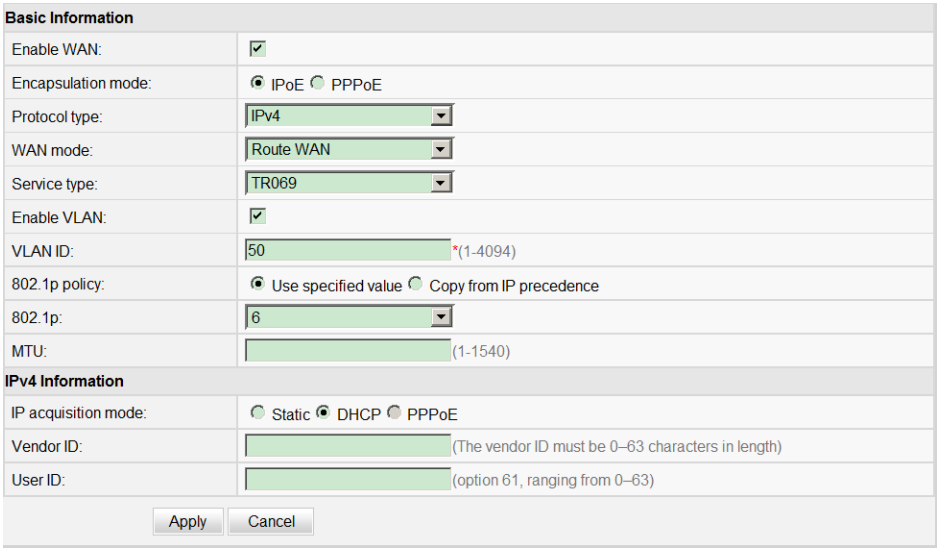
Figure 3-10 Process for commissioning interoperation between the U2560 and the ONT through the web page



Procedure

Step 1 Configure the parameters of the WAN interface.

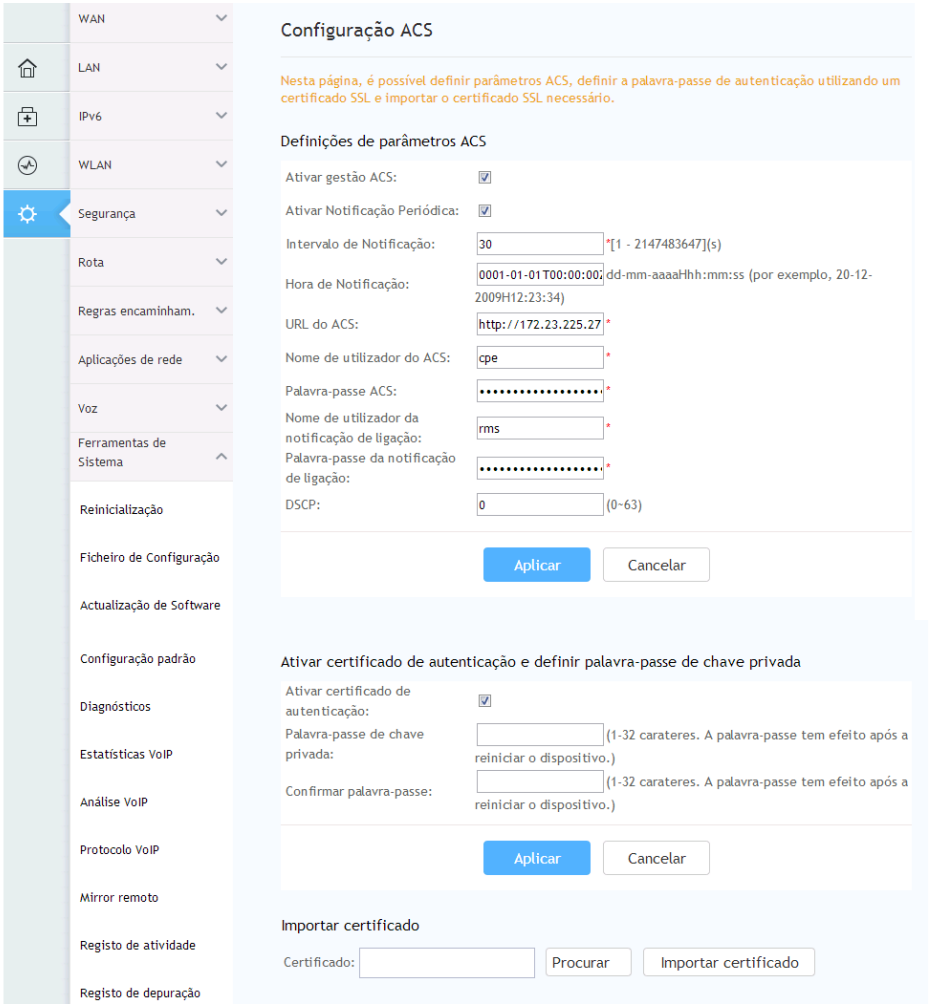
1. In the navigation tree on the left, choose **WAN** > **WAN Configuration**.
2. In the pane on the right, click **New**. In the dialog box that is displayed, configure the parameters of the WAN interface as follows:
   - Enable WAN: enabled
   - Encapsulation mode: IPoE
   - WAN mode: Route WAN
   - Service type: TR069
   - VLAN ID: 50
   - 802.1p: 6
   - IP acquisition mode: DHCP



3. Click **Apply**.

Step 2 Configure the TR-069 parameters.

1. In the navigation tree on the left, choose **System Tools** > **TR-069**.
2. In the pane on the right, set the TR-069 client parameters (other parameters use the default values) as follows:
   - ACS URL: http://10.11.11.1:9070
   - Connection Request User Name: server
   - Connection Request Password: server



3. Click **Apply**.

Step 3 Confirm the ONT.

Log in to the U2560 and then choose **Subnet view** > **TR-069 Subnet** from **WLAN and Home Network View** in the navigation tree on the left. In the pane on the right, right-click and choose **Refresh** from the shortcut menu. The reported ONT list is displayed. Then, select the ONT list, right-click, and choose **Confirm** from the shortcut menu.

----End

Result

On the U2560, you can configure ONT services. For details, see the configuration examples.

3.3.3.3 Data Plan

This topic plans the data in a unified manner for various example networks of connecting ONTs in an FTTH network. Subsequent examples are configured based on the following data plan.

Table 3-15 shows the unified data plan for the HSI service, VoIP service and Wi-Fi service in an FTTH network.

Table 3-15 Data plan for connecting ONTs in the FTTH network

Configuration Item	Data Item	Detailed Data	Remarks
WAN port data	HSI service (Layer 3 routing)	● Service type: Internet ● Connection mode: routing ● VLAN ID: 10 ● IP address obtainment mode: PPPoE (user name: iadtest@pppoe, password: iadtest) ● 802.1p: 1 ● NAT function: enable ● Bound port: LAN1 (LAN1 is a Layer 3 LAN)	● For configuring HSI service or Wi-Fi service, Internet or a combination containing Internet must be selected as the service type. For configuring VoIP service, VoIP or a combination containing VoIP must be selected as the service type. ● The VLAN ID of the ONT must be the same as the user-side VLAN ID configured on the OLT. ● PPPoE must use the same user name and password as the upper-layer BRAS. ● The HSI service involves the Layer 2, Layer 3 bridge and Layer 3 routing modes. In the Layer 2 mode, all configurations are required only on the OLT. The application mode of the Layer 3 bridge mode is similar to the Layer 2 mode. It is recommended that you use the Layer 2 mode. ● The Wi-Fi service does not support the Layer 2 mode.
	VoIP service	● Service type: VoIP ● Connection mode: routing ● VLAN ID: 20 ● IP address obtaining mode: DHCP ● 802.1p: 6	
	Wi-Fi service (Layer 3 bridge)	● Service type: Internet (not configurable) ● Connection mode: bridge ● VLAN ID: 40 ● 802.1p: 1 ● Bound port: SSID1	
	Wi-Fi service (Layer 3 routing)	● Service type: Internet ● Connection mode: routing ● VLAN ID: 40 ● IP address Obtainment mode: PPPoE (user name: iadtest@pppoe, password: iadtest) ● 802.1p: 1 ● NAT function: enable ● Bound port: SSID1	

Configuration Item	Data Item	Detailed Data	Remarks
VoIP service data	SIP parameters	● IP address of the primary server: 10.10.100.10 ● Port ID of the primary server: 5060 ● Home domain name: softx3000.huawei.com ● Digitmap: x.S|x.# (Default) ● User 1: – Phone number: 88001234 – Authentication user name: 88001234@softx3000.huawei.com – Password: iadtest1 ● User 2: – Phone number: 88001235 – Authentication user name: 88001235@softx3000.huawei.com – Password: iadtest2	-
	H.248 parameters	● Primary MGC address: 10.10.100.10 ● Primary MGC port: 2944 ● MID format: domain name ● MG domain name: 6877687714852901 ● TID: A0 and A1	-
Wi-Fi service	SSID1	ChinaNet-huawei	-
	Security mode	WPA Pre-Shared Key	
	WPA encryption mode	● TKIP&AES ● Key: chinahuawei	

3.3.3.4 Configuring the Internet Access Service Through the U2560

This topic provides an example of how to configure the Internet access service through the U2560.

Prerequisites

- The ONT is auto discovered on the U2560. For details, see **3.3.3.2 Commissioning Interoperation Between the U2560 and the ONT**.
- The user-side PC must be connected with the LAN port of an ONT by using network cables.

Context

The Internet access service includes the Layer 2 Internet access service and Layer 3 Internal access service.

- Layer 2 Internet access service: The PPPoE dialup is performed on the PC. The IP address is allocated by the upper-layer BRAS. The ONT is connected to the OLT and then to the upper-layer network in the Layer 2 mode to provide the high-speed Internet access service.
- Layer 3 Internet access service: The PPPoE auto dialup is performed on the ONT. The IP address is allocated by the DHCP IP address pool on the ONT. The ONT is connected to the OLT and then to the upper-layer network in the Layer 3 mode to provide the high-speed Internet access service.

You do not need to configure the Layer 2 Internet access service on the ONT, but you need to only enable the Layer 2 service channels between the OLT and ONT. This topic describes only how to configure the Layer 3 Internet access service.

Every data change must be saved. You can click **Save** in a window to save data changes. If you navigate to another node without saving data changes, a dialog box will be displayed prompting you to save the data changes. In this case, click **YES** in the dialog box. New data will be automatically applied to the ONTs after the data changes are saved.

NOTICE

When configuring services on the U2560, do not modify the WAN interface connecting the U2560 and the ONT. Otherwise, the U2560 loses communication with the ONT.

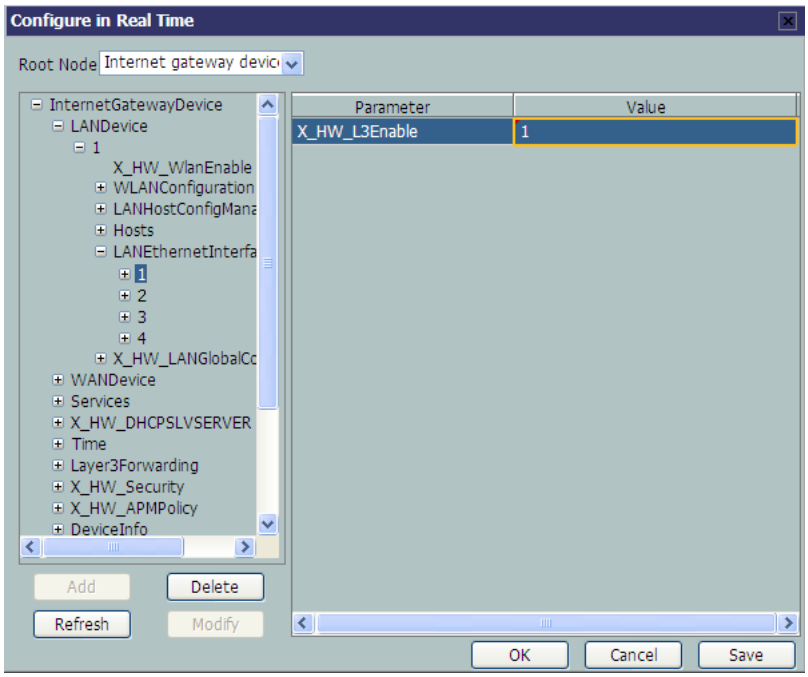
Procedure

Step 1 Log in to the U2560 and choose **Subnet View** > **TR069 Subnet** from the navigation tree. In the terminal list, right-click an ONT and choose **Tools** > **Configure in Real Time** from the shortcut menu.

Step 2 In the **Configure in Real Time** dialog box, set **Root Node** to **Internet gateway device**.

Step 3 Configure the working mode of a LAN port.

Choose **InternetGatewayDevice** > **LANDevice** > **1** > **LANEthernetInterfaceConfig** > **1** from the navigation tree. In the right pane, set **X_HW_L3Enable** to **1**, indicating that port LAN1 works in the L3 mode.



NOTE

- When **X_HW_L3Enable** is set to **0**, it indicates that the corresponding LAN port works in the L2 mode.
- When **X_HW_L3Enable** is set to **1**, it indicates that the corresponding LAN port works in the L3 mode.

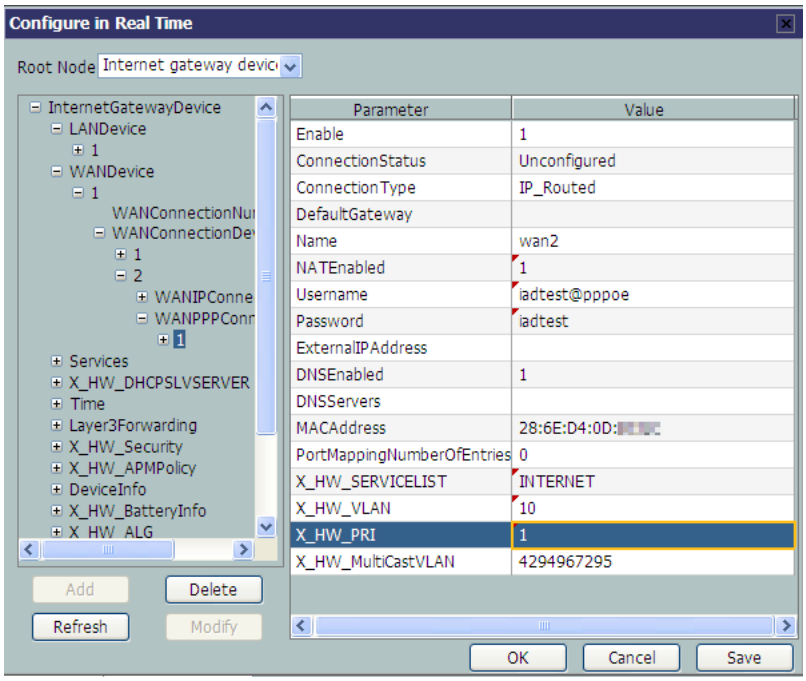
By default, **X_HW_L3Enable** is set to **0**.

Step 4 Configure the parameters of the WAN interface.

1. Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** from the navigation tree. Click **Add** in the lower left part to create an instance.
2. Choose **2** > **WANPPPConnection** from the navigation tree and click **Add** in the lower left part. Choose the new **1** branch from the navigation tree. In the right pane, set the parameters as follows:
   - Set **Enable** to **1**, indicating that the WAN connection is enabled.
   - Set **Connection Type** to **IP_Routed**, indicating that the connection type of the WAN interface is in routing mode.
   - Set **NATEnable** to **1**, indicating that the NAT function is enabled.
   - Set **Username** to **iadtest@pppoe** and **Password** to **iadtest**, indicating that the PPPoE user name is **iadtest@pppoe** and the password is **iadtest**.
   - Set **X_HW_SERVICELIST** to **INTERNET**, indicating that the WAN interface provides Internet access.
   - Set **X_HW_VLAN** to **10**, indicating that the VLAN ID of the WAN interface is 10.
   - Set **X_HW_PRI** to **1**, indicating that the priority level of the WAN interface is 1.

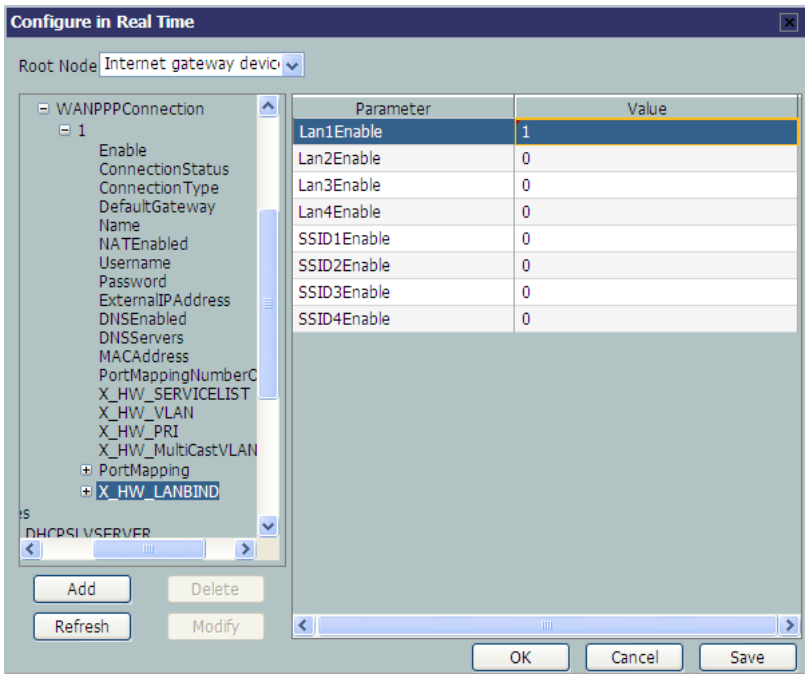
NOTE

- If the WAN interface obtains IP addresses in static or DHCP mode, choose **WANIPConnection** to set the parameters of the WAN interface.
- If the WAN interface obtains IP addresses in PPPoE mode, choose **WANPPPConnection** to set the parameters of the WAN interface.



Step 5 Bind a LAN port.

Choose **1X_HW_LANBIND** from the navigation tree. In the right pane, set **Lan1Enable** to **1** to bind the WAN interface to LAN port 1.



Step 6 Click **OK** after the configuration.

----End

Result

- Layer 2 Internet access:

Check whether the user successfully gains access to the Internet through dialup on the PC.

a. The LAN1 port of the ONT is connected to the Ethernet port of the PC properly.
b. Dial up on the PC using the PPPoE dialup software.
c. The user gains access to the Internet on the PC after the dialup is successful.

- Layer 3 Internet access:

  Check whether the user successfully gains access to the Internet through dialup on the PC.

  a. The LAN1 port of the ONT is connected to the Ethernet port of the PC properly.
  b. After the PC is configured to obtain its IP addresses automatically, the PC can obtain an IP address allocated by the ONT using DHCP.
  c. After automatic PPPoE dialup is performed successfully on the ONT, users can access the Internet.

3.3.3.5 Configuring SIP-based Voice Service Through the U2560

This topic provides an example of how to configure the SIP-based voice service through the U2560.

Prerequisites

- The ONT is auto discovered on the U2560. For details, see **3.3.3.2 Commissioning Interoperation Between the U2560 and the ONT**.
- Two telephone sets must be available and each must be connected to ports TEL1 and TEL2 respectively on the ONT.

Context

Every data change must be saved. You can click **Save** in a window to save data changes. If you navigate to another node without saving data changes, a dialog box will be displayed prompting you to save the data changes. In this case, click **YES** in the dialog box. New data will be automatically applied to the ONTs after the data changes are saved.

NOTICE

When configuring services on the U2560, do not modify the WAN interface connecting the U2560 and the ONT. Otherwise, the U2560 loses communication with the ONT.

Procedure

Step 1 Log in to the U2560 and choose **Subnet View** > **TR069 Subnet** from the navigation tree. In the terminal list, right-click an ONT and choose **Tools** > **Configure in Real Time** from the shortcut menu.

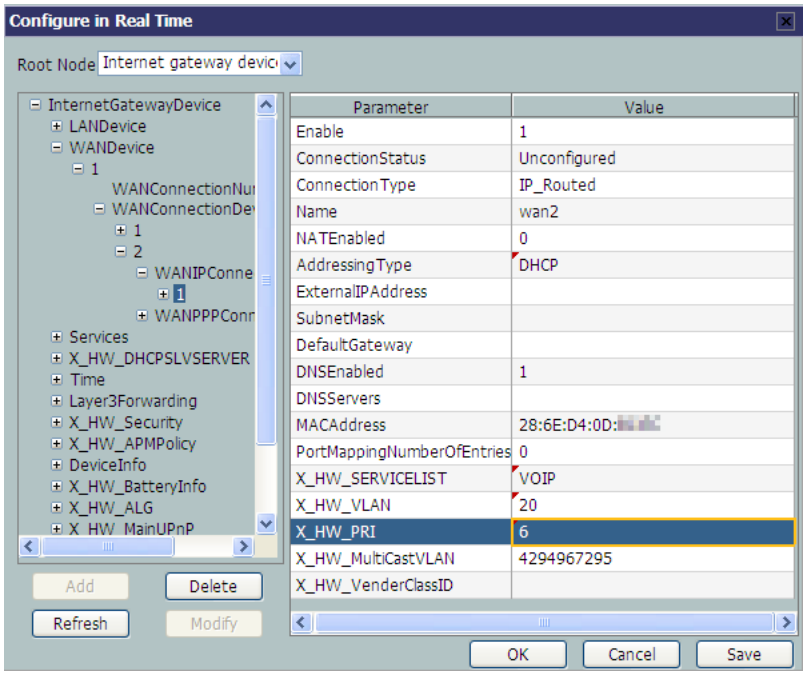
Step 2 In the **Configure in Real Time** dialog box, set **Root Node** to **Internet gateway device**.

Step 3 Configure the parameters of the voice WAN interface.

1. Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** from the navigation tree. Click **Add** in the lower left part to create an instance.
2. Choose **2** > **WANIPConnection** from the navigation tree. Click **Add** in the lower left part. Choose **1** from the navigation tree. In the right pane, set the parameters as follows:
   - Set **Enable** to **1**, indicating that the WAN connection is enabled.
   - Set **Connection Type** to **IP_Routed**, indicating that the connection type of the WAN interface is in routing mode.
   - Set **Addressing Type** to **DHCP**, indicating that the WAN interface obtains IP addresses in DHCP mode.
   - Set **X_HW_SERVICELIST** to **VOIP**, indicating that the WAN interface provides the VoIP access service.
   - Set **X_HW_VLAN** to **20**, indicating the VLAN ID of the WAN interface is 20.
   - Set **X_HW_PRI** to **6**, indicating that the priority level of the WAN interface is 6.

NOTE

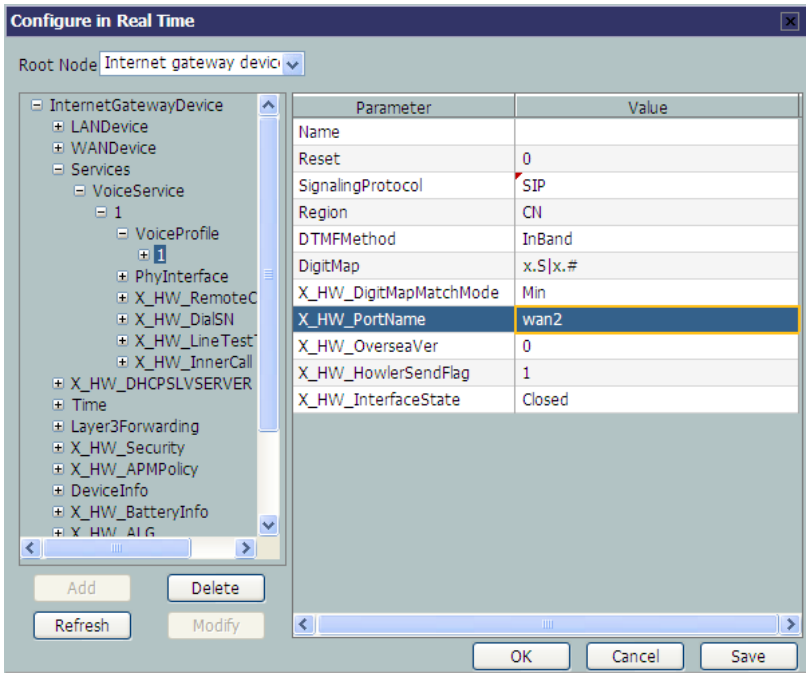
- If the WAN interface obtains IP addresses in static or DHCP mode, choose **WANIPConnection** to set the parameters of the voice WAN interface.
- If the WAN interface obtains IP addresses in PPPoE mode, choose **WANPPPConnection** to set the parameters of the voice WAN interface.



