

10 Layer 2 Forwarding

[10.1 MAC Address Management](#)

MAC address management is a basic Layer 2 management feature.

[10.2 VLAN](#)

Virtual local area network (VLAN) is a technology used to form virtual workgroups by logically grouping the devices of a LAN. The VLAN management feature facilitates carriers' service planning.

[10.3 Service Flow](#)

[10.4 Service Port Bundle](#)

[10.5 Layer 2 Forwarding Policy](#)

[10.6 Layer 2 User Bridging](#)

Layer 2 user bridging implements Layer 2 data exchange among users under the same MA5800.

10.1 MAC Address Management

MAC address management is a basic Layer 2 management feature.

10.1.1 What Is MAC Address Management

Definition

MAC address management is a basic Layer 2 management feature that enables system administrators to use the functions listed in the following table.

Table 10-1 Sub-functions of MAC address management

Sub-function of MAC Address Management	Description	Remarks
Setting the MAC address aging time	After a system administrator sets the MAC address aging time, the system periodically checks for aged dynamic MAC addresses. If the system detects no packets, whether sent or received, carrying specified source MAC addresses within one or two times of the aging time, the system deletes the MAC address from the MAC address table.	The system saves the MAC address table in its buffer. MAC address entries specify the mapping between the MAC addresses of device ports, port numbers, and VLAN IDs. When forwarding frames, the system consults the MAC address table according to the destination MAC addresses and VLAN IDs of these frames and quickly identifies the egress for them. This function prevents frame broadcast. MAC addresses in a MAC address table can be either manually configured or dynamically learned by the system.
Limiting the number of learnable dynamic MAC addresses	The system allows the system administrator to configure the number of learnable dynamic MAC addresses on a port or a service flow. When the number of learned MAC addresses reaches the maximum number, the port or service flow does not learn any new MAC addresses.	None
Setting the static MAC address	To connect a port to a device with a specified MAC address, the system administrator configures a static MAC address and VLAN on a port or configure a static MAC address on a service port. The system then forwards data according to this static MAC address.	None

Benefits

Benefits for Carriers

- The system ages dynamic MAC addresses to ensure timely updates of the MAC address table. If the MAC address table is full and not updated, the system will fail to learn new MAC addresses and will consequently fail to forward data.

- By limiting the number of learnable dynamic MAC addresses, the system administrator can limit the number of MAC addresses that can be used to enter the network and hence alleviate the load of network devices.
- By configuring static MAC addresses, the system administrator prohibits unauthorized users from accessing the system.

NOTE

- If a malicious user sets source MAC addresses of attack packets to the MAC addresses of authorized users and accesses the system through another port on the device, the device learns an incorrect MAC address entry and forwards to the malicious user the packets that were originally destined to an authorized user. To avoid this situation, the system administrator can manually add specific MAC address entries to the MAC address table to bind user devices to ports. This operation protects user data from MAC spoofing and enhances port security. The manually added MAC address entries (static MAC address entries) have higher priorities than automatically generated MAC address entries.
- The static MAC addresses, however, do not automatically update according to network device changes. The system administrator needs to modify the static MAC addresses manually. Using a large number of MAC addresses will require higher costs for network maintenance.

Benefits for Subscribers

Improved user security: After the system administrator sets the static MAC address of a service port and sets the maximum number of learnable MAC addresses to 0, the port receives only user data carrying the specified static MAC address.

10.1.2 MAC Address Management Process

MAC address management includes MAC address table establishment and management

Establishing MAC Address Tables

The system establishes a MAC address table by learning source MAC addresses or after users configure static MAC address entries.

- **MAC address learning**
 - When the OLT functions as a Layer 2 switching device, it learns MAC addresses in the distributed mode. Specifically, each board learns the source MAC address of packets sent from the board of its own and then forwards packets according to their destination MAC addresses. The learned MAC addresses are stored in the system buffer. Generally, the system buffer can hold a limited number of MAC address entries. If all these entries are filled in, no more MAC addresses can be learned.
 - Configuration command: **mac-address learning**

NOTE

The MAC address learning function takes effect only for unicast MAC addresses, but not for multicast or broadcast MAC addresses.

- **Configuration of static MAC address entries**
 - A user can manually configure static MAC address entries in which user device MAC addresses are bound to ports. After this configuration, the packets whose MAC addresses are included in the MAC address entries

are always forwarded through the bound ports. This configuration improves the efficiency for forwarding packets and improves the security of ports because it denies access from unauthenticated users. This method of establishing MAC address tables is widely used in private networks.

 NOTE

The same static MAC address can be configured on an upstream port belonging to different VLANs.

- Configuration command: **mac-address static**

The following table shows an example of a simplified MAC address table established by configuring static MAC address entries. The table lists the mapping between MAC addresses, ports, and VLAN IDs.

Table 10-2 Simplified MAC address table

VLAN ID	MAC Address	Port Number	MAC Address Attribute	Forwarding Attribute
2	00e0-fc00-0011	0/1/1	Dynamic	Forward
3	00e0-fc00-0033	0/1/2	Static	Forbid

Managing MAC Address Tables

When managing MAC address tables, users can configure MAC-related attributes as allowed by system resources and network security policies against potential risks. The optimized MAC address tables can better meet requirements of a live network. These MAC-related attributes are as follows:

- **Maximum number of MAC addresses learned based on service flows**

- After the number of access users reaches the limit, no new access user addresses will be learned. This attribute setting applies to networks, such as residential access networks and low-security internal enterprise networks, that have fixed access users but are not sufficiently secure.

 NOTE

- The maximum number of MAC addresses is independent of the number of manually added static MAC addresses.
- After a static MAC address is configured for a user port and the maximum number of learnable dynamic MAC addresses is set to 0, the port receives only packets that contain the configured static MAC address. In this case, the MAC address is bound to the port. This attribute setting helps improve user data security.
- Specifically, after a service flow is added to a bundle, the system uses the maximum number for the bundle as that for the service flow. The maximum number of learnable MAC addresses for the entire bundle is the same as that for each service flow in the bundle. When the maximum number for any service flow in a bundle changes, the maximum number for each bundle and that for each service flow in the bundle change as

well. The sum of MAC addresses learned for each service flow in a bundle cannot exceed the maximum number of learnable MAC addresses for the bundle.

- Configuration command: **mac-address max-mac-count**

- **Setting the function of sensing excess MAC addresses**

When a lot of MAC addresses are learnt by the system, it is difficult for trouble locating. When the function of sensing excess MAC addresses is enabled, the system queries MAC addresses every 15 minutes and determines whether an alarm needs to be reported according to the query result. If the query result exceeds the upper threshold for sensing excess MAC addresses set by users, an excess MAC address alarm is generated. If the query result is smaller than the lower threshold for sensing excess MAC addresses set by users, a fault clearing alarm is generated.

Configuration command: **overload-aware mac-address**

- **MAC address aging**

Generally, the system automatically establishes a MAC address table by learning source MAC addresses. The system can age out dynamic MAC addresses. When the system does not receive packets from or send packets to a device within a specified period, the system deletes the MAC address entry of the device from the MAC address table. The established MAC address table has to be updated according to network changes. However, after the network topology changes, the dynamic MAC address entries will not be automatically updated in a timely manner. Then the system cannot learn more MAC addresses and user data cannot be forwarded as expected. MAC address aging is intended to resolve the issue.

 NOTE

Disable MAC address aging if no MAC address aging issue has occurred.

The MAC address learning function can be configured for the control board and service boards separately.

Item	Description	Configuration Command
Specify the aging time of a MAC address	After a system administrator sets the MAC address aging time, the system periodically checks for aged dynamic MAC addresses. If the system detects no packets, whether sent or received, carrying specified source MAC addresses within one or two times of the aging time, the system deletes the MAC address from the MAC address table. Then the system creates another MAC address table by learning MAC addresses.	mac-address timer

Item	Description	Configuration Command
Sets the aging mode for a MAC address	After you set the MAC address aging mode, the control board and service board age MAC addresses accordingly. • Bidirectional aging mode: The system ages MAC address entries according to the source MAC address learning and receiving of packets destined for this MAC address. Specifically, if the system neither learns a source MAC address nor receives packets destined for this MAC address within an aging period, the system ages the MAC address entry. Bidirectional aging helps reduce the CPU usage required for aging and learning MAC addresses. • Unidirectional aging mode: The system ages MAC address entries according to the source MAC address learning. Specifically, if the system does not learn a MAC address again within an aging period, the system ages the MAC address entry.	mac-address aging-mode

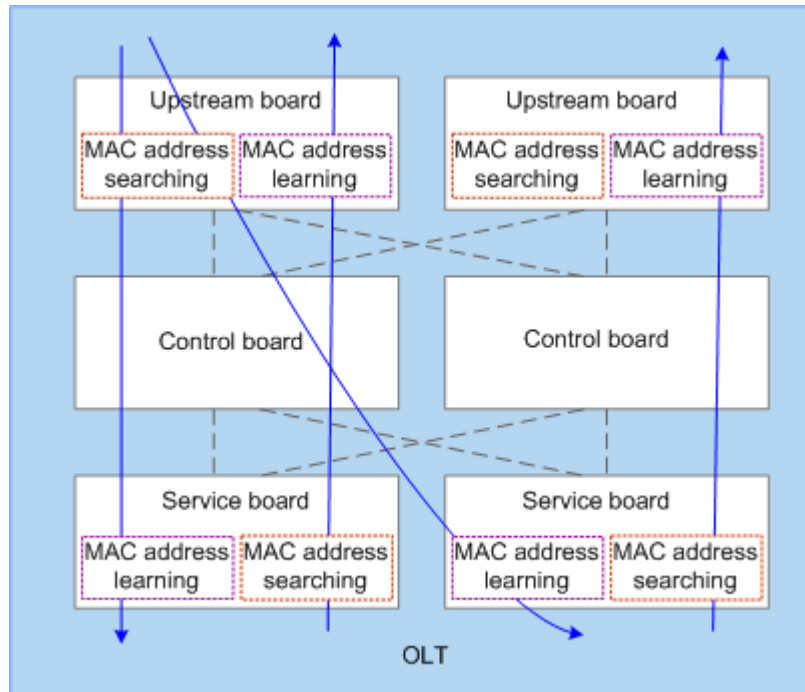
 NOTE

- MAC address hash conflict: HASH algorithm is an algorithm commonly used by the forwarding chip in order to accelerate finding forwarding entries. Based on VLAN + MAC forwarding mode, the system make the hash operation on VLAN + MAC address by a HASH algorithm when learning the MAC address to get a hash leaky bucket index. If the number of MAC address table entries of the leaky bucket corresponding to the index has reached the maximum, this MAC address that is operated would not be learned by the system. It is called to generate MAC address hash conflict. (The number of MAC address table entries in each leaky bucket is fixed. It may be different for different control board).
- The system uses the hash algorithm to calculate MAC address tables, so a hash conflict issue may occur.

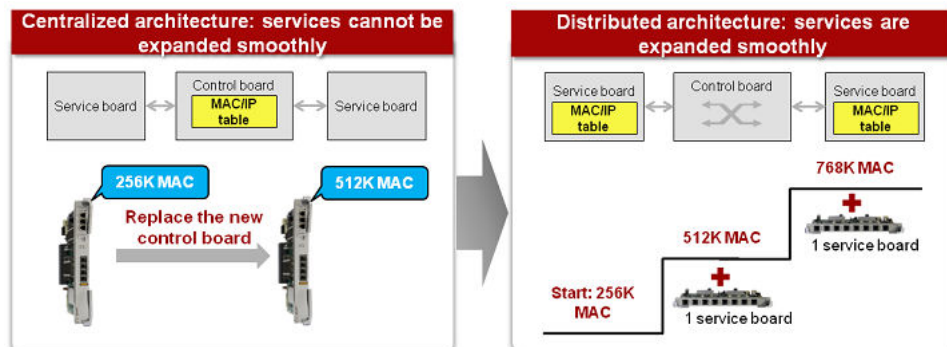
10.1.3 Smooth MAC Address Expansion

The MA5800 is designed in distributed architecture. Compared with devices in centralized architecture, MAC addresses of the MA5800 can be smoothly expanded.

The MA5800 learns and forwards MAC addresses as an entire system. Specifically, its egress board learns MAC addresses and its ingress board finds and forwards MAC addresses.



Compared with devices in centralized architecture, the MA5800 has the following advantages:



- Centralized architecture:
 - MAC address learning and forwarding are performed on the control board. For any MAC address expansion, the control board needs to be replaced.
 - In the initial stage of network construction, usage of the control board having high specifications is costly.
- Distributed architecture:
 - MAC address expansion is implemented by service board expansion but the control board does not need to be replaced.
 - MAC addresses are expanded smoothly, meeting customer requirements in different stages.

10.2 VLAN

Virtual local area network (VLAN) is a technology used to form virtual workgroups by logically grouping the devices of a LAN. The VLAN management feature facilitates carriers' service planning.

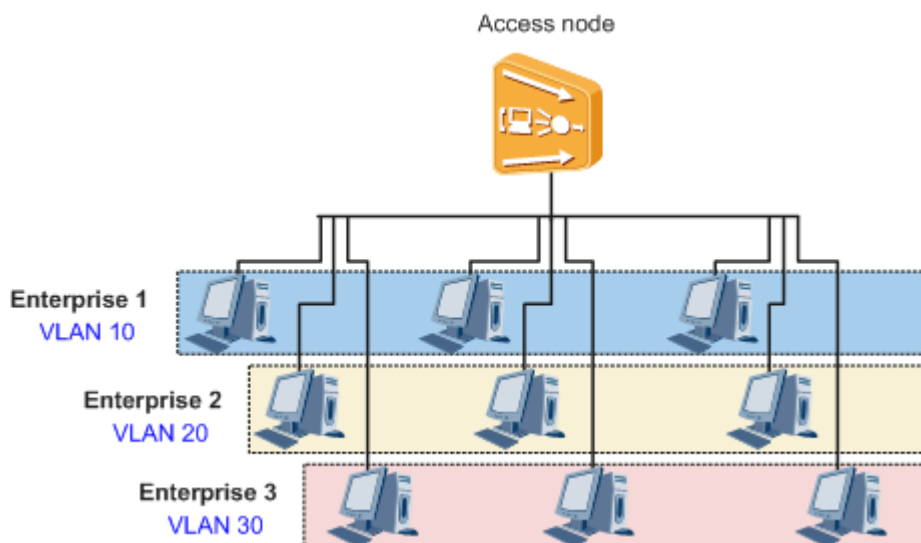
10.2.1 What Is VLAN

VLAN is a communications technology that divides a physical LAN into multiple logical broadcast domains (multiple VLANs). NEs in a VLAN can communicate with each other but NEs in different VLANs cannot.

VLAN allows packets to be broadcast only within a single VLAN, preventing bandwidth waste caused by broadcast storms. Furthermore, VLAN enhances network security, because NEs in different VLANs cannot communicate with each other directly.

For example, for users of different enterprises in the same office building, it is too costly to build separate LANs for each enterprise, and insecure if the enterprises are to share the existing LAN of the building. VLAN resolves this dilemma.

Figure 10-1 VLAN application

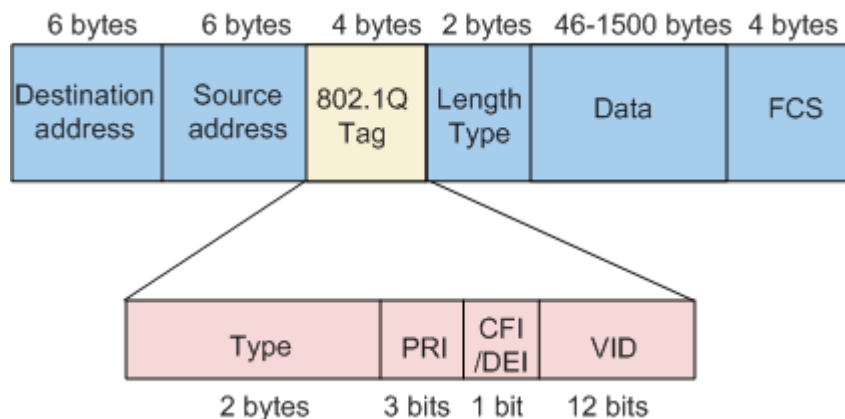


Make different enterprise users belonging to different VLANs. In this way, the enterprise users share the LAN facilities and at the same time each have their own secure networks.

10.2.2 VLAN Basic Concepts

802.1Q Frame Format for a VLAN

The format of Ethernet frames is modified in the IEEE 802.1Q standard. Specifically, a 4-byte 802.1Q tag is inserted between the source MAC address field and the protocol type field, as shown in the following figure.

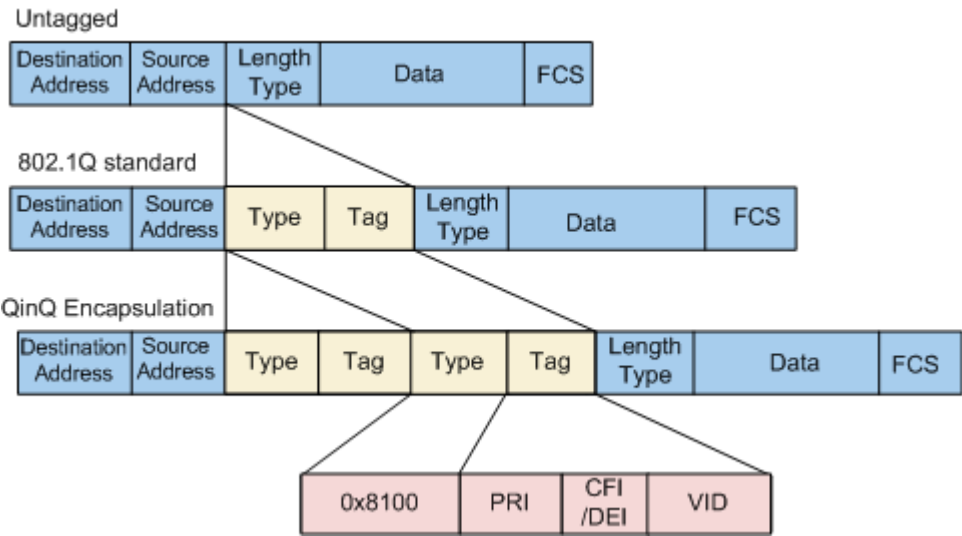
Figure 10-2 802.1Q frame format for a VLAN

The 802.1Q tag consists of four fields:

- **Type**
The Type field is 2 bytes long and indicates the frame type. The value 0x8100 of this field indicates that the frame carries an 802.1Q tag. Such a frame will be discarded if the receiving device does not support 802.1Q.
- **PRI**
The PRI field is 3 bits long and indicates the frame priority. It ranges from 0 to 7. The larger the value, the higher the priority. In case of network congestion, the system preferentially sends data frames with a higher priority.
- **CFI/DEI**
It is 1 bit long.
 - The CFI field indicates whether the MAC address is in canonical format. CFI 0 indicates that the MAC address is in the canonical format and CFI 1 indicates a non-canonical format. It is used to differentiate Ethernet frames, fiber distributed digital interface (FDDI) frames, and token ring frames. In an Ethernet network, CFI is 0.
 - The DEI field consists of one bit and represents the drop eligible indicator defined in the 802.1ad protocol. It is used to color the packet.
- **VID**
VID is the shortened form of VLAN ID. It is 12 bits long and indicates the VLAN to which a frame belongs.

PRI, CFI, and VID together are called a VLAN tag, which is the basis for VLAN communication. Frames that do not contain an 802.1Q tag are called untagged frames. 802.1Q frames in QinQ encapsulation have two 802.1Q tags. The following figure shows the structures of untagged frames, standard 802.1Q frames, and 802.1Q frames in QinQ encapsulation.

Figure 10-3 Structure comparison between untagged frame, standard 802.1Q frame, and 802.1Q frame in QinQ encapsulation



VLAN Types

Table 10-3 VLAN types

VLAN Type	The same points	Difference
Standard VLAN	- Ethernet ports in different VLANs are isolated from each other. - Ethernet ports can be communicated with each other. - A VLAN contains multiple upstream ports.	A standard VLAN does not contain a service port.
Smart VLAN		- A smart VLAN contains multiple service ports. - Service ports in a smart VLAN are isolated from each other. A VLAN provides access for multiple users and therefore saves VLAN resources.
MUX VLAN (Multiplex vlan)		- A MUX VLAN contains only one service port. - A service port in a MUX VLAN is isolated from a service port in another MUX VLAN.
Super VLAN	The super VLAN is based on Layer 3. A super VLAN can contain multiple sub VLANs. The type of the sub VLAN can be smart VLAN or MUX VLAN. The sub VLANs can communicate with each other by ARP proxy. The sub VLAN forwards the service at Layer 3 centrally by the Layer 3 interface of the super VLAN. A super VLAN aggregates Smart VLAN or MUX VLANs. For details, see 10.2.4 VLAN Aggregation (Super VLAN).	

The Smart VLAN restricts visits between users by isolating the service flows or service ports in the same VLAN.

The MUX VLAN realizes user isolation by dividing the user service flows or service ports into different VLANs.

VLAN Attributes

Table 10-4 VLAN Attributes

Attribute	Description	Services Supported by Service Flows Inside the VLAN	Transparent Transmission Capability
Common	A VLAN with the common attribute supports only one-tagged VLANs. This VLAN is used as a common Layer 2 VLAN. If it is used for Layer 3 forwarding, it needs a VLAN interface.	Supports DHCP Option82, DHCP Layer 2 relay, DHCP Layer 3 relay, PITP (PPPoE+), MAC anti-spoofing, IP anti-spoofing, IPTV, and ARP proxy.	Transparent transmission by hardware is general. The service board does not support transparent transmission by hardware for service flows having common and stacking VLANs and it captures DHCP, PPP, and IGMP packets globally (if the related features are enabled on a VLAN).
Stacking	A VLAN with the stacking attribute supports only two-tagged VLANs. Both the outer VLAN tag and inner VLAN tag of a stacking VLAN are allocated by the MA5800, which are used for dual VLAN authentication for the upper-layer BRAS and provide the wholesale service for the ISP.		
QinQ	A VLAN with the QinQ attribute supports one-tagged or multi-tagged VLANs, which is mainly used in transparent transmission and private line scenarios. If a multi-tagged VLAN is used, both the outer VLAN tag and inner VLAN tag are allocated on the MA5800. If a three-tagged VLAN is used, user-side packets carry one-tagged VLAN and the MA5800 adds the two-tagged VLAN.	Does not support DHCP Option82, DHCP Layer 2 relay, DHCP Layer 3 relay, PITP (PPPoE+), MAC anti-spoofing, IP anti-spoofing, IPTV, or ARP proxy.	Transparent transmission by hardware is powerful cause the service board supports transparent transmission by hardware for service flows having QinQ VLANs.

NOTE

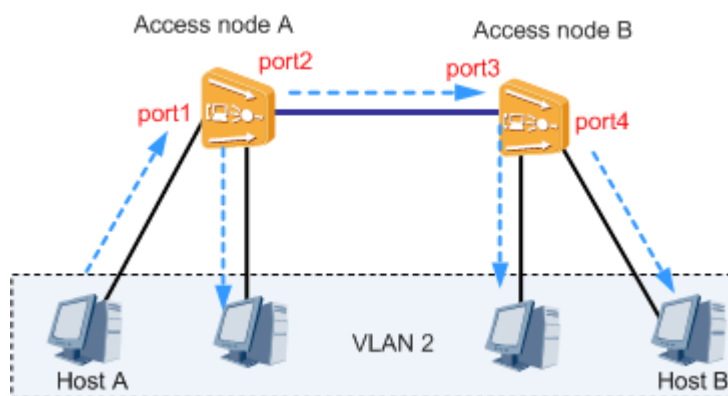
For details about QinQ VLANs and stacking VLANs, see [10.2.5 QinQ VLAN and Stacking VLAN](#).