Step 4 Configure the voice protocol parameters.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set the parameters as follows:

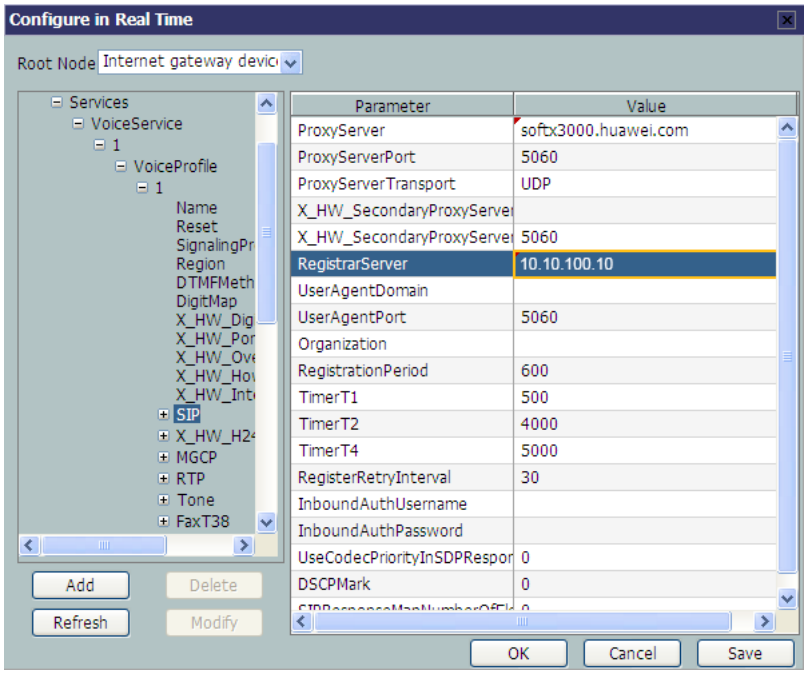
- Set **SignalingProtocol** to **SIP**, indicating that the SIP protocol is used.
- Set **Region** to **CN**, indicating the country code of China.
- Set **X_HW_PortName** to **wan2**, indicating that the new WAN interface 2 is bound.



Step 5 Configure the SIP service parameters.

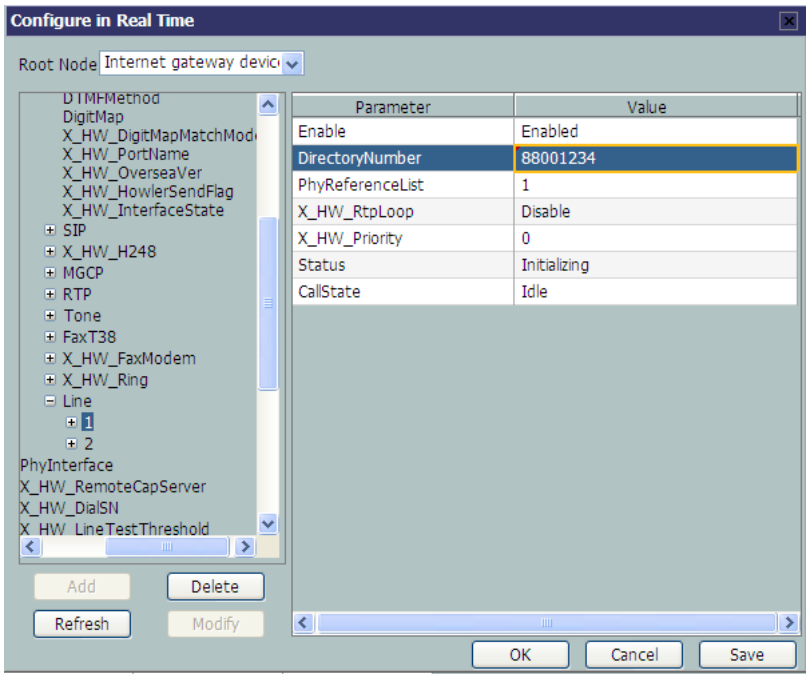
Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** > **SIP** from the navigation tree. In the right pane, set the parameters as follows:

- Set **ProxyServer** to **softx3000.huawei.com**, indicating that the address of the SIP proxy server is **softx3000.huawei.com**.
- Set **RegistarServer** to **10.10.100.10**, indicating that the SIP registration address is **10.10.100.10**.

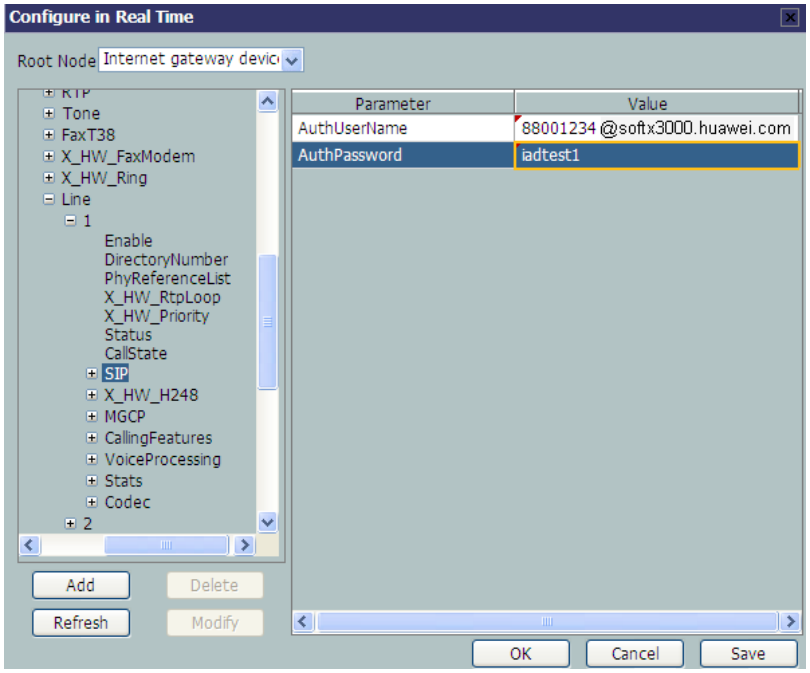


Step 6 Configure the information about SIP voice users.

1. Choose **InternetGatewayDevice** > **Service** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** > **1** from the navigation tree. In the right pane, set **DirectoryNumber** to **88001234**, indicating that the telephone number of SIP user 1 is 88001234.



2. Choose **1** > **SIP** from the navigation tree. In the right pane, set **AuthUserName** to **88001234@softx3000.huawei.com** and **AuthPassword** to **iadtest1**, indicating that the user name and password of user 1 for authentication are **88001234@softx3000.huawei.com** and **iadtest1** respectively.



3. Set information about SIP user 2 in the same way.

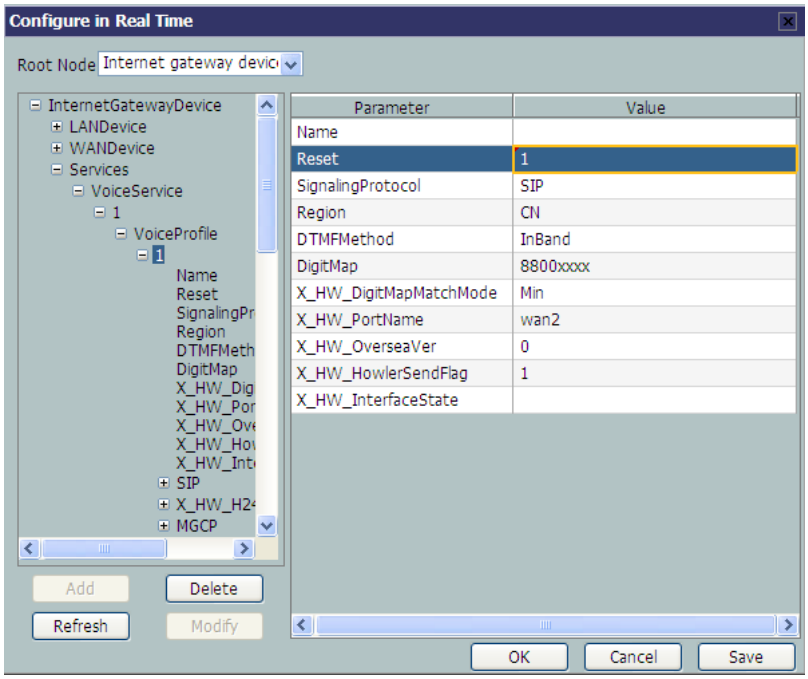
   Choose **InternetGatewayDevice** > **Service** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** from the navigation tree. Click **Add** in the lower left part. Choose **2** from the

navigation tree. In the right pane, set **DirectoryNumber** to **88001235**, indicating the telephone number of SIP user 2 is 88001235.

Choose **2** > **SIP** from the navigation tree. In the right pane, set **AuthUserName** to **88001235@softx3000.huawei.com** and **AuthPassword** to **iadtest2**, indicating that the user name and password of user 2 for authentication are **88001235@softx3000.huawei.com** and **iadtest2** respectively.

Step 7 Restart the voice process.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set **Reset** to **1**, indicating that the voice process will be restarted.



Step 8 Click **OK** after the configuration.

----End

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

3.3.3.6 Configuring the H.248-based Voice Service Through the U2560

This topic provides an example of how to configure the H.248-based voice service through the U2560.

Prerequisites

- The ONT is auto discovered on the U2560. For details, see **3.3.3.2 Commissioning Interoperation Between the U2560 and the ONT**.
- Two telephone sets must be available and each must be connected to ports TEL1 and TEL2 respectively on the ONT.

Context

Every data change must be saved. You can click **Save** in a window to save data changes. If you navigate to another node without saving data changes, a dialog box will be displayed prompting you to save the data changes. In this case, click **YES** in the dialog box. New data will be automatically applied to the ONTs after the data changes are saved.

NOTICE

When configuring services on the U2560, do not modify the WAN interface connecting the U2560 and the ONT. Otherwise, the U2560 loses communication with the ONT.

Procedure

Step 1 Log in to the U2560 and choose **Subnet View** > **TR069 Subnet** from the navigation tree. In the terminal list, right-click an ONT and choose **Tools** > **Configure in Real Time** from the shortcut menu.

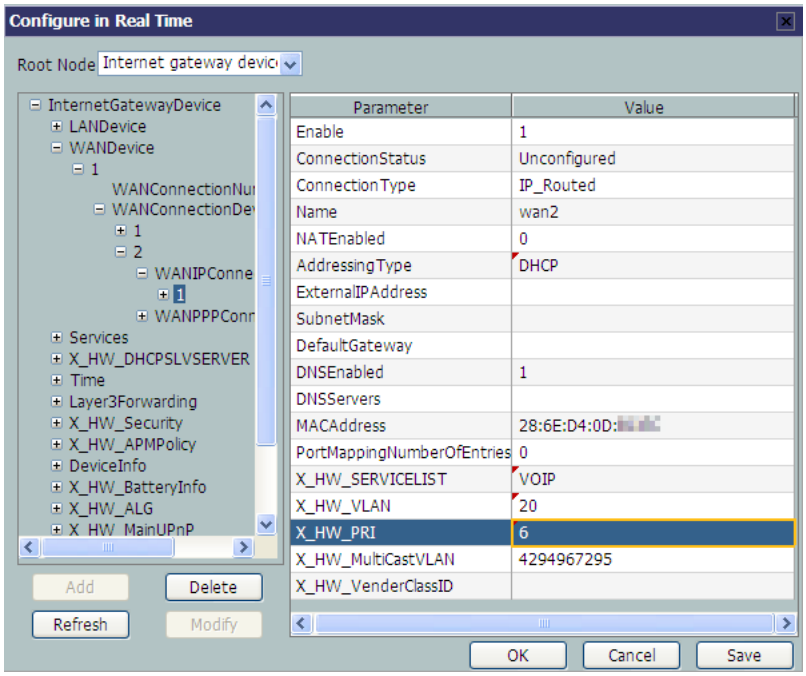
Step 2 In the **Configure in Real Time** dialog box, set **Root Node** to **Internet gateway device**.

Step 3 Configure the parameters of the voice WAN interface.

1. Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** from the navigation tree. Click **Add** in the lower left part to create an instance.
2. Choose **2** > **WANIPConnection** from the navigation tree. Click **Add** in the lower left part. Choose **1** from the navigation tree. In the right pane, set the parameters as follows:
   - Set **Enable** to **1**, indicating that the WAN connection is enabled.
   - Set **Connection Type** to **IP_Routed**, indicating that the connection type of the WAN interface is in routing mode.
   - Set **Addressing Type** to **DHCP**, indicating that the WAN interface obtains IP addresses in DHCP mode.
   - Set **X_HW_SERVICELIST** to **VOIP**, indicating that the WAN interface provides the VoIP access service.
   - Set **X_HW_VLAN** to **20**, indicating the VLAN ID of the WAN interface is 20.
   - Set **X_HW_PRI** to **6**, indicating that the priority level of the WAN interface is 6.

NOTE

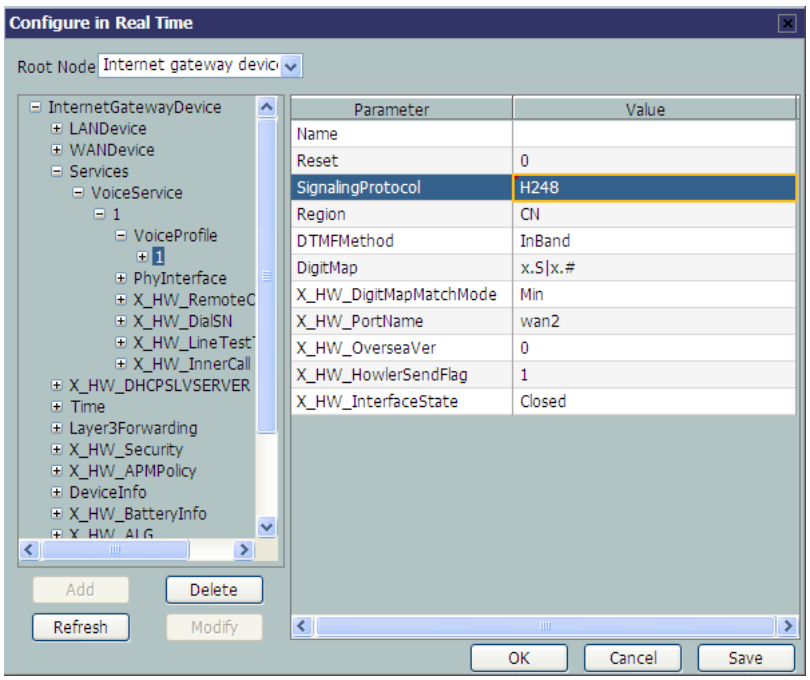
- If the WAN interface obtains IP addresses in static or DHCP mode, choose **WANIPConnection** to set the parameters of the voice WAN interface.
- If the WAN interface obtains IP addresses in PPPoE mode, choose **WANPPPConnection** to set the parameters of the voice WAN interface.



Step 4 Configure the voice protocol parameters.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set the parameters as follows:

- Set **SignalingProtocol** to **H248**, indicating that the H.248 protocol is used.
- Set **Region** to **CN**, indicating the country code of China.
- Set **X_HW_PortName** to **wan2**, indicating that the new WAN interface 2 is bound.



Step 5 Configure the H.248 service parameters.

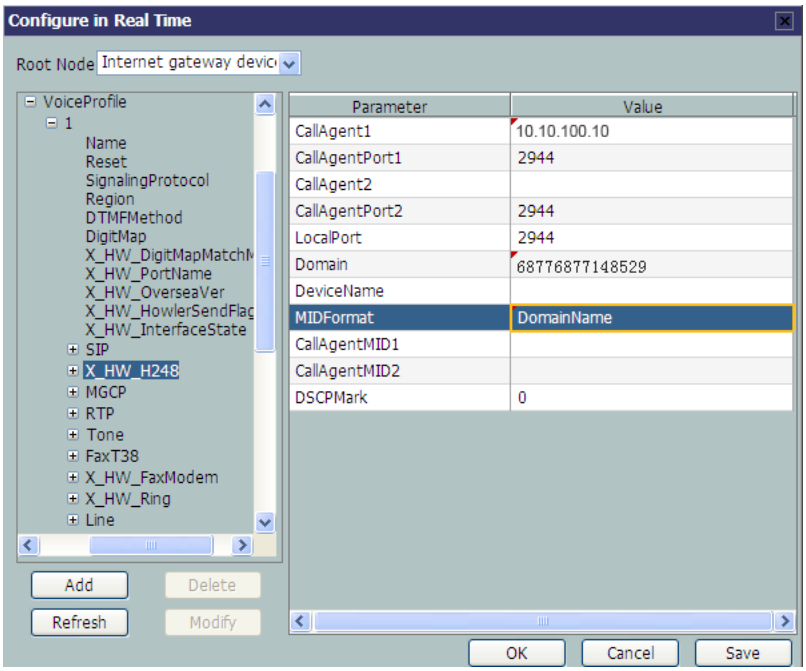
Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** > **X_HW_H248** from the navigation tree. In the right pane, set the parameters as follows:

- Set **CallAgent1** to **10.10.100.10**, indicating that the IP address of the MGC server is **10.10.100.10**.
- Set **Domain** to **6877687714852901**, indicating that the MG registration address is **6877687714852901**.

NOTE

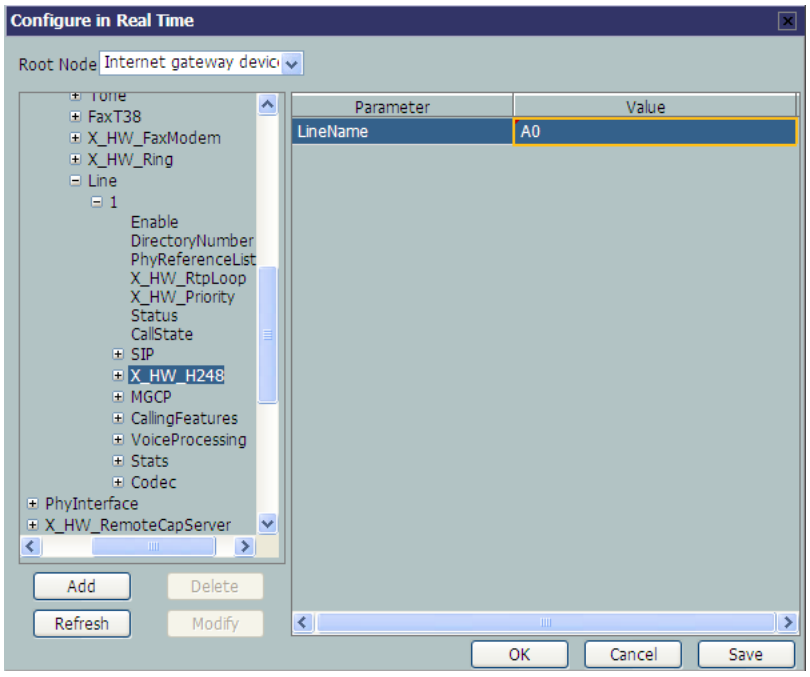
Domain is ONT's domain name registered on the MGC. It is globally unique. **Domain** in this example is ONT's SN.

- Set **MIDFormat** to **DomainName**, indicating that the MG uses its domain name to register.



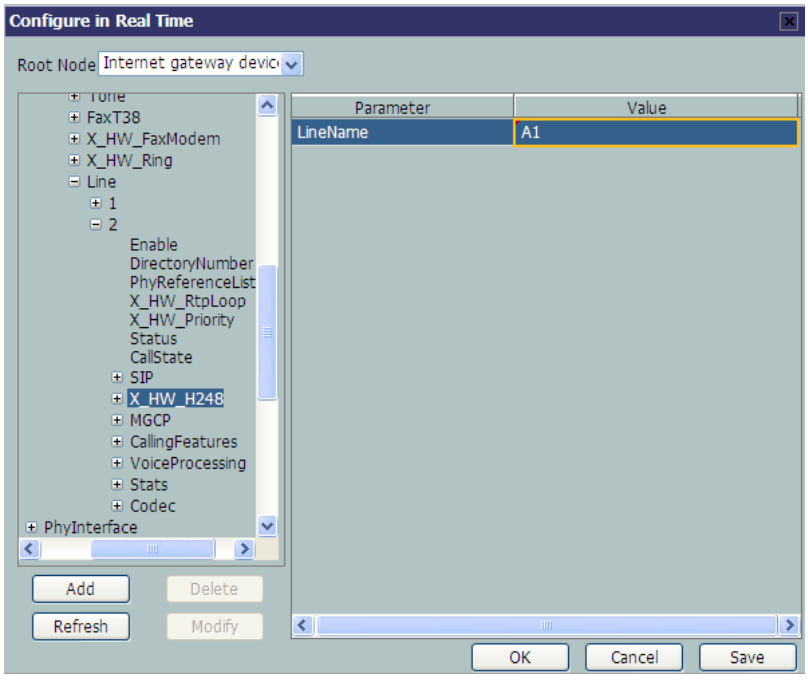
Step 6 Configure the TIDs of H.248 voice users.

1. Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** > **1** > **X_HW_H248** from the navigation tree. In the right pane, set **LineName** to **A0**, indicating that the TID of H.248 voice user 1 is A0. The user telephone number set on the MGC is 88001234.



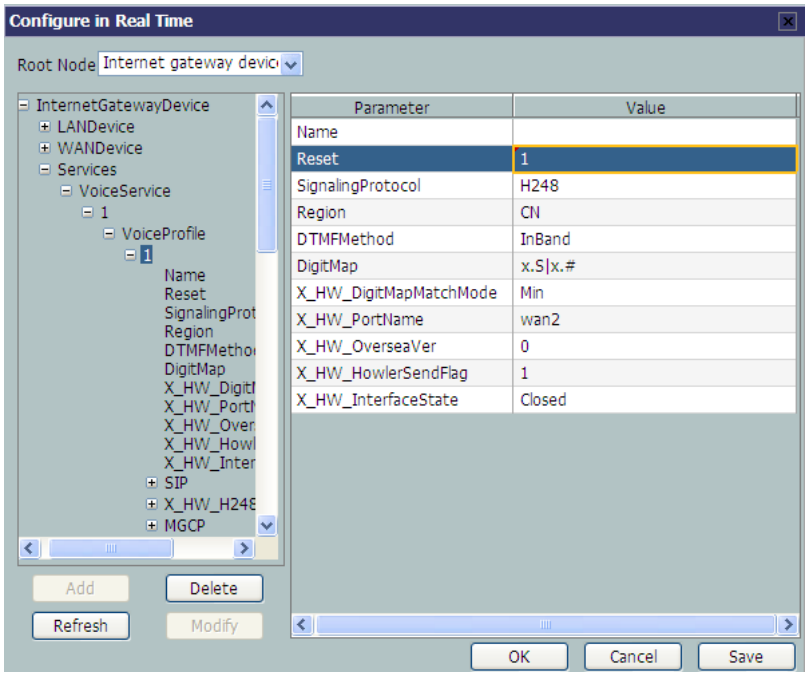
2. Configure the TID of H.248 voice user 2 in the same way.

   Choose **InternetGatewayDevice** > **Service** > **VoiceService** > **1** > **VoiceProfile** > **1** > **Line** from the navigation tree. Click **Add** in the lower left part. Choose **2** > **X_HW_H248** from the navigation tree. In the right pane, set **LineName** to **A1**, indicating that the TID of H.248 voice user 2 is A1. The user telephone number set on the MGC is 88001235.



Step 7 Restart the voice process.

Choose **InternetGatewayDevice** > **Services** > **VoiceService** > **1** > **VoiceProfile** > **1** from the navigation tree. In the right pane, set **Reset** to **1**, indicating that the voice process will be restarted.



Step 8 Click **OK** after the configuration.

----End

Result

Check whether the telephone functions properly. Connect two common telephones phone 1 and phone 2 to two TEL ports on the ONT and test the dialing between phone 1 and phone 2. In normal cases:

- The caller hears the dial tone after taking the phone off the hook.
- When the caller dials the telephone number of the callee, the phone of the callee rings successfully, and the caller hears the ring back tone.
- The caller and the callee communicate with each other successfully.
- After the callee hangs up, the caller hears the busy tone.

3.3.3.7 Configuring the Wi-Fi Access Service Through the U2560

This topic provides an example of how to configure the Wi-Fi access service through the TR-069 server.

Prerequisites

- The ONT is auto discovered on the U2560. For details, see **3.3.3.2 Commissioning Interoperation Between the U2560 and the ONT**.
- A portable computer with the Wi-Fi function must be available.

Context

The Wi-Fi wireless access service includes the Layer 3 bridge Wi-Fi service and the Layer 3 route Wi-Fi service.