10.2.3 VLAN Communication Principle

Intra-VLAN Communication Principle

Users in a VLAN can communicate with each other. An access node implements the communication by distinguishing between the VLAN tags carried in Ethernet frames. In the following figure, there are 4 hosts in VLAN 2, and uses the example of host A and host B to illustrate communication inside a VLAN.

Figure 10-4 Intra-VLAN communication



1. Host A sends Ethernet frames to port 1 of access node A.
2. Port 1 of access node A attaches a VLAN tag (VID is filled in with VLAN 2) to the Ethernet frames.
3. Access node A sends the tagged Ethernet frames to ports (except port 1) that belong to VLAN 2.
4. Port 2 of access node A sends the tagged Ethernet frames to port 3 of access node B.
5. Access node B identifies the VLAN tag (VLAN 2) carried in the Ethernet frames and sends these frames to all ports of access node B that belong to VLAN 2.
6. Port 4 of access node B sends these Ethernet frames to host B.

Inter-VLAN Communication Principle

Hosts in different VLANs cannot communicate with each other at Layer 2. If these hosts need to communicate with each other, they need IP routes. The MA5800, serving as a Layer 3 switch, supports communication between hosts in different VLANs.

To ensure that the Layer 3 switch can transmit the data flow for the first time, the routing table must have correct routing entries. Therefore, configuring a Layer 3

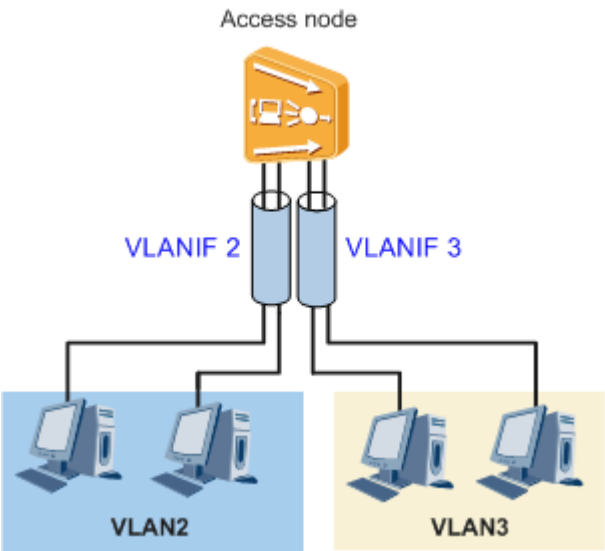
interface and a routing protocol on the Layer 3 switch is required. A VLANIF interface is a Layer 3 logical interface and its IP address can be manually specified.

 NOTE

Layer 3 switching combines routing and switching technologies to implement routing inside a switch, thereby improving the performance of the entire network. After using the routing table to send the first data flow, a Layer 3 switch generates ARP table for MAC addresses and IP addresses. When the ARP entry exists for the corresponding destination IP, the system directly finds the out port by the ARP table entries and translates the destination MAC address, source MAC address, and VLAN.

In the following figure, the access node supports both VLAN 2 and VLAN 3. In this scenario, VLAN interface 2 and VLAN interface 3 can be created on the switch. After IP addresses and correct routes are configured for these two VLAN interfaces, VLAN 2 can communicate with VLAN 3.

Figure 10-5 Inter-VLAN communication



Default VLAN of an Upstream Port

The default VLAN (port default VLAN ID, or PVID) of a port is also called a native VLAN. If a default VLAN is configured on an Ethernet port, the processing rule of Ethernet port for different VLAN tag in sent packets is shown as follows.

Table 10-5 The processing rule of Ethernet port for different VLAN tag in received packets

VLAN Tag in Sent Packets on An Ethernet Port	Processing Rule of Ethernet port
Untagged	The Ethernet port tags the packets with the default VLAN before forwarding them.

VLAN Tag in Sent Packets on An Ethernet Port	Processing Rule of Ethernet port
VLAN ID is the same as the default VLAN ID	The Ethernet port removes the VLAN tag from the packets before forwarding them.
VLAN ID is different from the default VLAN ID	The Ethernet port directly forwards these packets with the VLAN tag unchanged.

 NOTE

If the MA5800 connects to an upper-layer router, packets sent by the router may or may not carry a VLAN tag, depending on whether the router can identify a VLAN tag. The default VLAN can be configured on the upstream port of the MA5800 to adapt the router.

10.2.4 VLAN Aggregation (Super VLAN)

Context

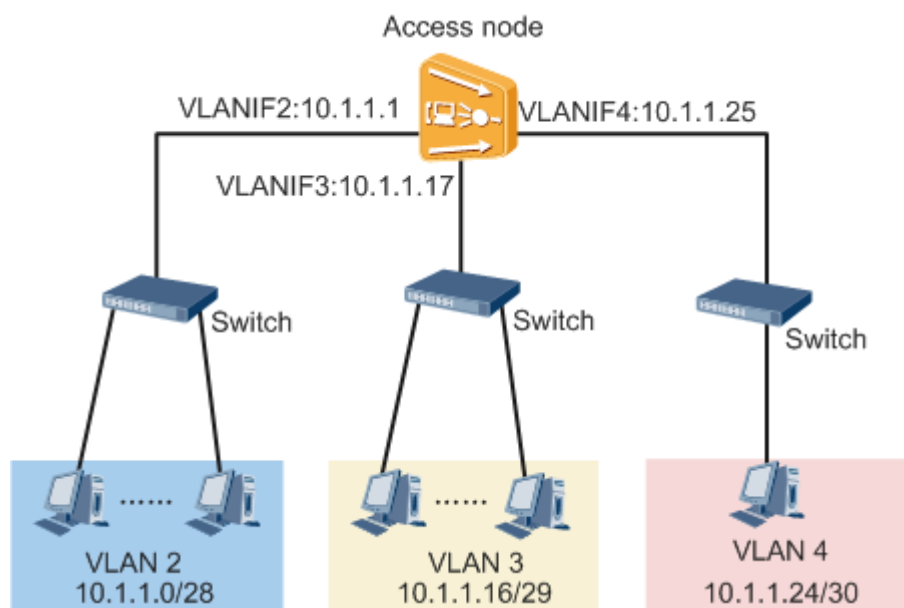
VLAN is widely applied to switching networks because of its flexible control of broadcast domains and convenient deployment. On a Layer-3 switch, interconnection between broadcast domains is implemented using one VLAN to correspond to a single Layer-3 logical interface. However, such an implementation may lead to inefficient use of IP addresses. VLAN aggregation, also known as a super VLAN, can solve this problem.

 NOTE

Here takes an example of host address assignment in VLANs to show the inefficient use of IP addresses.

Example

The following figure shows a typical VLAN planning.

Figure 10-6 Typical VLAN planning**Table 10-6** Example of host address assignment in VLANs

VLAN	Subnet	Gateway Address	Number of Available Addresses	Number of Available Hosts	Actual Requirements
2	10.1.1.0/28	10.1.1.1	14	13	10
3	10.1.1.16/29	10.1.1.17	6	5	5
4	10.1.1.24/30	10.1.1.25	2	1	1

As shown in the preceding table,

- VLAN 2 requires 10 host addresses. Subnet 10.1.1.0/28 with a mask of 28 bits is assigned to VLAN 2. Here, 10.1.1.0 is the subnet address, and 10.1.1.15 is the directed broadcast address. These two addresses cannot be used as the host address. In addition, as the default gateway address of the subnet, 10.1.1.1 cannot be used as the host address, either. The other 13 addresses ranging from 10.1.1.2 to 10.1.1.14 can be used by the hosts. In this way, although VLAN 2 needs only 10 addresses, 13 addresses need to be assigned to it according to the subnetting principle.
- VLAN 3 requires five host addresses, and subnet 10.1.1.16/29 with a mask of 29 bits needs to be assigned to VLAN 3. VLAN 4 requires only one address, and subnet 10.1.1.24/30 with a mask of 30 bits needs to be assigned to VLAN 4.

 NOTE

Directed broadcast address: In a network divided into different subnets, data packets are sent to all hosts in a subnet after a directed broadcast address is specified as the destination address of the packets. Subnet directed broadcasting is usually used to obtain data of a host in a subnet, such as the neighboring relationship.

In the above example, only 16 (10+5+1) addresses are actually required for all the VLANs. The VLAN planning, however, needs 28 (16+8+4) addresses according to the common VLAN addressing principle, even if the optimal addressing scheme is used. Therefore, nearly half of the addresses will be wasted. In addition, if VLAN 2 is accessed by only three hosts instead of ten, the remaining addresses will also be wasted because such addresses cannot be used by other VLANs.

This addressing plan is inconvenient for future network upgrades and expansion. If VLAN 4 needs addition two hosts and does not want to change the assigned IP addresses, and the addresses after 10.1.1.24 has been assigned to others, a new sub network with the mask length as 29 bits and a new VLAN need to be assigned for the new users of VLAN 4. As a result, VLAN 4's customers only have three hosts, but the customers are assigned to two different subnets in separate VLANs, which makes network management difficult.

In the above example, several IP addresses are used as subnet addresses, subnet directed broadcast addresses, and default addresses of subnet gateways. Such IP addresses cannot be used as host addresses in the VLAN. This address assigning mechanism greatly reduces addressing flexibility and causes address usage waste. VLAN aggregation is developed to resolve these issues.

Principle

VLAN aggregation, divides a physical network into broadcast domains by using VLANs so that different VLANs can belong to the same subnet. VLAN aggregation consists of two basic concepts, super VLAN and sub VLAN.

- **Super VLAN:** Super VLANs differ from common VLANs. In super VLANs, only Layer 3 interfaces are created and physical ports are not involved. A super VLAN can be regarded as a logical Layer 3 collection of many sub VLANs.
- **Sub VLAN:** Sub VLANs are used to isolate broadcast domains. In sub VLANs, only physical ports are contained and Layer 3 VLAN interfaces cannot be created. The Layer 3 switching between a sub VLAN and the external network is implemented through the Layer 3 interface of the super VLAN.

A super VLAN can contain one or more sub VLANs, each sub VLAN with different broadcast domains. The sub VLAN does not occupy an independent subnet segment. In the same super VLAN, IP addresses of hosts belong to the super VLAN's subnet segment, regardless of the mapping between hosts and sub VLANs.

The same Layer 3 interface is shared by sub VLANs, allowing fewer subnet IDs, default gateway addresses of the subnet, and directed broadcast addresses of the subnet to be used. In the mean time, different broadcast domains can use the unused addresses in the same subnet segment. As such, addressing becomes flexible and efficient.

 NOTE

The following still uses [Table 10-6](#) as an example to explain the implementation principle of VLAN aggregation.

Example

Supposing that user demands are the same. In VLAN 2, ten host addresses are demanded; in VLAN 3, five host addresses are demanded; in VLAN 4, one host address is demanded.

Create VLAN 10 and configure VLAN 10 as a super VLAN. Then assign subnet address 10.1.1.0/24 with a mask of 24 bits to VLAN 10, where 10.1.1.0 is the subnet ID and 10.1.1.1 is the gateway address of the subnet, as shown in the following figure. The corresponding sub VLAN address assignment of VLAN 2, VLAN 3, and VLAN 4 is shown in [Table 10-7](#).

Figure 10-7 VLAN aggregation schematic diagram

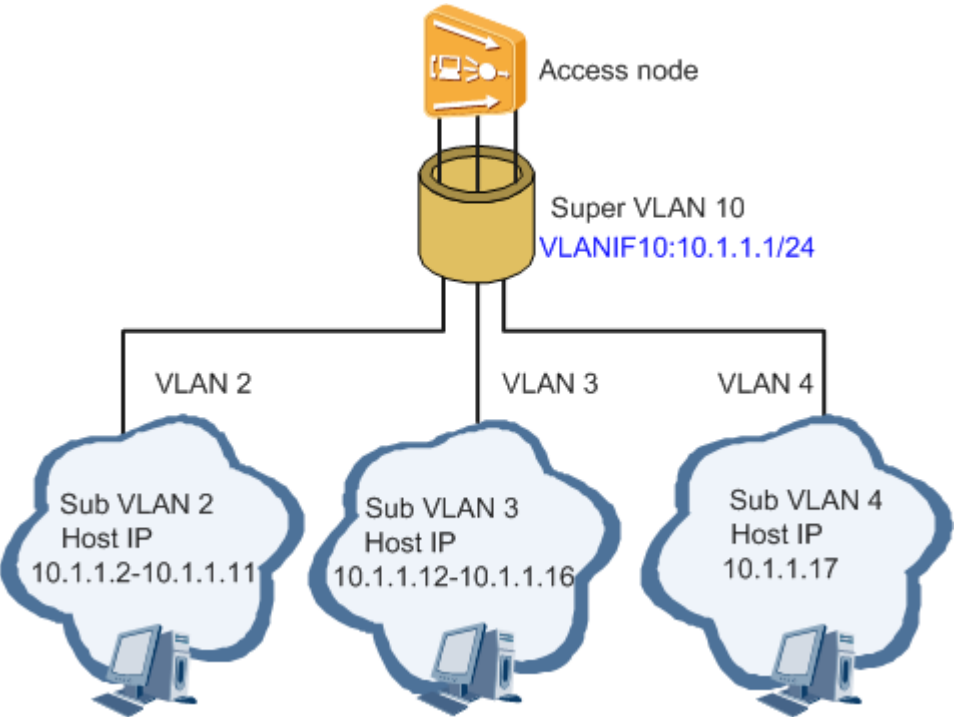


Table 10-7 Example of host address assignment in VLAN aggregation mode

VLAN	Subnet	Gateway Address	Number of Available Addresses	Available Addresses	Actual Requirements
2	10.1.1.0/24	10.1.1.1	10	10.1.1.2-10.1.1.11	10
3			5	10.1.1.12-10.1.1.16	5
4			1	10.1.1.17	1

In VLAN aggregation, sub VLANs are not divided according to the previous subnet border. Instead, their addresses are flexibly assigned among the super VLAN's

subnets according to the required number of hosts. VLAN 2, VLAN 3, and VLAN 4 share a subnet (10.1.1.0/24), a default gateway address of the subnet (10.1.1.1), and a directed broadcast address of the subnet (10.1.1.255). In this manner, the subnet ID (10.1.1.16, 10.1.1.24), the default gateway of the subnet (10.1.1.17, 10.1.1.25), and the directed broadcast address of the subnet (10.1.1.15, 10.1.1.23, and 10.1.1.27) can be used as host IP addresses.

In total, 16 addresses (10+5+1) are required for the three VLANs. In practice, in this subnet, a total of 16 addresses (10.1.1.2 to 10.1.1.17) are assigned to the three VLANs. A total of 19 IP addresses are used, that is, the 16 host addresses together with the subnet ID (10.1.1.0), the default gateway of the subnet (10.1.1.1), and the directed broadcast address of the subnet (10.1.1.255). In the network segment, 236 addresses (255 - 19) are available, which can be used by any host in the sub VLAN.

Communication Between Sub VLANs

VLAN aggregation ensures that different VLANs can use the IP addresses in the same subnet segment; however, this leads to an issue with Layer 3 forwarding between sub VLANs.

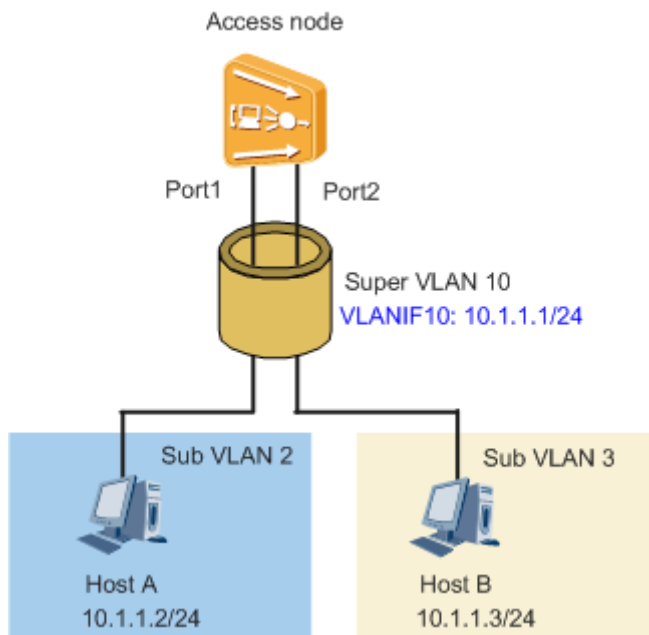
In common VLAN mode, the hosts of different VLANs can communicate with each other based on Layer 3 forwarding through their respective gateways. In VLAN aggregation mode, however, hosts in a super VLAN use IP addresses in the same network segment and share the same gateway address. Since hosts in different sub VLANs belong to the same subnet, they communicate with each other based on Layer 2 forwarding, not Layer 3 forwarding through a gateway. As a result, hosts in different sub VLANs cannot communicate with each other because the hosts are separated at Layer 2.

The Address Resolution Protocol (ARP) proxy resolves this issue.

- **Layer 3 communication between different sub VLANs**

As shown in the following figure, the super VLAN, namely, VLAN 10, contains two sub VLANs, VLAN 2 and VLAN 3.

Figure 10-8 Networking diagram of Layer 3 communication between different sub VLANs based on ARP proxy



Communication between host A in sub VLAN 2 and host B in sub VLAN 3 is implemented as follows:

NOTE

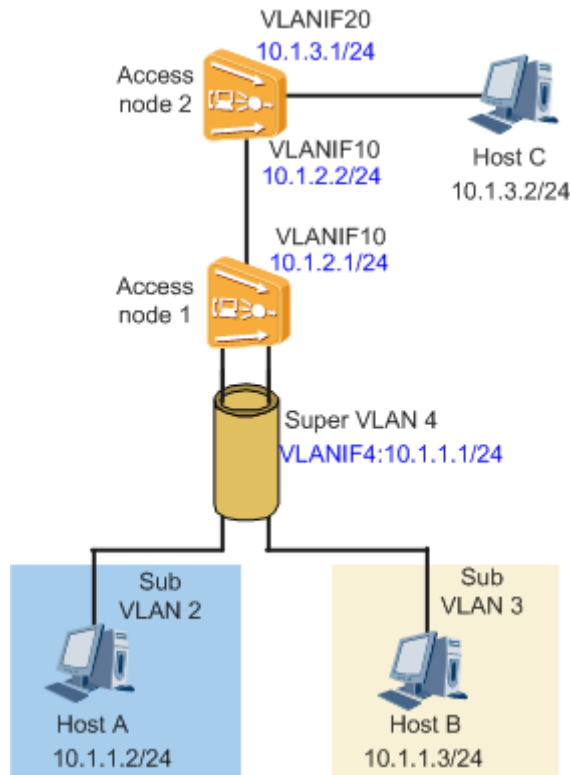
Suppose that host A's ARP table has no corresponding entry for host B, and the gateway between the sub VLANs is enabled with ARP proxy.

- After comparing the IP address (10.1.1.3) of host B with its own IP address, host A learns that both IP addresses are in the same network segment (10.1.1.0/24), and its ARP table has no entry corresponding to host B.
- Host A initiates ARP broadcasting to request host B's MAC address.
- Host B is not in the broadcast domain of sub VLAN 2, and cannot receive the ARP request.
- Since the gateway's ARP proxy is enabled between the sub VLANs, after receiving host A's ARP request, the gateway discovers that the IP address of host B (10.1.1.3) is the IP address of a directly-connected interface. The gateway then initiates ARP broadcasting to all other sub VLAN interfaces to request host B's MAC address.
- After receiving an ARP request, host B replies with an ARP response.
- After receiving host B's ARP response, the gateway replies to host A with the gateway's MAC address. Host A will regard this MAC address as host B's MAC address.
- The ARP tables in both the gateway and host A have entries corresponding to host B.
- To send packets to host B, host A initially sends packets to the gateway, and then the gateway performs Layer 3 forwarding to implement communication between host A and host B.

The process used by host B to send packets to host A works in the same way.

- **Layer 3 communication between a sub VLAN and an external network**

Figure 10-9 Networking diagram of Layer 3 communication between a sub VLAN and an external network



As shown in the preceding figure, access node 1 is configured with super VLAN 4, sub VLAN 2, sub VLAN 3, and common VLAN 10. Access node 2 is configured with two common VLANs, VLAN 10 and VLAN 20. Host A in sub VLAN 2 that belongs to the super VLAN 4 needs to access host C in access node 2.

NOTE

Suppose that access node 1 is configured with a route to network segment 10.1.3.0/24, and access node 2 is configured with a route to network segment 10.1.1.0/24.

- After comparing the IP address (10.1.3.2) of host C with its IP address, host A learns that two IP addresses are not in the same network segment 10.1.1.0/24.
- Host A initiates ARP broadcasting to its gateway, requesting the gateway's MAC address.
- After receiving the ARP request, access node 1 identifies the correlation between the sub VLAN and the super VLAN, and replies with an ARP response to host A through sub VLAN 2. The source MAC address in the ARP response packet is the MAC address of VLANIF4 of super VLAN 4.
- Host A learns the gateway's MAC address.
- Host A sends the packet to the gateway, the destination MAC address being the MAC address of VLANIF4 of super VLAN 4, and the destination IP address being 10.1.3.2.

- f. After receiving the packet, access node 1 performs Layer 3 forwarding and sends the packet to access node 2, with the next hop address 10.1.2.2, and the outgoing interface VLANIF10.
- g. After receiving the packet, access node 2 performs Layer 3 forwarding and sends the packet to host C through the directly-connected interface VLANIF20.
- h. The response packet from host C reaches access node 1 after access node 2 performs Layer 3 forwarding.
- i. After receiving the packet, access node 1 performs Layer 3 forwarding and sends the packet to host A through the super VLAN.

10.2.5 QinQ VLAN and Stacking VLAN

Introduction to QinQ

As Ethernet technology is deployed in more and more carrier networks (metro Ethernet networks), the standard VLAN defined in IEEE 802.1Q alone cannot completely distinguish between and isolate a large number of users. This is because the 12-bit VLAN tag field identifies a maximum of only 4096 VLANs. The 802.1Q-in-802.1Q (QinQ) technology is developed to solve this problem.

The QinQ technology improves VLAN utilization by adding another 802.1Q tag to a packet that already carries an 802.1Q tag. With this technology, the system supports up to 4096 x 4096 VLANs. QinQ allows two VLAN headers to be inserted into a single frame. Therefore, packets transmitted in the backbone network have two 802.1Q tag headers: a public network VLAN tag and a private network VLAN tag.

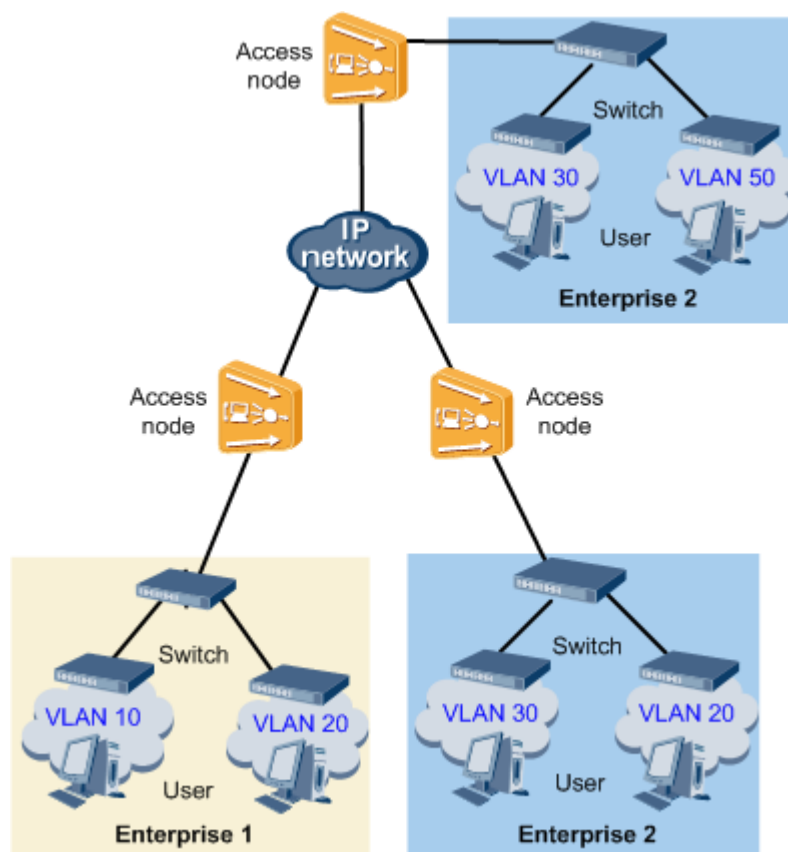
For details about the format of 802.1Q frames encapsulated by QinQ, see [10.2.2 VLAN Basic Concepts](#).

As metro Ethernet grows and a greater variety of services are deployed, there are more scenarios in which QinQ double tags can be applied.

- QinQ VLAN: Packets with two VLAN tags traverse carrier networks. The inner VLAN tag is transparently transmitted to the public network. QinQ VLAN is also a simple and practical VPN technology.
- Stacking VLAN: The inner tag indicates the user; the outer tag indicates the carrier.

QinQ VLAN

In the following network, enterprise 2 has two locations, which communicate through the carrier network (public network).

Figure 10-10 QinQ VLAN application

The access node provides the following configurations to deploy the QinQ VLAN so that enterprise 2 can communicate at two locations, but enterprise 1 and enterprise 2 cannot communicate with each other.

- The service VLAN is the same as the public network VLAN and the VLAN attribute is QinQ.
- The access node performs traffic classification for user packets based on service flows. Each user is mapped to one service flow. The inner and outer VLAN tags are configured for the service flows according to the VLAN plan in the following table.

Table 10-8 QinQ VLAN plan

Enterprise	Private Network VLAN (Inner VLAN)	Public Network VLAN (Outer VLAN)
Enterprise 1	VLANs 10 and 20	VLAN 10
Enterprise 2	VLANs 20, 30, and 50	VLAN 20

The following uses enterprise 2 users in the same private network (VLAN 30) as an example to describe packet processing:

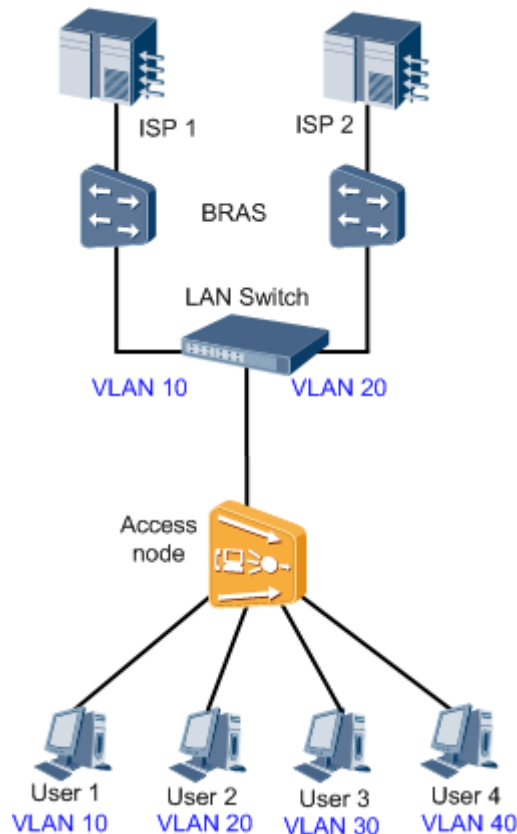
1. Untagged user packets are transmitted upstream. The packets then reach the Layer 2 switch.

2. The Layer 2 switch adds the private network VLAN tag (VLAN 30) to the packets and transmits them to the access node in the upstream direction.
3. The access node adds the public network VLAN tag (VLAN 20) to the packets and transmits the packets upstream to the upper-layer network.
4. The upper-layer network device transmits the packets to the interconnected access node according to the public network VLAN tag.
5. The interconnected access node removes the public network VLAN tag after receiving the packets, and transmits them to the switch on the same side.
6. The switch identifies and removes the private VLAN tag (VLAN 30), and forwards the untagged packets to the specified user in the private network (VLAN 30).

Stacking VLAN

The following network supports Internet service providers (ISPs) 1 and 2. User 1 and user 2 access ISP 1; user 3 and user 4 access ISP 2. The system uses the stacking VLAN to quickly provision ISP-provisioned services to specified users. Specifically, the outer VLAN tag indicates the ISP and the inner VLAN tag indicates the user.

Figure 10-11 Stacking VLAN application



The stacking VLAN is deployed according to the following configurations to connect users.

- Attribute stacking is specified for created service VLANs (different ISPs have different outer VLAN tags).

- A service flow is created for each user.
- The inner and outer VLAN tags are configured according to the VLAN plan in the following table.

Table 10-9 Stacking VLAN plan

User	Inner VLAN Tag (Identifying Users)	Outer VLAN Tag (Identifying ISPs)
User 1	VLAN 10	VLAN 10
User 2	VLAN 20	
User 3	VLAN 30	VLAN 20
User 4	VLAN 40	

- The following uses user 2 as an example to describe the processing of packets with the stacking VLAN from a user to an ISP:
1. User 2 sends untagged packets to the access node.
 2. The access node adds two VLAN tags (inner VLAN 20 and outer VLAN 10) to the untagged packets.
 3. The switch forwards the packets to ISP 1 according to outer VLAN 10.
 4. ISP 1 removes outer VLAN 10 after receiving the packets and then provisions services to different users according to inner VLAN 20.

10.2.6 VLAN Translation

VLAN translation is also called VLAN mapping, which converts between user VLAN IDs and carrier VLAN IDs and allows carriers' VLAN planning to be flexible.

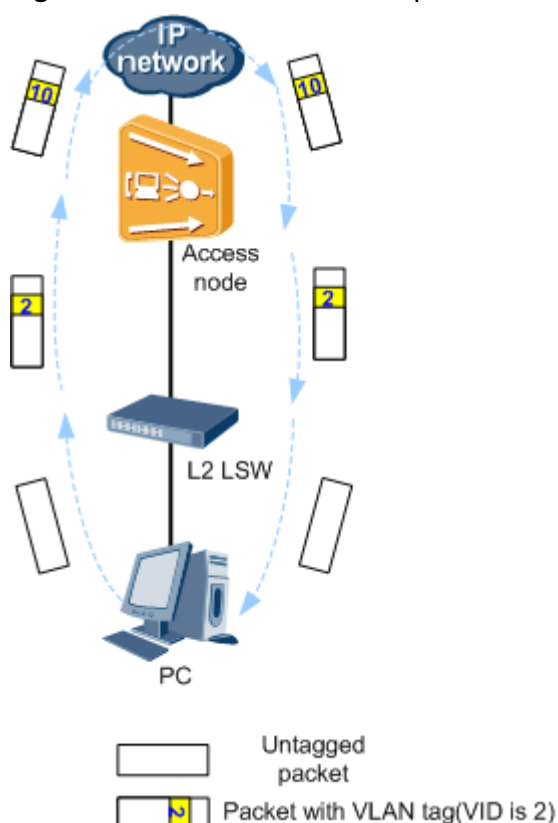
VLAN Translation Policies

The access node supports the following VLAN translation policies:

- N to 1 translation
In the receive direction, the access node translates untagged packets, single-tagged packets, and double-tagged packets into packets with a specified VLAN tag. In the transmit direction, the access node translates this specified VLAN tag to the original VLAN tag(s) when sending packets to users.
- N to 2 translation
In the receive direction, the access node translates untagged packets, single-tagged packets, and double-tagged packets into packets with two specified VLAN tags. In the transmit direction, the access node translates these specified VLAN tags to the original VLAN tag(s) when sending packets to users.

The following figure shows the VLAN translation process, assuming that 1 to 1 VLAN translation is used. The access node translates VLAN tag (VID 2) to VLAN tag (VID 10).

Figure 10-12 VLAN translation process

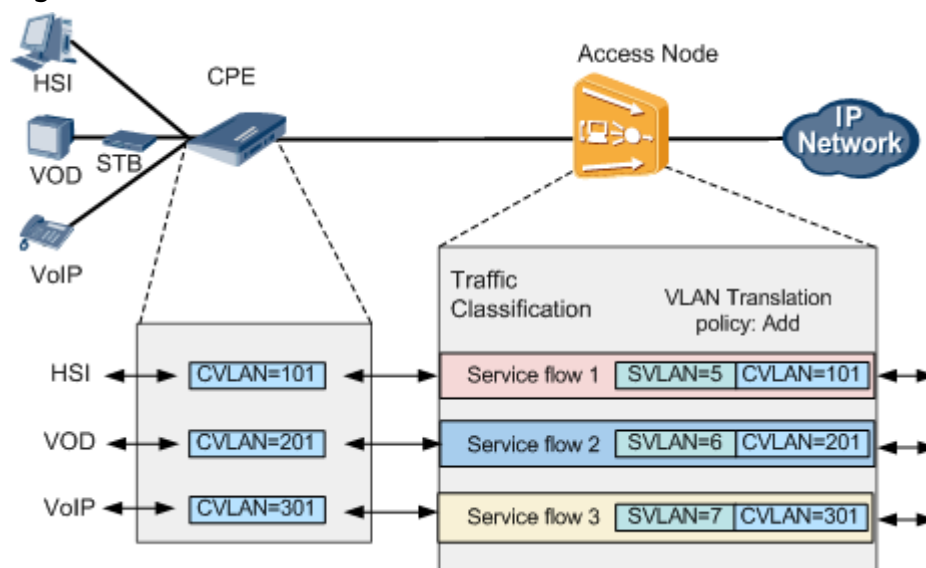


1. After receiving packets from the user side, the access node translates the VLAN tag of the packets according to the specified VLAN translation policy and then forwards the packets to the upper-layer network.
2. After receiving packets from the network side, the access node reverse translates the VLAN tag (restoring the original VLAN tag), and then sends the restored user packets to users.

VLAN Translation Based on Service Flow

The access node performs traffic classification for user packets based on service flows. Therefore, VLAN translation configuration and function are also implemented based on service flows.

The following figure uses VLAN translation policy "add" as an example to show the VLAN translation process on the access node.

Figure 10-13 VLAN translation based on service flow

1. The CPE attaches different C-VLAN tags to service packets (C-VLAN indicates the user-side VLAN, that is, the VLAN tag carried in user packets. In multi-service applications, it is usually used to identify a user).
2. The access node classifies traffic according to the C-VLAN tag and uses service flows to represent different classes.
3. The VLAN translation policy is specified to add (S-VLAN indicates the service VLAN in service flows) when service flows are configured.
4. The access node attaches an S-VLAN tag to packets matching the service flows and then forwards the packets to the upper-layer network. For example, the access node attaches VLAN tag carrying VID 5 to packets (with VLAN tag carrying VID 101) that match service flow 1.

10.2.7 VLAN Planning Suggestion

Properly plan VLAN types and attributes to meet various service requirements.

Selecting a VLAN Type

An access device connects to users in various access modes through service flows. Select a VLAN type based on service flow requirements. A standard or super VLAN does not support the creation of service flows. Therefore, a smart or MUX VLAN is used. A MUX VLAN supports only one service flow while a smart VLAN supports multiple ones. Therefore, a smart VLAN is more popular.

A standard VLAN supports the adding of only uplink ports. Therefore, it is used for managing devices.

A super VLAN applies in Layer 3 interconnection of Layer 2 isolation. Specifically, sub-VLANs in a super VLAN can communicate with each other at Layer 3 after Address Resolution Protocol (ARP) proxy is enabled.

Selecting a VLAN Attribute

Plan the number of VLAN tags for an access device based on service requirements. For example, plan one VLAN tag for simple services and two VLAN tags for

wholesale services. One is used to identify Internet service providers (ISPs) and another is used to identify users. Then, select a VLAN attribute according to the number of VLAN tags.

- If one VLAN tag is required, select a common or QinQ VLAN, but not a stacking VLAN.
- If two VLAN tags are required, select a stacking or QinQ VLAN, but not a common VLAN.

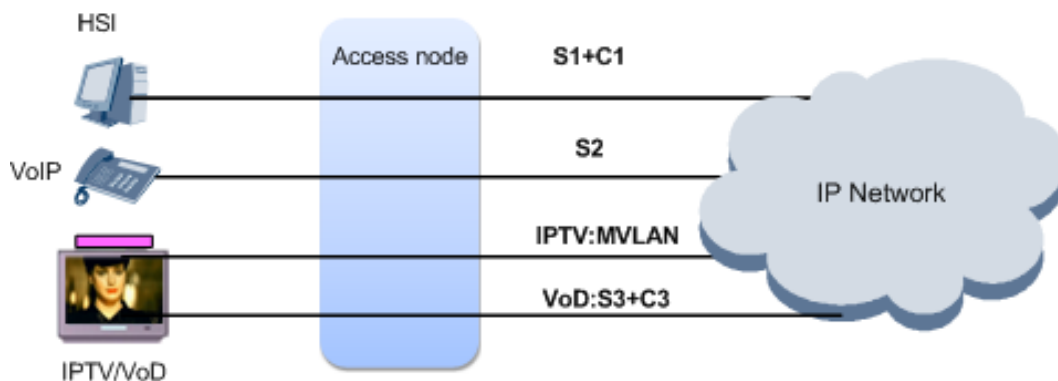
The further VLAN attribute selection rules are as follows:

- Select a QinQ VLAN for private line or transparent transmission services. The reason is that the QinQ VLAN ensures the transparent transmission of all protocol packets through hardware to the best extent.
- Select a common or stacking VLAN for enabling secure features, such as IP address anti-spoofing and MAC address anti-spoofing, Dynamic Host Configuration Protocol (DHCP) Option 82, Policy Information Transfer Protocol (PITP), and multicast functions. The reason is that a QinQ VLAN does not support the preceding functions.

VLAN Usage in the Typical Triple-play Service Scenario

In the triple-play service scenario, multiple services are provisioned for a user, such as the high-speed Internet (HSI), VoIP, IPTV, and video on demand (VoD) services.

Figure 10-14 VLAN usage in the typical triple-play service scenario



In the preceding figure:

- The HSI service uses a stacking VLAN with two VLAN tags, service VLAN (S-VLAN) tag and customer VLAN (C-VLAN) tag. S+C (S1+C1 in the preceding figure) indicates each service for each user. Enable DHCP Option 82 and PITP. Enable IP address anti-spoofing or MAC address anti-spoofing based on site requirements.
- The voice service uses a common VLAN with one VLAN tag. Enable IP address anti-spoofing and MAC address anti-spoofing.
- The VoD service uses a stacking VLAN with two VLAN tags, S-VLAN tag and C-VLAN tag (S3+C3 in the preceding figure).
- The multicast VLAN (MVLAN) of the IPTV service is a common VLAN with a VLAN tag.
- Add a VoD service flow to the MVLAN as a multicast user. The Internet Group Management Protocol (IGMP) is carried over the service flow. Therefore, the

S-VLAN of the VoD service cannot be a QinQ VLAN. The reason is that a QinQ VLAN transparently transmits IGMP packets through hardware but not capture the packets. For details, see [10.2.2 VLAN Basic Concepts](#).

VLAN Usage in the Typical Enterprise Private Line Service Scenario

In the enterprise private line service scenario, the headquarter (HQ) and branches of an enterprise need to communicate with each other. Both the HQ and branches are in X1 VLAN.

Figure 10-15 VLAN usage in the typical enterprise private line service scenario



In the preceding figure, the VLAN tag of both access devices 1 and 2 is S1 VLAN. The X1 VLAN transparently transmits packets. DHCP or other protocols may be used in the enterprise. Therefore, use a QinQ VLAN (S1+X1 in the preceding figure) to transparently transmit the protocol packets through hardware to the best extent. This prevents global capturing and forwarding of the protocol packets through software by mistake and ensures the performance of the enterprise private line service.

10.2.8 VLAN Translation Policies Specifications

VLAN translation policies

Table 10-10 VLAN translation policies

VLAN Tag Before Translation	VLAN Tag After Translation	VLAN Translation Policy	Description	Usage Scenario
Untagged	Service VLAN (S-VLAN)	add	An S-VLAN tag is attached.	Service flows whose S-VLAN is a QinQ VLAN Transparent LAN service (TLS) flows

VLAN Tag Before Translation	VLAN Tag After Translation	VLAN Translation Policy	Description	Usage Scenario
	Service VLAN + customer VLAN (S-VLAN + C-VLAN)	add double	Two VLAN tags, the outer S-VLAN tag and inner C-VLAN tag, are attached.	Single service flows whose S-VLAN is a stacking VLAN, and multiple service flows classified by the following rules. • untagged user-side VLAN • user-side 802.1p priority • user-side encapsulation mode Service flows whose S-VLAN is a QinQ VLAN
C-VLAN	C-VLAN	transparent	The VLAN tag is transparently transmitted.	Service flows whose GEM port is configured with the cascade attribute Service flows whose S-VLAN is a QinQ VLAN
	S-VLAN	translate	One VLAN tag is translated.	Multiple service flows whose S-VLAN is a common VLAN, classified by the following rules. • user-side VLAN • combination of user-side VLAN, user-side encapsulation mode • combination of user-side VLAN, user-side 802.1p priority Service flows whose S-VLAN is a QinQ VLAN
	S-VLAN + C-VLAN	add	An S-VLAN tag is attached.	-

VLAN Tag Before Translation	VLAN Tag After Translation	VLAN Translation Policy	Description	Usage Scenario
	S-VLAN +C'-VLAN	translate and add	The C-VLAN tag is translated and the S-VLAN tag is attached.	Multiple service flows whose S-VLAN is a stacking VLAN, classified by the following rules. • user-side VLAN • combination of user-side VLAN, user-side encapsulation mode • combination of user-side VLAN, user-side 802.1p priority Service flows whose S-VLAN is a QinQ VLAN
	Untagged	remove	This is a special VLAN translation mode for connection-oriented service flows. In this mode, service flows carry one VLAN tag when arriving from the destination end, and have this VLAN tag removed when transmitted from the source end. Therefore, service flows are finally untagged.	-
S-VLAN +C-VLAN	S'-VLAN +C'-VLAN	translate double	Both the S-VLAN and C-VLAN tags are translated.	Service flows whose S-VLAN is a stacking VLAN or QinQ VLAN, classified by S'-VLAN+C'-VLAN
	S'-VLAN	translate and remove	The C-VLAN tag is removed and the S-VLAN tag is translated.	Service flows whose S-VLAN is a common or QinQ VLAN, classified by S-VLAN+C-VLAN

VLAN Tag Before Translation	VLAN Tag After Translation	VLAN Translation Policy	Description	Usage Scenario
	Untagged	remove double	This is a special VLAN translation mode for connection-oriented service flows. In this mode, service flows carry two VLAN tags (S-VLAN+C-VLAN) when arriving from the destination end, and have these VLAN tags removed when transmitted from the source end. Therefore, service flows are finally untagged.	-

10.2.9 Configuring a VLAN

A virtual local area network (VLAN) is used to separate broadcast domains. VLANs have enhanced security and support expansion and flexible networking. Configuring VLAN is a prerequisite for configuring a service. Hence, before configuring a service, make sure that the VLAN configuration based on planning is complete.

Application Context

VLAN application is specific to user types. For details on the VLAN application, see [Table 10-11](#).

Table 10-11 VLAN application and planning

Application Scenario	VLAN Planning	Remarks
The device communicates with a network management system (NMS) or the devices are cascaded.	VLAN type: standard VLAN attribute: common VLAN forwarding mode: VLAN+MAC	This plan is only applicable to Ethernet ports. A standard VLAN only contains multiple uplink ports. The Ethernet ports in one VLAN can communicate with each other and the Ethernet ports in different VLANs are separated.
N:1 access	VLAN type: smart VLAN attribute: common VLAN forwarding mode: by VLAN+MAC	In the upstream direction of a single VLAN, services of multiple users are aggregated to the same VLAN, reducing the number of VLANs. One smart VLAN can contain multiple upstream ports and multiple service ports. The service ports included in the same Smart VLAN are isolated from each other. Service ports of different VLANs are also isolated from each other.
1:1 access - Multi-ISP wholesale service (ISP is the abbreviation of Internet service provider.) - VLAN ID expansion service	VLAN type: smart Attribute: stacking VLAN forwarding mode: by S+C	A stacking VLAN packet contains two VLAN tags (inner and outer VLAN) assigned by the MA5800. The outer VLAN identifies a service (service VLAN) and the inner VLAN identifies a user (customer VLAN). The service used by a user is identified by a unique VLAN ID (S+C VLAN). The upper layer broadband remote access server (BRAS) authenticates a service by the two VLAN tags contained in the service packets. In this manner, the BRAS can receive packets from more users. On a Layer-2 upper layer network of the MA5800, packets can also be forwarded by the outer VLAN+MAC ID. This function enables ISPs to provide the wholesale services.

Application Scenario	VLAN Planning	Remarks
Enterprise private line service access	VLAN type: smart VLAN attribute: QinQ VLAN forwarding mode: by VLAN+MAC or S+C.	A QinQ VLAN contains an inner VLAN tag from the user private network, and an outer VLAN tag assigned by the MA5800. The outer VLAN forms a Layer 2 virtual private network (VPN) on the user private network for transparently transmitting user services on the private network.

10.2.9.1 Creating a VLAN

Creating VLAN is a prerequisite for configuring a VLAN or service. Hence, before configuring a VLAN, make sure that the VLAN creating based on planning is complete.

Default Configuration

[Table 10-12](#) lists the default parameter settings of VLAN.

Table 10-12 Default parameter settings of VLAN

Parameter	Default Setting	Remarks
Default VLAN of the system	VLAN ID: 1 Type: smart VLAN	You can run the defaultvlan modify command to modify the VLAN type but cannot delete the VLAN.
Reserved VLAN of the system	VLAN ID range: 4079-4093	You can run the vlan reserve command to modify the VLAN reserved by the system.

Prerequisite

- The VLAN to be added should not exist in the system.
- Service VLAN cannot be reserve VLAN.

Procedure

Step 1 Create a VLAN.

Run the **vlan** to create a VLAN. VLANs of different types are applicable to different scenarios.