- Layer 3 Wi-Fi service: Search for the SSID is performed on the PC. After the user passes the verification, the PPPoE auto dialup is performed on the PC. The IP address is allocated by the upper-layer BRAS. The ONT is connected to the OLT and then to the upper-layer network in the Layer 3 mode to provide the high-speed Internet access service.
- Layer 3 route Wi-Fi service: Search for the SSID is performed on the PC. After the user passes the verification, the PPPoE auto dialup is performed on the PC. The ONT is connected to the OLT and then to the upper-layer network in the Layer 3 mode to provide the high-speed Internet access service.

Every data change must be saved. You can click **Save** in a window to save data changes. If you navigate to another node without saving data changes, a dialog box will be displayed prompting you to save the data changes. In this case, click **YES** in the dialog box. New data will be automatically applied to the ONTs after the data changes are saved.

NOTICE

When configuring services on the U2560, do not modify the WAN interface connecting the U2560 and the ONT. Otherwise, the U2560 loses communication with the ONT.

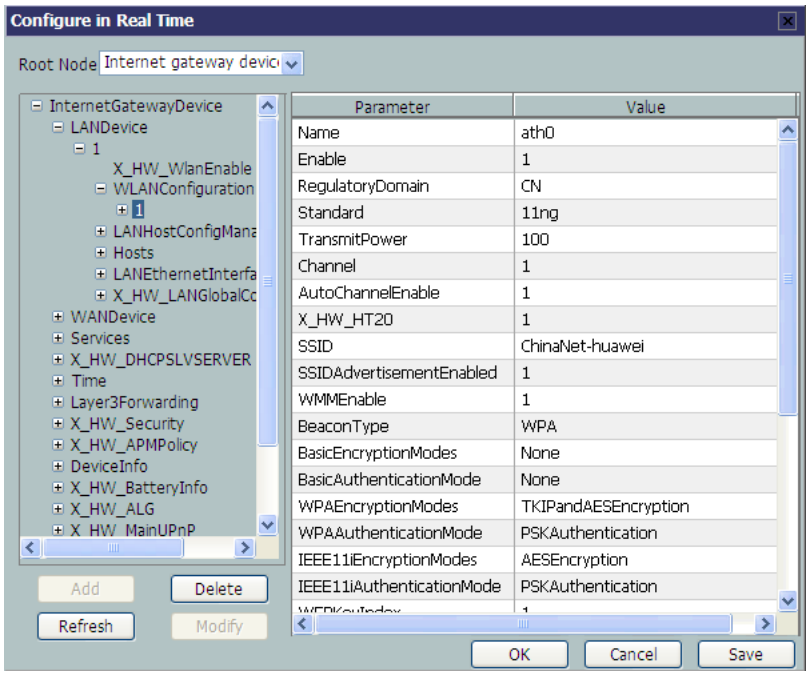
Procedure

Step 1 Log in to the U2560 and choose **Subnet View** > **TR069 Subnet** from the navigation tree. In the terminal list, right-click an ONT and choose **Tools** > **Configure in Real Time** from the shortcut menu.

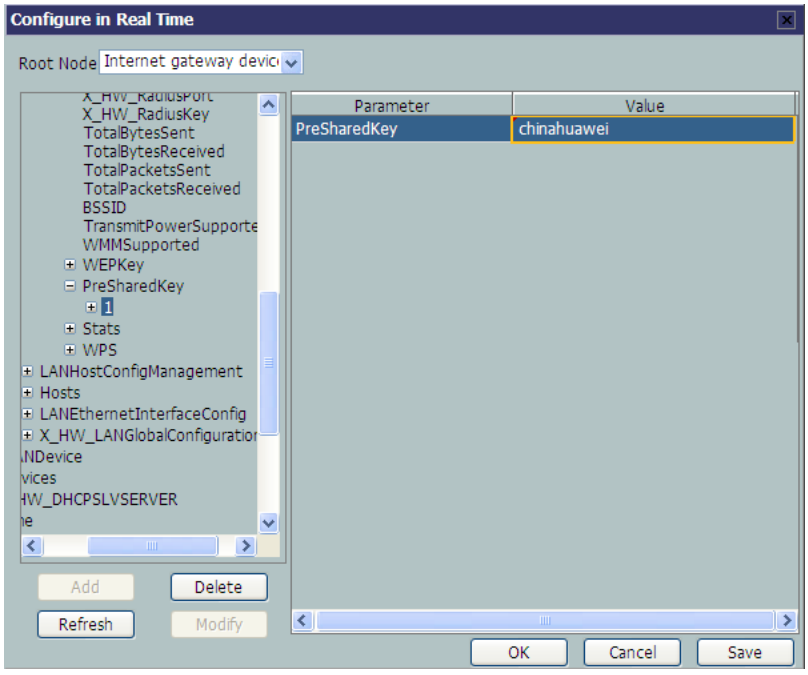
Step 2 In the **Configure in Real Time** dialog box, set **Root Node** to **Internet gateway device**.

Step 3 Configure the Wi-Fi parameters.

1. Choose **InternetGatewayDevice** > **LANDevice** > **1** > **WLANConfiguration** > **1** from the navigation tree. In the right pane, set the parameters as follows:
   - Set **Enable** to **1**, indicating that the WLAN service is enabled.
   - Set **RegulatoryDomain** to **CN**, indicating the country code of China.
   - Set **SSID** to **ChinaNet-huawei**.
   - Set **BeaconType** to **WPA** and **WPAEncryptionModes** to **TKIPandAESEncryption**, indicating that the encryption mode of the WPA is **TKIP&AES**.
   - Set **WPAAuthenticationMode** to **PSKAuthentication**, indicating that the authentication mode is **Pre-Shared Key**.



2. Choose **PreSharedKey** > **1**, **1** from the navigation tree. In the right pane, set **PreSharedKey** to **chinahuawei**, indicating that the WPA encryption key is **chinahuawei**.



Step 4 Configure the parameters of the WAN interface.

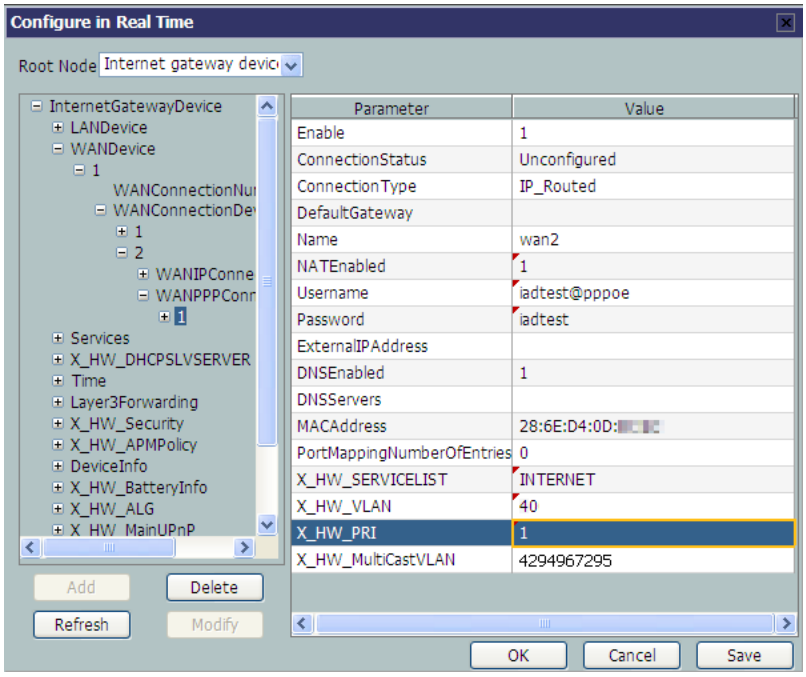
- Configure the parameters of the WAN interface – Route

1. Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** from the navigation tree. Click **Add** in the lower left part to create an instance.
2. Choose **2** > **WANPPPConnection** from the navigation tree. Click **Add** in the lower left part. Choose the new **1** branch from the navigation tree. In the right pane, set the parameters as follows:

- Set **Enable** to **1**, indicating that the WAN connection is enabled.
- Set **Connection Type** to **IP_Routed**, indicating that the connection type of the WAN interface is in routing mode.
- Set **NATEnable** to **1**, indicating that the NAT function is enabled.
- Set **Username** to **iadtest@pppoe** and **Password** to **iadtest**, indicating that the PPPoE user name is **iadtest@pppoe** and the password is **iadtest**.
- Set **X_HW_SERVICELIST** to **INTERNET**, indicating that the service type of the WAN interface is Internet.
- Set **X_HW_VLAN** to **40**, indicating that the VLAN ID of the WAN interface is 40.
- Set **X_HW_PRI** to **1**, indicating that the priority level of the WAN interface is 1.

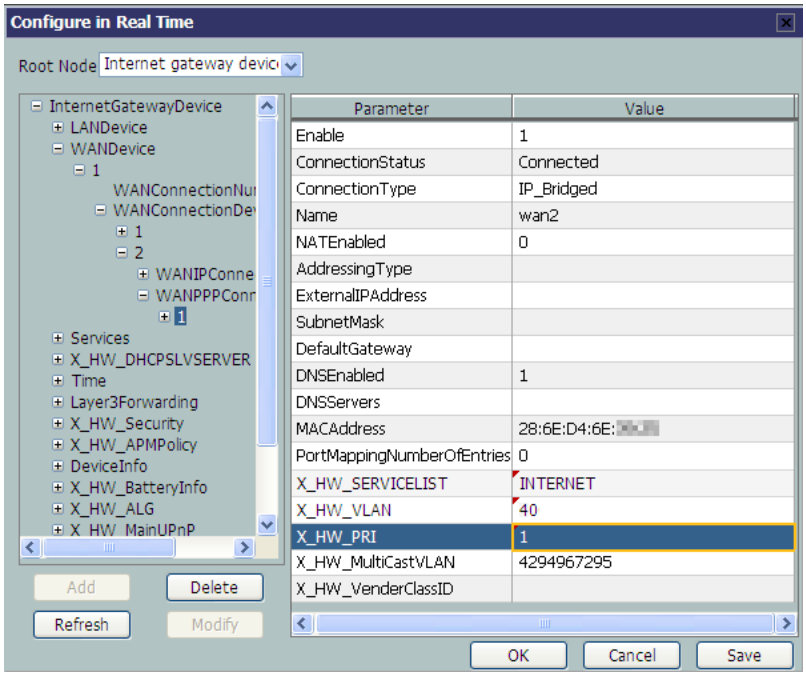
NOTE

- If the WAN interface obtains IP addresses in static or DHCP mode, choose **WANIPConnection** to set the parameters of the WAN interface.
- If the WAN interface obtains IP addresses in PPPoE mode, choose **WANPPPConnection** to set the parameters of the WAN interface.



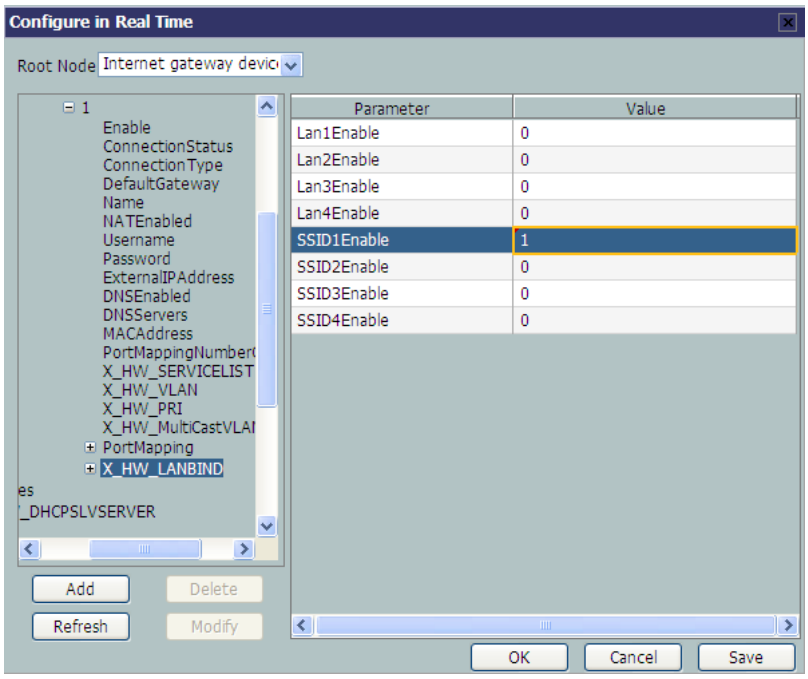
- Configure the parameters of the WAN interface – Bridge
  a. Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** from the navigation tree. Click **Add** in the lower left part to create an instance.
  b. Choose **2** > **WANPPPConnection** from the navigation tree. Click **Add** in the lower left part. Choose the new **1** branch from the navigation tree. In the right pane, set the parameters as follows:
- Set **Enable** to **1**, indicating that the WAN connection is enabled.
- Set **Connection Type** to **IP_Bridged**, indicating that the connection type of the WAN interface is in bridge mode.
- Set **X_HW_SERVICELIST** to **INTERNET**, indicating that the service type of the WAN interface is Internet.
- Set **X_HW_VLAN** to **40**, indicating that the VLAN ID of the WAN interface is 40.

- Set **X_HW_PRI** to **1**, indicating that the priority level of the WAN interface is 1.



Step 5 Bind the SSID.

Choose **InternetGatewayDevice** > **WANDevice** > **1** > **WANConnectionDevice** > **1** > **WANIPConnection** > **1** > **X_HW_LANBIND** from the navigation tree. In the right pane, set **SSID1Enable** to **1**, indicating that the WAN interface is bound to SSID 1.



----End

Result

- Layer 3 bridge Wi-Fi service: SSID radio signals can be searched on the Wi-Fi terminal. After the user enter the authentication key and pass the authentication, the user can access the Internet.
- Layer 3 route Wi-Fi service: SSID radio signals can be searched on the Wi-Fi terminal. After the user enter the authentication key and pass the authentication, the Wi-Fi terminal can obtain the IP address allocated by the DHCP IP address pool on the ONT. After the PPPoE dialup is successfully performed on the ONT, the user can access the Internet.

NOTE

The security mode and encryption configured on a Wi-Fi terminal must be the same as those of an ONT. If you cannot find the following encryption modes: TKIP&AES, and AES. The reason may lie in an old Wi-Fi driver version. If so, replace the old version with a new one.

3.3.3.8 Guide to Configure SoftGRE-Based Wi-Fi Sharing

The following describes how to configure SoftGRE-based Wi-Fi sharing.

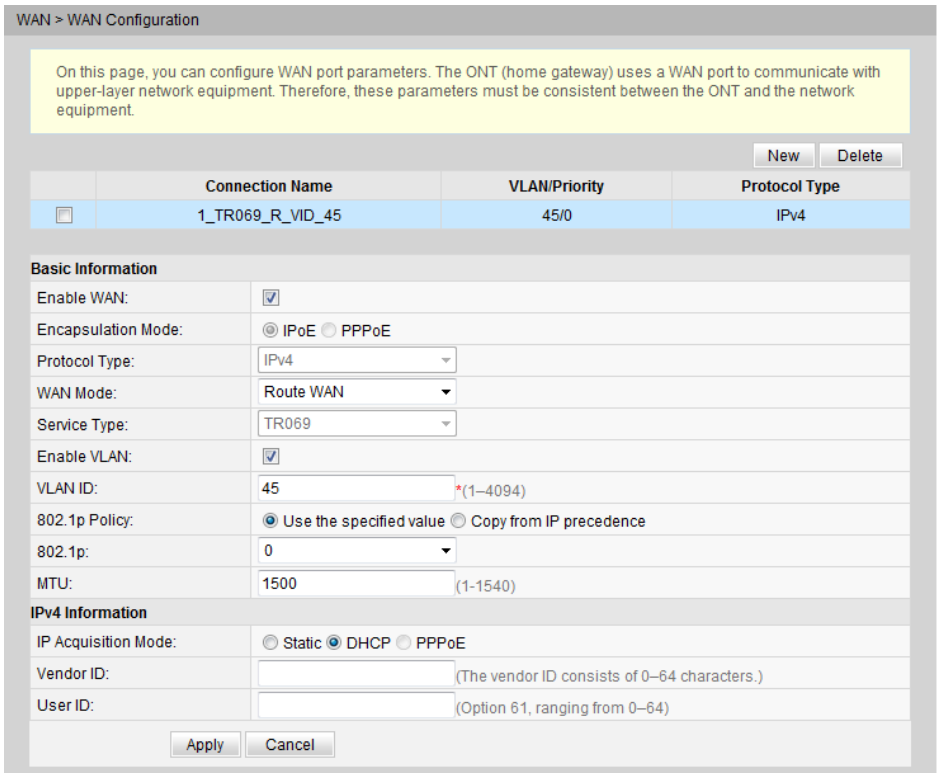
Prerequisites

- The SoftGRE tunnel solution requires the related upper-layer device (BRAS) to support the EoGRE tunnel protocol. Based on the protocol, GRE packets are encapsulated and decapsulated.
- Currently an ONT is usually interconnected with Huawei ME60. To support SoftGRE, the ME60 in a specific version needs to work with a specific service board. If the ONT is interconnected with a third-party router, make sure that the router supports the EoGRE tunnel protocol.

Procedure

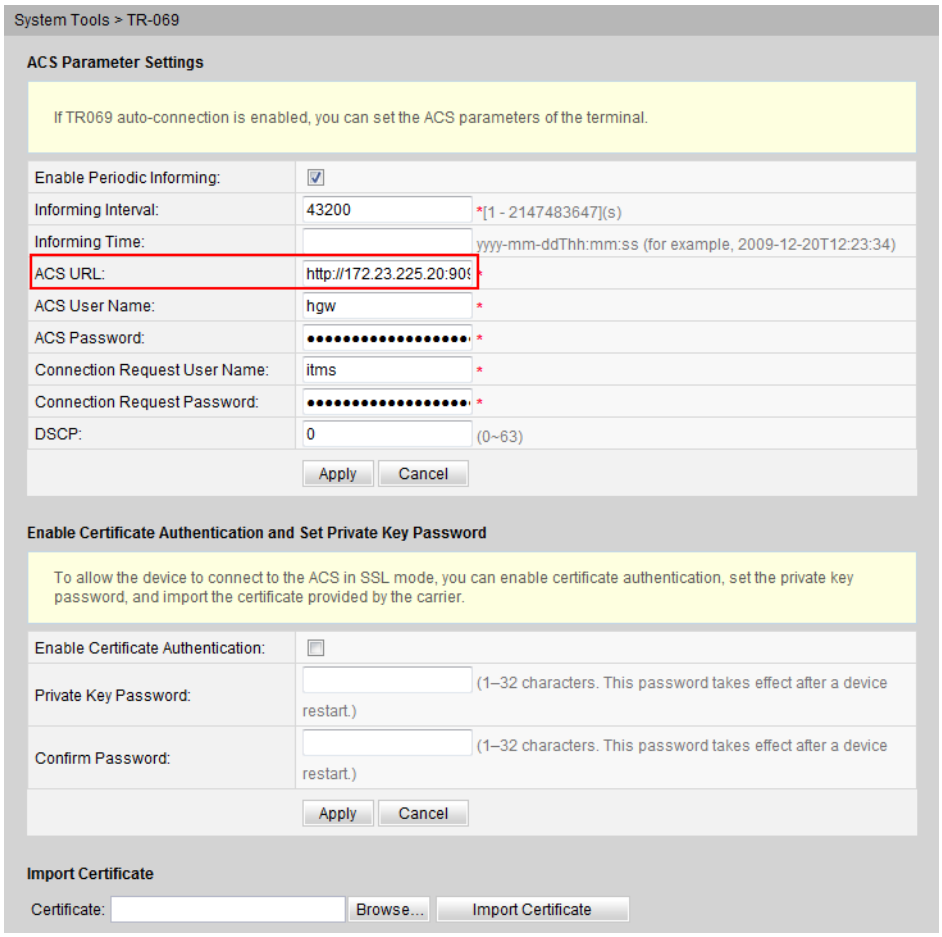
Step 1 On the ONT web page, configure a TR069 WAN.

1. On the ONT web page,choose **WAN** > **WAN Configuration** from the navigation tree in the left-side pane of the tab page.
2. In the right-side pane, click **New**. In the dialog box that is displayed, set WAN interface parameters in sequence as follows:
   a. Select **Enable WAN** to enable a new WAN connection.
   b. Set **Encapsulation Mode** to **IPoE**.
   c. Set **Service Type** to **TR069**.
   d. Set **WAN Mode** to **Route WAN**.
   e. Select **Enable VLAN**.
   f. Set **VLAN ID** to **45**(which must be consistent with the user-side VLAN ID configured on the OLT).
   g. Set **802.1p** to the largest value.
   h. Set **IP Acquisition Mode** to **DHCP**.



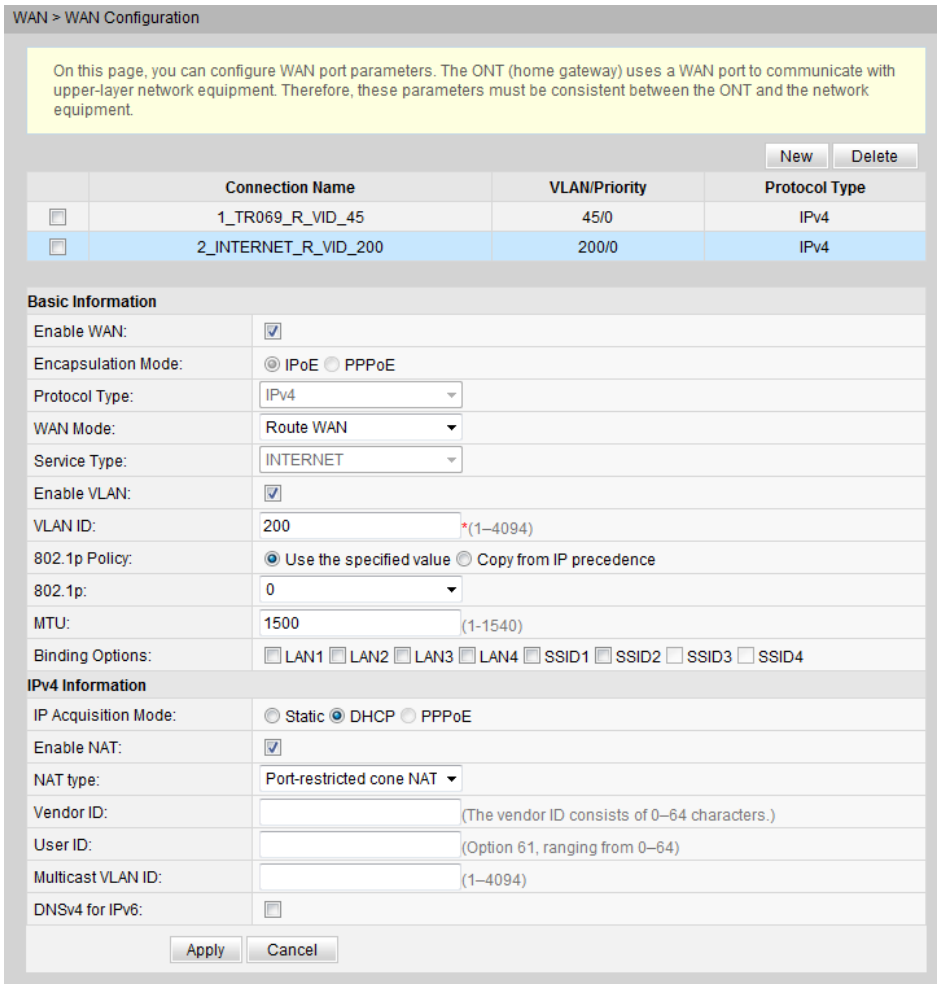
Step 2 Configure TR069 management information, so that the ONT can be managed through the TR069 channel.

1. On the ONT web page,choose **System Tools** > **TR-069** from the navigation tree in the left-side pane of the tab page.
2. In the right-side pane, set ACS parameters in sequence as follows:
   a. Set the **ACS URL** to the **IP address of the ITMS server**.
   b. Set **ACS User Name** and **ACS Password** according to the settings on the ITMS server.
   c. Set **Connection Request User Name** and **Connection Request Password** according to the settings on the ITMS server.