Table 10-13 VLAN types and application scenarios

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Standard VLAN	To add a standard VLAN, run the vlan vlanid standard command.	Standard VLAN. Ethernet ports in a standard VLAN are interconnected with each other but Ethernet ports in different standard VLANs are isolated from each other.	Only available to Ethernet ports and specifically to network management and subtending.
Smart VLAN	To add a smart VLAN, run the vlan vlanid smart command.	A VLAN contains one or more xPON service ports. Service ports in the same smart VLAN are isolated. Service ports in different VLANs are also isolated. A VLAN provides access for multiple users and therefore saves VLAN resources.	Smart VLANs can be applied in residential communities to provide xPON service access.
MUX VLAN	To add a MUX VLAN, run the vlan vlanid mux command.	One VLAN contains only one xPON service port. The traffic streams in different VLANs are isolated from each other. One-to-one mapping can be set up between a VLAN and an access user. Therefore, a VLAN uniquely identifies an access user.	MUX VLANs are applicable to xPON service access and can distinguish users.

VLAN Type	Configuration Command	VLAN Description	Application Scenario
Super VLAN	To add a super VLAN, run the vlan vlanid super command.	The super VLAN is based on Layer 3. One super VLAN contains multiple sub-VLANs. Through an ARP proxy, the sub-VLANs in a super VLAN can be interconnected at Layer 3.	Super VLANs save IP addresses and improve the utilization of IP addresses. For a super VLAN, sub-VLANs must be configured. You can run the supervlan command to add a sub-VLAN to a specified super VLAN. A sub-VLAN must be a smart VLAN or MUX VLAN.

 NOTE

- To add VLANs with consecutive IDs in batches, run the **vlan vlanid to end-vlanid** command.
- To add VLANs with non-consecutive IDs in batches, run the **vlan vlan-list** command.

----End

Example

Create VLAN 50 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 50 smart
```

Create VLAN 55-60 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 55 to 60 smart
```

Create VLAN 65, 73 and 52 for extension of the VLAN ID. And the type of VLAN is smart.

```
huawei(config)#vlan 65,73,52 smart
```

10.2.9.2 Configuring the VLAN attribute

Configuring the VLAN attribute is a prerequisite for configuring a VLAN. Hence, before configuring a service, make sure that the VLAN configuration based on planning is complete.

Default Configuration

Table 10-14 lists the default parameter settings of VLAN.

Table 10-14 Default attribute settings of VLAN

Parameter	Default Setting
Default attribute of a new VLAN	Common

Prerequisite

- The VLAN to be configured should have been created.
- The VLAN attribute must be planned properly according to the application scenarios.

Procedure

Step 1 Configure the VLAN attribute.

The default attribute for a new VLAN is "common". You can run the **vlan attrib** command to configure the attribute of the VLAN.

Configure the attribute according to VLAN planning.

Table 10-15 VLAN attributes and application scenarios

VLAN Attribute	Configuration Command	VLAN Type	VLAN Description	Application Scenario
Common	The default attribute for a new VLAN is "common".	The VLAN with this attribute can be a standard VLAN, smart VLAN, MUX VLAN, or super VLAN.	A VLAN with the common attribute can function as a common Layer 2 VLAN or function for creating a Layer 3 interface.	Applicable to the N:1 access scenario.

VLAN Attribute	Configuration Command	VLAN Type	VLAN Description	Application Scenario
QinQ VLAN	To configure QinQ as the attribute of a VLAN, run the vlan attrib vlanid q-in-q command.	The VLAN with this attribute can be a standard VLAN, smart VLAN or MUX VLAN. The attribute of a sub VLAN, the VLAN with a Layer 3 interface, and the default VLAN of the system cannot be set to QinQ VLAN.	The packets from a QinQ VLAN contain two VLAN tags, that is, inner VLAN tag from the private network and outer VLAN tag from the MA5800. Through the outer VLAN, a Layer 2 VPN tunnel can be set up to transparently transmit the services between private networks.	Applicable to the enterprise private line scenario. A QinQ VLAN does not support the following services: DHCP Option 82, DHCP Layer 2 relay, DHCP Layer 3 relay, PITP P mode, IP address anti-spoofing, MAC address anti-spoofing, multicast IPTV, and ARP proxy.

VLAN Attribute	Configuration Command	VLAN Type	VLAN Description	Application Scenario
VLAN Stacking	To configure stacking as the attribute of a VLAN, run the vlan attrib vlanid stacking command.	The VLAN with this attribute can only be a smart VLAN or MUX VLAN. The attribute of a sub VLAN, the VLAN with a Layer 3 interface, and the default VLAN of the system cannot be set to VLAN stacking.	The packets from a stacking VLAN contain two VLAN tags, that is, inner VLAN tag and outer VLAN tag from the MA5800. The upper-layer BRAS authenticates the access users according to the two VLAN tags. In this manner, the number of access users is increased. On the upper-layer network in the Layer 2 working mode, a packet can be forwarded directly by the outer VLAN tag and MAC address mode to provide the wholesale service for ISPs.	Applicable to the 1:1 access scenario for the wholesale service or extension of VLAN IDs. In the case of a stacking VLAN, to configure the inner tag of the service port, run the stacking label command.

 NOTE

- To configure attributes for the VLANs with consecutive IDs in batches, run the **vlan attrib vlanid to end-vlanid** command.
- To configure attributes for the VLANs with non-consecutive IDs in batches, run the **vlan attrib vlan-list** command.

----End

Example

To configure the attribute of VLAN 50 to **stacking** for extending VLAN IDs, do as follows:

```
huawei(config)#vlan attrib 50 stacking
```

To configure the attributes of VLANs 55-60 (used for enterprise users) to **QinQ**, do as follows:

```
huawei(config)#vlan attrib 55 to 60 q-in-q
```

To configure the attributes of service VLANs 65, 73, and 52 to **stacking**, do as follows:

```
huawei(config)#vlan attrib 65,73,52 stacking
```

10.2.9.3 Configuring Upstream Port of a VLAN

The upstream port on an access device connects to the upper layer device to forward access device data to the upstream network and forward upper layer device data to users.

Prerequisites

The planned virtual local area network (VLAN) is already configured.

Procedure

Step 1 Configure an upstream port for the VLAN.

Run the **port vlan** command to add the upstream ports to the VLAN.

----End

Example

Assume that the 0/9/0 and 0/9/1 upstream ports are to be added to VLAN 50. To configure such upstream ports, do as follows:

```
huawei(config)#port vlan 50 0/9 0  
huawei(config)#port vlan 50 0/9 1
```

10.2.9.4 Configuring a VLAN Service Profile

A VLAN service profile is a collection of service-related parameters for VLAN attributes. After a VLAN is bound to a VLAN service profile, the VLAN has all the VLAN attributes defined in the VLAN service profile. Binding a VLAN service profile is an efficient way of configuring a VLAN.

Application Context

VLAN, as a basic and also important concept of access equipment, involves discrete configurations of many parameters. These parameters include forwarding mode, security feature, protocol enabling/disabling, transparent transmission of protocol packets, and packet forwarding policy. Service parameters are related to specific VLANs and in actual usage there are a lot of VLANs, causing complex configuration. Against this backdrop, the VLAN service profile is introduced to achieve simplified and highly-efficient configuration. A VLAN service profile is abstracted from specific VLANs and supports centralized configuration of VLAN-related service parameters. Different VLANs of the same attribute can flexibly be

bound to (or unbound from) a VLAN service profile to possess (or release) the attributes defined in the VLAN service profile.

Prerequisite

The VLAN to which the VLAN service profile is bound must be created.

- When a VLAN profile is bound to a QinQ VLAN, both the anti-IP spoofing and anti-MAC spoofing functions are unavailable.
- SVLAN+CVLAN forwarding and anti-MAC spoofing cannot be enabled at the same time in a VLAN profile.
- After a VLAN profile is bound to a VLAN, if the VLAN attribute is Common, the packet forwarding mode cannot be set to vlan-connect (SVLAN+CVLAN forwarding).

Configuration Process

1. Create a VLAN service profile.
2. Configure the following service parameters according to service requirements:
 - Forwarding mode
 - Forwarding policy
 - Protocol switch
 - Transparent transmission function
 - Security function
3. Commit to save the current parameters.
4. Bind the VLAN service profile to the VLAN.

Procedure

Step 1 Create a VLAN service profile.

Run the **vlan service-profile** command to create a VLAN service profile or enter the configuration mode of the VLAN service profile. When the profile does not exist, running this command to create a VLAN service profile and enter the configuration mode of the service profile. If the profile exists, running this command to directly enter the configuration mode of this service profile.

Step 2 Configure the VLAN forwarding mode.

Forwarding mode refers to the Layer 2 packet forwarding mechanism, including VLAN+MAC forwarding (default) and SVLAN+CVLAN (or S+C) forwarding. In VLAN+MAC forwarding, the system needs to dynamically learn the mapping relationship between VLAN, source MAC address, and port. In S+C forwarding, the system does not need to dynamically learn MAC addresses but determines the forwarding entry according to SVLAN and CVLAN. Because S+C forwarding does not depend on MAC address learning, it has the following advantages:

1. Saving MAC addresses
2. Preventing occurrence of unknown unicast packets caused by aging of dynamic MAC addresses
Broadcasting unknown unicast packets threatens the security of the device

3. Ensuring security by solving problems such as MAC spoofing and attack
 - Run the **forwarding** command to configure the VLAN forwarding policy.
 - Run the **user-bridging** command to configure the bridging function of the VLAN service profile. After the bridging function is enabled, two users in the same VLAN can directly communicate with each other at Layer 2.

Step 3 Configure the VLAN forwarding policy.

Forwarding policy refers to the discard policy of packets such as downstream broadcast, downstream unknown unicast, and unknown multicast packets.

- Run the **packet-policy** command to configure the forwarding policy for the downstream broadcast packets, downstream unknown unicast packets, and unknown multicast packets in the VLAN. Two policies namely forward and discard are supported.
- Run the **igmp mismatch** command to configure the mismatch IGMP policy of the VLAN, supports the transparent and discard policies.

Step 4 Configure the VLAN protocol switch.

Protocol switch refers to whether to enable certain types of protocols or certain functions of a protocol. VMAC aging and PPPoE MAC conflict with S+C forwarding.

- Run the **dhcp mode** command to configure the DHCPv4 forwarding mode, that is, to switch between the DHCP Layer 2 forwarding mode and the DHCP Layer 3 forwarding mode.
- Run the **dhcpv6 mode** command to configure the DHCPv6 forwarding mode, that is, to switch between the DHCP Layer 2 forwarding mode and the DHCP Layer 3 forwarding mode.
- Run the **pppoe mac-mode** command to configure the MAC address allocation mode for PPPoE users. Two modes namely, single-mac and multi-mac are supported.
- Run the **vmac aging-mode** command to configure the VMAC aging mode, which can be common aging or DHCP-based aging.
- Run the **pitp** command to configure the PITP function to implement authentication of bound user account and access port.
- Run the **dhcp option82** command to configure the DHCPv4 option 82 feature.
- Run the **dhcpv6 option82** command to enable or disable the DHCPv6 option feature.
- Run the **dhcp proxy** command to configure the DHCP proxy function. After the DHCP proxy function is enabled, the server ID proxy function and lease time proxy function will be enabled.

Step 5 Configure the VLAN transparent transmission function.

In transparent transmission, the system does not process specified types of protocol packets but transparently transmits them.

- Run the **bpdu tunnel** command to configure the BPDU transparent transmission switch. After transparent transmission is enabled, the Layer 2 BPDUs of the private network can be transmitted transparently over the public network.

- Run the **vtp-cdp tunnel** command to configure the VTP/CDP packet transparent transmission switch. After the switch is enabled, VTP/CDP packets are transparently transmitted based on the VLAN.
- Run the **rip tunnel** command to configure the RIP Layer 2 transparent transmission switch. After the transparent transmission switch is enabled, RIP packets can be transparently transmitted at Layer 2 based on VLAN on the device without running the RIP protocol.
- Run the **l3-protocol tunnel** command to configure the L2 transparent transmission for the L3 protocol packets except RIP and OSPF packets. After this function is enabled, the L3 protocol packets can be transparently transmitted at Layer 2 based on VLAN on the device without running the L3 protocol.
- Run the **ipv6 dad proxy** command to configure the DAD proxy (duplicate address detect proxy). DAD proxy prevents repeated LLA configuration on the user side.

Step 6 Configure the VLAN security function.

The security function is used to prevent malicious users from attacking the system by forging the IP address or MAC address of an authorized user. VMAC and anti-MAC spoofing conflict with S+C forwarding.

- Run the **security anti-ipspoofing** command to configure the anti-IPv4 spoofing function. After the anti-IPv4 spoofing function is enabled, the system automatically and dynamically binds the IPv4 address to the user. The packet can be transmitted upstream through the device only when the source IPv4 address of the packet is the same as the bound IPv4 address. Otherwise, the packet is discarded.
- Run the **security anti-ipv6spoofing** command to configure the anti-IPv6 spoofing function. After the anti-IPv6 spoofing function is enabled, the system automatically and dynamically binds the IPv6 address to the user. The packet can be transmitted upstream through the device only when the source IPv6 address of the packet is the same as the bound IPv6 address. Otherwise, the packet is discarded.
- Run the **security anti-macspoofing** command to configure the anti-MAC spoofing function. After the anti-MAC spoofing function is enabled, the system automatically and dynamically binds the MAC address to the traffic stream. When the source MAC address of the traffic stream is the same as the bound MAC address, the traffic stream can be upstream transmitted through the device. Otherwise, the packets are discarded.
- Run the **security arp-reply** command to enable the network-side ARP proxy response function. If the network-side ARP proxy response function is enabled, the system searches for user's going online information based on the destination IP address and VLAN after it receives network-side ARP request packets. If there is an online user, the system performs proxy response. If there is no online user, the system discards or forwards the ARP request packets based on the setting in the **security arp-reply unknown-policy** command. This prevents ARP request packets from being sent to user ports and reduces system resources.
- Run the **security ns-reply** command to enable the network-side NS proxy response function. If network-side NS proxy reply is enabled, the system searches for user's going online information based on the destination IP address and VLAN after it receives network-side NS packets. If there is an

online user, the system performs proxy response. If there is no online user, the system discards or forwards the NS packets based on the setting in the **security ns-reply unknown-policy** command. This prevents NS packets from being sent to user ports and reduces system resources.

- Run the **security bind-route-nd** command to configure the function of binding route with neighbor entry. After the function of binding route with neighbor entry is enabled, the system automatically generates the route and neighbor entry of a DHCPv6 user based on the user information recorded when the user goes online. This function reduces the effort of configuring static routes manually, prevents neighbor packets from being sent to the user side, and enhances system security.
- Run the **vmac** command to enable or disable VMAC. By default, VMAC is disabled.

Step 7 Commit to save the current parameters.

Run the **commit** command to commit the current parameter configuration of the VLAN service profile. After the configuration is completed, run the commit command to make the configuration take effect.

Step 8 Bind the VLAN service profile to the VLAN.

Run the **vlan bind service-profile** command to bind the configured VLAN service profile to a specified VLAN. After the binding, the VLAN-level feature control switch is based on the configuration of the VLAN service profile. Independent configuration commands for VLAN-based features are no longer effective.

----End

Result

You can query the configuration of the VLAN service profile by the **display vlan service-profile** command.

After a VLAN service profile is bound to a VLAN, regarding the parameters whose **Committed** state is **NotConfig**, the configuration commands that are independent of the VLAN take effect; other parameters adopt the control parameters of the profile. Modifying the feature parameters relevant to the VLAN does not take effect.

Example

Add VLAN service profile 3 and bind it to VLAN 100. The profile parameters are planned as follows:

- VLAN forwarding mode VLAN+MAC address (vlan-mac)
- BPDU transparent transmission: enabled
- Unknown multicast packet: discarded

Adopt the default values for other parameters.

```
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#forwarding vlan-mac
huawei(config-vlan-srvprof-3)#bpd tunnel enable
huawei(config-vlan-srvprof-3)#packet-policy multicast discard
huawei(config-vlan-srvprof-3)#commit
```

```
huawei(config-vlan-srvprof-3)#quit  
huawei(config)#vlan bind service-profile 100 profile-id 3
```

10.2.9.5 Example: Configuring the QinQ VLAN

The QinQ-VLAN-based private line service can achieve the interconnection and secure communication among branches in different areas within the enterprise private network.

Prerequisites

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

- An enterprise requires to achieve the interconnection and secure communication between its headquarters and the branches located in different areas through Layer 2 switching network, and to isolate the data of different departments.
- The access device uses PON access.

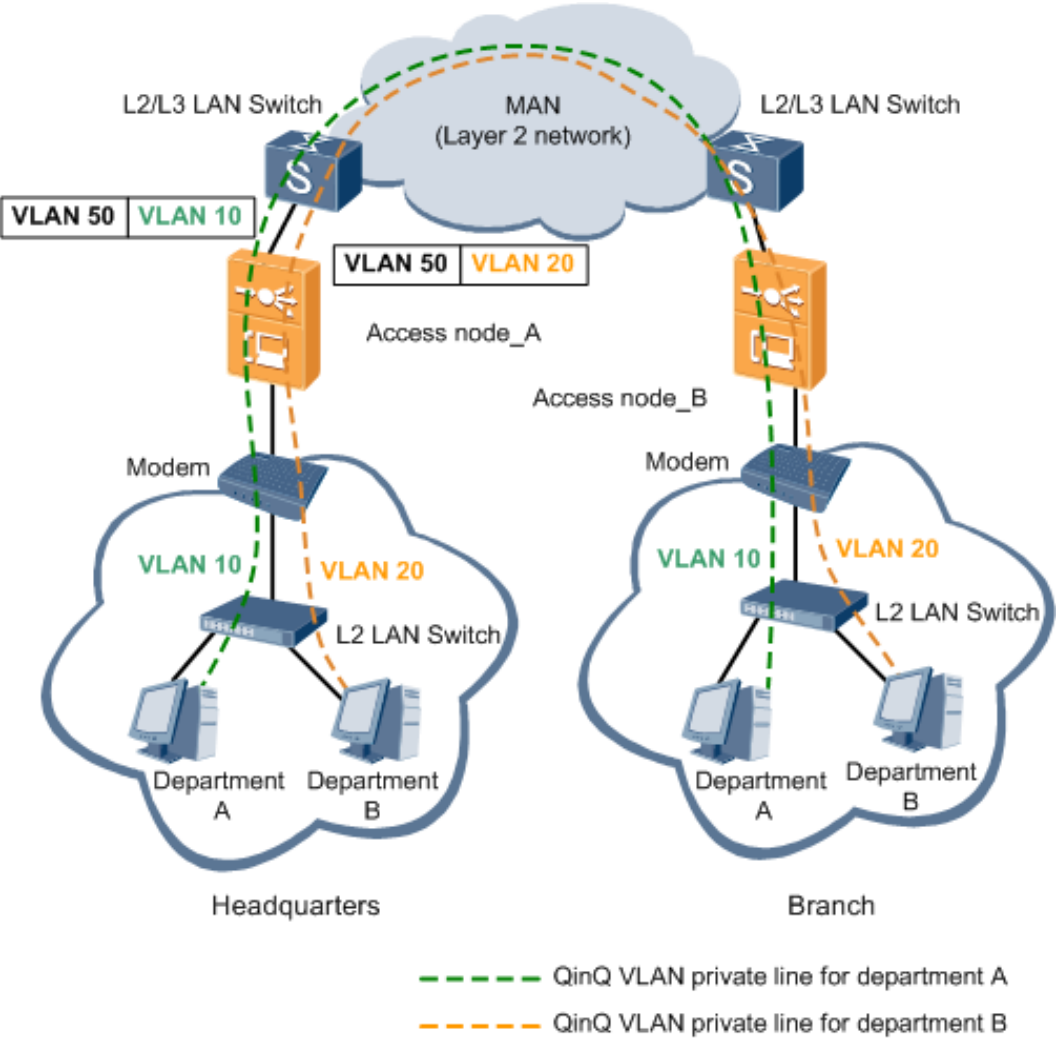
Networking

Figure 10-16 shows an example network for configuring the private line service.

The two branches of the enterprise are connected to the (metropolitan area network) MAN through the MA5800. The upper-layer network must work in the Layer 2 mode, and must forward packets according to the VLAN and the MAC address.

On the MA5800, the attribute of the upstream VLAN of user packets is configured as QinQ private line service. A VLAN tunnel is created in Layer 2/Layer 3 MAN for transmitting data carrying the VLAN tag. Different VLAN IDs are used for different departments to achieve user isolation and data security. In this way, the service packets of the enterprise private network can be transparently transmitted through the public network, and the two branches can communicate with each other securely.

Figure 10-16 Example network for configuring the private line service



The configuration on MA5800_A is the same as the configuration on MA5800_B. The following uses the configuration on MA5800_A as examples to describe how to configure the private line service implemented through a QinQ VLAN.

Data Plan

Table 10-16 lists the key data planning of the QinQ VLAN private line service on MA5800_A.

Table 10-16 Data plan for configuring the QinQ VLAN private line service

Item	Data	Remarks
VLAN	• VLAN ID: 50 • VLAN type: smart VLAN • VLAN attribute: QinQ	The public network VLAN, namely outer VLAN, is configured here. The inner VLAN belongs to the enterprise private network, which can be planned by the enterprise self.
Transparent transmission of Layer 2 packets	Enable the transparent transmission of BPDUs.	This function is mainly used in the QinQ service to provide a transparent and secure data channel for the enterprise branches located in two places within the enterprise private network. After the transparent transmission of BPDUs is enabled, the Layer 2 protocol packets of a private network can be transparently transmitted through the public network.
Upstream port	0/9/0	-
Traffic profile	• Traffic profile ID: 10 • CIR: 4 Mbit/s • Priority copy policy: user-cos • Default 802.1p priority of the packet: 4 • Priority-based scheduling policy of the downstream packets: local-setting	The CIR depends on the user bandwidth requirement.

Item	Data	Remarks
GPON port	- GPON port ID: 0/2/0 - DBA profile: - Profile type: type3 - Profile name: DBA_bandwidth - Assured bandwidth: 10 Mbit/s - ONT line profile - Profile ID: 10 - T-CONT ID: 4 - ONT service profile ID: 10 - ONT port VLAN ID: 10 - Default ONT alarm profile ID: 1	-
Service virtual port	- Service port: 0/2/0 - ID of the traffic profile in Rx direction: 10 - ID of the traffic profile in Tx direction: 10	The traffic profile that meets the service requirement is used.

Procedure

Step 1 Configure a DBA profile.

The profile type is Type3, assured bandwidth is 10 Mbit/s, and profile name is DBA_10M.

```
huawei(config)#dba-profile add profile-name DBA_10M type3 assure 10240 max 10240
```

Step 2 Configure a GPON ONT line profile.

Create a GPON ONT line profile with an index number of 10, and T-CONT ID is 4.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name DBA_10M
huawei(config-gpon-lineprofile-10)#gem add 10 eth tcont 4
huawei(config-gpon-lineprofile-10)#gem mapping 10 0 vlan 10
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

Step 3 Configure a GPON ONT service profile.

Create a GPON ONT service profile with index 10, set the VLAN ID of the ONT port to 10, and set the port capability set of the ONT to adaptive. The system automatically adapts to the actual capability of online ONTs.

```
huawei(config)#ont-srvprofile gpon profile-id 10
huawei(config-gpon-srvprofile-10)#ont-port eth adaptive
huawei(config-gpon-srvprofile-10)#port vlan eth 1 10
huawei(config-gpon-srvprofile-10)#commit
huawei(config-gpon-srvprofile-10)#quit
```

Step 4 Configure a GPON ONT.

Enable the automatic ONT discovery function. The following uses port 0/2/0 as an example. The configuration of the other GPON ports is similar to that of port 0/2/0.

NOTE

- By default, a port is in the activated state. Before binding a profile to the port, you must deactivate the port.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000001 always-on omci ont-lineprofile-id 10
ont-srvprofile-id 10
huawei(config-if-gpon-0/2)#quit
```

Step 5 Create a VLAN.

The VLAN ID is 50, and the VLAN is a smart VLAN.

```
huawei(config)#vlan 50 smart
```

Step 6 Set the VLAN attribute to QinQ.

```
huawei(config)#vlan attrib 50 q-in-q
```

Step 7 Enable the transparent transmission of BPDUs.

Enable the transparent transmission of BPDUs so that the Layer 2 protocol packets of a private network can be transparently transmitted through the public network. By default, the transparent transmission of BPDUs is disabled.

```
huawei(config)#bpd tunnel vlan 50 enable
```

Step 8 Add an upstream port to the VLAN.

Add upstream port 0/9/0 to VLAN 50.

```
huawei(config)#port vlan 50 0/9 0
```

Step 9 Add a traffic profile.

The profile ID is 10, the CIR is 4 Mbit/s, and packets are scheduled according to the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 10 cir 4096 priority user-cos 4 priority-policy local-Setting
```

Step 10 Add a service port to the VLAN.

Add a service port to the VLAN 50, and use traffic profile 10 that meets the service requirements. The user port is 0/2/0.

```
huawei(config)#service-port vlan 50 gpon 0/2/0 ont 1 gempport 10 inbound traffic-table index 10
outbound traffic-table index 10
```

Step 11 Save the data.

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

----End

Result

After the configuration, the two branches of the enterprise can communicate with each other.

Configuration File

```
dba-profile add profile-name DBA_10M type3 assure 10240 max 10240
ont-lineprofile gpon profile-id 10
tcont 4 dba-profile-name DBA_10M
gem add 10 eth tcont 4
gem mapping 10 0 vlan 10
commit
quit
ont-srvprofile gpon profile-id 10
ont-port eth adaptive
port vlan eth 1 10
commit
interface gpon 0/2
port 0 ont-auto-find enable
ont add 0 password-auth 0100000001 always-on omci ont-lineprofile-id 10 ont-srvprofile-id 10
quit
vlan 50 smart
vlan attrib 50 q-in-q
bpdu tunnel vlan 50 enable
port vlan 50 0/9 0
traffic table ip index 10 cir 4096 priority user-cos 4 priority-policy local-Setting
service-port vlan 50 gpon 0/2/0 ont 1 gemport 10 inbound traffic-table index 10 outbound traffic-table
index 10
save
```

10.2.9.6 Example: Configuring VLAN Stacking Multi-ISP Wholesale Access

In a Layer-2 switching metropolitan area network (MAN), there are multiple Internet service providers (ISPs). To provision the services provided by the ISP to the specified user group rapidly, the outer VLAN tags of VLAN stacking can be used to identify ISPs, while the inner VLAN tags to identify users. In this way, different user groups can be connected to the specified ISPs in batches through different outer VLAN tags to obtain services from the ISPs.

Prerequisites

- Network devices and lines must be in the normal state.
- The authentication data of the access user must be configured on the BRAS.
- The system is working properly.

Service Requirements

- The two ISPs in the Layer-2 switching MAN provide broadband services to enterprise users. Different enterprise user groups are bulk connected to the specified ISP to obtain services provided by the ISP.
- The access device uses GPON access.

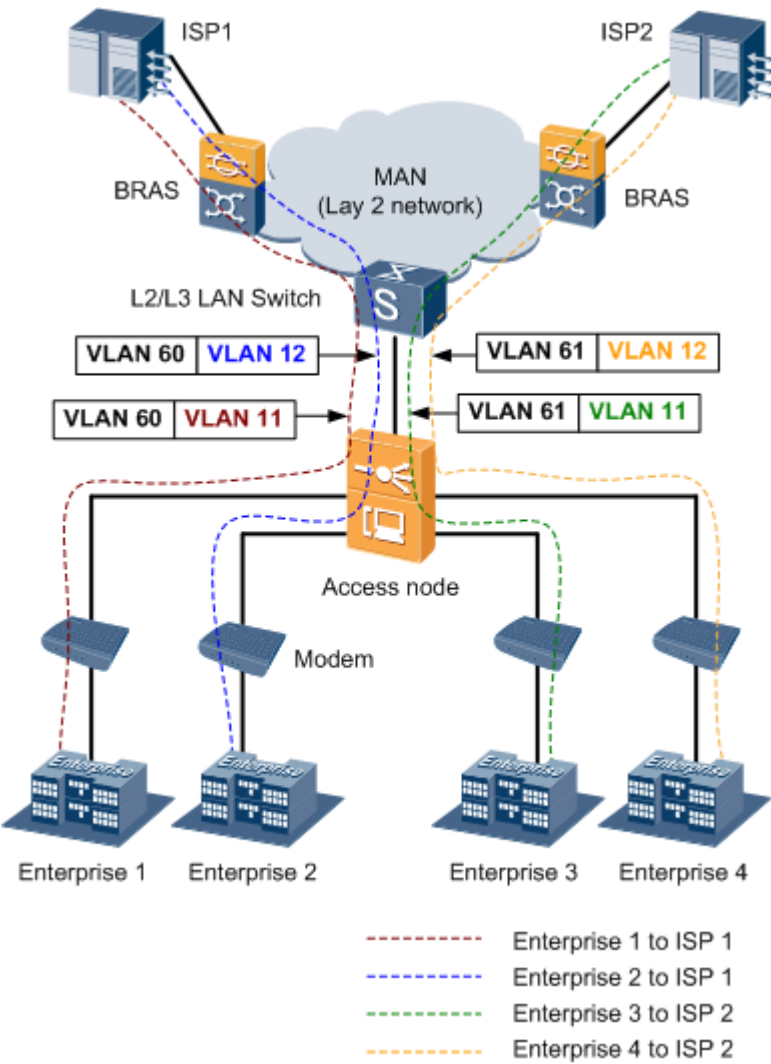
Networking

Figure 10-17 shows an example network for configuring the VLAN stacking multi-ISP wholesale access.

Enterprise 1 and 2 belong to ISP 1, and enterprise 3 and 4 belong to ISP 2. Based on the VLAN stacking feature. The upper-layer network must work in the Layer 2 mode, and must forward packets according to the VLAN and the MAC address. The MA5800 adds the outer VLAN tag to differentiate ISPs and inner VLAN tag to differentiate users and forwards the user packet to the Layer 2 network. Then the Layer 2/Layer 3 LAN switch forwards the user packets to the specified ISP BRAS

based on the outer VLAN tag. The ISP BRAS removes the outer VLAN tag and identify the users based on the inner VLAN tag. After passing the authentication, the enterprise users can obtain various services provided by the ISP.

Figure 10-17 Example network for configuring the VLAN stacking multi-ISP wholesale access



Data Plan

Table 10-17 lists the key data planning of the VLAN stacking wholesale service on the MA5800.

Table 10-17 Data plan for configuring the VLAN stacking wholesale service

Item	Data	Remarks
VLAN	VLAN ID: - ISP1: 60 - Enterprise user 1: 11 - Enterprise user 2: 12 - ISP2: 61 - Enterprise user 3: 11 - Enterprise user 4: 12 - VLAN type: smart VLAN - VLAN attribute: stacking	The outer VLAN identifies the ISP, and inner VLAN identifies the user. The inner VLAN tags must be unique under the same ISP, but can be the same under different ISPs.
Upstream port	0/9/0	-
Traffic profile	- Traffic profile ID: 10 - CIR: 2 Mbit/s - Priority copy policy: user-cos - Default 802.1p priority of the packet: 4 - Priority-based scheduling policy of the downstream packets: local-setting	The CIR depends on the user bandwidth requirement.
GPON port	- GPON port ID: - Enterprise user 1: 0/2/0 - Enterprise user 2: 0/2/1 - Enterprise user 3: 0/3/0 - Enterprise user 4: 0/3/1 - DBA profile: - Profile type: type3 - Profile name: DBA_bandwidth - Assured bandwidth: 10 Mbit/s - ONT line profile - Profile ID: 10 - T-CONT ID: 4 - Default ONT service profile ID: 0 - Default ONT alarm profile ID: 1	-

Item	Data	Remarks
Service virtual port	• Service port ID: – Enterprise user 1: 0 – Enterprise user 2: 1 – Enterprise user 3: 2 – Enterprise user 4: 3 • ID of the traffic profile in Rx direction: 10 • ID of the traffic profile in Tx direction: 10	• The VPI/VCI is the same as the management VPI/VCI on the peer modem.

Procedure

Step 1 Configure a DBA profile.

The profile type is Type3, assured bandwidth is 10 Mbit/s, and profile name is DBA_10M.

```
huawei(config)#dba-profile add profile-name DBA_10M type3 assure 10240 max 10240
```

Step 2 Configure a GPON ONT line profile.

Create a GPON ONT line profile with an index number of 10, and T-CONT ID is 4.

```
huawei(config)#ont-lineprofile gpon profile-id 10
huawei(config-gpon-lineprofile-10)#tcont 4 dba-profile-name DBA_10M
huawei(config-gpon-lineprofile-10)#gem add 10 eth tcont 4
huawei(config-gpon-lineprofile-10)#gem add 11 eth tcont 4
huawei(config-gpon-lineprofile-10)#gem mapping 10 0 vlan 60
huawei(config-gpon-lineprofile-10)#gem mapping 11 0 vlan 61
huawei(config-gpon-lineprofile-10)#commit
huawei(config-gpon-lineprofile-10)#quit
```

Step 3 Create VLANs.

The outer VLAN IDs are 60 and 61, and the VLANs are smart VLANs.

```
huawei(config)#vlan 60-61 smart
It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
Are you sure to add VLANs? (y/n)[n]:y
```

Step 4 Set the VLAN attribute to stacking.

```
huawei(config)#vlan attrib 60-61 stacking
It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
Are you sure to continue? (y/n)[n]:y
```

Step 5 Add an upstream port to the VLANs.

Add an upstream port 0/9/0 to VLANs 60 and 61.

```
huawei(config)#port vlan 60-61 0/9 0
It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
Are you sure to add standard port(s)? (y/n)[n]:y
```

Step 6 Add a traffic profile.

The profile ID is 10, the CIR is 2 Mbit/s, and packets are scheduled according to the priority specified in the traffic profile.

```
huawei(config)#traffic table ip index 10 cir 2048 priority user-cos 4 priority-policy local-Setting
```

Step 7 Configure a GPON ONT.

Enable the automatic ONT discovery function. The following uses port 0/2/0 as an example. The configuration of the other three GPON ports are similar to that of port 0/2/0.

```
huawei(config)#interface gpon 0/2
huawei(config-if-gpon-0/2)#port 0 ont-auto-find enable
huawei(config-if-gpon-0/2)#ont add 0 password-auth 0100000001 always-on omci ont-lineprofile-id 10
ont-srvprofile-id 0
huawei(config-if-gpon-0/2)#quit
```

Step 8 Add service ports to the VLANs.

Add service ports to the VLANs, and use traffic profile 10 that meets the service requirements.

```
huawei(config)#service-port 0 vlan 60 gpon 0/2/0 ont 1 gemport 10 rx-cttr 10 tx-cttr 10
huawei(config)#service-port 1 vlan 60 gpon 0/2/1 ont 1 gemport 10 rx-cttr 10 tx-cttr 10
huawei(config)#service-port 2 vlan 61 gpon 0/3/0 ont 1 gemport 11 rx-cttr 10 tx-cttr 10
huawei(config)#service-port 3 vlan 61 gpon 0/3/1 ont 1 gemport 11 rx-cttr 10 tx-cttr 10
```

Step 9 Set the inner VLAN tags.

The inner VLAN tag identifies the user. Note that the inner VLAN tag must be unique in one ISP domain, and the inner VLAN tags can be the same in different ISP domains.

```
huawei(config)#stacking label service-port 0 11
huawei(config)#stacking label service-port 1 12
huawei(config)#stacking label service-port 2 11
huawei(config)#stacking label service-port 3 12
```

Step 10 Save the data.

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

----End

Result

- After passing the authentication by the ISP1 BRAS, enterprise 1 and enterprise 2 can obtain the service provided by ISP1.
- After passing the authentication by the ISP2 BRAS, enterprise 3 and enterprise 4 can obtain the service provided by ISP2.

Configuration File

```
dba-profile add profile-name DBA_10M type3 assure 10240 max 10240
ont-lineprofile gpon profile-id 10
tcont 4 dba-profile-name DBA_10M
gem add 10 eth tcont 4
gem add 11 eth tcont 4
gem mapping 10 0 vlan 60
gem mapping 11 0 vlan 61
commit
quit
vlan 60-61 smart
```

```
It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
Are you sure to add VLANs? (y/n)[n]:y
The total of the VLANs having been processed is 2
The total of the added VLANs is 2

vlan attrib 60-61 stacking
It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
Are you sure to continue? (y/n)[n]:y
The total of the VLANs having been processed is 2
The total of the VLAN(s) which have been operated successfully is 2
port vlan 60-61 0/9 0
It will take several minutes, and console may be timeout, please use command
idle-timeout to set time limit
Are you sure to add standard port(s)? (y/n)[n]:y
The total of the VLANs having been processed is 2
The total of the port VLAN(s) having been added is 2
traffic table ip index 100 cir 2048 priority user-cos 4 priority-policy local-Setting
interface gpon 0/2
port 0 ont-auto-find enable
ont add 0 password-auth 0100000001 always-on omci ont-lineprofile-id 0 ont-srvprofile-id 0
quit
service-port 0 vlan 60 gpon 0/2/0 ont 1 gemport 10 rx-cttr 10 tx-cttr 10
service-port 1 vlan 60 gpon 0/2/1 ont 1 gemport 10 rx-cttr 10 tx-cttr 10
service-port 2 vlan 61 gpon 0/3/0 ont 1 gemport 11 rx-cttr 10 tx-cttr 10
service-port 3 vlan 61 gpon 0/3/1 ont 1 gemport 11 rx-cttr 10 tx-cttr 10
stacking label service-port 0 11
stacking label service-port 1 12
stacking label service-port 2 11
stacking label service-port 3 12
save
```

10.2.10 VLAN Reference Standards and Protocols

The following lists the reference standards and protocols of this feature:

Table 10-18 Reference standards and protocols of VLAN feature

Document name	Description
IEEE 802.1Q	IEEE standards for Local and metropolitan area networks-Virtual Bridged Local Area Networks
IEEE 802.1ad	Virtual Bridged Local Area Networks Amendment 4: Provider Bridges
RFC3069	VLAN Aggregation for Efficient IP Address Allocation

10.3 Service Flow

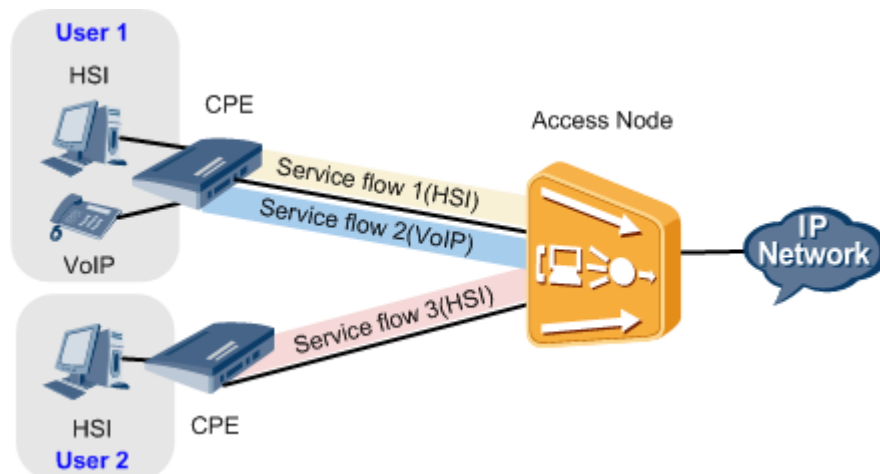
10.3.1 Introduction to Service Flow

An access device provides services to a large number of users, and each user requires multiple types of services (for example, HSI and VoIP services). The access device is required to differentiate between different user services when processing user packets, so that the services do not interfere with each other. To address this requirement, the access node provides the service flow feature.

Definition

Service flow, also called service port, is a result of traffic classification by characteristics of an Ethernet packet on a physical or logical port. Service flow is also a Layer 2 logical channel that carries services between the access node and users (Specify the Layer 2 forwarding path).

Figure 10-18 Service flows model



Services from different users (service flows 1 and 3) or services from the same user (service flows 1 and 2) are carried over different service flows.

Purpose

A service flow is the basis for provisioning each type of service on the access node. That is, the configuration of service flows is mandatory. In addition to traffic classification, a service flow is the smallest unit of user service processing. Hence, differentiated and fine-grained management, such as QoS, line identification, and security policies, of user services can be implemented based on service flows.

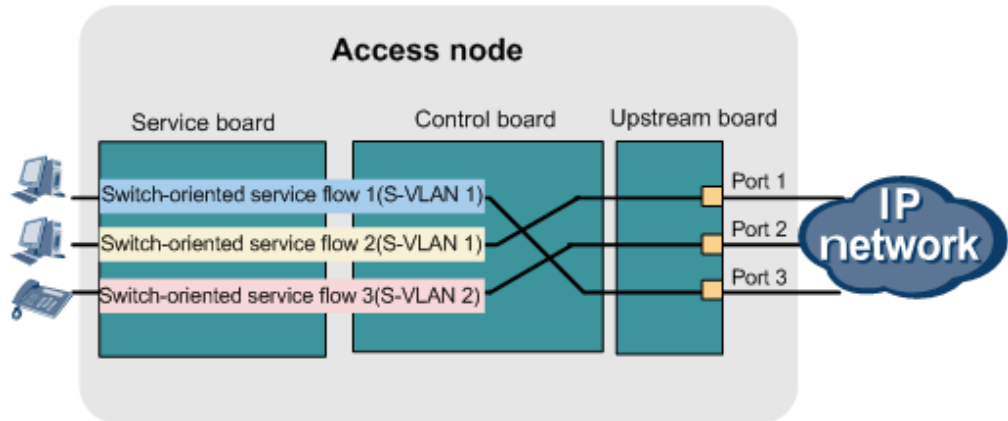
10.3.2 Service Flow Principles

Service Flow Classification

Based on the service type, service flows can be classified as follows:

- **Switch-oriented service flow:** It is a Layer 2 service channel from the user access port on a device to the VLAN (S-VLAN) of the switching core. In an S-VLAN, one upstream port can be bound to multiple switch-oriented service flows and one switch-oriented service flow can be bound to multiple upstream ports. Since user information is terminated at service boards, S-VLAN based switching is performed on the MA5800. Therefore, the service flows transmitted in the Layer 2 service channel are called switch-oriented service flows.

Figure 10-19 The schematic diagram for switch-oriented service flows



NOTE

Switching on the MA5800: When a packet arrives at the MA5800, the MA5800 selects an egress port and forwards the packet from this port. This process is called switching (or forwarding) on the MA5800.

Traffic Classification Rules

Packets are classified based on traffic classification rules, with each type of packets corresponding to a service flow. The traffic classification rule for a service flow is specified when you run the **service-port** command to add the service flow. After packets are mapped to different service flows, the system processes the service flows based on the configured policies (including VLAN translation policy and QoS policy).

Traffic classification rules supported by the MA5800 can be generalized into two types:

- Classification based on physical ports or logical ports.
- Classification based on Ethernet packet attributes (such as priority).

Table 10-19 Traffic classification rules supported by the MA5800

Service Flow Type	Classification Rule Based on Physical Ports or Logical Ports		Classification Rule Based on Ethernet Packet Attributes
	Physical Port	Logical Port Identifier	
Switch-oriented service flow	Indicates the type of the physical port for a user to access the MA5800. The options are as follows: - xPON - Ethernet - Ethernet ports on ONTs in xPON access mode: The service flow created using this type of port is an end-to-end service flow between an OLT and an ONT.	- GPON access mode: GEM port - xPON access mode: IPHOST voice port on an ONT. The IPHOST voice port is a virtual port of an ONT and implements communication between the voice chip and GMAC chip. The service flow created using this port is an end-to-end (voice) service flow between an OLT and an ONT.	Switch-oriented service flows support all the classification rules Transparent LAN service (TLS) flows are also called other-all service flows. After user packets are transparently transmitted to a VLAN, VLAN tags are added to the packets. When the packets are transmitted out of the network, VLAN tags are stripped.

Attributes of Service Flows

Table 10-20 Attributes of service flows

Name	Description	Configuration Command
Service flow index	Each service flow has a unique index on the MA5800. The index can be used when other features based on the service flow are configured. For example, you can configure a user as a multicast user simply by specifying the service flow index.	service-port index
Description of the service flow	There are usually a large number of service flows in an access node. The description (for example, the area in which the user is located and service characteristics) of a service flow facilitates service maintenance.	service-port desc
Description of the remote device of the service flow	The description includes information about the remote device of the user side of a service flow and helps determine the terminal type when many types of terminals are used, which facilitates maintenance.	service-port remote-desc
Administrative status	Users can pause and resume the transmission of services on a service flow by setting the administrative status of the service flow.	service-port adminstatus

Automatic Service Flow Creation

The OLT supports pre-configuration of service flow creation policies on a PON port. Then, after an ONU goes online, services flows are automatically created based on the pre-configured policies. This function simplifies the configuration process and improves the installation and deployment efficiency.

O&M for these automatically created service flows is the same as that for commonly created service flows.