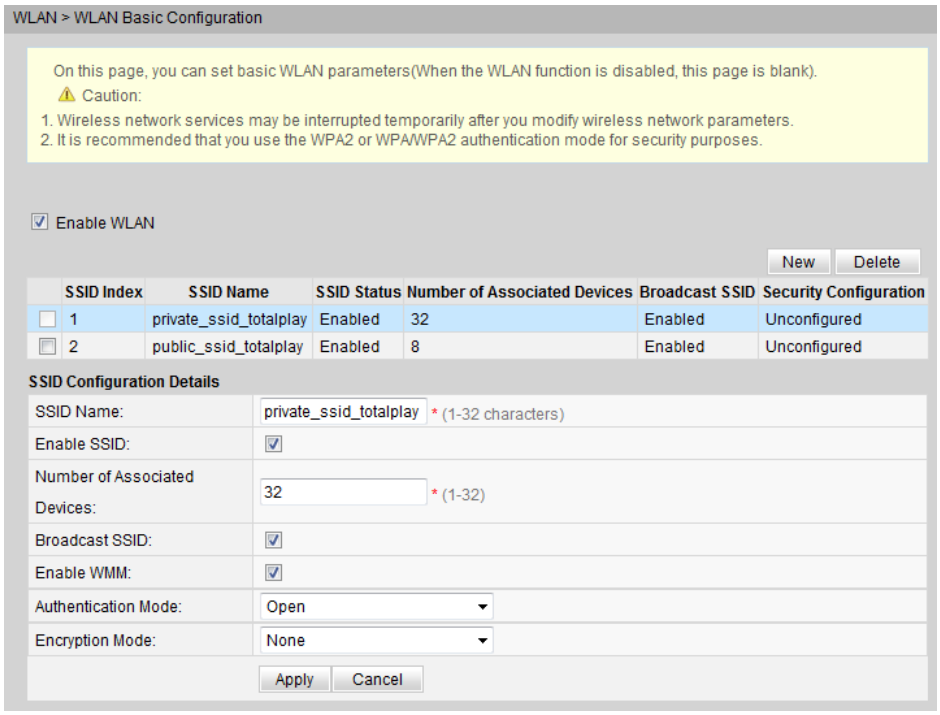
Step 3 Create a route WAN with service type being Internet, as the upstream channel for carrying public Wi-Fi services.

1. On the ONT web page,choose **WAN** > **WAN Configuration** from the navigation tree in the left-side pane of the tab page.
2. In the right-side pane, click **New**. In the dialog box that is displayed, set WAN interface parameters in sequence as follows:
   a. Select **Enable WAN** to enable the new WAN connection.
   b. Set **Encapsulation Mode** to **IPoE** or **PPPoE**.
   c. Set **WAN Mode** to **Route WAN**.
   d. Set **Service Type** to **OTHER** or **INTERNET**.
   e. Set **VLAN ID** to **200**(which must be consistent with the user-side VLAN ID configured on the OLT).
   f. Set **MTU** to **1500**.
   g. Select **Enable VLAN**.
3. onfigure IPV4 information.
   a. Set **IP Acquisition Mode** to **DHCP**.
   b. Select **Enable NAT**.



Step 4 Configure two SSIDs.

1. On the ONT web page,choose **WLAN** > **WLAN Basic Configuration** from the navigation tree in the left-side pane of the tab page.
2. In the right-side pane, click **New** In the dialog box that is displayed, set WAN interface parameters in sequence as follows:
   a. Set **SSID Name** to **private_ssid_totalplay**.
   b. Set **Authentication Mode** and **Encryption Mode**.



Step 5 On the TR069 server, configure ISP SSID (SSID2 as the ISP SSID).

1. Navigate to the following node path: InternetGatewayDevice.LANDevice.1.X_HW_WLANForISP.
2. Create an instance and set parameters in sequence as follows:
   a. Set **SSID_IDX** to **2** (corresponding to SSID INDEX in **Step 4**).
   b. Set **SSID** to **a public hotspot name**.
   c. Set **AuthenticationMode** to **802.1x-EAP**.(If the WebPortal authentication is required, set AuthenticationMode to WebPortal for the ISP SSID)
   d. Set **RadiusServer** to **RadiusKey**.

Step 6 Configure the SoftGRE tunnel.

1. Navigate to the following node path:InternetGatewayDevice.X_HW_GRETunnel.
2. Create an instance and set parameters in sequence as follows:
   - Set **EgressInterface** to the WAN port node path, that is, InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANIPConnection.1 (or WANPPPConnection if Encapsulation Mode is set to PPPoE).
   - Set **Remoteaddress** to the **peer IP address** (also the router IP address that can be obtained according to the router settings).
3. Configure the ingress interface of the SoftGRE tunnel.
   - Navigate to the following node path: InternetGatewayDevice.X_HW_GRETunnel.1.IngressInterface.1.
   - Create an interface instance and set InterfaceName to a public SSID path such as InternetGatewayDevice.LANDevice.1.WLANConfiguration.2.
4. Configure a static route that supports 802.1x-EAP(or WebPortal) authentication, and enable authentication packets to pass through the WAN through the egress interface of the SoftGRE tunnel.

- Navigate to the following node path: InternetGatewayDevice.Layer3Forwarding.Forwarding.
- Create a static route instance and set parameters in sequence as follows:
- Set **DestIPAddress** to the **IP address** of the RADIUS server.
- Set **DestSubnetMask** to **255.255.255.255**.
- Set **Interface** to the WAN port node path, that is, InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANIPConnection.1 (or WANPPPConnection if Encapsulation Mode is set to PPPoE).
- Set **X_HW_WanName** to **wan1.2.ip1** (corresponding to the WAN port node path).

----End

3.4 IPv6 Scenarios

This topic describes configurations on the U2000, OLT, and ONT for the FTTH IPv6 solution which is part of Huawei fixed broadband network IPv6 solutions. For configurations on upper-layer devices, refer to the FBB solution configuration guide.

Context

NOTE

- This topic uses the HG8245H as an example, and the OLT V300R019C00&V500R019C00 and U2000 V200R015C50 are used. Screenshots may be different for various versions but the configuration procedures are similar. For details about the configuration, see the NMS configuration manuals.
- Gateway ONTs and bridging ONTs support different IPv6 application scenarios. For example, a bridging ONT does not support NAT444. For details, see **3.4.1 IPv6 Solutions and Application Scenarios**.

3.4.1 IPv6 Solutions and Application Scenarios

This topic describes the IPv6 solutions and application scenarios.

Currently, IPv6 mainly has the following solutions: IPv6 Rapid Deploy (6RD) and its correlative solution 6RD+NAT444, dual stack and its correlative solutions (NAT444, dual stack+NAT444, dual stack+L2TP, and L2NAT), and Dual-Stack Lite (DS-Lite). The following describes the widely used and recommended Huawei fixed broadband network IPv6 solutions, as shown in **Table 3-16**. You are advised to select a solution based on actual network conditions.

Table 3-16 IPv6 solutions and application scenarios

IPv6 Solution	Advantage	Disadvantage	Application Scenario
Dual stack	● A mature future-oriented technology supports IPv4 and IPv6 services at the same time. ● Network Address Translation (NAT) is not used, free of source tracing and service traversal issues.	● This solution cannot relieve the shortage of IPv4 addresses. ● All devices on the network need to be upgraded to support dual stack, which is costly.	● IPv4 addresses are sufficient. ● Smooth evolution to IPv6 in large-scale is required in the future.
NAT444	The NAT technology is mature and saves IPv4 addresses.	● Two-level NAT translation needs to be performed, which affects services, for example, point-to-point (PTP) application and ALG traversal. ● The IPv6 is not deployed, and devices need to be upgraded to support IPv6.	● Demand for IPv6 is weak. ● NAT444 can solve the problem of IPv4 address exhaustion.
Dual stack +NAT444	● A future-oriented solution supports IPv4 and IPv6 services at the same time. ● Only small changes need to be made to devices on the network. ● This solution saves IPv4 addresses and has a strong service traversal capability.	● All devices on the network need to be upgraded to support dual stack, which is costly. ● Two-level NAT translation needs to be performed, which affect services.	● IPv4 addresses are insufficient. ● Smooth evolution to IPv6 in large-scale is required in the future.

IPv6 Solution	Advantage	Disadvantage	Application Scenario
DS-Lite	● A mature future-oriented technology supports IPv4 and IPv6 services at the same time. ● Only one-level NAT translation is performed, which has little impact on services. ● No planning or analysis is required for IPv4 addresses, and the network deployment is simple.	● All devices on the network need to be upgraded to support dual stack, which is costly. ● NAT performed on the CGN side has considerable impact on services. ● IPv4 service flows are carried over IPv6 channels, which has the following disadvantages due to the immature IPv6 technology: – Fragmentation is performed on IPv4 packets, which lowers the forwarding efficiency. – The IPv4 gateway application mode is changed, which affects existing IPv4 applications.	● There is a strong demand for IPv6. ● IPv4 addresses are insufficient, and IPv6 reconstruction on the network is difficult.

Service configuration in the FTTH IPv6 solutions mainly involves configuration of the Internet access service. In the configuration, the bridging ONT and gateway ONT process IPv6 in different ways. Specifically, the bridging ONT forwards IPv6 packets at Layer 2 and the gateway ONT processes IPv6 packets according to actual scenarios. For details about ONT types, see Reference of GPON ONT Capability Sets. **Table 3-17** describes the service (Internet access service) processing mode of access devices in different IPv6 networking scenarios.

NOTE

The OLT implements Layer 2 forwarding on IPv6 packets. Therefore, service flows need to be configured for IPv6 services on the OLT to forward the services to the corresponding IPv6 server.

Currently, the TR-069 management service, voice service, and IPTV service are still implemented through IPv4. IPv6 is not involved. Therefore, the service configurations are the same as those for IPv4. For details, refer to **3.4 IPv6 Scenarios**.

Table 3-17 Service processing mode of devices in different IPv6 solutions

Networking	IPv6 Solution	OLT	ONT	Remarks
FTTH (Bridging-type ONT)	NAT444	NA	NA	Bridging ONTs do not support this scenario.
	Dual stack	Layer 2 forwarding	Layer 2 forwarding	-
	Dual stack +NAT444	NA	NA	Bridging ONTs do not support this scenario.
	DS-Lite	Layer 2 forwarding	Layer 2 forwarding	A software needs to be installed on the PC to support DS-Lite.
FTTH (Gateway-type ONT)	NAT444	Layer 2 forwarding	The ONT uses the IPv4 single stack. The NAT function needs to be enabled on the WAN port.	Only the basic function of two-level mapping is supported. The UPNP function is not supported, because it may cause unavailability of some applications.
	Dual stack	Layer 2 forwarding	The ONT uses dual stack. IPv4 and IPv6 must be enabled on the WAN port at the same time.	-
	Dual stack +NAT444	Layer 2 forwarding	The ONT uses dual stack. IPv4 and IPv6 must be enabled on the WAN port at the same time.	-
	DS-Lite	Layer 2 forwarding	The ONT uses DS-Lite. IPv4 and IPv6 must be enabled on the WAN port at the same time.	-

3.4.2 IPv6 Data Plan

This topic describes the IPv6 data plan.

Table 3-18 Plan of key data

Item	Data
DBA profile	Profile name: ftth_dba DBA Type: assured bandwidth/maximum bandwidth (Type 3) Assured bandwidth: 8 Mbit/s Maximum bandwidth: 20 Mbit/s
ONT line profile	Profile name: ftth T-CONT ID: 4 GEM port ID for the internet access service: 14
ONT service profile	Profile name: ftth Number of POTS ports: Adaptive Number of ETH ports: Adaptive Number of CATV ports: Adaptive
Networking data	Upstream port: 0/19/0 PON port: 0/1/0 ONT ID: 1
VLAN plan	Double VLAN tags ● S-VLAN ID: 100 ● S-VLAN type: smart ● S-VLAN attribute: stacking ● C-LAN ID: 1001 ● C'VLAN ID: 1010 **NOTE** VLAN translation policy: ● ONT: uses the same VLAN configurations and adds C-VLAN tags to packets. All ONTs use the same C-VLAN. ● OLT: performs VLAN translation: C<->S+C'. C'VLANs for ONTs differ from each other.
ONT value-added service configured using the NMS (Layer 3 route mode)	Profile name: ONT-HSI WAN VLAN ID: 1001 Service type: INTERNET Connection type: route IP address acquisition mode: PPPoE (user name: iadtest@pppoe, password: iadtest) Priority: 0 Binding port: LAN1 (Layer 3 LAN)

Item	Data
WAN port configured on the Web page (Layer 3 route mode)	Service list: INTERNET Connection type: route VLAN ID: 1001 (which must be consistent with the user-side VLAN ID configured on the OLT) IP address acquisition mode: PPPoE (user name: iadtest@pppoe, password: iadtest) 802.1p priority: 0 Binding port: LAN1 (Layer 3 LAN)

3.4.3 Configuring IPv6 Services Using the NMS

This topic describes how to configure IPv6 services using the NMS.

3.4.3.1 Configuring the IPv6 Internet Access Service Using the NMS (NA)

This topic describes how to configure the IPv6 Internet access service using the U2000 when the NAT444 solution is used and the ONT is a gateway-type ONT.

Application Context

Networking description:

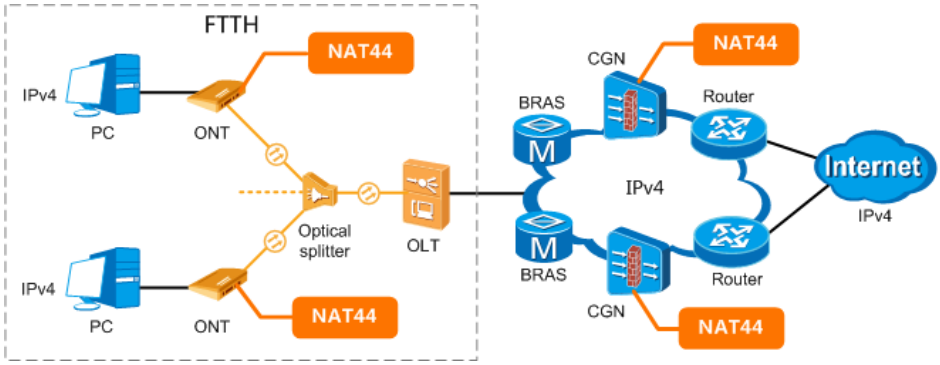
- The BRAS assigns an IPv4 private address (for example, 10.*.*.*) to the ONT. The ONT is enabled with the NAT function and assigns another IPv4 private address (for example, 192.168.*.*) to the PC.
- NAT44 translation is performed twice on IPv4 packets, first on the ONT and then on the CGN.
- The OLT implements Layer 2 forwarding, and the ONT implements Layer 3 forwarding.

Device reconstruction:

- The IP address pool on the BRAS needs to be replanned to support private IP addresses.
- The CGN device supporting NAT44 needs to be deployed on the network.
- The RADIUS needs to be upgraded or a log recording device needs to be deployed to address source tracing of private IP addresses.

Figure 3-11 shows the NAT444 networking diagram.

Figure 3-11 NAT444 networking diagram



Procedure

- Configure the Layer 3 Internet access service.

NOTE

In the NAT444 solution, the ONT needs to perform a NAT translation. In the IPv4 configuration, the NAT function also needs to be enabled on the ONT side. Therefore, all configurations on the OLT and ONT are the same as those for the IPv4 Layer 3 Internet access service. For details, refer to **3.3.1.1.2 Configuring the GPON FTTH Layer 3 Internet Access Service on the NMS**.

3.4.3.2 Configuring the IPv6 Internet Access Service Using the NMS (Dual Stack/ Dual Stack+NA)

This topic describes how to configure the IPv6 Internet access service using the U2000 when the dual stack or dual stack+NAT444 solution is used and the ONT is a gateway-type ONT.

NOTE

The OLT implements Layer 2 transparent transmission in the dual stack or dual stack+NAT444 scenario. Configurations on the OLT are the same as those for IPv4.

The FTTH configuration difference between the dual stack solution and the dual stack+NAT444 solution lies in NAT configuration on the ONT.

- In the dual stack solution, if the IP address of the PC on the internal network is a private address, the NAT function must be enabled, that is, dual stack+NAT44. The NAT function is disabled when it is not required.
- In the dual stack+NAT444 solution, the NAT function must be enabled.

Dual Stack Application Context

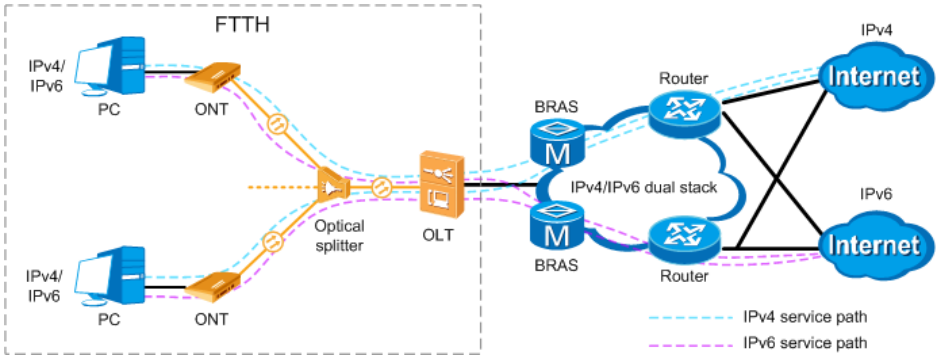
Networking description:

- All NEs on the network must support IPv4 and IPv6 dual stacks.
- The BRAS assigns IPv4 and IPv6 addresses to ONTs. The ONT assigns IPv4 and IPv6 addresses to PCs.
- PCs use IPv4 and IPv6 addresses to access the IPv4 Internet and IPv6 Internet respectively.
- The OLT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction: All NEs on the network need to be upgraded to support IPv4 and IPv6 dual stacks.

Figure 3-12 shows the dual-stack networking diagram.

Figure 3-12 Dual-stack networking diagram



Dual Stack+NAT444 Application Context

Networking description:

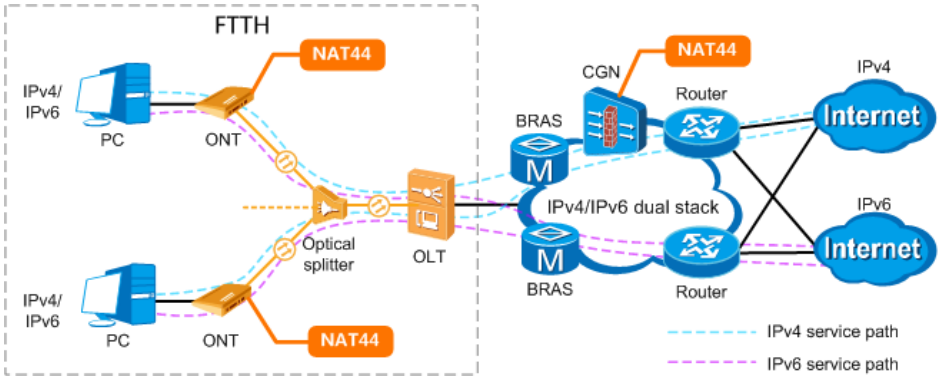
- All NEs on the network must support IPv4 and IPv6 dual stacks.
- The CGN device supporting NAT44 needs to be deployed on the network.
- The BRAS assigns an IPv4 private address (for example, 10.*.*.*) and IPv6 address to the ONT. The ONT is enabled with the NAT function and assigns another IPv4 private address (for example, 192.168.*.*) to the PC.
- NAT44 translation is performed twice on IPv4 packets, first on the ONT and then on the CGN. IPv6 packets are forwarded directly.
- The OLT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction:

- All NEs on the network need to be upgraded to support IPv4 and IPv6 dual stack.
- The IP address pool on the BRAS needs to be replanned to support private IP addresses.
- The CGN device supporting NAT44 needs to be deployed on the network.
- The RADIUS needs to be upgraded or a log recording device needs to be deployed to address source tracing of private IP addresses.

Figure 3-13 shows the dual stack+NAT444 networking diagram.

Figure 3-13 Dual stack+NAT444 networking diagram



Typical Configuration

Table 3-19 describes the typical IPv6 prefix and address configuration. This configuration has the best compatibility and can be applied to any scenarios.

Table 3-19 Typical IPv6 prefix and address configuration

Item	Parameter on NMS	Recommended Value	Remarks
IP address acquisition mode on the ONT WAN side	Mechanism via which the IP address was assigned	AutoConfigured	-
Prefix acquisition mode on the ONT WAN side	Mechanism via which the prefix was assigned	DHCPv6–PD	-
Address/prefix assignment mode for the LAN-side PC	M flag	0 (that is, SLAAC)	When the value is **1**, addresses/prefixes are assigned in the DHCPv6 mode. Currently, the Windows XP OS does not support this assignment mode.
Other information assignment mode for the LAN-side PC	O flag	1 (that is, DHCPv6)	Other information refers to the IPv6 address in payloads of packets such as DNS packets. When the value is 0, the information is assigned in the SLAAC mode. Currently, no OS supports the SLAAC mode.

Procedure

- **Configure the OLT.**

NOTE

The OLT implements Layer 2 transparent transmission. The procedure for configuring the OLT on the U2000 is the same as that for IPv4. For detailed configuration procedure, refer to "Implement pre-configurations", "Add an ONT" and "Add a service virtual port on the OLT side" in **3.3.1.1.2 Configuring the GPON FTTH Layer 3 Internet Access Service on the NMS**.

1. (Optional) Configure the DHCPv6 option.

   When the access mode of IPv6 users is IPoE and the BRAS uses the binding authentication mode, users do not need to enter user names or passwords for authentication because the BRAS performs authentication based on users' physical information. In this case, DHCPv6 Option18 needs to be configured on the OLT. For the mapping relationship between DHCPv6 Option and the BRAS, see **3.4.3.2 Configuring the IPv6 Internet Access Service Using the NMS (Dual Stack/Dual Stack+NA)**.

Table 3-20 DHCPv6 Option mapping

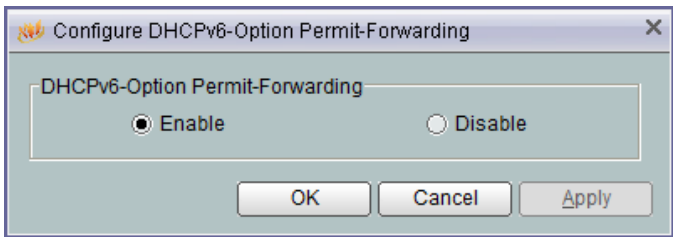
DHCPv6 Option	OLT	BRAS
Option17	N/A	Optional
Option18	Mandatory	Mandatory
Option37	Optional	Optional

NOTE

By default, the global DHCPv6 Option configuration is **disable**, the VLAN-level DHCPv6 Option configuration is **enable**, and the upstream/cascaded port-level DHCPv6 Option configuration is **enable**. Therefore, you only need to enable DHCPv6 Option globally.

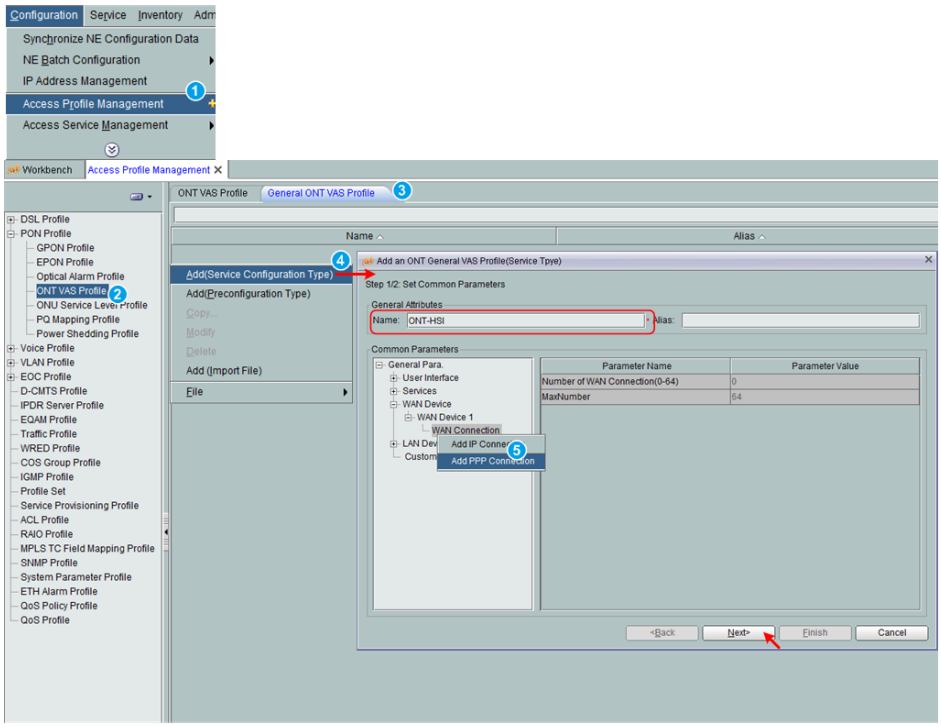
After DHCPv6 Option is enabled, the OLT inserts Option18 and Option37 into DHCPv6 packets for authentication by the BRAS.

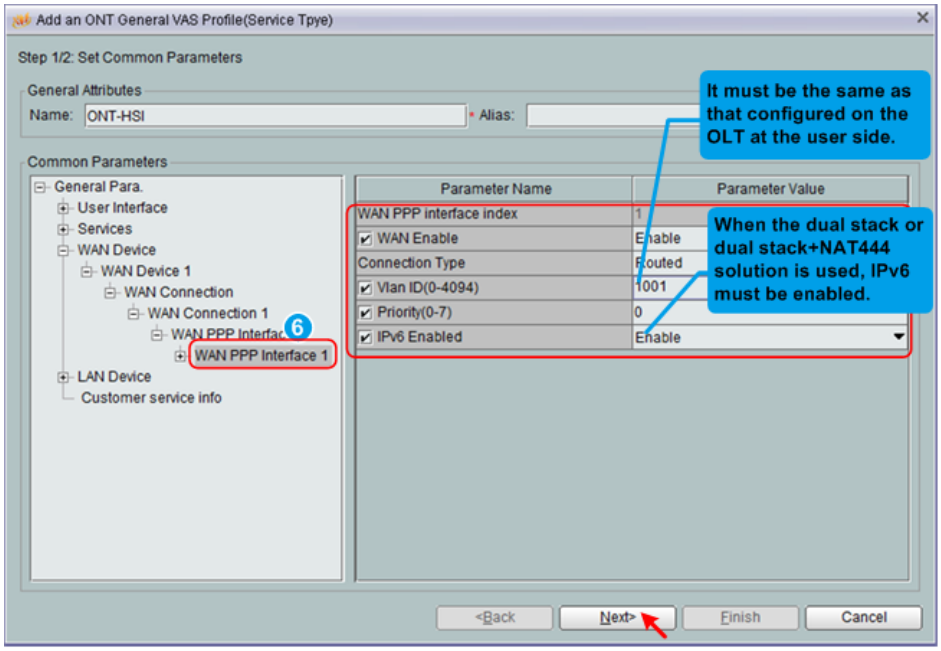
1. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.
2. Choose **GPON** > **GPON Management** from the navigation tree.
3. On the **GPON ONU** tab page, set the filter criteria or click  to display the GPON ONUs.
4. Right-click a required ONT and choose **Configure DHCPv6–Option Permit-Forwarding**.
5. In the dialog box that is displayed, select **Enable**.

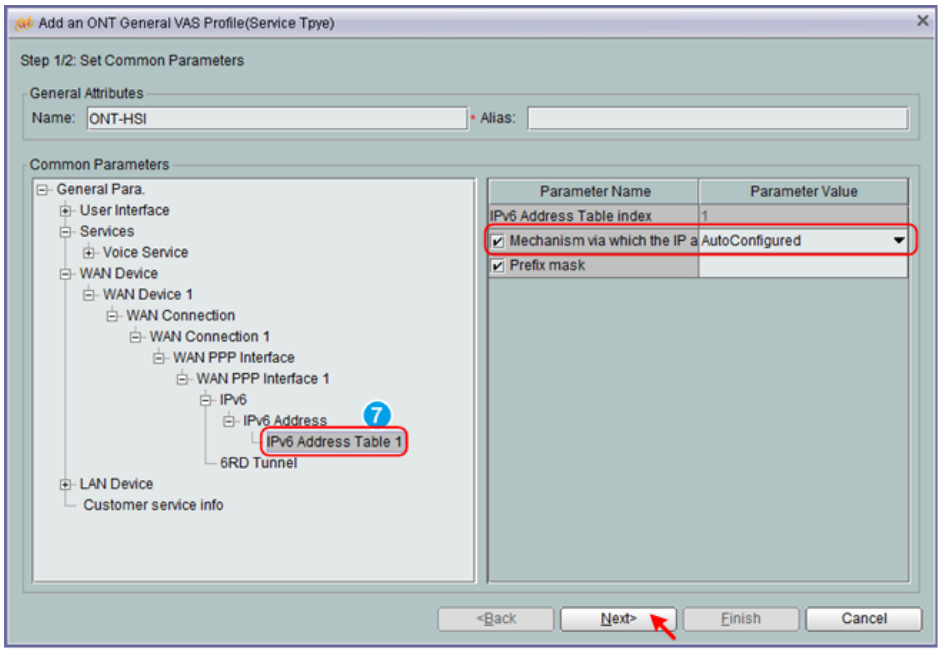


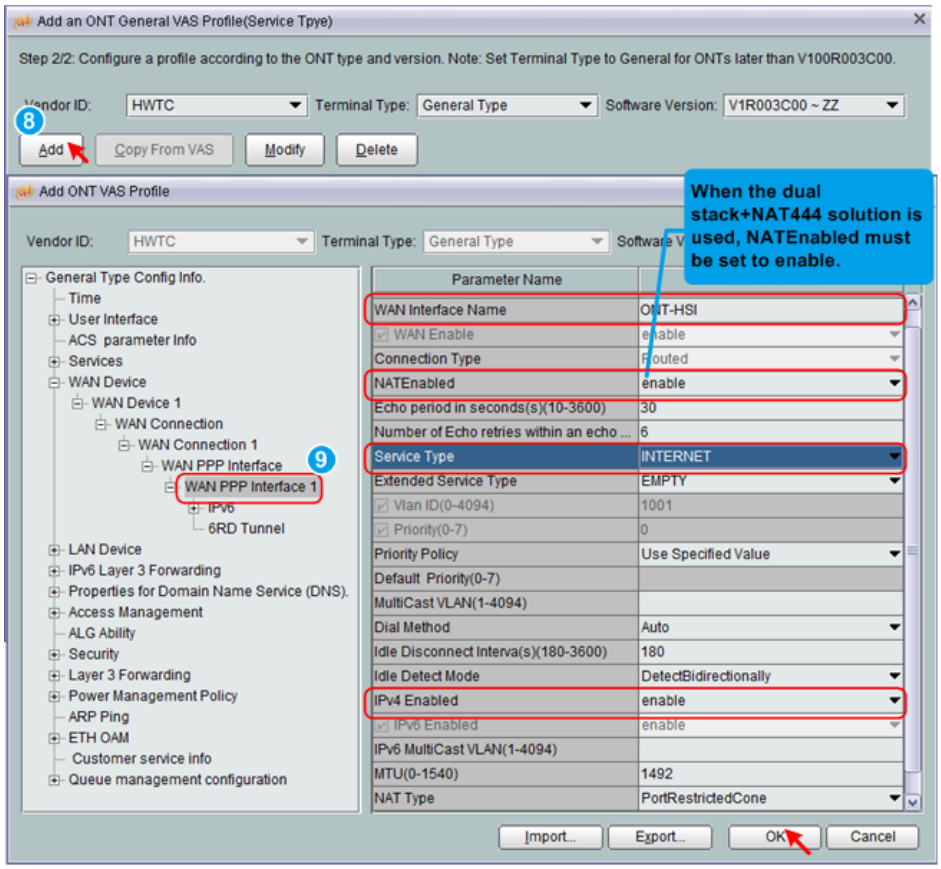
1. Click **OK**.

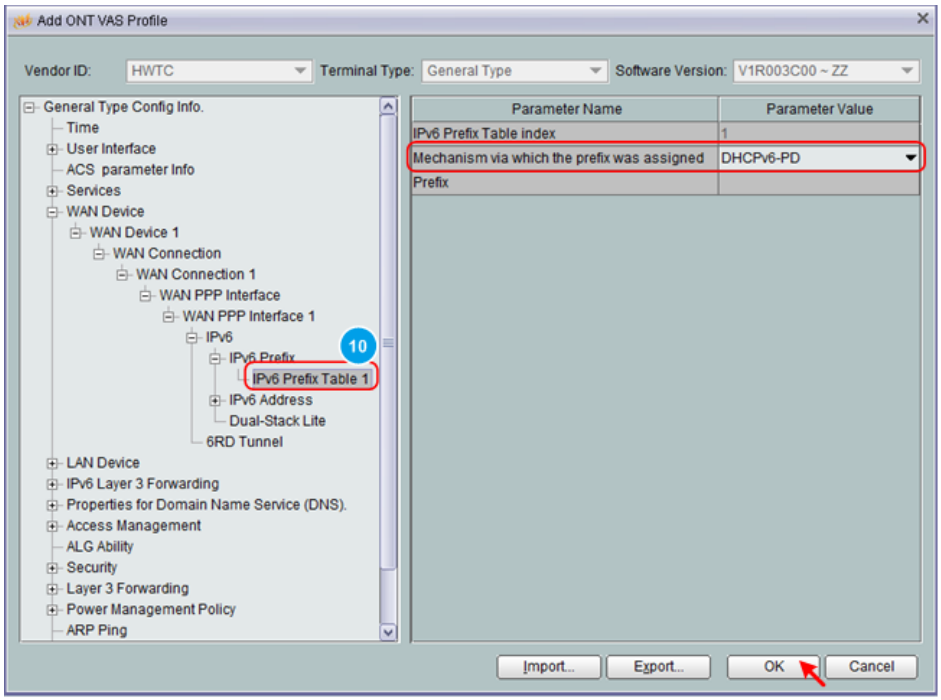
- **Configure and bind a general value-added service (VAS) profile for the ONT.**
  a. **Configure a general VAS profile for the ONT.**

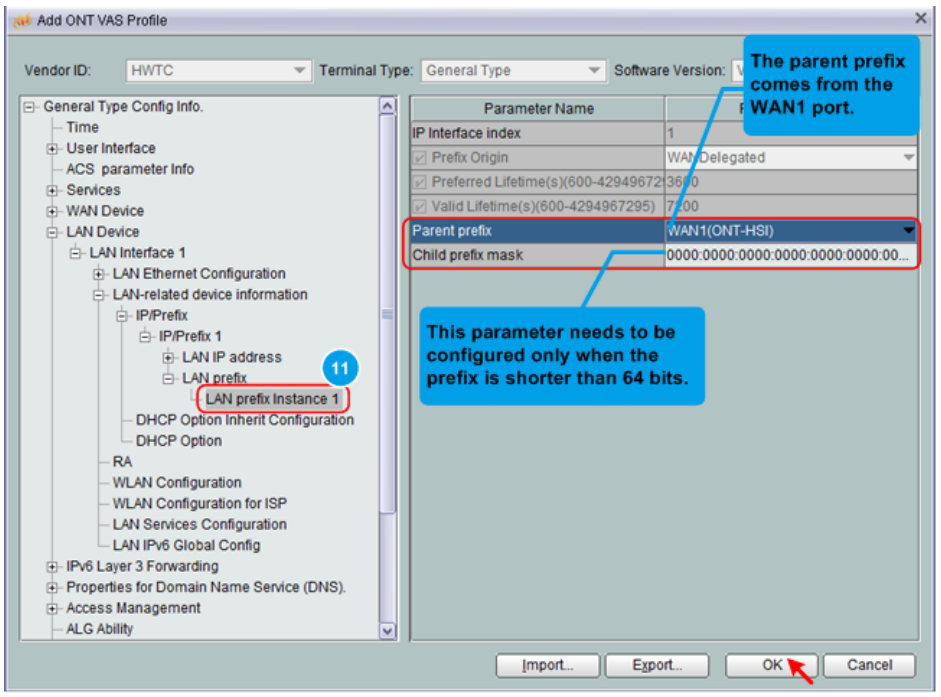

Configuration
Service
Inventory
Synchronize NE Configuration Data
NE Batch Configuration
IP Address Management
Access Profile Management
Access Service Management
Workbench
Access Profile Management
ONT VAS Profile
General ONT VAS Profile
DSL Profile
PON Profile
GPON Profile
EPON Profile
Optical Alarm Profile
ONT VAS Profile
ONU Service Level Profile
PQ Mapping Profile
Power Shedding Profile
Voice Profile
VLAN Profile
EOC Profile
D-CMTS Profile
IPDR Server Profile
EQAM Profile
Traffic Profile
WRED Profile
COS Group Profile
IGMP Profile
Profile Set
Service Provisioning Profile
ACL Profile
RAIO Profile
MPLS TC Field Mapping Profile
SNMP Profile
System Parameter Profile
ETH Alarm Profile
QoS Policy Profile
QoS Profile
Name
Alias
Add(Service Configuration Type)
Add(Preconfiguration Type)
Copy...
Modify
Delete
Add (Import File)
File
Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-HSI
Alias:
Common Parameters
General Para.
User Interface
Services
WAN Device
WAN Device 1
WAN Connection
Add IP Connection
Add PPP Connection
Parameter Name
Parameter Value
Number of WAN Connection(0-64)
MaxNumber
64
<Back
Next>
Finish
Cancel
1
2
3
4
5

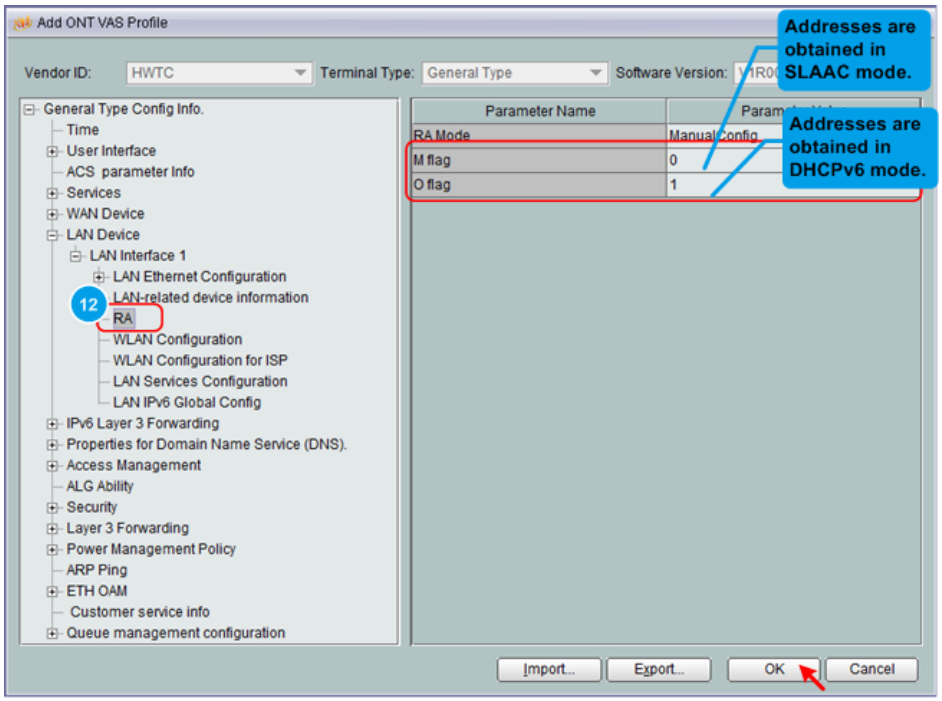

Add an ONT General VAS Profile(Service Tpye)
Step 1/2: Set Common Parameters
General Attributes
Name: ONT-HSI
Alias:
Common Parameters
General Para.
User Interface
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interface 1
LAN Device
Customer service info
Parameter Name
Parameter Value
WAN PPP interface index
WAN Enable
Enable
Connection Type
Routed
Vlan ID(0-4094)
1001
Priority(0-7)
0
IPv6 Enabled
Enable
It must be the same as that configured on the OLT at the user side.
When the dual stack or dual stack+NAT444 solution is used, IPv6 must be enabled.
<Back
Next>
Finish
Cancel
6

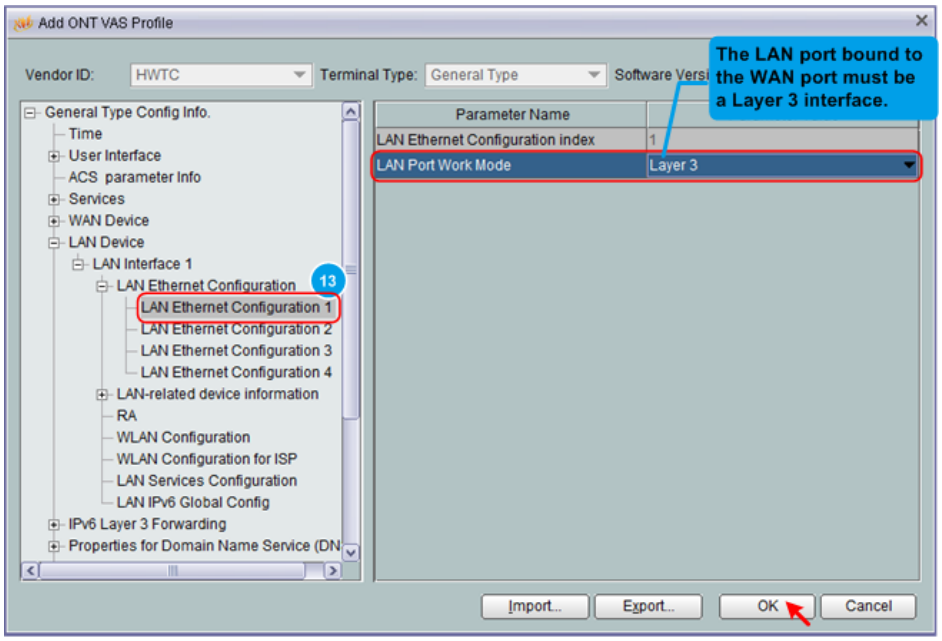


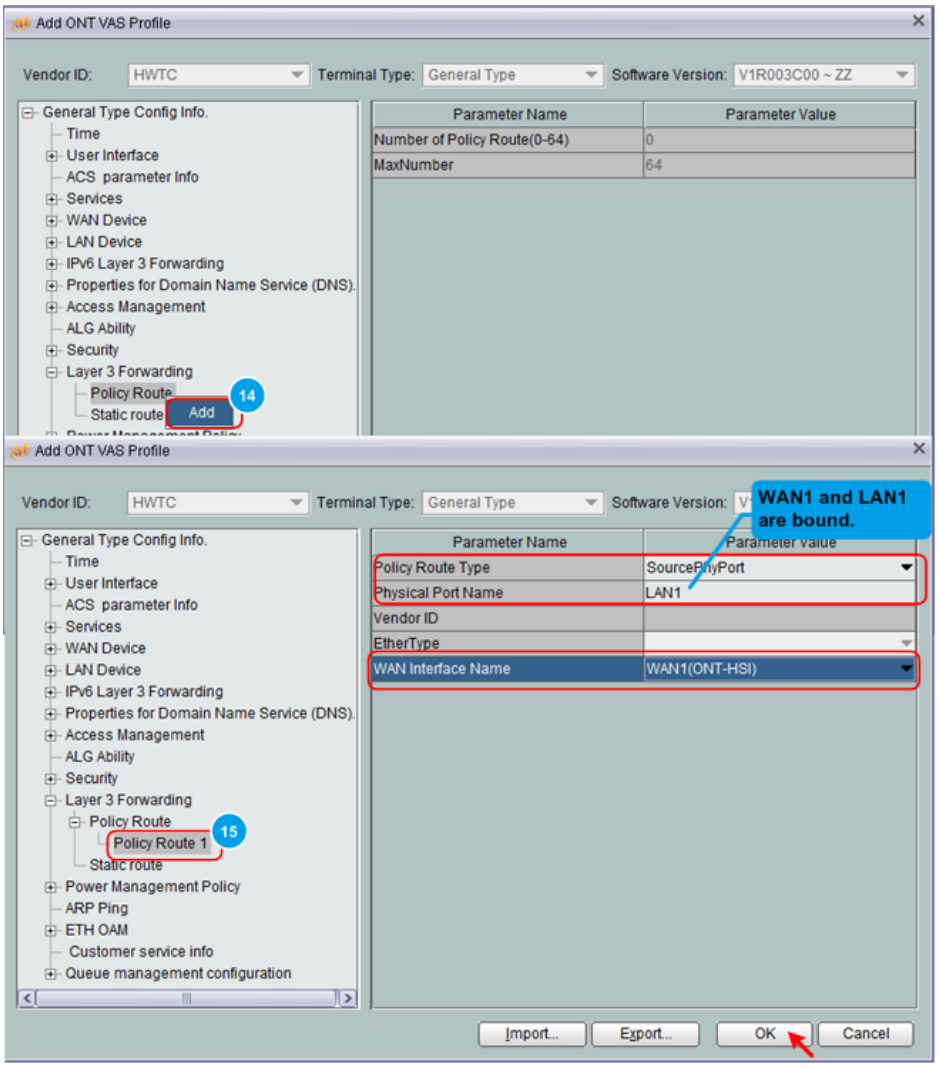












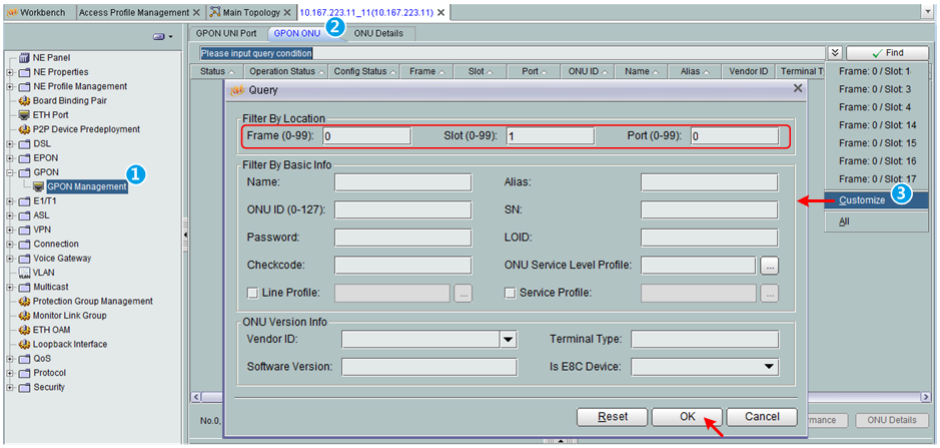
NOTE

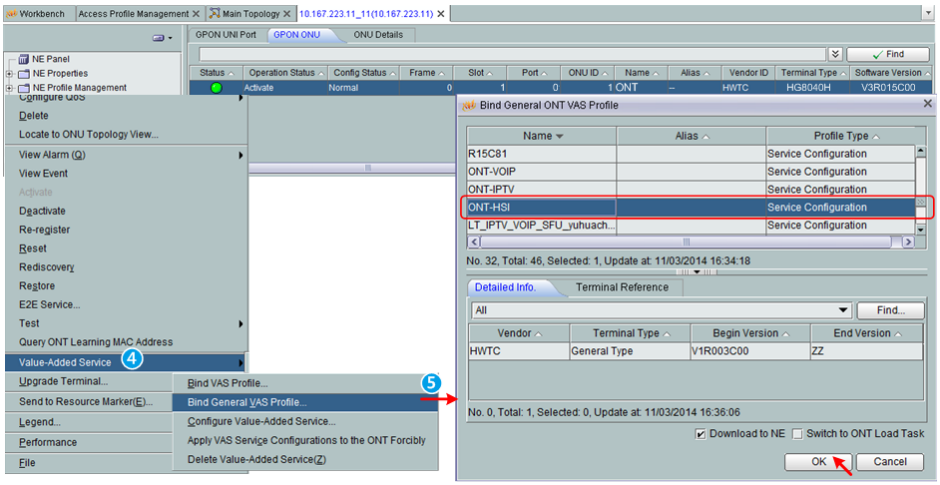
The ONT supports only one IPv6 (single-stack or dual-stack) Internet WAN port.

Parameters	Description
Mechanism via which the IP address was assigned	The ONT address mode can be **Numbered** or **Unnumbered**. In **Numbered** mode, the ONT WAN port has its own IPv6 GUA address. In **Unnumbered** mode, the ONT WAN port has an LLA address but no GUA address, which is not good for network management and fault location. Therefore, the **Numbered** mode is recommended. ● When the **Numbered** mode is used, the setting of **Mechanism via which the IP address was assigned** is as follows: – When M=1 is set for the RA packet on the BRAS, IP addresses are obtained in DHCPv6 mode on the WAN side. Then, **Mechanism via which the IP address was assigned** can be set to **DHCPv6** or **AutoConfigured**. **AutoConfigured** is recommended. – When M=0 is set for the RA packet on the BRAS, IP addresses are obtained in ND (stateless address allocation) mode on the WAN side. Then, **Mechanism via which the IP address was assigned** can be set to **AutoConfigured**. ● When the **Unnumbered** mode is used, **Mechanism via which the IP address was assigned** can be set to **None**.
Mechanism via which the prefix was assigned	● If **Mechanism via which the prefix was assigned** is set to **DHCPv6–PD**, the BRAS assigns prefixes to the ONT in DHCPv6 mode. ● If **Mechanism via which the prefix was assigned** is set to **None**, no prefix will be obtained. If no prefix is obtained, services may be unavailable. Usually, **Mechanism via which the prefix was assigned** is set to **None** during TR-069 or management channel configuration. It cannot be set to **None** for the Internet access service. ● The **RouterAdvertisement** or **AutoConfigured** mode is an extended mode which is not supported by current standards/protocols. Therefore, it is not recommended. The **DHCPv6–PD** mode is recommended.
M flag	M flag indicates the IP address and prefix assignment mode on the LAN side. **1** indicates that addresses/prefixes are assigned in the DHCPv6 mode which corresponds to the DHCPv6 mode (stateful) on the Web page. **0** indicates that addresses/prefixes are assigned in the ND mode which corresponds to the SLAAC mode (stateless) on the Web page. The SLAAC mode is recommended.