Figure 10-20 Process of automatic service flow creation (no ONU is manually added)

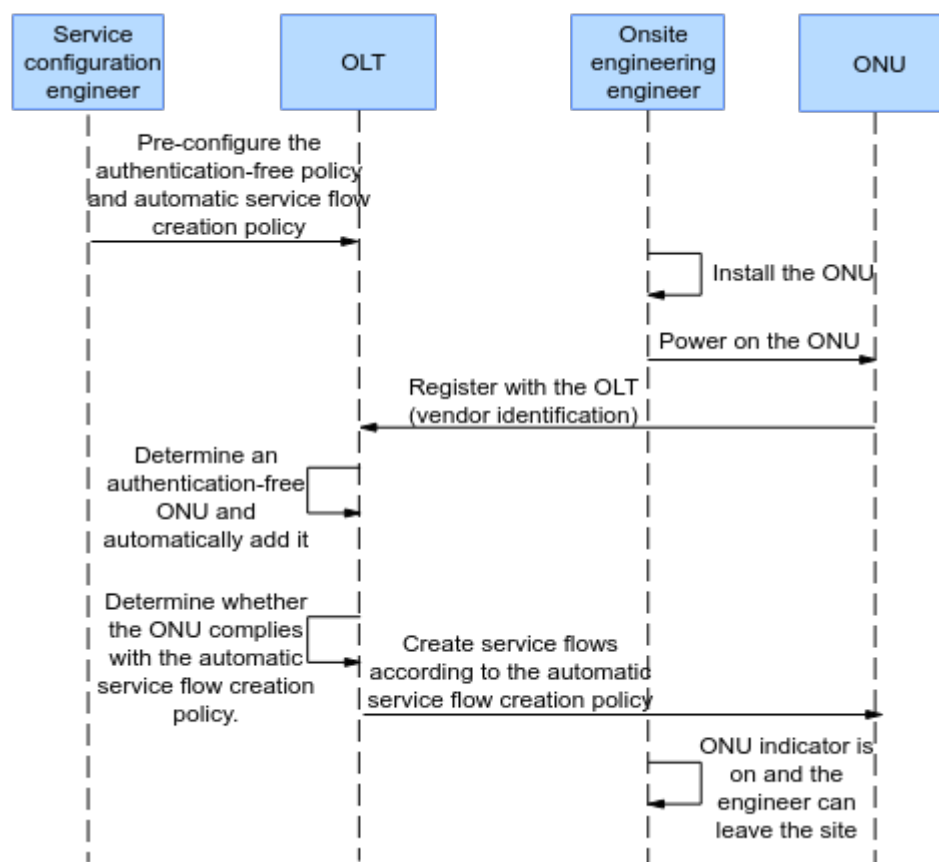
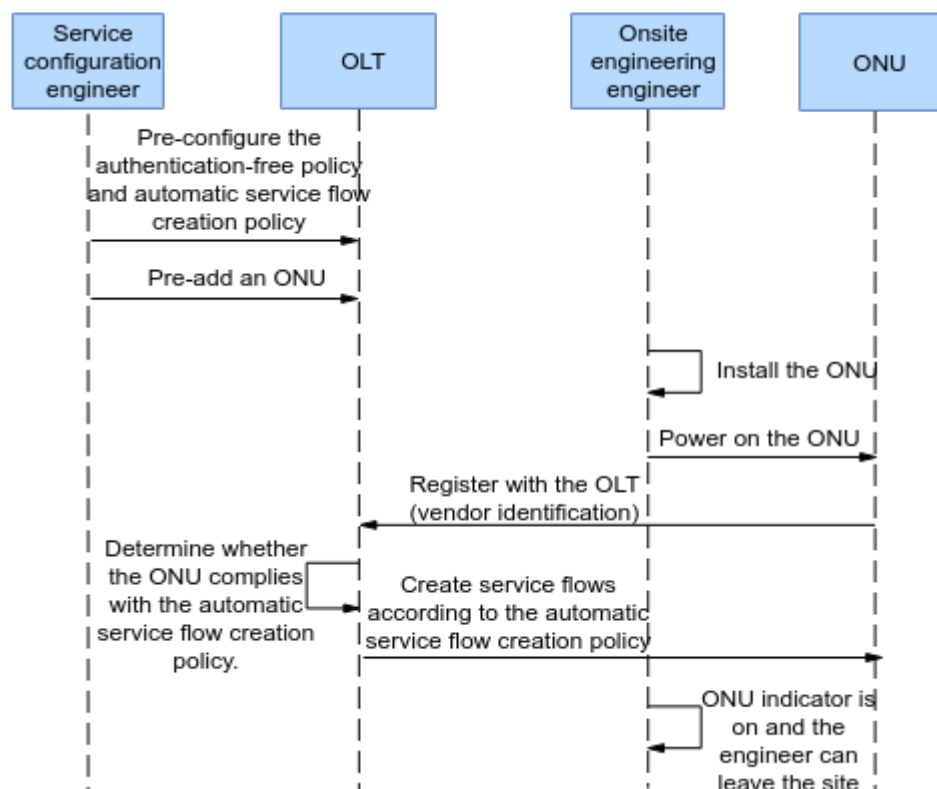


Figure 10-21 Process of automatic service flow creation (ONU is manually added)

10.3.3 Configuring Service Flow

The method of configuring service flows varies according to the access mode. You can locate the desired configuration description according to the access mode.

10.3.3.1 Creating an Ethernet Service Flow

An Ethernet service flow is a service channel connecting the user side to the network side. Configure a service flow before provisioning services.

Context

A service flow can carry a single service or multiple services. A multi-service flow is used to carry triple-play services. A service port can carry a single service flow or multiple service flows. If a service port carries multiple service flows, the OLT supports traffic classification and identifies users or services based on:

- User-side VLAN.
- User-side service encapsulation type. For example, PPPoE is used for the Internet access service and IPoE is used for multicast services.
- VLAN+user-side packet priority. For example, the priority of multicast services is higher than that of the Internet access service.
- VLAN+user-side service encapsulation type.

Before creating a service flow, run the **display traffic table** command to query whether the desired traffic profile has existed in the system. If no desired traffic

profile is available, run the **traffic table ip** command to create a traffic profile for the service flow. The OLT provides seven default traffic profiles with IDs ranging from 0 to 6.

Table 10-21 lists the default settings of a service flow.

Table 10-21 Default settings of a service flow

Parameter	Default Setting
Traffic profile ID	0-6
Management status	Activated

Procedure

Step 1 Create a service flow or multiple service flows in batches.

- Run the **service-port** command to create a service flow.
 - Single-service flow:
Select **single-service** or do not set **multi-service**.
 - Multi-service flow based on the user-side VLAN:
Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** | **other-all** }.
 - **untagged**: If this parameter is specified, user packets do not carry a tag.
 - *user-vlanid*: If this parameter is specified, user packets carry a tag, which is the customer VLAN (C-VLAN).
 - **priority-tagged**: When **priority-tagged** is selected, the VLAN tag is 0 and the priorities of user-side packets are 0-7. (The highest priority is 7.)
 - **other-all**: If this parameter is specified, the created service flow carries QinQ transparent LAN service (TLS) services for enterprises. User packets are matched based on the specified user VLAN (or untagged attribute). The unmatched packets are transmitted on the TLS service flow to the upper-layer network.
 - Multi-service flow based on the user-side service encapsulation mode:
Select **multi-service user-encap** *user-encap*.
 - Multi-service flow based on the VLAN+user-side packet priority (802.1p)
Select **multi-service user-8021p** *user-8021p* [**user-vlan** *user-vlanid*].
 - Multi-service flow based on the VLAN+user-side service encapsulation mode (user-encap)
Select **multi-service user-vlan** { **untagged** | *user-vlanid* | **priority-tagged** } **user-encap** *user-encap*.

 NOTE

- The OLT supports the service flow configuration by index. Each service flow has a unique index. In this manner, users do not need to input a large number of flow parameters, thereby simplifying service flow configurations. When creating a service flow, the service flow index parameter *index* is optional. If *index* is not set, the OLT automatically allocates an idle index starting from the configured maximum index, regardless of whether the maximum index has been deleted. If the idle index is greater than the upper index threshold, the OLT searches for the new idle index starting from 0.
 - **vlan** is an S-VLAN, which can only be a smart or MUX VLAN.
 - The access mode can be ATM or PTM. In ATM access mode, the VPI and VCI must be input and the same as the VPI and VCI of the access terminal.
 - **rx-cttr** is the same as **outbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the user side to the network side.
- Run the **multi-service-port** command to create service flows in batches.

Step 2 (Optional) Run the **service-port desc** command to configure the description of the service flow. The description includes the purpose of the service flow creation and the services carried over the service flow. Therefore, the description of the service flow facilitates maintenance.

Step 3 (Optional) Run the **service-port index adminstatus** command to configure the management status of the service flow. A service port activated by default.

A service can be provisioned at two levels: port level and service flow level. The service takes effect only after both the access port and service flow are activated.

----End

Example

The following configurations are used as an example to provision the Internet access service: The access port is 0/4/1. The ID of the user side VLAN is 2. The ID of the upstream VLAN is 100. The Internet access service uses traffic profile 8. The profile name is net, the CIR is set to 10240, the upstream priority is set to 0, and the packet priority selection policy is the traffic profile for scheduling based on the local priority.

```
huawei(config)#traffic table ip index 8 name net cir 10240 priority 0 priority-policy
local-setting
Create traffic descriptor record successfully
-----
TD Index      : 8
TD Name       : net
Priority      : 0
Copy Priority  : -
CTAG Mapping Priority: -
CTAG Default Priority: 0
Priority Policy : local-pri
CIR           : 10240 kbps
CBS           : 329680 bytes
PIR           : 20480 kbps
PBS           : 657360 bytes
Color Mode    : color-blind
Referenced Status : not used
-----
huawei(config)#service-port 1 vlan 100 eth 0/4/1 multi-service user-vlan 2 rx-cttr 8 tx-cttr 8
```

10.3.3.2 Creating a GPON Service Flow

A GPON service flow is a service channel connecting the user side to the network side. Configure a service flow before provisioning services.

Context

A service flow can carry a single service or multiple services. A multi-service flow is used to carry triple-play services. A service port can carry a single service flow or multiple service flows. If a service port carries multiple service flows, the OLT supports traffic classification and identifies users or services based on:

- User-side VLAN.
- User-side service encapsulation type.
- VLAN+user-side packet priority.
- VLAN+user-side service encapsulation type.

Table 10-22 lists the default settings of a service flow.

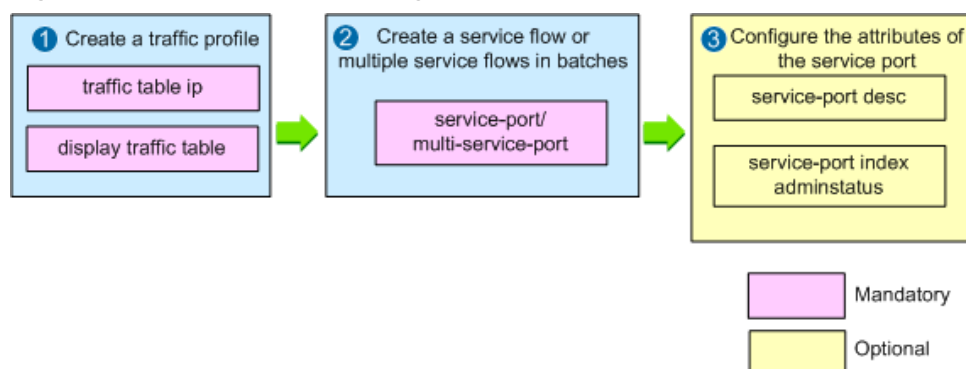
Table 10-22 Default settings of a service flow

Parameter	Default Setting
Traffic profile ID	0-6
Management status	Activated

Configuration Process

Figure 10-22 shows the process of creating a GPON service flow.

Figure 10-22 Process of creating a GPON service flow



Procedure

Step 1 Create a traffic profile.

Run the **traffic table ip** command to create a traffic profile. The OLT provides seven default traffic profiles with IDs ranging from 0 to 6.

Before creating a service flow, run the **display traffic table** command to query whether the desired traffic profile has existed in the system. If no desired traffic

profile is available, run the **traffic table ip** command to create a traffic profile for the service flow.

Step 2 Create a service flow or multiple service flows in batches.

- Run the **service-port** command to create a service flow.
 - Single-service flow:
Do not set **multi-service**.
 - Multi-service flow based on the user-side VLAN:
Select **multi-service user-vlan { untagged | user-vlanid | priority-tagged | other-all }**.
 - **untagged**: If this parameter is specified, user packets do not carry a tag.
 - *user-vlanid*: If this parameter is specified, user packets carry a tag, which is the customer VLAN (C-VLAN).
 - **priority-tagged**: When priority-tagged is selected, the VLAN tag is 0 and the priorities of user-side packets are 0-7.
 - **other-all**: If this parameter is specified, the created service flow carries QinQ transparent LAN service (TLS) services for enterprises. User packets are matched based on the specified user VLAN (or untagged attribute). The unmatched packets are transmitted on the TLS service flow to the upper-layer network.
 - Multi-service flow based on the user-side service encapsulation mode:
Select **multi-service user-encap user-encap**.
 - Multi-service flow based on the VLAN+user-side packet priority (802.1p)
Select **multi-service user-8021p user-8021p [user-vlan user-vlanid]**.
 - Multi-service flow based on the VLAN+user-side service encapsulation mode (user-encap)
Select **multi-service user-vlan { untagged | user-vlanid | priority-tagged } user-encap user-encap**.

 NOTE

- The OLT supports the service flow configuration by index. Each service flow has a unique index. In this manner, users do not need to input a large number of flow parameters, thereby simplifying service flow configurations. When creating a service flow, the service flow index parameter *index* is optional. If *index* is not set, the OLT automatically allocates an idle index starting from the minimum unused value.
- **vlan** is an S-VLAN, which can only be a smart or MUX VLAN.
- **rx-cttr** is the same as **outbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the user side to the network side. The traffic profile bound to the service flow is the one created in [Step 1](#).
- Run the **multi-service-port** command to create service flows in batches.

Step 3 Configure the attributes of the service port. Configure the attributes of the service port according to requirements.

- Run the **service-port desc** command to configure the description of the service flow. The description includes the purpose of the service flow creation

and the services carried over the service flow. Therefore, the description of the service flow facilitates maintenance.

- Run the **service-port index adminstatus** command to configure the management status of the service flow. A service port activated by default.

A service can be provisioned at two levels: port level and service flow level. The service takes effect only after both the access port and service flow are activated.

----End

Example

The following configurations are used as an example to provision the Internet access service for a user:

- GPON port 0/2/0 on an OLT connects to an ONT.
- The planned configurations of the user are as follows:
 - The rate of the Internet access service is 4096 Kbit/s.
 - The index of the GEM port carrying the Internet access service is 135.
 - The ID of the service VLAN (S-VLAN) is 1000.
- No proper traffic profile is available and traffic profile 10 is created.
- The user has not registered. Do not provision the Internet access service for the user.

```
huawei(config)#traffic table ip index 10 cir 4096 priority 3 priority-policy local-Setting
huawei(config)#service-port 5 vlan 1000 gpon 0/2/0 ont 1 gemport 135 inbound traffic-table index 10
outbound traffic-table index 10
huawei(config)#service-port 5 adminstatus disable
```

The following configurations are used as an example to provision the Internet access service for a commercial user:

- GPON port 0/2/0 on an OLT connects to an ONT.
- The planned configurations of the user are as follows:
 - The rate of the Internet access service is 8192 Kbit/s.
 - The Internet access service is in multi-service mode to facilitate follow-up service expansion.
 - The user is identified by C-VLAN.
 - The ID of the S-VLAN is 1023.
 - The ID of the C-VLAN is 100.
 - The index of the GEM port carrying the Internet access service is 130.
- No proper traffic profile is available and traffic profile 8 is created.
- The description of the service flow is added to facilitate maintenance.
- The Internet access service needs to be provisioned immediately.

```
huawei(config)#traffic table ip index 8 cir 8192 priority 4 priority-policy local-Setting
huawei(config)#service-port 10 vlan 1023 gpon 0/2/0 gemport ont 1 130 multi-service user-vlan 100
inbound traffic-table index 8 outbound traffic-table index 8
huawei(config)#service-port desc 10 description gpon/vlanid:1023/uservlan:100
```

10.3.3.3 Creating a GPON Service Flow (in Profile Mode with Universal Configurations)

A GPON service flow is a service channel connecting the user side to the network side. Configure a service flow before provisioning services.

Context

A service flow can carry a single service or multiple services. A multi-service flow is used to carry triple-play services. A service port can carry a single service flow or multiple service flows. If a service port carries multiple service flows, the OLT supports traffic classification and identifies users or services based on:

- User-side VLAN.
- User-side service encapsulation type.
- VLAN+user-side packet priority.
- VLAN+user-side service encapsulation type.

Table 10-23 lists the default settings of a service flow.

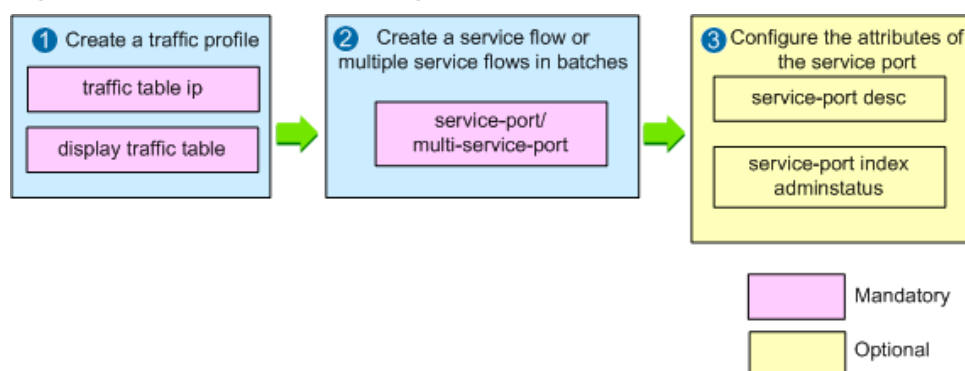
Table 10-23 Default settings of a service flow

Parameter	Default Setting
Traffic profile ID	0-6
Management status	Activated

Configuration Process

Figure 10-23 shows the process of creating a GPON service flow.

Figure 10-23 Process of creating a GPON service flow



Procedure

Step 1 Create a traffic profile.

Run the **traffic table ip** command to create a traffic profile. The OLT provides seven default traffic profiles with IDs ranging from 0 to 6.

Before creating a service flow, run the **display traffic table** command to query whether the desired traffic profile has existed in the system. If no desired traffic profile is available, run the **traffic table ip** command to create a traffic profile for the service flow.

Step 2 Create a service flow or multiple service flows in batches.

- Run the **service-port** command to create a service flow.
 - Single-service flow:
Do not set **multi-service**.
 - Multi-service flow based on the user-side VLAN:
Select **multi-service user-vlan { untagged | user-vlanid | priority-tagged | other-all }**.
 - **untagged**: If this parameter is specified, user packets do not carry a tag.
 - *user-vlanid*: If this parameter is specified, user packets carry a tag, which is the customer VLAN (C-VLAN).
 - **priority-tagged**: When priority-tagged is selected, the VLAN tag is 0 and the priorities of user-side packets are 0-7.
 - **other-all**: If this parameter is specified, the created service flow carries QinQ transparent LAN service (TLS) services for enterprises. User packets are matched based on the specified user VLAN (or untagged attribute). The unmatched packets are transmitted on the TLS service flow to the upper-layer network.
 - Multi-service flow based on the user-side service encapsulation mode:
Select **multi-service user-encap user-encap**.
 - Multi-service flow based on the VLAN+user-side packet priority (802.1p)
Select **multi-service user-8021p user-8021p [user-vlan user-vlanid]**.
 - Multi-service flow based on the VLAN+user-side service encapsulation mode (user-encap)
Select **multi-service user-vlan { untagged | user-vlanid | priority-tagged } user-encap user-encap**.

 NOTE

- The OLT supports the service flow configuration by index. Each service flow has a unique index. In this manner, users do not need to input a large number of flow parameters, thereby simplifying service flow configurations. When creating a service flow, the service flow index parameter *index* is optional. If *index* is not set, the OLT automatically allocates an idle index starting from the configured maximum index, regardless of whether the maximum index has been deleted. If the idle index is greater than the upper index threshold, the OLT searches for the new idle index starting from 0.
 - **vlan** is an S-VLAN, which can only be a smart or MUX VLAN.
 - **rx-cttr** is the same as **outbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the user side to the network side. The traffic profile bound to the service flow is the one created in [Step 1](#).
- Run the **multi-service-port** command to create service flows in batches.

Step 3 Configure the attributes of the service port. Configure the attributes of the service port according to requirements.

- Run the **service-port desc** command to configure the description of the service flow. The description includes the purpose of the service flow creation and the services carried over the service flow. Therefore, the description of the service flow facilitates maintenance.
- Run the **service-port index adminstatus** command to configure the management status of the service flow. A service port activated by default.
A service can be provisioned at two levels: port level and service flow level. The service takes effect only after both the access port and service flow are activated.

----End

Example

The following configurations are used as an example to provision the Internet access service for a user:

- GPON port 0/2/0 on an OLT connects to ONT 1.
- The planned configurations of the user are as follows:
 - The rate of the Internet access service is 4096 Kbit/s.
 - The index of the GEM port carrying the Internet access service is 126.
 - The ID of the service VLAN (S-VLAN) is 1000.
- No proper traffic profile is available and traffic profile 10 is created.
- The user has not registered. Do not provision the Internet access service for the user.

```
huawei(config)#traffic table ip index 10 cir 4096 priority 3 priority-policy local-Setting
Create traffic descriptor record successfully
-----
TD Index      : 10
TD Name       : ip-traffic-table_10
Priority      : 3
Mapping Priority : -
Mapping Index  : -
CTAG Mapping Priority: -
CTAG Mapping Index : -
CTAG Default Priority: 0
Priority Policy : local-pri
CIR            : 4096 kbps
CBS            : 133072 bytes
PIR            : 8192 kbps
PBS            : 264144 bytes
Fix            : 0 kbps
CAR Threshold Profile: -
Color Mode     : color-blind
Color policy    : dei
Referenced Status : not used
-----
huawei(config)#service-port 5 vlan 1000 gpon 0/2/0 ont 1 gemport 126 inbound
traffic-table index 10 outbound traffic-table index 10
huawei(config)#service-port 5 adminstatus disable
```

The following configurations are used as an example to provision the Internet access service for a commercial user:

- GPON port 0/2/0 on an OLT connects to ONT 2.
- The planned configurations of the user are as follows:
 - The rate of the Internet access service is 8192 Kbit/s.
 - The Internet access service is in multi-service mode to facilitate follow-up service expansion.
 - The user is identified by C-VLAN.
 - The ID of the S-VLAN is 1023.
 - The ID of the C-VLAN is 100.
 - The index of the GEM port carrying the Internet access service is 126.
- No proper traffic profile is available and traffic profile 8 is created.
- The description of the service flow is added to facilitate maintenance.
- The Internet access service needs to be provisioned immediately.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:
```

Command:

display traffic table ip from-index 0

TID	CIR (kbps)	CBS (bytes)	PIR (kbps)	PBS (bytes)	Pri	Copy-policy	Pri-Policy
0	1024	34768	2048	69536	6	-	tag-pri
1	2496	81872	4992	163744	6	-	tag-pri
2	512	18384	1024	36768	0	-	tag-pri
3	576	20432	1152	40864	2	-	tag-pri
4	64	4048	128	8096	4	-	tag-pri
5	2048	67536	4096	135072	0	-	tag-pri
6	off	off	off	off	0	-	tag-pri

Total Num : 7

```
huawei(config)#traffic table ip index 8 cir 8192 priority 4 priority-policy
local-Setting
```

Create traffic descriptor record successfully

```
-----
TD Index      : 8
TD Name       : ip-traffic-table_8
Priority      : 4
Copy Priority  : -
Mapping Index : -
CTAG Mapping Priority: -
CTAG Mapping Index : -
CTAG Default Priority: 0
Priority Policy : local-pri
CIR           : 8192 kbps
CBS           : 264144 bytes
PIR           : 16384 kbps
PBS           : 526288 bytes
Fix           : 0 kbps
CAR Threshold Profile: -
Color Mode    : color-blind
Color policy  : dei
Referenced Status : not used
-----
```