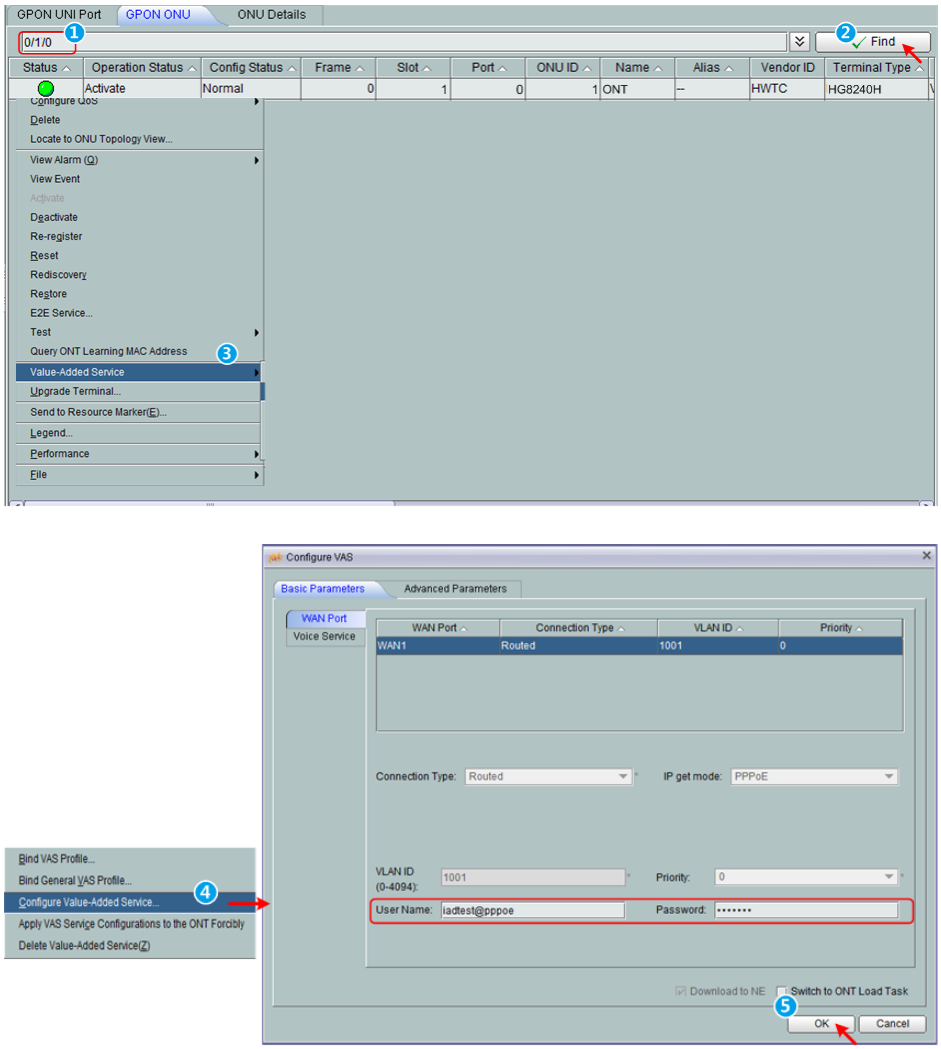
Parameters	Description
O flag	O flag indicates the assignment mode of other information on the LAN side. **1** indicates that the information is assigned in the DHCPv6 mode which corresponds to the DHCPv6 mode (stateful) on the Web page. **0** indicates that the information is assigned in the ND mode which corresponds to the SLAAC mode (stateless) on the Web page. The DHCPv6 mode is recommended.

b. **Bind the general VAS profile.**





c. **Configure the ONT VAS service.**



3.4.3.3 Configuring the IPv6 Internet Access Service Using the NMS (DS-Lite)

This topic describes how to configure the IPv6 Internet access service using the U2000 when the DS-Lite solution is used and the ONT is a gateway-type ONT.

Application Context

Networking description:

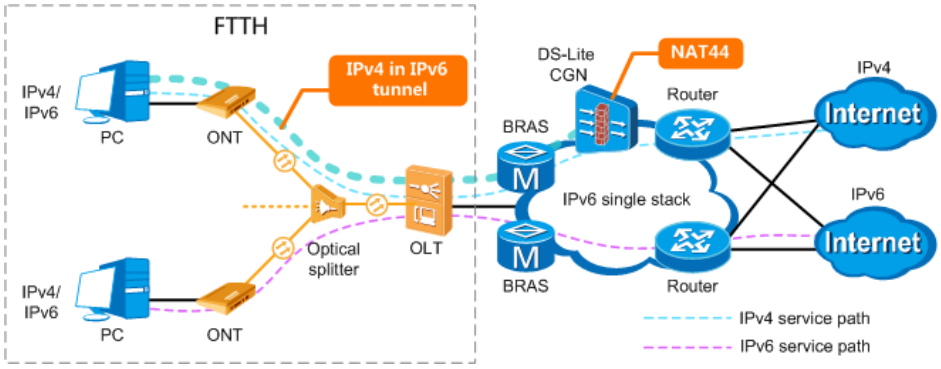
- The BRAS assigns an IPv6 prefix (not an IPv4 address) and the URL address of the DS-Lite CGN gateway to the ONT.
- The ONT assigns an IPv4 private address and IPv6 address to a PC.
- IPv6 packets are forwarded directly by the ONT, OLT, and BRAS.
- IPv4 packets are encapsulated into IPv6 packets on the ONT and sent to the DS-Lite CGN. The DS-Lite CGN decapsulates the packets, performs NAT44 translation on the packets, and then forwards them to the IPv4 Internet.
- The OLT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction:

- The ONT needs to be upgraded to support DS-Lite.
- Devices such as OLT and BRAS in the downstream of the DS-Lite CGN need to be upgraded to support the IPv6 single stack.
- The DS-Lite CGN device needs to be deployed.

Figure 3-14 shows the DS-Lite networking diagram.

Figure 3-14 DS-Lite networking diagram



Typical Configuration

Table 3-21 describes the typical IPv6 prefix and address configuration. This configuration has the best compatibility and can be applied to any scenarios.

Table 3-21 Typical IPv6 prefix and address configuration

Item	Parameter on NMS	Recommended Value	Remarks
IP address acquisition mode on the ONT WAN side	Mechanism via which the IP address was assigned	AutoConfigured	-
Prefix acquisition mode on the ONT WAN side	Mechanism via which the prefix was assigned	DHCPv6–PD	-
Address/prefix assignment mode for the LAN-side PC	M flag	0 (that is, SLAAC)	When the value is **1**, addresses/prefixes are assigned in the DHCPv6 mode. Currently, the Windows XP OS does not support this assignment mode.

Item	Parameter on NMS	Recommended Value	Remarks
Other information assignment mode for the LAN-side PC	O flag	1 (that is, DHCPv6)	Other information refers to the IPv6 address in payloads of packets such as DNS packets. When the value is 0, the information is assigned in the SLAAC mode. Currently, no OS supports the SLAAC mode.

Procedure

- **Configure the OLT.**

NOTE

The OLT implements Layer 2 transparent transmission. The procedure for configuring the OLT on the U2000 is the same as that for IPv4. For detailed configuration procedure, refer to "Implement pre-configurations", "Add an ONT" and "Add a service virtual port on the OLT side" in **3.3.1.1.2 Configuring the GPON FTTH Layer 3 Internet Access Service on the NMS**

1. (Optional) Configure the DHCPv6 option.

   When the access mode of IPv6 users is IPoE and the BRAS uses the binding authentication mode, users do not need to enter user names or passwords for authentication because the BRAS performs authentication based on users' physical information. In this case, DHCPv6 Option18 needs to be configured on the OLT. For the mapping relationship between DHCPv6 Option and the BRAS, see **Table 3-22**.

Table 3-22 DHCPv6 Option mapping

DHCPv6 Option	OLT	BRAS
Option17	N/A	Optional
Option18	Mandatory	Mandatory
Option37	Optional	Optional

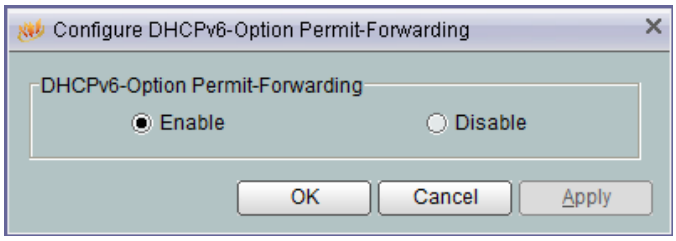
NOTE

By default, the global DHCPv6 Option configuration is **disable**, the VLAN-level DHCPv6 Option configuration is **enable**, and the upstream/cascaded port-level DHCPv6 Option configuration is **enable**. Therefore, you only need to enable DHCPv6 Option globally.

After DHCPv6 Option is enabled, the OLT inserts Option18 and Option37 into DHCPv6 packets for authentication by the BRAS.

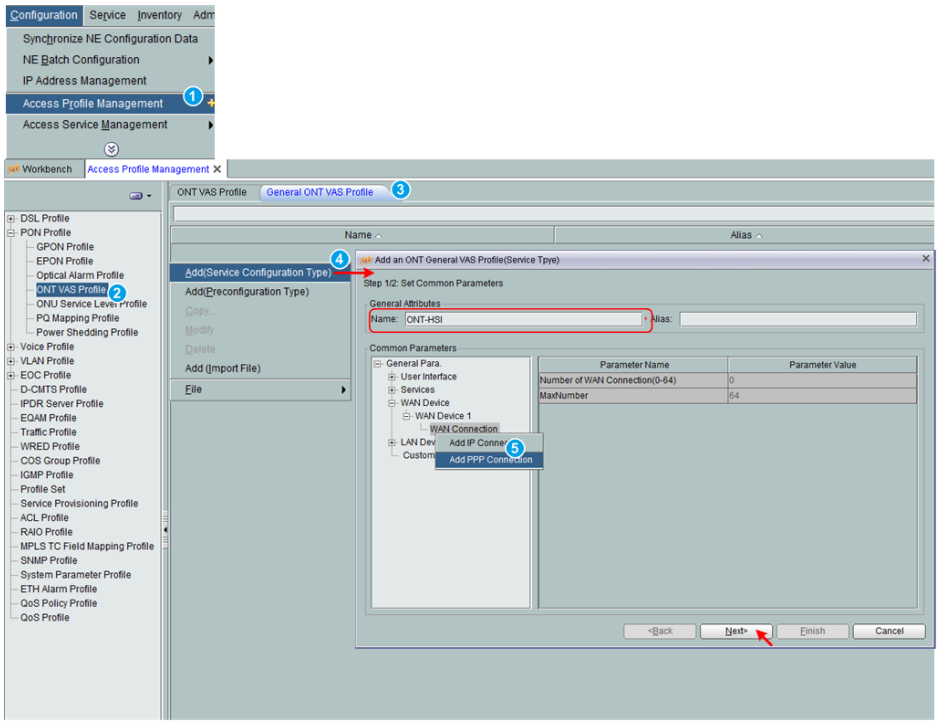
1. In the Main Topology, double-click the required OLT in the **Physical Root** navigation tree; or right-click the required OLT and choose **NE Explorer** from the shortcut menu.
2. Choose **GPON** > **GPON Management** from the navigation tree.

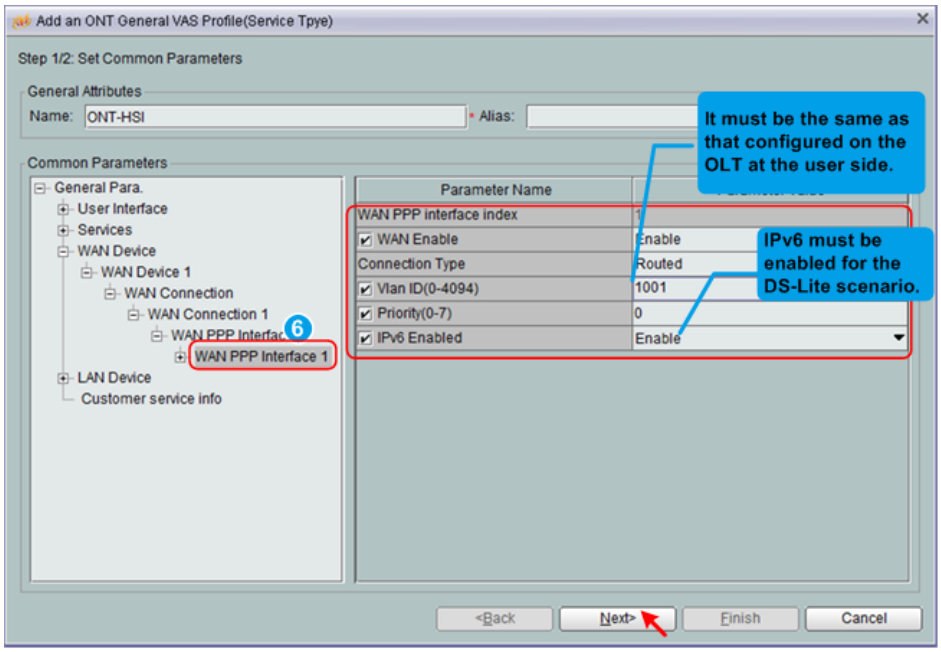
3. On the **GPON ONU** tab page, set the filter criteria or click to display the GPON ONUs.
4. Right-click a required ONT and choose **Configure DHCPv6–Option Permit-Forwarding**.
5. In the dialog box that is displayed, select **Enable**.

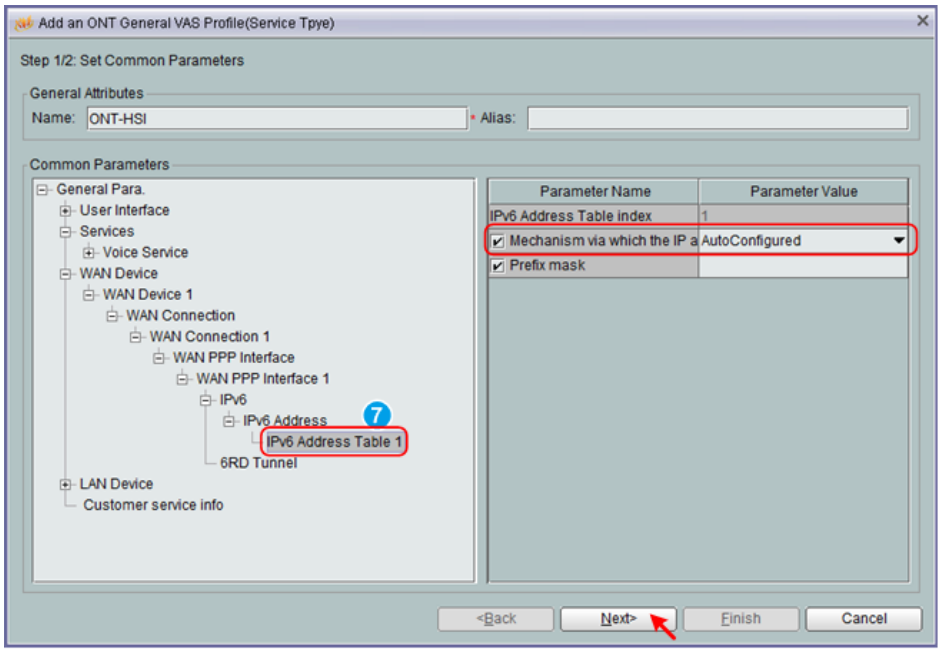


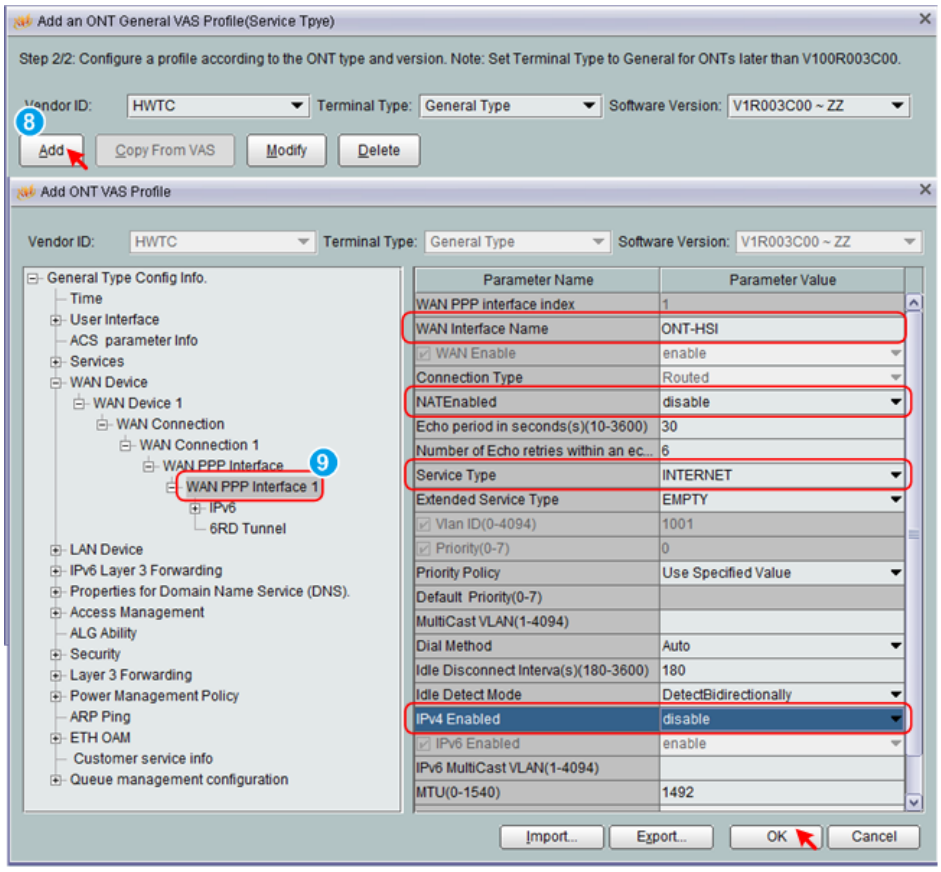
1. Click **OK**.

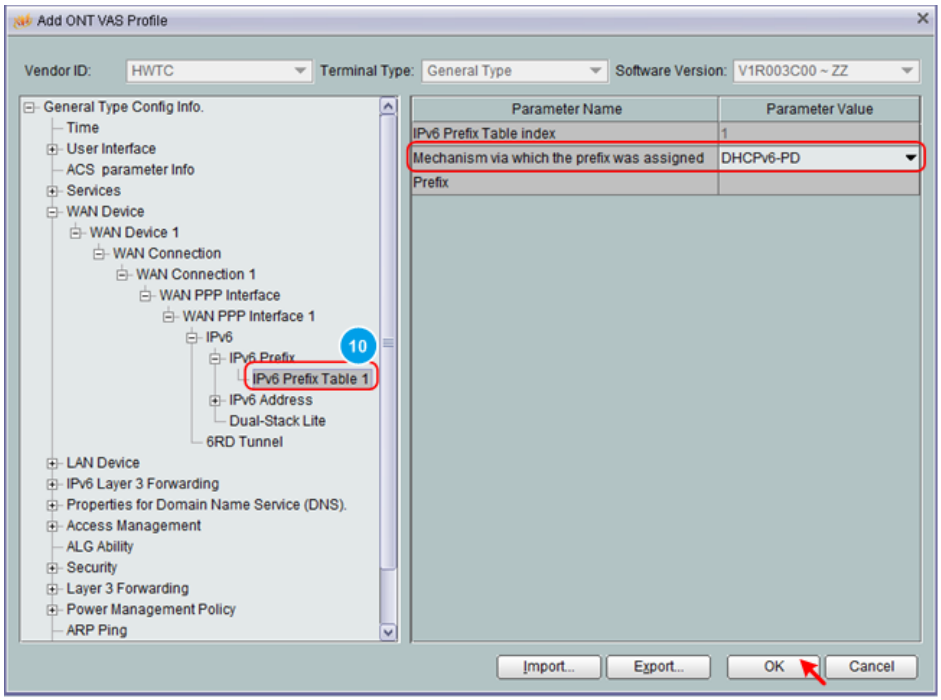
- **Configure and bind a general value-added service (VAS) profile for the ONT.**
  a. **Configure a general VAS profile for the ONT.**

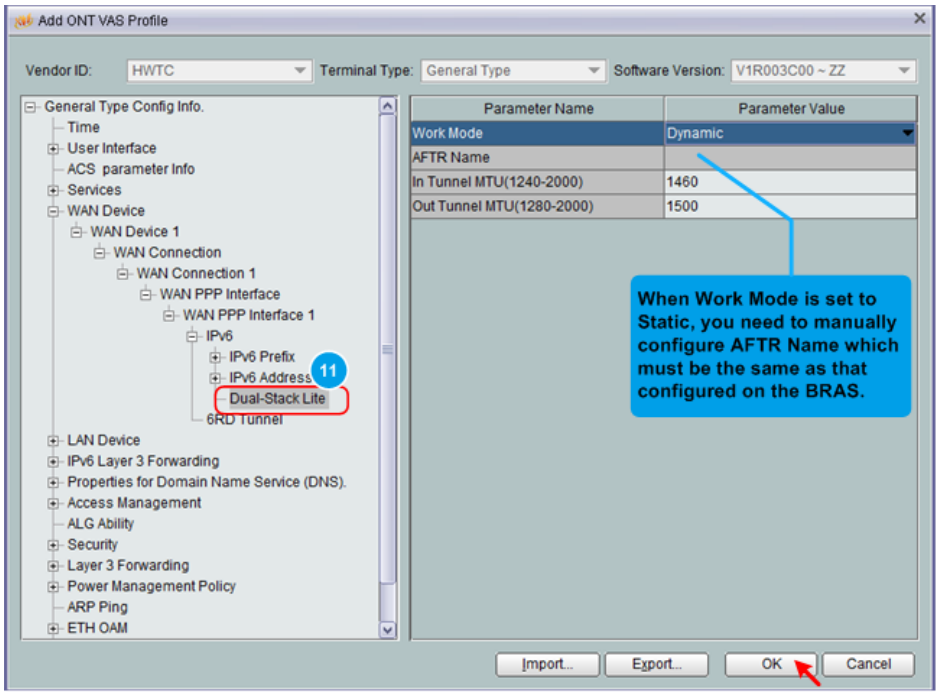


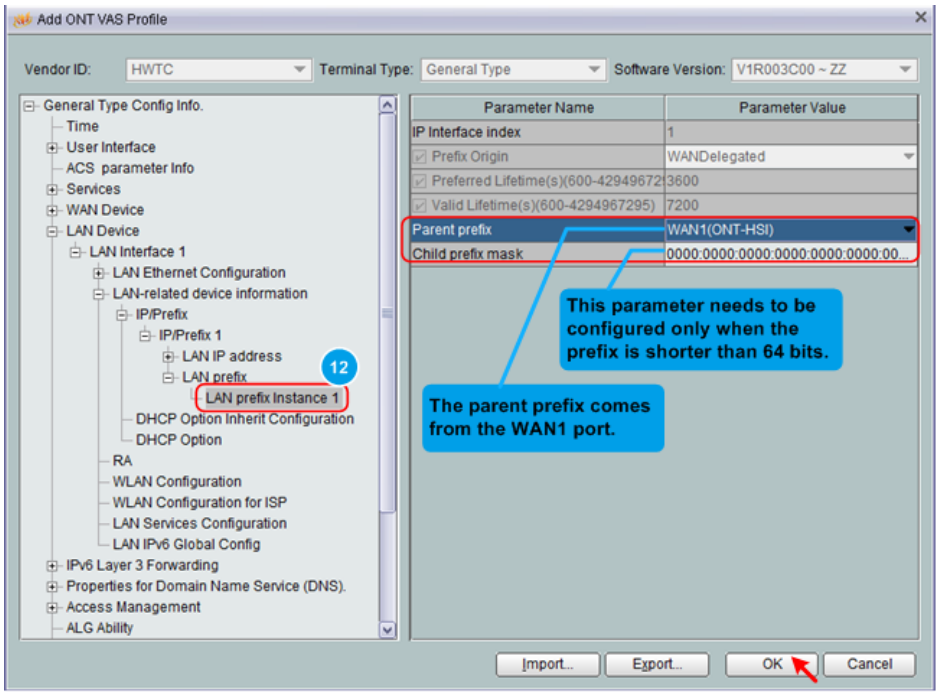


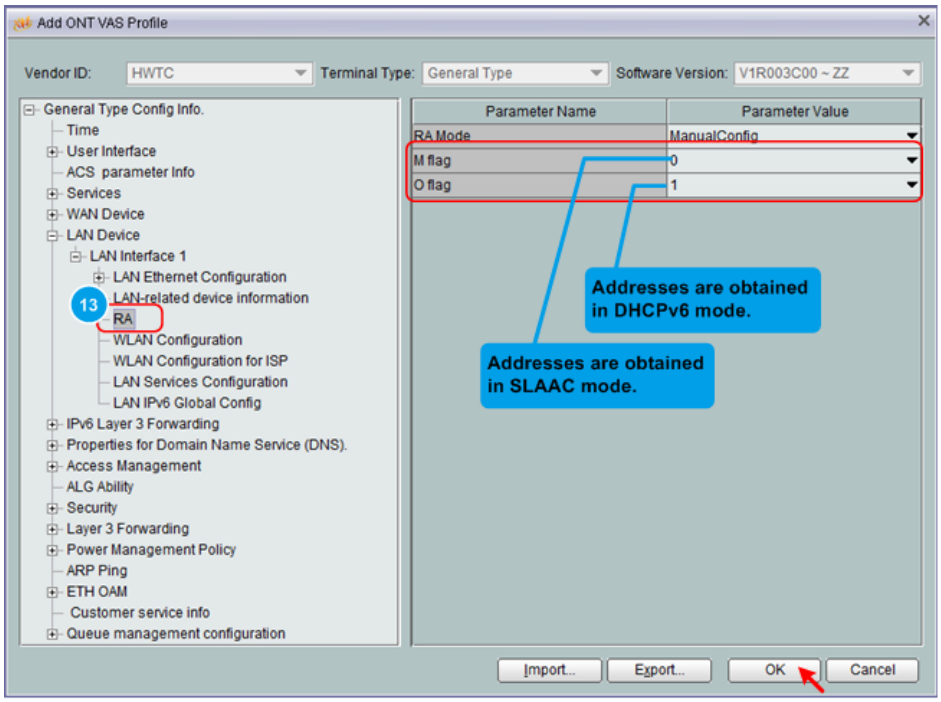


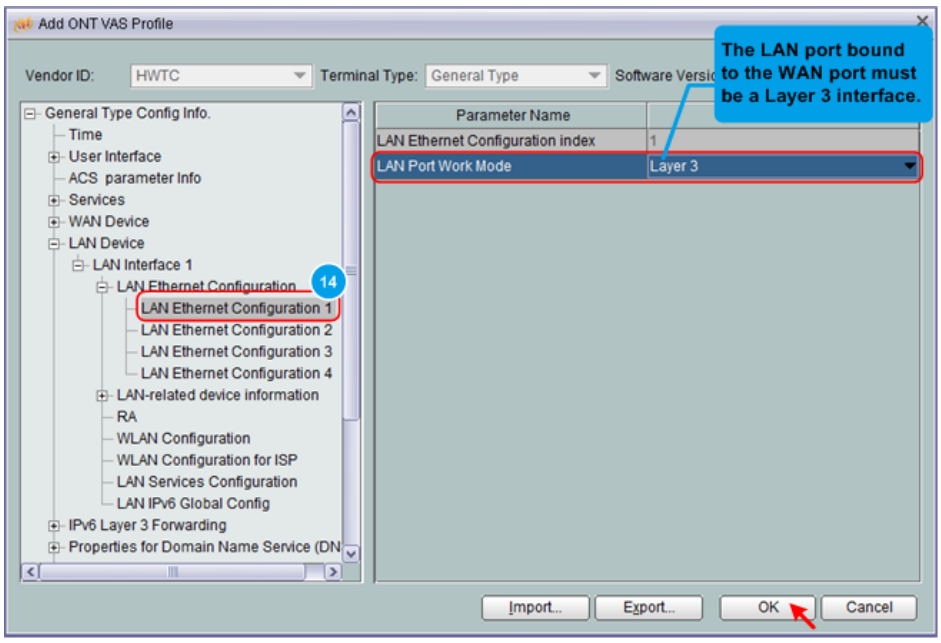

Add an ONT General VAS Profile(Service Tpye)
Step 2/2: Configure a profile according to the ONT type and version. Note: Set Terminal Type to General for ONTs later than V100R003C00.
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
8
Add
Copy From VAS
Modify
Delete
Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interface
9
WAN PPP Interface 1
IPv6
6RD Tunnel
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DNS).
Access Management
ALG Ability
Security
Layer 3 Forwarding
Power Management Policy
ARP Ping
ETH OAM
Customer service info
Queue management configuration
Parameter Name
Parameter Value
WAN PPP interface index
1
WAN Interface Name
ONT-HSI
WAN Enable
enable
Connection Type
Routed
NATEnabled
disable
Echo period in seconds(s)(10-3600)
30
Number of Echo retries within an ec...
6
Service Type
INTERNET
Extended Service Type
EMPTY
Vlan ID(0-4094)
1001
Priority(0-7)
0
Priority Policy
Use Specified Value
Default Priority(0-7)
MultiCast VLAN(1-4094)
Dial Method
Auto
Idle Disconnect Interva(s)(180-3600)
180
Idle Detect Mode
DetectBidirectionally
IPv4 Enabled
disable
IPv6 Enabled
enable
IPv6 MultiCast VLAN(1-4094)
MTU(0-1540)
1492
Import...
Export...
OK
Cancel

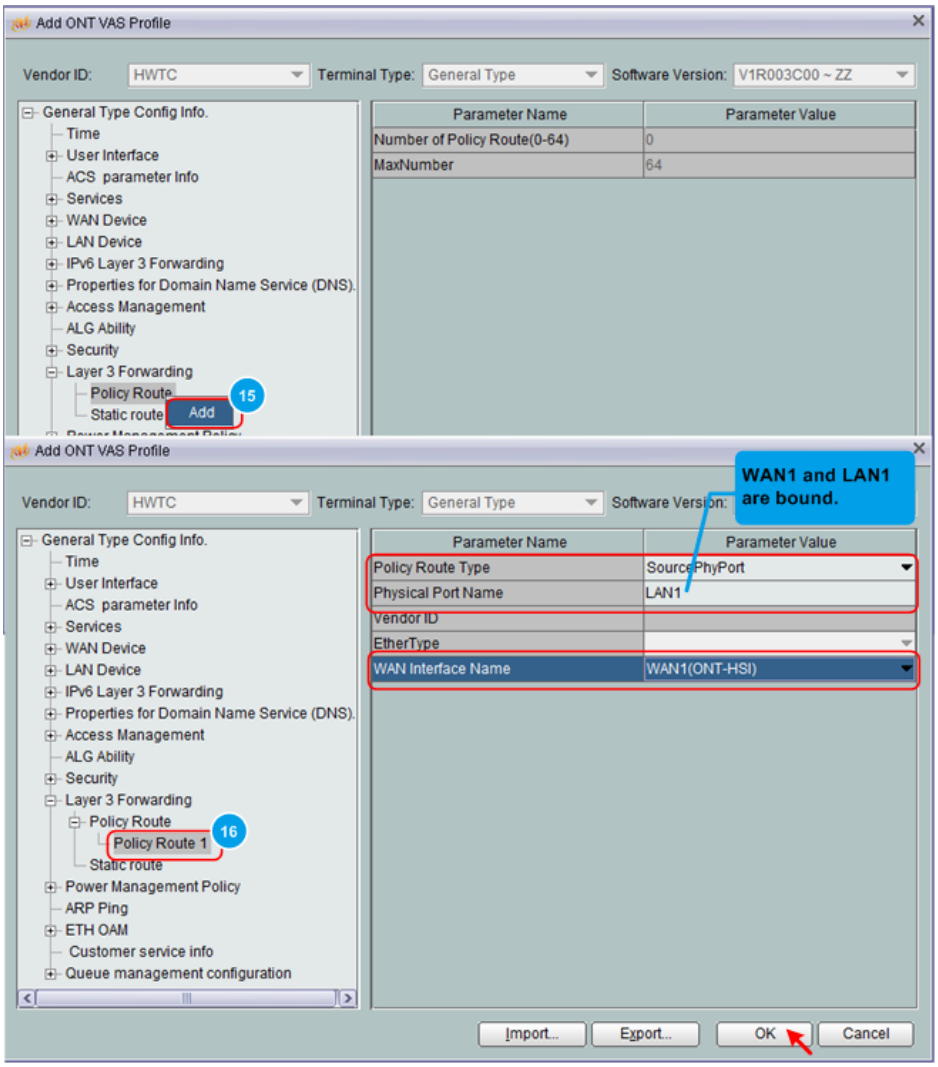

Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
WAN Device 1
WAN Connection
WAN Connection 1
WAN PPP Interface
WAN PPP Interface 1
IPv6
10
IPv6 Prefix
IPv6 Prefix Table 1
IPv6 Address
Dual-Stack Lite
6RD Tunnel
LAN Device
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DNS).
Access Management
ALG Ability
Security
Layer 3 Forwarding
Power Management Policy
ARP Ping
Parameter Name
Parameter Value
IPv6 Prefix Table index
1
Mechanism via which the prefix was assigned
DHCPv6-PD
Prefix
Import...
Export...
OK
Cancel






Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
Software Version: V1R003C00 ~ ZZ
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
LAN Interface 1
LAN Ethernet Configuration
LAN-related device information
13
RA
WLAN Configuration
WLAN Configuration for ISP
LAN Services Configuration
LAN IPv6 Global Config
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DNS).
Access Management
ALG Ability
Security
Layer 3 Forwarding
Power Management Policy
ARP Ping
ETH OAM
Customer service info
Queue management configuration
Parameter Name
Parameter Value
RA Mode
ManualConfig
M flag
0
O flag
1
Addresses are obtained in DHCPv6 mode.
Addresses are obtained in SLAAC mode.
Import...
Export...
OK
Cancel


Add ONT VAS Profile
Vendor ID: HWTC
Terminal Type: General Type
The LAN port bound to the WAN port must be a Layer 3 interface.
General Type Config Info.
Time
User Interface
ACS parameter Info
Services
WAN Device
LAN Device
LAN Interface 1
LAN Ethernet Configuration
14
LAN Ethernet Configuration 1
LAN Ethernet Configuration 2
LAN Ethernet Configuration 3
LAN Ethernet Configuration 4
LAN-related device information
RA
WLAN Configuration
WLAN Configuration for ISP
LAN Services Configuration
LAN IPv6 Global Config
IPv6 Layer 3 Forwarding
Properties for Domain Name Service (DN
Parameter Name
LAN Ethernet Configuration index
1
LAN Port Work Mode
Layer 3
Import...
Export...
OK
Cancel



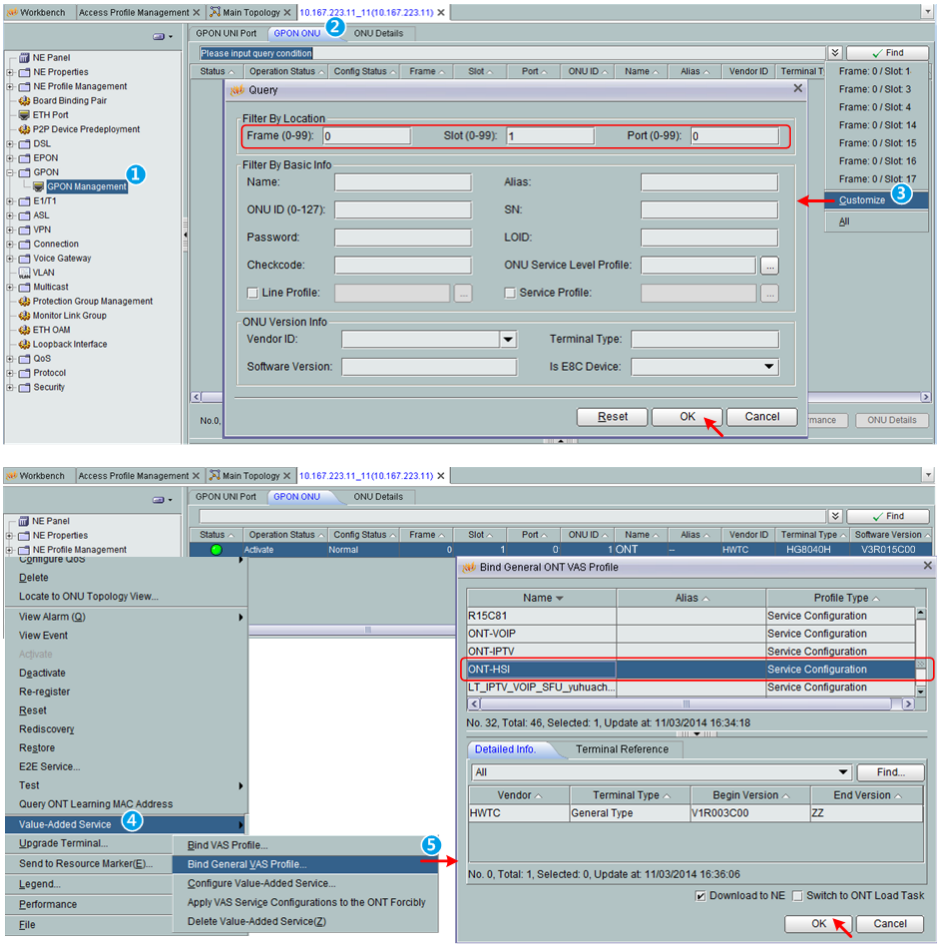
NOTE

The ONT supports only one IPv6 (single-stack or dual-stack) Internet WAN port.

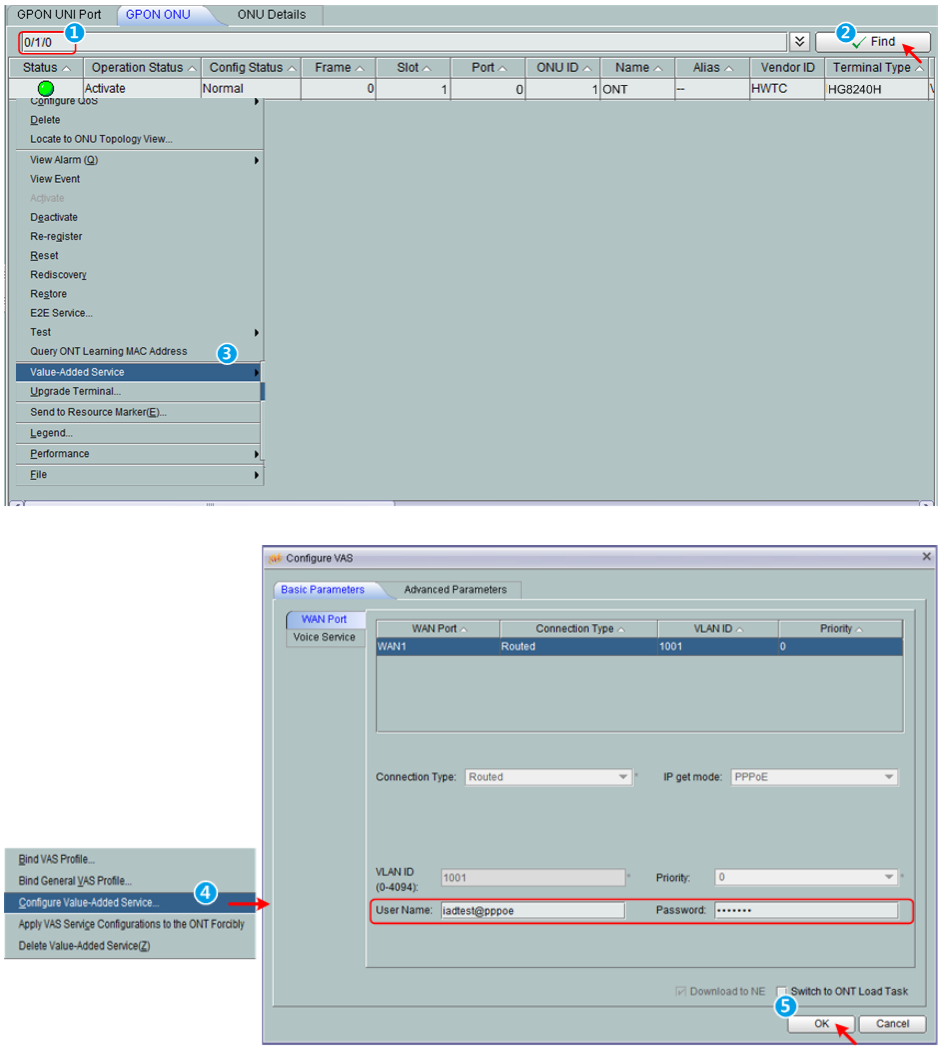
Parameters	Description
Mechanism via which the IP address was assigned	The ONT address mode can be **Numbered** or **Unnumbered**. In **Numbered** mode, the ONT WAN port has its own IPv6 GUA address. In **Unnumbered** mode, the ONT WAN port has an LLA address but no GUA address, which is not good for network management and fault location. Therefore, the **Numbered** mode is recommended. ● When the **Numbered** mode is used, the setting of **Mechanism via which the IP address was assigned** is as follows: – When M=1 is set for the RA packet on the BRAS, IP addresses are obtained in DHCPv6 mode on the WAN side. Then, **Mechanism via which the IP address was assigned** can be set to **DHCPv6** or **AutoConfigured**. **AutoConfigured** is recommended. – When M=0 is set for the RA packet on the BRAS, IP addresses are obtained in ND (stateless address allocation) mode on the WAN side. Then, **Mechanism via which the IP address was assigned** can be set to **AutoConfigured**. ● When the **Unnumbered** mode is used, **Mechanism via which the IP address was assigned** can be set to **None**.
Mechanism via which the prefix was assigned	● If **Mechanism via which the prefix was assigned** is set to **DHCPv6–PD**, the BRAS assigns prefixes to the ONT in DHCPv6 mode. ● If **Mechanism via which the prefix was assigned** is set to **None**, no prefix will be obtained. If no prefix is obtained, services may be unavailable. Usually, **Mechanism via which the prefix was assigned** is set to **None** during TR-069 or management channel configuration. It cannot be set to **None** for the Internet access service. ● The **RouterAdvertisement** or **AutoConfigured** mode is an extended mode which is not supported by current standards/protocols. Therefore, it is not recommended. The **DHCPv6–PD** mode is recommended.
M flag	M flag indicates the IP address and prefix assignment mode on the LAN side. **1** indicates that addresses/prefixes are assigned in the DHCPv6 mode which corresponds to the DHCPv6 mode (stateful) on the Web page. **0** indicates that addresses/prefixes are assigned in the ND mode which corresponds to the SLAAC mode (stateless) on the Web page. The SLAAC mode is recommended.

Parameters	Description
O flag	O flag indicates the assignment mode of other information on the LAN side. **1** indicates that the information is assigned in the DHCPv6 mode which corresponds to the DHCPv6 mode (stateful) on the Web page. **0** indicates that the information is assigned in the ND mode which corresponds to the SLAAC mode (stateless) on the Web page. The DHCPv6 mode is recommended.

b. **Bind the general VAS profile.**



c. **Configure the ONT VAS service.**



3.4.4 Configuring IPv6 Services Using OLT Commands

This topic describes how to configure IPv6 services using OLT commands.

3.4.4.1 Configuring the IPv6 Internet Access Service Using OLT Commands (NA)

This topic describes how to configure the IPv6 Internet access service using OLT commands when the NAT444 solution is used and the ONT is a gateway-type ONT.

Prerequisite

- The Layer 2 service flow channel between the OLT and ONT is available by running the OLT command.
- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configurations, see the configuration guide.
- The VLAN of the port on the LSW that connects to the OLT must be the same as that of the upstream port on the OLT.

Application Context

Networking description:

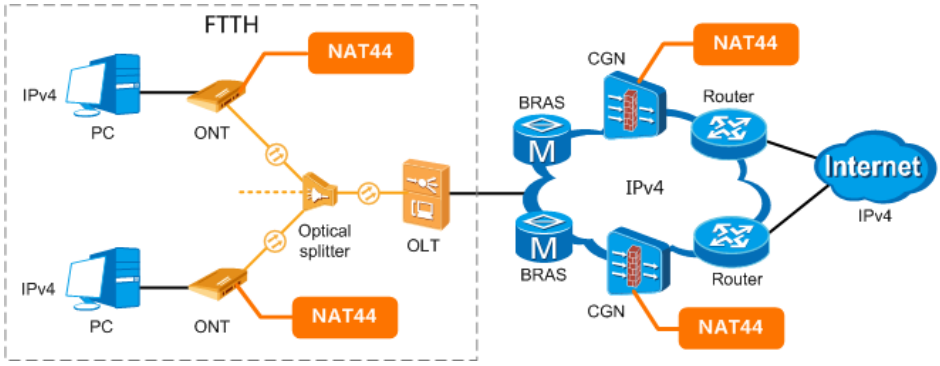
- The BRAS assigns an IPv4 private address (for example, 10.*.*.*) to the ONT. The ONT is enabled with the NAT function and assigns another IPv4 private address (for example, 192.168.*.*) to the PC.
- NAT44 translation is performed twice on IPv4 packets, first on the ONT and then on the CGN.
- The OLT implements Layer 2 forwarding, and the ONT implements Layer 3 forwarding.

Device reconstruction:

- The IP address pool on the BRAS needs to be replanned to support private IP addresses.
- The CGN device supporting NAT44 needs to be deployed on the network.
- The RADIUS needs to be upgraded or a log recording device needs to be deployed to address source tracing of private IP addresses.

Figure 3-15 shows the NAT444 networking diagram.

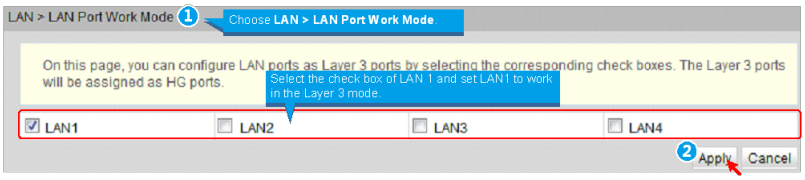
Figure 3-15 NAT444 networking diagram



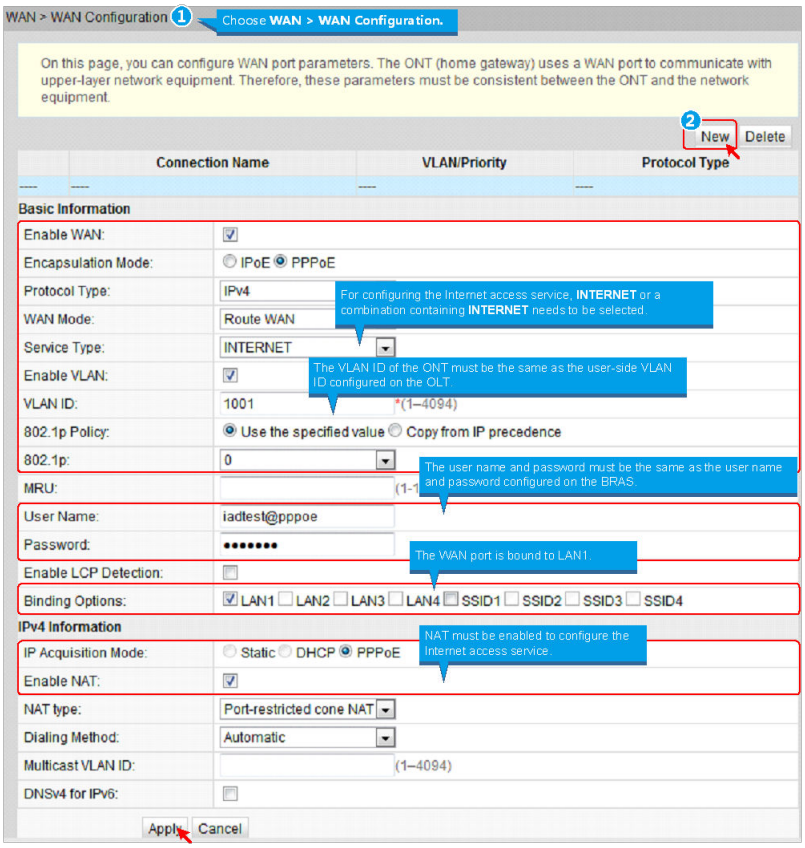
Procedure

- Configurations on the ONT:
  a. Configure the working mode of a LAN port.

     The LAN port bound to the WAN port must work in the Layer 3 mode. Therefore, set the working mode to Layer 3 for the LAN port connected to the PC.