```
huawei(config)#service-port 10 vlan 1023 gpon 0/2/0 ont 2 gemport 126 multi-service
user-vlan 100 inbound traffic-table index 8 outbound traffic-table index 8
huawei(config)#service-port desc 10 description gpon/Vlanid:1023/uservlan:100
```

10.3.3.4 Creating a GPON Service Flow in Profile Mode with Simplified Configurations

A GPON service flow is a service channel connecting the user side to the network side. Configure a service flow before provisioning services. In a simplified service flow, the system only cares about only the translation between the SVLAN and the CVLAN and does not care about the GEM port mapping.

Context

A service port can carry a single service or multiple services. When a service port carries multiple services, the OLT supports traffic classification. In simplified configuration mode, the OLT supports only C-VLAN-based traffic classification.

Table 10-24 lists the default settings of a service flow.

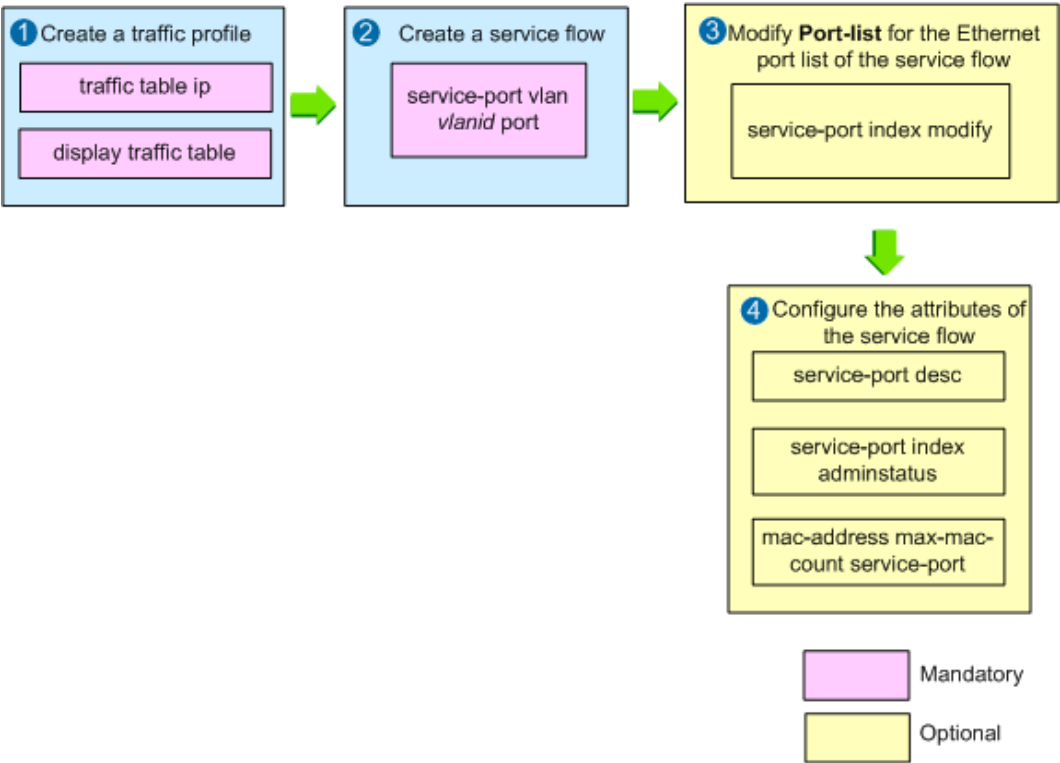
Table 10-24 Default settings of a service flow

Parameter	Default Setting
Traffic profile ID	0-6
Management status	Activated
Maximum number of learnable MAC addresses	1023

Configuration Process

Figure 10-24 shows the process of creating a GPON service flow.

Figure 10-24 Process of creating a GPON service flow



Procedure

Step 1 Run the **traffic table ip** command to create a traffic profile.

The OLT provides seven default traffic profiles with IDs ranging from 0 to 6.

Before creating a service flow, run the **display traffic table** command to check whether a traffic profile meeting service requirement is available. If no such a traffic profile is available, create a traffic profile.

Step 2 Run the **service-port vlan vlanid port** command to create a service flow.

In simplified configuration mode, a service flow is an end-to-end configuration to a port on an optical network terminal (ONT) from the OLT. Then, users only need to pay attention to the switching between the S-VLAN and C-VLAN.

- Select the type of an ONT port from **ont ontid { eth | iphost }**.
 - eth**: an Ethernet port, which is used for the Internet access or multicast service.
 - iphost**: a POTS port, which is used for the voice service.
- Select a C-VLAN tag from **multi-service user-vlan { untagged | user-vlanid }**.
 - untagged**: indicates that the user-side packets are untagged.
 - user-vlanid**: indicates that the user-side packets are tagged. The tag value is the same as the C-VLAN tag.

The preceding parameters are set based on the ONT type. Therefore, specify the ONT type before creating a service flow.

- For a bridging ONT (SFU), the ONT port provisioning the POTS service is set to **iphost** and ONT ports provisioning other services are set to **eth**.
- For a gateway ONT (HGU), the ONT port provisioning the Internet access service with untagged packets is set to **iphost**; other services cannot be configured on physical ports but on the ONT.

Table 10-25 lists the commands involved in parameter settings.

Table 10-25 Commands involved in parameter settings

Service Type	Bridging ONT	Gateway ONT
Tagged high-speed Internet (HSI) service	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> eth <i>port-index-list</i> multi-service...	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> multi-service...
Untagged HSI service	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> eth <i>port-index-list</i> multi-service...	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> iphost multi-service... NOTE Services can be identified only after a native VLAN is configured for ONT ports.

Service Type	Bridging ONT	Gateway ONT
Voice service	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> iphost multi-service...	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> multi-service...
IPTV service	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> eth <i>port-index-list</i> multi-service...	service-port [<i>index</i>] vlan <i>vlanid</i> port <i>frameid/slotid/portid</i> ont <i>ontid</i> multi-service...

In the preceding table, "..." indicates the omitted command format.

NOTE

- The OLT supports the service flow configuration by index. Each service flow has a unique index. In this manner, users do not need to input a large number of flow parameters, thereby simplifying service flow configurations. When creating a service flow, the service flow index parameter *index* is optional. If *index* is not set, the OLT automatically allocates an idle index starting from the configured maximum index, regardless of whether the maximum index has been deleted. If the idle index is greater than the upper index threshold, the OLT searches for the new idle index starting from 0.
- **vlan** is an S-VLAN, which can only be a smart or MUX VLAN.
- **rx-cttr** is the same as **outbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the network side to the user side. **tx-cttr** is the same as **inbound** in terms of meaning and function. Either parameter indicates the index of the service flow from the user side to the network side. The traffic profile bound to the service flow is the one created in [Step 1](#).

Step 3 (Optional) Run the **service-port index modify** command to modify **Port-list** for the Ethernet port list of the service flow.

Perform this step if the service planning for a user port is changed.

Step 4 (Optional) Configure the attributes of the service flow.

- Run the **service-port desc** command to configure the description of the service flow. The description includes the purpose of the service flow creation and the services carried over the service flow. Therefore, the description of the service flow facilitates maintenance.
- Run the **service-port index adminstatus** command to configure the management status of the service flow. A service port activated by default. A service can be provisioned at two levels: port level and service flow level. The service takes effect only after both the access port and service flow are activated.
- Run the **mac-address max-mac-count service-port** command to set the maximum number of MAC addresses learned by the service port. This configuration restricts the maximum number of PCs that can access the Internet by using the same user account. The maximum number of learnable MAC addresses of a service flow is 1023 by default.

----End

Example

The following configurations are used as an example to provision the Internet access service for a user:

- GPON port 0/2/0 on an OLT connects to ONT 1.
- The planned configurations of the user are as follows:
 - The rate of the Internet access service is 4096 kbit/s.
 - The user connects to Ethernet port 1 on the ONT.
 - The ID of the service VLAN (S-VLAN) is 1000.
 - At most three users can concurrently access the Internet using the same account.
- No proper traffic profile is available and traffic profile **hsi** is created.
- The user has not registered. Do not provision the Internet access service for the user.

```
huawei(config)#traffic table ip name hsi cir 4096 priority 3 priority-policy local-Setting
```

al-Setting

Create traffic descriptor record successfully

```
-----
TD Index      : 10
TD Name       : hsi
Priority       : 3
Copy Priority   : -
Mapping Index  : -
CTAG Mapping Priority: -
CTAG Mapping Index : -
CTAG Default Priority: 0
Priority Policy : local-pri
CIR           : 4096 kbps
CBS           : 133072 bytes
PIR           : 8192 kbps
PBS           : 264144 bytes
Fix           : 0 kbps
CAR Threshold Profile: -
Color Mode     : color-blind
Color policy    : dei
Referenced Status : not used
-----
```

```
huawei(config)#service-port 5 vlan 1000 gpon 0/2/0 ont 1 gemport 120 inbound traffic-table name hsi
outbound traffic-table name hsi
```

```
huawei(config)#mac-address max-mac-count service-port 5 3
```

```
huawei(config)#service-port 5 adminstatus disable
```

The following configurations are used as an example to provision the Internet access service for a commercial user:

- GPON port 0/2/0 on an OLT connects to ONT 2.
- The planned configurations of the user are as follows:
 - The rate of the Internet access service is 8192 kbit/s.
 - The Internet access service is in multi-service mode to facilitate follow-up service expansion.
 - The user is identified by customer VLAN (C-VLAN).
 - The ID of the S-VLAN is 1023.
 - The ID of the C-VLAN is 100.
 - ONT port 2 connects to the service flow.
- No proper traffic profile is available and traffic profile **internet** is created.

- The description of the service flow is added to facilitate maintenance.
- The Internet access service needs to be provisioned immediately.

```
huawei(config)#display traffic table ip from-index 0
{ <cr>|to-index<K> }:
```

Command:

```
display traffic table ip from-index 0
```

TID	CIR(kbps)	CBS(bytes)	PIR(kbps)	PBS(bytes)	Pri	Copy-policy	Pri-Policy
0	1024	34768	2048	69536	6	-	tag-pri
1	2496	81872	4992	163744	6	-	tag-pri
2	512	18384	1024	36768	0	-	tag-pri
3	576	20432	1152	40864	2	-	tag-pri
4	64	4048	128	8096	4	-	tag-pri
5	2048	67536	4096	135072	0	-	tag-pri
6	off	off	off	off	0	-	tag-pri

Total Num : 7

```
huawei(config)#traffic table ip name internet cir 8192 priority 4 priority-policy local-Setting
Create traffic descriptor record successfully
```

```
-----
TD Index      : 8
TD Name       : internet
Priority      : 4
Copy Priority  : -
Mapping Index : -
CTAG Mapping Priority: -
CTAG Mapping Index : -
CTAG Default Priority: 0
Priority Policy : local-pri
CIR           : 8192 kbps
CBS           : 264144 bytes
PIR           : 16384 kbps
PBS           : 526288 bytes
Fix           : 0 kbps
CAR Threshold Profile: -
Color Mode    : color-blind
Color policy  : dei
Referenced Status : not used
-----
```

```
huawei(config)#service-port 10 vlan 1023 port 0/2/0 ont 2 eth 2 multi-service user-vlan 100 inbound
traffic-table name internet outbound traffic-table name internet
huawei(config)#service-port desc 10 description gpon/Vlanid:1023/uservlan:100
```

A home user initially configures the Internet access service on ONT port 1. Later, the user needs to use the Internet access service ONT ports 2 and 3. The original service flow ID is 10.

```
huawei(config)#service-port 10 modify ont eth 1-3
```

10.3.3.5 Configuring Automatic Service Flow Creation (GPON)

The OLT supports configuration of service flow creation policies on PON ports. After an ONU goes online under the PON port, service flows are automatically created according to the preset policies. This topic uses MA5671-24FE as an example for the ONU. Configuration methods are similar for other device models.

Data Plan

Table 10-26 Key data plan

Item	Data
Networking data	Upstream port: 0/9/0 PON port: 0/1/0 ONU ID: 1
VLAN	Internet access VLAN (SVLAN): - SVLAN ID: 100 - SVLAN type: smart - For the SVLAN planned with single-tagged VLAN, the attribute of the SVLAN is common by default and no configuration is required. For the SVLAN planned with double-tagged VLAN, the attribute of the SVLAN is QinQ or stacking. For a PC connected on the user side, user packets are untagged.
Traffic profile	Profile name: ftto_hsi CIR: 10 Mbit/s PIR: 20 Mbit/s Priority policy: user-cos Default 802.1p priority of packets: 0 Enqueuing priority scheduling policy of packets: Tag-In-Package
Automatic flow creation policy	Maximum number of flows automatically created on the ONU: 24 (If the actual flow number exceeds 24, extra flows can still be created successfully. However, an alarm, which indicates that the flow number range is exceeded, is reported.) Upstream traffic profile: ftto_hsi Downstream traffic profile: ftto_hsi VLAN translation policy: - When a service flow with the single-tagged VLAN is created, all ONUs have the same CVLAN range, the OLT implements VLAN translation, and the SVLAN is added in the upstream direction. That is, CVLAN<->SVLAN. - When a service flow with the double-tagged VLAN is created, all ONUs have the same CVLAN range, and the OLT implements VLAN translation. The start value of inner VLAN (C'VLAN) on the network side is 2000. The SVLAN and C'VLAN are added in the upstream direction. That is, CVLAN<->SVLAN + C'VLAN.
DBA profile	Profile name: ftto_dba Profile type: Type3 Assured bandwidth: 10 Mbit/s Maximum bandwidth: 20 Mbit/s

Item	Data
ONU line profile	Profile name: ftto_line T-CONT ID: 1 GEM Port ID for the Internet access service: 1, 2, or 3 NOTE For example, to deploy services on 24 Ethernet ports, 3 GEM ports need to be configured, because each GEM port can be mapped to 8 Ethernet ports.
ONU service profile	Profile name: ftto_ser ONU port capability set: 24
ONU automatic adding policy	Device type: MA5671-F24 ONU line profile name: ftto_line ONU service profile name: ftto_ser

Procedure

Step 1 Configure an Internet access service VLAN (SVLAN).

Create Internet service VLAN 100, and add upstream port 0/9/0 to VLAN 100.

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

If the double-tagged SVLAN is planned, perform the following operation. If the single-tagged VLAN is planned, no configuration is required.

```
huawei(config)#vlan attrib 100 q-in-q
```

Step 2 Configure a traffic profile.

Run the **display traffic table ip** command to query 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 ftto_hsi cir 10240 pir 20480 priority user-cos 0 priority-policy tag-in-package
```

Step 3 Configure an automatic flow creation policy.

A PON port can be configured with one policy at one time. The policy is configured based on a PON port or board. In this example, configure the automatic flow creation policy on GPON port 0/1/0.

- Create a service flow with the single-tagged VLAN.

Create a service flow with the single-tagged VLAN on an ONU, add a specified SVLAN tag in the upstream direction, and remove the tag in the downstream direction.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#auto-service-port port 0 vlan 100 single-vlan onu-vlan-num 24
inbound traffic-table name ftto_hsi outbound traffic-table name ftto_hsi
huawei(config-if-gpon-0/1)#quit
```

- Create a service flow with the double-tagged VLAN.

Create a service flow for each port of the ONU and add the C' VLAN and SVLAN tags to the service flow in the upstream direction. The C' VLAN is calculated as Start VLAN + ONU ID x onu-vlan-num. The C' VLAN ID of the port is increased by 1. For example, if the start VLAN is 2000, ONU ID is 1, and onu-vlan-num is 24, C'VLAN ID = 2000 + 1 x 24 = 2024. For the 24 Ethernet ports of the ONU the value range of C'VLAN is 2024–2047.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#auto-service-port port 0 vlan 100 double-vlan from-vlan 2000 onu-
vlan-num 24 inbound traffic-table name ftto_hsi outbound traffic-table name ftto_hsi
huawei(config-if-gpon-0/1)#quit
```

Step 4 Configure GPON ONU profiles.

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

- DBA profile: A DBA profile describes GPON traffic parameters. A T-CONT is bound to a DBA profile for dynamic bandwidth allocation, improving upstream bandwidth usage.
- Line profile: A line profile describes the binding between the T-CONT and the DBA profile, the QoS mode of the service flow, and the mapping between the GEM port and the ONU-side service.
- Service profile: A service profile provides the service configuration channel for the ONU that is managed through OMCI.
- Alarm profile: An alarm profile contains a series of alarm thresholds to measure and monitor the performance of activated ONU lines. When a statistical value reaches the threshold, the NE is notified and an alarm is reported to the log NE 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 DBA profiles existing in the system cannot meet the requirements, you need to run the **dba-profile add** command to add one.

```
huawei(config)#dba-profile add profile-name ftto_dba type3 assure 10240 max 20480
```

NOTE

Select a DBA profile of the proper bandwidth type and configure proper bandwidths according to the service types and total number of users of the ONU. 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 ONU line profile.

Create a GPON ONU line profile named **ftto_line** and bind it to DBA profile **ftto_dba**.

```
huawei(config)#ont-lineprofile gpon profile-name ftto_line
huawei(config-gpon-lineprofile-1)#tcont 1 dba-profile-name ftto_dba
```

Bind GEM ports 1, 2, and 3 to T-CONT 1.

```
huawei(config-gpon-lineprofile-1)#gem add 1 eth tcont 1
huawei(config-gpon-lineprofile-1)#gem add 2 eth tcont 1
huawei(config-gpon-lineprofile-1)#gem add 3 eth tcont 1
```

Configure the mapping between 3 GEM ports and 24 CVLANs.

- When user packets are untagged and the MA5671 adopts the automatic adding policy, all Ethernet ports are configured with different native VLANs. The value of the native VLAN is the Ethernet port ID.
- When user packets carry CVLAN tags, configure relevant VLANs for mapping on the line profile. That is, replace VLAN IDs with corresponding CVLAN IDs. For example, when Ethernet port 1 on the MA5671 receives user packets with CVLAN 24, run the **gem mapping 1 0 vlan 24** command.

```
huawei(config-gpon-lineprofile-1)#gem mapping 1 0 vlan 1
huawei(config-gpon-lineprofile-1)#gem mapping 1 1 vlan 2
huawei(config-gpon-lineprofile-1)#gem mapping 1 2 vlan 3
huawei(config-gpon-lineprofile-1)#gem mapping 1 3 vlan 4
huawei(config-gpon-lineprofile-1)#gem mapping 1 4 vlan 5
huawei(config-gpon-lineprofile-1)#gem mapping 1 5 vlan 6
huawei(config-gpon-lineprofile-1)#gem mapping 1 6 vlan 7
huawei(config-gpon-lineprofile-1)#gem mapping 1 7 vlan 8
huawei(config-gpon-lineprofile-1)#gem mapping 2 0 vlan 9
huawei(config-gpon-lineprofile-1)#gem mapping 2 1 vlan 10
huawei(config-gpon-lineprofile-1)#gem mapping 2 2 vlan 11
huawei(config-gpon-lineprofile-1)#gem mapping 2 3 vlan 12
huawei(config-gpon-lineprofile-1)#gem mapping 2 4 vlan 13
huawei(config-gpon-lineprofile-1)#gem mapping 2 5 vlan 14
huawei(config-gpon-lineprofile-1)#gem mapping 2 6 vlan 15
huawei(config-gpon-lineprofile-1)#gem mapping 2 7 vlan 16
huawei(config-gpon-lineprofile-1)#gem mapping 3 0 vlan 17
huawei(config-gpon-lineprofile-1)#gem mapping 3 1 vlan 18
huawei(config-gpon-lineprofile-1)#gem mapping 3 2 vlan 19
huawei(config-gpon-lineprofile-1)#gem mapping 3 3 vlan 20
huawei(config-gpon-lineprofile-1)#gem mapping 3 4 vlan 21
huawei(config-gpon-lineprofile-1)#gem mapping 3 5 vlan 22
huawei(config-gpon-lineprofile-1)#gem mapping 3 6 vlan 23
huawei(config-gpon-lineprofile-1)#gem mapping 3 7 vlan 24
```

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

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

3. Configure an ONU service profile.

Create a GPON ONU service profile named **ftto_ser**. Configure the Ethernet port capability set to 24.

```
huawei(config)#ont-srvprofile gpon profile-name ftto_ser
huawei(config-gpon-srvprofile-1)#ont-port eth 24
```

When user packets carry CVLAN tags, replace VLAN IDs with corresponding CVLAN IDs. For example, when Ethernet port 1 on the MA5671 receives user packets with CVLAN 24, run the **port vlan eth 1 24** command.

```
huawei(config-gpon-srvprofile-1)#port vlan eth 1 1
huawei(config-gpon-srvprofile-1)#port vlan eth 2 2
huawei(config-gpon-srvprofile-1)#port vlan eth 3 3
huawei(config-gpon-srvprofile-1)#port vlan eth 4 4
huawei(config-gpon-srvprofile-1)#port vlan eth 5 5
huawei(config-gpon-srvprofile-1)#port vlan eth 6 6
huawei(config-gpon-srvprofile-1)#port vlan eth 7 7
huawei(config-gpon-srvprofile-1)#port vlan eth 8 8
huawei(config-gpon-srvprofile-1)#port vlan eth 9 9
huawei(config-gpon-srvprofile-1)#port vlan eth 10 10
huawei(config-gpon-srvprofile-1)#port vlan eth 11 11
huawei(config-gpon-srvprofile-1)#port vlan eth 12 12
huawei(config-gpon-srvprofile-1)#port vlan eth 13 13
huawei(config-gpon-srvprofile-1)#port vlan eth 14 14
huawei(config-gpon-srvprofile-1)#port vlan eth 15 15
```

```
huawei(config-gpon-srvprofile-1)#port vlan eth 16 16
huawei(config-gpon-srvprofile-1)#port vlan eth 17 17
huawei(config-gpon-srvprofile-1)#port vlan eth 18 18
huawei(config-gpon-srvprofile-1)#port vlan eth 19 19
huawei(config-gpon-srvprofile-1)#port vlan eth 20 20
huawei(config-gpon-srvprofile-1)#port vlan eth 21 21
huawei(config-gpon-srvprofile-1)#port vlan eth 22 22
huawei(config-gpon-srvprofile-1)#port vlan eth 23 23
huawei(config-gpon-srvprofile-1)#port vlan eth 24 24
```

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 threshold profile.

- The ID of the default GPON alarm threshold profile is 1. The thresholds of all the alarm parameters in the default alarm profile are 0, which indicates that no alarm is reported.
- In this example, the default alarm threshold profile is used and therefore, the configuration of the alarm profile is not required.
- To configure the alarm threshold parameters for monitoring the performance statistics of an activated ONU line, run the **gpon alarm-profile add** command to configure a GPON alarm threshold profile.

Step 5 Configure an ONT automatic adding policy.

The value of **equipment** is determined based on the actual device type.

Different types of ONTs must be configured with different automatic adding policies. The MA5671, which has 24 FE ports and supports local power supply, is used as an example.

When **auto-confirm** is **enable**, do not need to run the **ont confirm** command on the GPON port to confirm the ONT. When **auto-confirm** is **disable**, run the **ont confirm** command on the GPON port.

```
huawei(config)#ont auto-add-policy gpon equipment MA5671-F24 omci ont-lineprofile-name ftto_line
ont-srvprofile-name ftto_ser auto-confirm enable
```

After the configuration is complete, run the **display ont auto-add-policy** command to query the information.

```
huawei(config)#display ont auto-add-policy gpon all
-----
Index          : 1
Ont EquipmentID : MA5671-F24(0x4d41353637312d463234)
PON mode       : GPON
Management mode : OMCI
Line profile ID : 1
Line profile name : ftto_line
Service profile ID : 1
Service profile name : ftto_ser
Auto-confirm    : enable
-----
```

Step 6 (Optional) When the device supports reverse power over Ethernet (PoE), configure reversed PoE work modes for the ONU.

There are 3 reversed PoE work modes:

- **all-port**: Reversed PoE is provided for all ports regardless of the powered port.