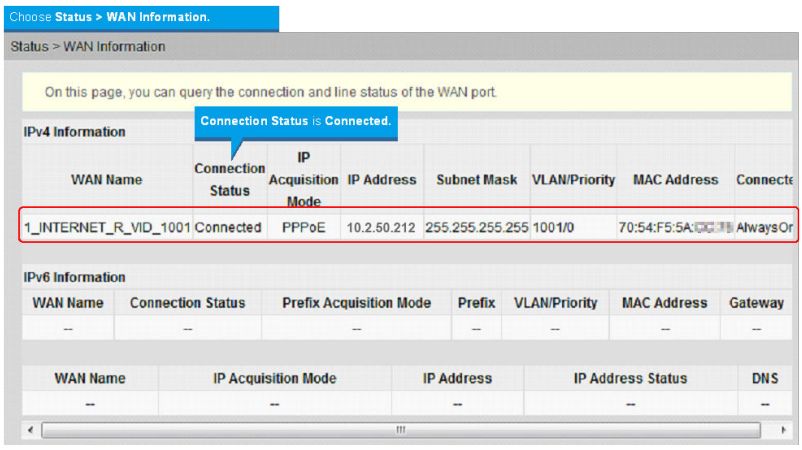
  b. Configure parameters of a WAN port.



NOTE

In the NAT444 solution, a NAT translation must be performed on the ONT. Therefore, the NAT function must be enabled for the ONT.

c. Check the ONT connection status.



3.4.4.2 Configuring the IPv6 Internet Access Service Using OLT Commands (Dual Stack/Dual Stack+NA)

This topic describes how to configure the IPv6 Internet access service using the OLT commands when the dual stack or dual stack+NAT444 solution is used and the ONT is a gateway-type ONT.

NOTE

The OLT implements Layer 2 transparent transmission in the dual stack or dual stack+NAT444 scenario. Configurations on the OLT are the same as those for IPv4.

The FTTH configuration difference between the dual stack solution and the dual stack+NAT444 solution lies in NAT configuration on the ONT.

- In the dual stack solution, if the IP address of the PC on the internal network is a private address, the NAT function must be enabled, that is, dual stack+NAT44. The NAT function is disabled when it is not required.
- In the dual stack+NAT444 solution, the NAT function must be enabled.

Prerequisite

- The Layer 2 service flow channel between the OLT and ONT is available by running the OLT command.
- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configurations, see the configuration guide.
- The VLAN of the port on the LSW that connects to the OLT must be the same as that of the upstream port on the OLT.

Dual Stack Application Context

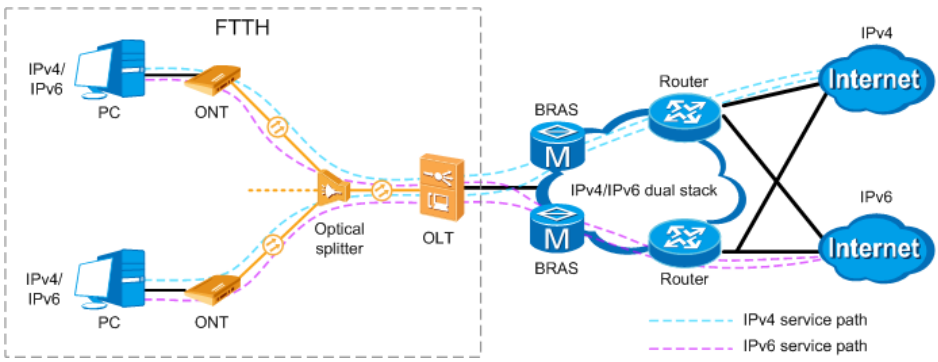
Networking description:

- All NEs on the network must support IPv4 and IPv6 dual stacks.
- The BRAS assigns IPv4 and IPv6 addresses to ONTs. The ONT assigns IPv4 and IPv6 addresses to PCs.
- PCs use IPv4 and IPv6 addresses to access the IPv4 Internet and IPv6 Internet respectively.
- The OLT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction: All NEs on the network need to be upgraded to support IPv4 and IPv6 dual stacks.

Figure 3-16 shows the dual-stack networking diagram.

Figure 3-16 Dual-stack networking diagram



Dual Stack+NAT444 Application Context

Networking description:

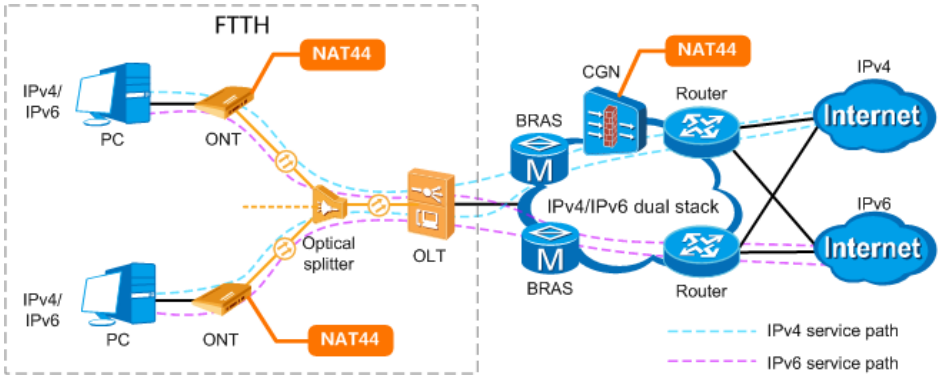
- All NEs on the network must support IPv4 and IPv6 dual stacks.
- The CGN device supporting NAT44 needs to be deployed on the network.
- The BRAS assigns an IPv4 private address (for example, 10.*.*.*) and IPv6 address to the ONT. The ONT is enabled with the NAT function and assigns another IPv4 private address (for example, 192.168.*.*) to the PC.
- NAT44 translation is performed twice on IPv4 packets, first on the ONT and then on the CGN. IPv6 packets are forwarded directly.
- The OLT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction:

- All NEs on the network need to be upgraded to support IPv4 and IPv6 dual stack.
- The IP address pool on the BRAS needs to be replanned to support private IP addresses.
- The CGN device supporting NAT44 needs to be deployed on the network.
- The RADIUS needs to be upgraded or a log recording device needs to be deployed to address source tracing of private IP addresses.

Figure 3-17 shows the dual stack+NAT444 networking diagram.

Figure 3-17 Dual stack+NAT444 networking diagram



Typical Configuration

Table 3-23describes the typical IPv6 prefix and address configuration. This configuration has the best compatibility and can be applied to any scenarios.

Table 3-23 Typical IPv6 prefix and address configuration

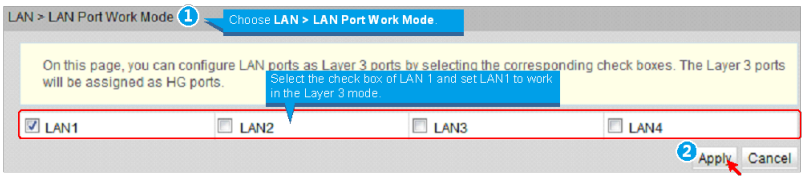
Item	Parameter on Web Page	Recommended Value	Remarks
IP address acquisition mode on the ONT WAN side	IP acquisition mode	Auto	-

Item	Parameter on Web Page	Recommended Value	Remarks
Prefix acquisition mode on the ONT WAN side	Prefix acquisition mode	DHCPv6–PD	-
Address/prefix assignment mode for the LAN-side PC	Address/Prefix assignment mode	SLAAC	Currently, the Windows XP OS does not support the DHCPv6 address/ prefix assignment mode.
Other information assignment mode for the LAN-side PC	Other information assignment mode	DHCPv6	Other information refers to the IPv6 address in payloads of packets such as DNS packets. Currently, no OS supports the SLAAC assignment mode.

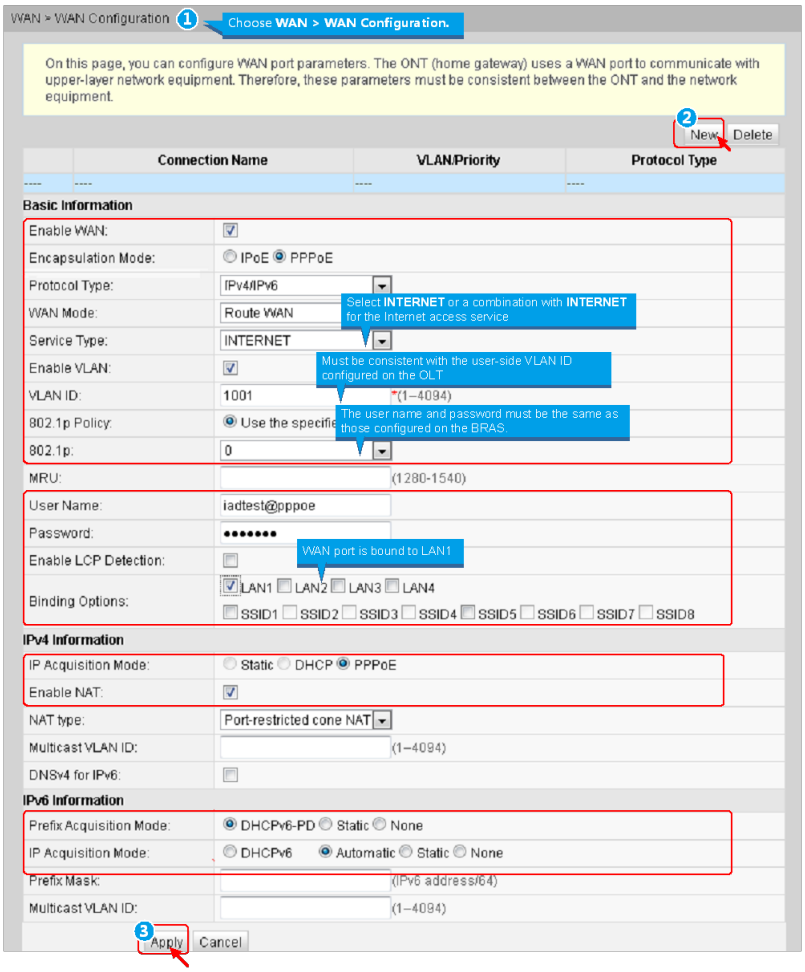
Procedure

- Configurations on the ONT:
  a. Configure the working mode of a LAN port.

     The LAN port bound to the WAN port must work in the Layer 3 mode. Therefore, set the working mode to Layer 3 for the LAN port connected to the PC.

  b. Configure parameters of a WAN port.



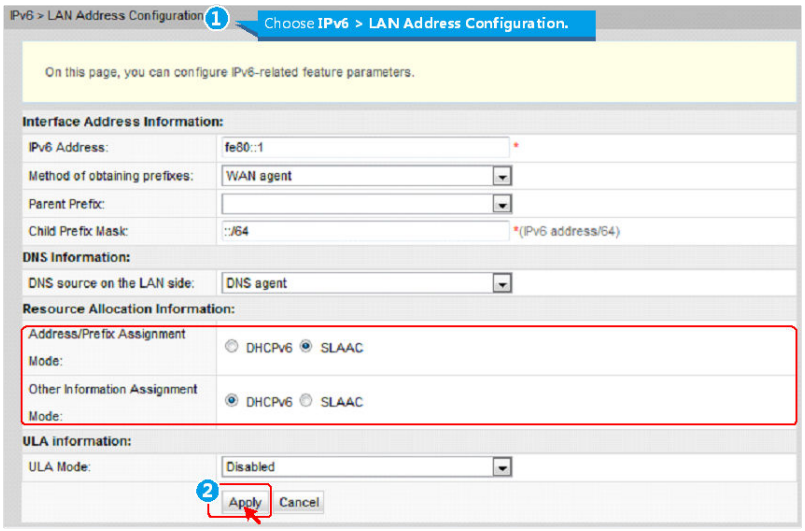
NOTE

The ONT supports only one IPv6 (single-stack or dual-stack) Internet WAN port.

Parameters	Parameters
NAT	● When the dual stack solution is used, the NAT function must be enabled if the IP address of the PC on the internal network is a private address. In this case, select **NAT**; that is, dual stack+NAT44. You do not need to select **NAT** if the NAT function is not required. ● When the dual stack+NAT444 solution is used, select **NAT**.

Parameters	Parameters
Prefix acquisition mode	● When **Prefix acquisition mode** is set to **DHCPv6–PD**, the BRAS assigns prefixes to the ONT in DHCPv6 mode. ● When **Prefix acquisition mode** is set to **None**, no prefix is obtained. If no prefix is obtained, services may be unavailable. Usually, **Prefix acquisition mode** is set to **None** during TR-069 or management channel configuration. It cannot be set to **None** for the Internet access service. ● The **RA** or **Auto** mode is an extended mode, which is not supported by current standards/protocols. Therefore, it is not recommended. The **DHCPv6–PD** mode is recommended.
IP acquisition mode	There are two ONT address modes: **Numbered** and **Unnumbered**. In **Numbered** mode, the ONT WAN port has its own IPv6 GUA address. In **Unnumbered** mode, the ONT WAN port has an LLA address but no GUA address, which is not good for network management and fault location. Therefore, the **Numbered** mode is recommended. ● When the **Numbered** mode is used, the setting of **IP acquisition mode** is as follows: – When M=1 is set for the RA packet on the BRAS, IP addresses are obtained in DHCPv6 mode on the WAN side. Then, **IP acquisition mode** can be set to **DHCPv6** or **Automatic**. **Automatic** is recommended. – When M=0 is set for the RA packet on the BRAS, IP addresses are obtained in ND (stateless address allocation) mode on the WAN side. Then, **IP acquisition mode** can be set to **Automatic**. ● When the **Unnumbered** mode is used, **IP acquisition mode** is set to **None**.

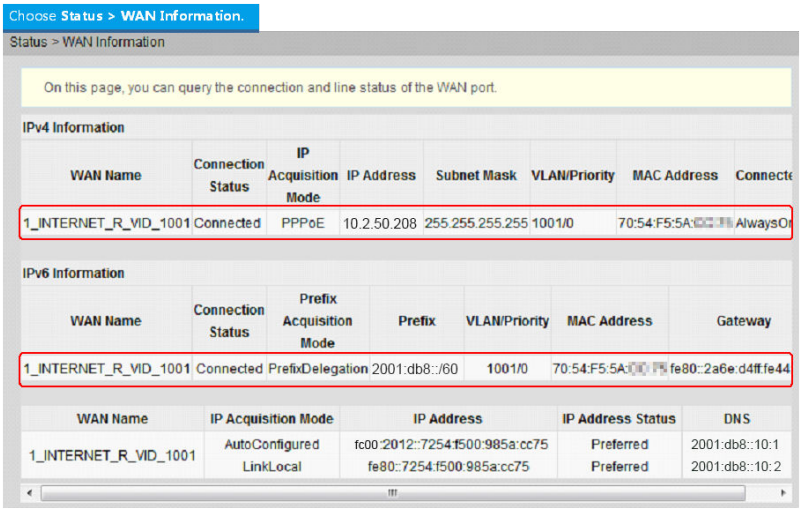
c. Configure the LAN-side address.



NOTE

- **Address/Prefix assignment mode** indicates the IP address and prefix assignment mode on the LAN-side host. Set it to **DHCPv6** when the assignment mode is DHCPv6 (stateful); set it to **SLAAC** when the assignment mode is ND (stateless). The SLAAC mode is recommended.
- **Other information assignment mode** indicates the assignment mode for the IPv6 address in payloads of packets such as DNS packets. Set it to **DHCPv6** when the assignment mode is DHCPv6 (stateful); set it to **SLAAC** when the assignment mode is ND (stateless). The DHCPv6 mode is recommended.

d. Check the ONT connection status.



3.4.4.3 Configuring the IPv6 Internet Access Service Using OLT Commands (DS-Lite)

This topic describes how to configure the IPv6 Internet access service using OLT commands when the DS-Lite solution is used and the ONT is a gateway-type ONT.

Prerequisite

- The Layer 2 service flow channel between the OLT and ONT is available by running the OLT command.

- The OLT is connected to the BRAS.
- Related configurations are performed on the BRAS according to the authentication and accounting requirements for dialup users. For details about the configurations, see the configuration guide.
- The VLAN of the port on the LSW that connects to the OLT must be the same as that of the upstream port on the OLT.

Application Context

Networking description:

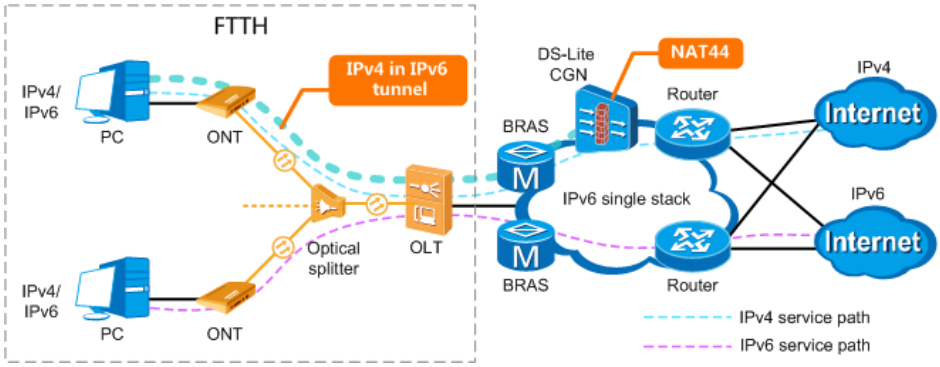
- The BRAS assigns an IPv6 prefix (not an IPv4 address) and the URL address of the DS-Lite CGN gateway to the ONT.
- The ONT assigns an IPv4 private address and IPv6 address to a PC.
- IPv6 packets are forwarded directly by the ONT, OLT, and BRAS.
- IPv4 packets are encapsulated into IPv6 packets on the ONT and sent to the DS-Lite CGN. The DS-Lite CGN decapsulates the packets, performs NAT44 translation on the packets, and then forwards them to the IPv4 Internet.
- The OLT implements Layer 2 forwarding. Only IPv6 service flows need to be added.

Device reconstruction:

- The ONT needs to be upgraded to support DS-Lite.
- Devices such as OLT and BRAS in the downstream of the DS-Lite CGN need to be upgraded to support the IPv6 single stack.
- The DS-Lite CGN device needs to be deployed.

Figure 3-18 shows the DS-Lite networking diagram.

Figure 3-18 DS-Lite networking diagram



Typical Configuration

3.4.4.3 Configuring the IPv6 Internet Access Service Using OLT Commands (DS-Lite) describes the typical IPv6 prefix and address configuration. This configuration has the best compatibility and can be applied to any scenarios.

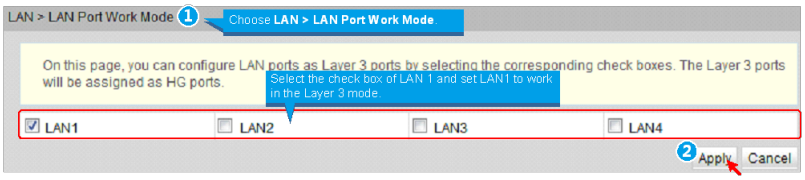
Table 3-24 Typical IPv6 prefix and address configuration

Item	Parameter on Web Page	Recommended Value	Remarks
IP address acquisition mode on the ONT WAN side	IP acquisition mode	Auto	-
Prefix acquisition mode on the ONT WAN side	Prefix acquisition mode	DHCPv6–PD	-
Address/prefix assignment mode for the LAN-side PC	Address/Prefix assignment mode	SLAAC	Currently, the Windows XP OS does not support the DHCPv6 address/ prefix assignment mode.
Other information assignment mode for the LAN-side PC	Other information assignment mode	DHCPv6	Other information refers to the IPv6 address in payloads of packets such as DNS packets. Currently, no OS supports the SLAAC assignment mode.

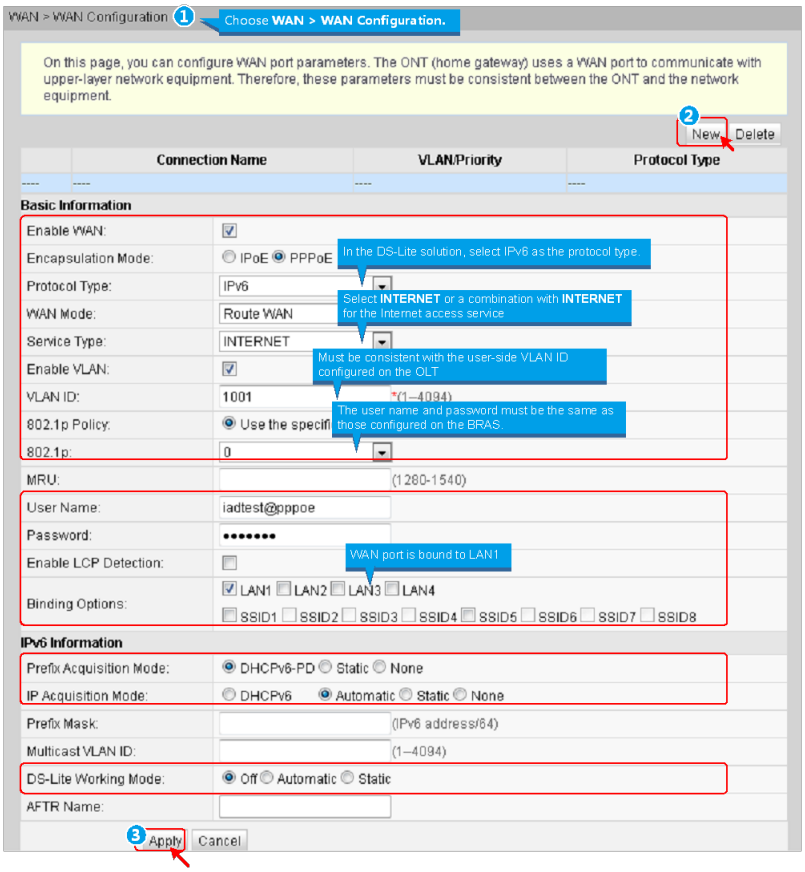
Procedure

- Configurations on the ONT:
  a. Configure the working mode of a LAN port.

     The LAN port bound to the WAN port must work in the Layer 3 mode. Therefore, set the working mode to Layer 3 for the LAN port connected to the PC.

  b. Configure IPv6 parameters for a WAN port.

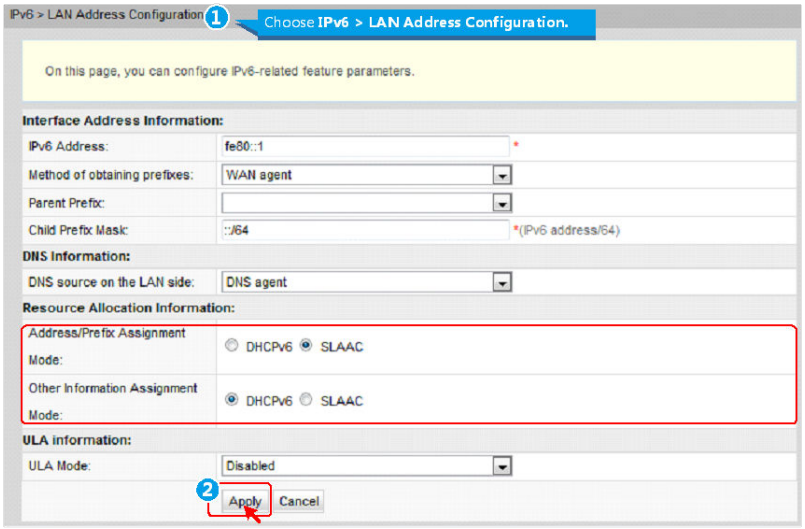


NOTE

The ONT supports only one IPv6 (single-stack or dual-stack) Internet WAN port.

In the DS-Lite solution, the setting rules for **Prefix acquisition mode** and **IP acquisition mode** are the same as those for the dual stack solution, except that the DS-Lite function needs to be enabled. When **DSLite work mode** is set to **Static**, you need to manually configure **AFTR Name** which must be the same as that configured on the BRAS.

c. Configure the LAN-side address.



NOTE

- **Address/Prefix assignment mode** indicates the IP address and prefix assignment mode on the LAN-side host. Set it to **DHCPv6** when the assignment mode is DHCPv6 (stateful); set it to **SLAAC** when the assignment mode is ND (stateless). The SLAAC mode is recommended.
- **Other information assignment mode** indicates the assignment mode for the IPv6 address in payloads of packets such as DNS packets. Set it to **DHCPv6** when the assignment mode is DHCPv6 (stateful); set it to **SLAAC** when the assignment mode is ND (stateless). The DHCPv6 mode is recommended.

d. Check the ONT connection status.

In the right pane, only the IPv6 information is displayed. No IPv4 address is obtained. The IPv6 connection status is connected, and the obtained IPv6 address is displayed in the **IP Address** column.