- **powered-port:** Reversed PoE is provided for the powered port only. Non-powered ports are shut down and services on them are interrupted.
- **unconcern:** The OLT does not issue reversed PoE configuration to the ONU. The default value is **unconcern**.

```
huawei(config)#interface gpon 0/1
huawei(config-if-gpon-0/1)#ont reverse-poe work-mode 0 0 all-port
huawei(config-if-gpon-0/1)#quit
```

Run the **display ont reverse-poe** command to query the reversed PoE work mode of the ONU and reversed PoE status on all Ethernet ports.

```
huawei(config-if-gpon-0/1)#display ont reverse-poe 0 0
```

Port-ID	Port-type	Power-state
1	ETH	No
2	ETH	Yes
3	ETH	No
4	ETH	Yes

Whether the reversed PoE has local power supply: Yes
Note: Local power supply of the device supporting reversed PoE is used for only commissioning and it cannot be used for normal power supply

- Reverse PoE work mode indicates the reversed PoE work mode.
- Power-state indicates reverse power supply status. **Yes** indicates that reversed PoE exists on a port. **No** indicates that reversed PoE does not exist on a port. - indicates that reversed PoE is not supported on a port.
- For Whether the reversed PoE has local power supply, **Yes** indicates that the local power supply exists, **No** indicates that the local power supply does not exist, and - indicates that reversed PoE is not supported. The local power supply of the reversed PoE is used for commissioning only. It cannot be used as the working power supply.

Step 7 (Optional) Configure ONU maintenance measures.

1. Configure ONU automatic migration.

When the ONU automatic migration function is enabled, if a PON port or fiber is faulty, the ONU connected to this faulty PON port is migrated to another PON port. If the ONU automatic adding policy is met, the ONU is automatically removed from the original PON port, and then added to the new PON port. In this process, the OLT does not report the SN authentication conflict alarm. The ONU connected to the original PON port must meet the following conditions:

- The ONU is offline.
- The ONU supports OMCI management.
- The ONU is not a member of the type C protection group.
- The ONU supports SN authentication.

```
huawei(config)#ont auto-migration enable
```

2. Configure ONU automatic aging.

When an offline ONU is aged and meets automatic adding policy, the OLT automatically deletes the aged ONU to save resources. The ONU automatic aging period can be configured. The value range is 1–365. The default value is

no-aging, which indicates no aging. For an aged ONU that meets the automatic adding policy, it will be automatically registered after being powered on.

```
huawei(config)#ont auto-aging 15
```

3. Run the **display ont global-config** or **display xpon global-config** to check whether the ONU automatic migration or aging function is enabled.

```
huawei(config)#display ont global-config
```

```
.....  
ONT auto-migration switch      : enable  
ONT auto-aging time(day)       : 15  
.....
```

Step 8 Add an ONU.

1. Enable the ONU automatic discovery function on a GPON port.

When the ONU automatic adding policy is configured, the ONU does not need to be added in the offline mode, because it will be automatically found after it goes online.

```
huawei(config)#interface gpon 0/1  
huawei(config-if-gpon-0/1)#port 0 ont-auto-find enable
```

2. (Optional) Confirm an ONU.

During ONU automatic adding, if **auto-confirm** is **disable**, run the **ont-confirm** command to confirm the ONU. When the **ont confirm** command is run and no line profile or service profile is specified, if the ONU type is matched with that ONU type configured in the automatic adding policy, the ONU is bound to the line and service profiles configured in the automatic adding policy. If the ONU type is not matched, the ONU is bound to default line profile 0.

```
huawei(config-if-gpon-0/1)#display ont autofind 0 /This command is run to display information  
about all ONTs connected to the GPON port through the optical splitter.  
huawei(config-if-gpon-0/1)#ont confirm 0 ontid 1 sn-auth 3230313126595540 omci
```

3. (Optional) Change the ONU description.

Run the **ont modify portid ontid desc describe-value** command to change the ONU description. It is recommended that information about the location and time be added for each ONU to facilitate the fault locating and maintenance.

```
huawei(config-if-gpon-0/1)#ont modify 0 1 desc fttto_2015
```

4. (Optional) Bind an alarm threshold profile.

In this example, the default profile (profile 1) is used.

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

5. Check ONU status.

After the ONU is added, run the **display ont info** command to query current ONU status. Ensure that Control flag 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 ONU is activated.  
Run state   : online  //Indicates that the ONU is online.  
.....
```

```
Config state      : normal //Indicates that the ONU configuration state is normal.
Match state       : match  //Indicates that the capability profile bound to the ONU is consistent
with actual ONU capability.
...//
```

When **Config state** is **failed** and **Run state** is **offline**,

- If **Control flag** is **deactive**, run the **ont activate** command to activate the ONU in the GPON port mode.
- If **Run state** is **offline**, a physical line may be disconnected 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.

Run the **display ont info summary** command to query ONU information about the SN, type, operating status, online time, offline time, and offline cause.

Step 9 Query the configuration status of a service flow.

After the MA5671-FE24 is powered on and connected to the PON, the service flow is automatically created after about 1 minute. Run the **display service-port all** command to check whether the service flow is successfully configured.

```
huawei(config)#display service-port all
Switch-Oriented Flow List
-----
INDEX VLAN VLAN  PORT F/ S/ P VPI VCI FLOW FLOW  RX TX STATE
  ID  ATTR  TYPE              TYPE PARA
-----
  0 100 common  gpon 0/1 /0 1 1  vlan 1      7 7  up
  1 100 common  gpon 0/1 /0 1 1  vlan 2      7 7  up
  ...
  8 100 common  gpon 0/1 /0 1 2  vlan 9      7 7  up
  9 100 common  gpon 0/1 /0 1 2  vlan 10     7 7  up
  ...
 16 100 common  gpon 0/1 /0 1 3  vlan 17     7 7  up
 17 100 common  gpon 0/1 /0 1 3  vlan 18     7 7  up
  ...
```

The main parameters are described as follows:

- **VPI** indicates the ONU ID.
- **VCI** indicates the GEM port ID.
- **FLOW PARA** indicates the user VLAN.

When a service flow with double-tagged VLAN is created, run the **display service-port index** command to query the inner VLAN on the network side. For example, for a service flow which is automatically created, the start VLAN is 2000, the ONU ID is 1, the number of ONU ports is 24, and the ONU user port ID is 1, the query results are shown in the following. Among them, **Label** indicates the inner VLAN on the network side.

```
huawei(config)#display service-port 0
-----
Index          : 0
VLAN ID        : 100
VLAN attr      : QinQ
Port type      : gpon
```

```
F/S/P      : 0/1/0
ONT ID     : 1
GEM port index : 1
ONT Port   : 1
Flow type   : vlan
Flow para   : 1
TX         : 7
Inbound table name : fcto_hsi
RX         : 7
Outbound table name : fcto_hsi
Admin status : enable
State       : up
Label       : 2025
Priority     : 0
PVC bundle  : no
Max MAC count : 1023
Tag transform : translate-and-add
Description :
Remote description :
Service-port bundle : -
Cos         : -
Car-Group   : -
Static MAC   :
IP address   :
-----
```

----End

10.3.4 Maintenance and Diagnosis

A service flow is a Layer 2 forwarding channel between an access node and a user. Check the status of a service flow using the following methods:

- After a user goes online, run the **display mac-address** command to query the MAC address of the user. This method is used to check whether the configuration of the service flow is correct.
- After a service is provisioned, run the **display statistics service-port** command to query the packet statistics of the service flow or run the **display traffic service-port** command to query the packet transmit and receive rate of the service flow in real time. The query results can be used to detect a service exception or locate a fault.

10.4 Service Port Bundle

10.4.1 What Is Service Port Bundle

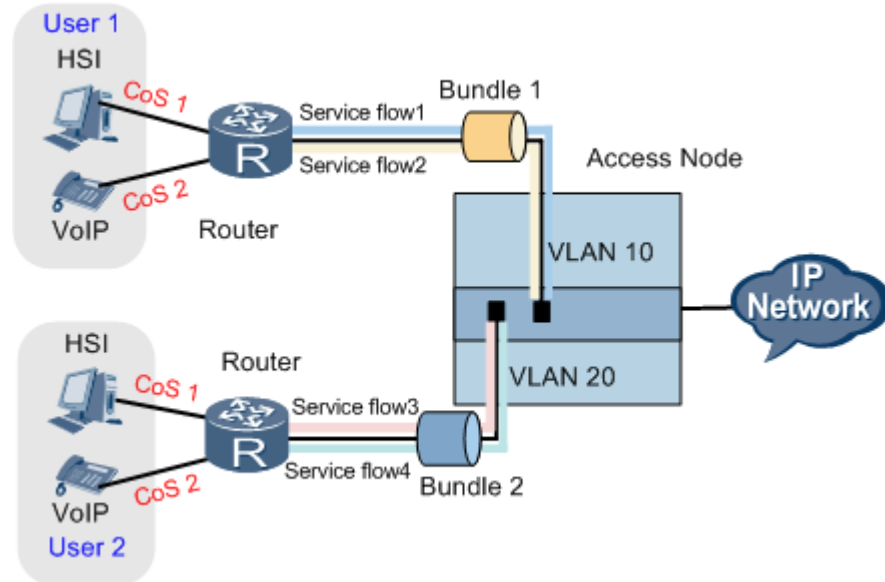
Definition

In a network where VLANs are planned based on ports on the access node and the access node connects to users through a router, the packets transmitted from a user to the access node through the router may carry the same MAC address even when they carry different services. As a result, MAC address transfer may occur between different service flows (service flow 1 and service flow 2) on the access node. The service port bundle feature addresses this issue by using CoS-based route selection.

Service port bundle, also named service flow bundle or flow bundle, is a CoS-based packet forwarding model. Each service port bundle corresponds to a group

of services for a user. Each service flow carries one type of service and has a CoS level. A service port bundle can also be considered a bundle of service flows. The following figure shows the schematic diagram for service port bundle.

Figure 10-25 Schematic diagram for service port bundle



Benefits

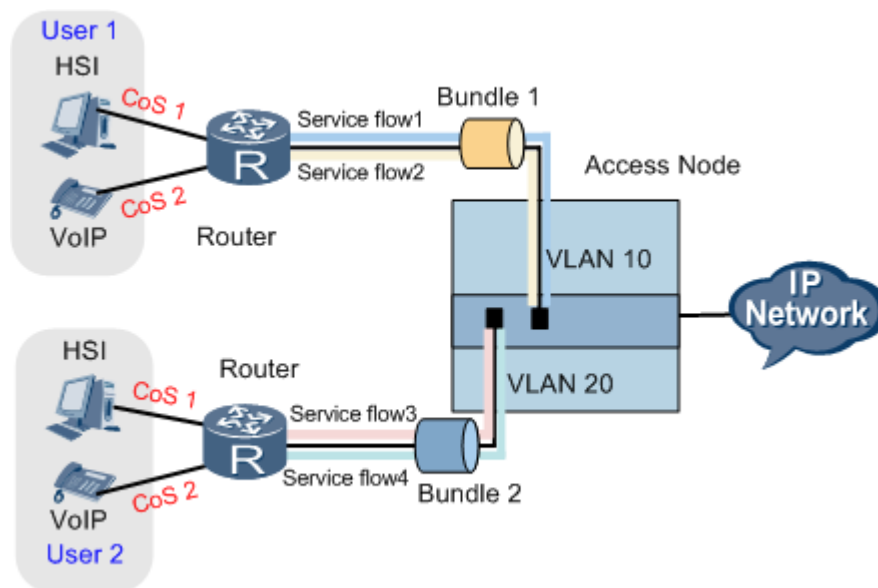
Benefits to carriers

CoS identification is introduced to the service port bundle principle. Consequently, service port bundle breaks the VLAN+MAC and S-VLAN+C-VLAN forwarding policies for the access node down to the VLAN+MAC+CoS and S-VLAN+C-VLAN+CoS forwarding policies and improves the flexibility in service planning for carriers.

10.4.2 Schematic Diagram For Service Port Bundle

The following explains the schematic diagram for service port bundle.

- The access node connects to users through a router. CoS levels are used to distinguish different services of a user.
- VLANs on the access node are planned based on ports. Services of different users are carried by different service flows. Service flows of a user are bundled together, called the service port bundle, or service flow bundle.

Figure 10-26 Schematic diagram for service port bundle

Upstream direction

The Access node receives packets of the service port bundle, and forwards the received packets to the upper-layer network through upstream ports in the S-VLAN (in the above figure, service flows 1 and 2 in service port bundle 1 are converged to the upstream port in VLAN 10). At the same time, the Access node obtains the service port bundle identifier from the ARL table (learned from the user port) and creates an entry for the service port bundle.

Downstream direction

The Access node determines the user port based on S-VLAN+MAC or S-VLAN+C-VLAN, queries the service port bundle table, determines a service flow based on the CoS value, and forwards the received packets through the service flow. In this way, the Access node implements the VLAN+MAC+CoS or S-VLAN+C-VLAN+CoS forwarding policy.

For more information about Layer 2 forwarding policies, see [10.5 Layer 2 Forwarding Policy](#).

10.4.3 Configuring a Service Port Bundle

On an access node, VLANs are planned based on ports. If the access node connects to users through a router, configure a service port bundle to prevent MAC address flapping between various service flows of the users.

Procedure

Step 1 Run the **service-port-bundle** command to create a service port bundle.

A service port bundle corresponds to a group of services. It is recommended that you plan a unique service port bundle ID for a user.

Run the **service-port-bundle** command to create a service port bundle.

- Step 2** Add service flows to the service port bundle and set classes of service (CoSs) for the service flows.

The services in a service flow bundle are carried by service flows. Add the service flows to the service port bundle and set a CoS for each service flow. In this way, the router forwards service packets according to the CoS.

Run the **service-port** command to set **bundle *bundleid* cos *cos*** when creating a service flow. *bundleid* is the ID of the service port bundle created in the preceding step.

 NOTE

- A service port bundle implements packet forwarding based on CoS levels, meeting the QoS demands of the upper-layer network. Hence, it requires that packets from the upper-layer network devices to the access device contain correct CoS values. The CoS value of a service that is defined by the service port bundle at the access node must be consistent with the CoS value defined by the upper-layer network.
- For users in a service port bundle, one user goes online, updates the lease, and goes offline through only one service flow, and the CoS value of upstream packets must be consistent with that of downstream packets.

----End

Example

The following is an example of the configurations used to configure a service port bundle to prevent MAC address flapping between Internet access and multicast service flows of user A:

- GPON port 0/2/1 on the access node connects to user A .
- The VLANs of the access node are planned based on ports.
- GPON port 0/2/1 is in VLAN 10.
- User A requires the Internet access and broadcast services.
- The ID of the service port bundle for user A is 10.
- The Internet access and broadcast services of user A are differentiated based on CoS values.
- For the Internet access service:
 - The CoS value is 1.
 - The ID of the traffic profile is 10.
- For the broadcast service:
 - The CoS value is 3.
 - The ID of the traffic profile is 20.

```
huawei(config)#service-port-bundle 10
huawei(config)#service-port 10 vlan 10 eth 0/2/1 multi-service user-vlan 10 bundle 10 cos 1 inbound
traffic-table index 10 outbound traffic-table index 10
huawei(config)#service-port 11 vlan 10 eth 0/2/1 multi-service user-vlan 20 bundle 10 cos 3 inbound
traffic-table index 20 outbound traffic-table index 20
```

10.5 Layer 2 Forwarding Policy

10.5.1 Layer 2 Forwarding Policy Overview

The MA5800, as Layer 2 network equipment, supports the ability to transparently transmit or forward packets at Layer 2. Traditionally, Layer 2 packet forwarding is based on VLANs and MAC addresses of packets (VLAN+MAC). If the destination MAC address of a packet becomes ineffective due to dynamic MAC address aging, VLAN+MAC searching fails. The packet becomes an unknown unicast packet and is broadcast within the VLAN, which poses a security threat. In addition, VLAN+MAC forwarding is subject to MAC spoofing and attacks, which lead to security problems.

To address the preceding problems, you can use S-VLAN+C-VLAN forwarding instead.

In S-VLAN+C-VLAN forwarding, two VLAN tags form a Layer 2 forwarding mapping relationship. Packets are forwarded based on VLANs rather than MAC addresses.

10.5.2 Layer 2 Forwarding Policy Principles

The MA5800 supports VLAN+MAC forwarding, S-VLAN+C-VLAN forwarding, and two other forwarding modes derived from the first two: VLAN+MAC+CoS and S-VLAN+C-VLAN+CoS.

VLAN+MAC Forwarding

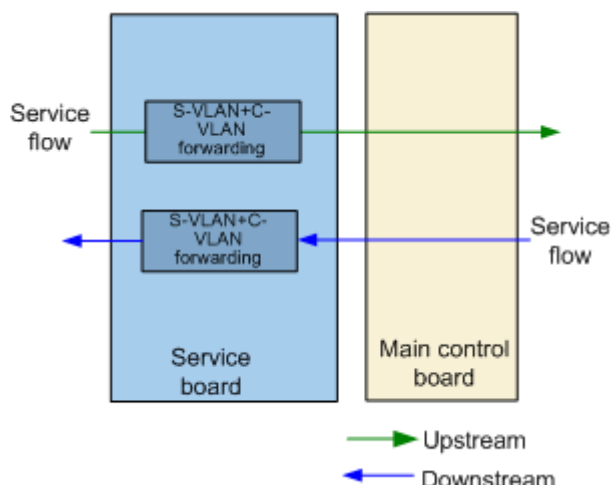
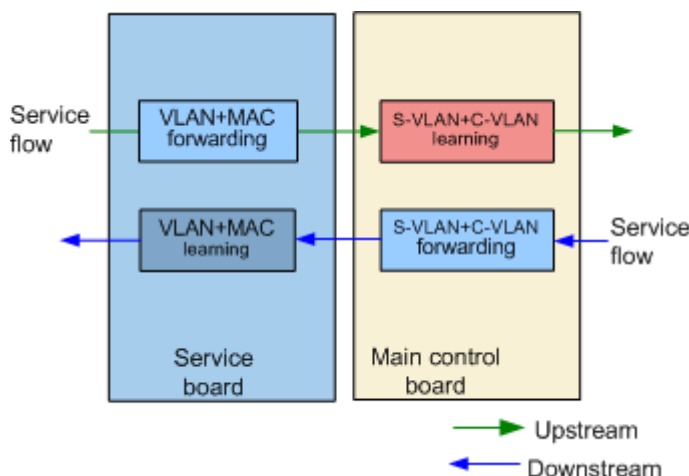
With the VLAN+MAC forwarding policy, the system automatically learns the mapping between the VLAN, source MAC address, and incoming port when packets enter the system. According to the VLAN and destination MAC address, the system then searches for the outgoing port and transmits the packets through this port.

In the VLAN+MAC forwarding policy, if the source MAC address is a broadcast or unicast MAC address, packets are broadcast in the VLAN. That is, packets are duplicated and transmitted to every port in the VLAN.

S-VLAN+C-VLAN Forwarding

The two VLANs (S-VLAN and C-VLAN) are an extension of VLAN. This expands the VLAN ID range. In addition, S and C have different meanings. S stands for service, and C stands for customer (user). Each S-VLAN+C-VLAN uniquely identifies a user service, and S-VLAN+C-VLAN forwarding can be implemented.

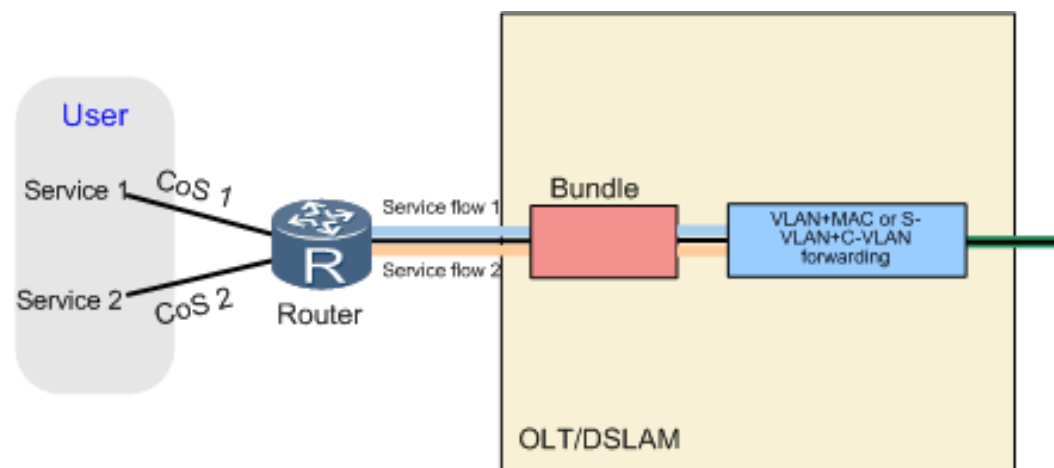
In S-VLAN+C-VLAN forwarding, two VLAN tags form a Layer 2 forwarding mapping relationship to implement VLAN-based forwarding. S-VLAN+C-VLAN forwarding is classified into non-strict S-VLAN+C-VLAN forwarding and strict S-VLAN+C-VLAN forwarding. Strict S-VLAN+C-VLAN forwarding entries do not need to be learned dynamically. The system automatically creates static forwarding entries during the establishment of service flows. Non-strict S-VLAN+C-VLAN forwarding entries need to be dynamically learned. According to the forwarding entries, upstream packets are transmitted through the corresponding upstream port and downstream packets are transmitted through the corresponding service port.

Figure 10-27 Strict S-VLAN+C-VLAN forwarding model**Figure 10-28** Non-strict S-VLAN+C-VLAN forwarding model

VLAN+MAC+CoS and S-VLAN+C-VLAN+CoS Forwarding

VLAN+MAC+CoS and S-VLAN+C-VLAN+CoS forwarding policies are derived from VLAN+MAC and S-VLAN+C-VLAN forwarding policies of the MA5800 respectively after class of service (CoS) identification is introduced based on service port bundles. The forwarding policies based on CoS resolve the problem of different service flows with the same VLAN+MAC or S-VLAN+C-VLAN and therefore improve service planning flexibility.

Figure 10-29 shows the CoS-based forwarding model.

Figure 10-29 VLAN+MAC+CoS and S-VLAN+C-VLAN+CoS forwarding model**Upstream direction**

All service flows from the same user converge to a service port bundle. The MA5800 learns the service port bundle identifier of the service flows, creates a service port bundle entry, and performs Layer 2 packet forwarding based on VLAN+MAC or S-VLAN+C-VLAN.

Downstream direction

The OLT determines a unique user based on VLAN+MAC or S-VLAN+C-VLAN, queries the service port bundle entries, finds the service flows based on CoS, and forwards packets.

10.5.3 Configuring a Layer 2 Forwarding Policy

Layer 2 forwarding policy configuration is the basis of VLAN configuration and an important step to ensure correct service forwarding. Before configuring services, ensure that the VLAN forwarding policy has been configured as planned.

Prerequisites

- VLAN IDs have been created correctly.
- VLAN attributes have been set correctly.

Context

A VLAN forwarding policy is a type of Layer 2 forwarding policy. Two types of VLAN forwarding policy are available: **vlan-connect** or **vlan-mac**. **vlan-mac** indicates VLAN+MAC forwarding and **vlan-connect** indicates S-VLAN+C-VLAN forwarding.

To implement VLAN+MAC+CoS or S-VLAN+C-VLAN+CoS forwarding, configure the VLAN forwarding policy and service port bundles separately.

Default Configuration

Table 10-27 lists the default VLAN forwarding policy settings.

Table 10-27 Default VLAN forwarding policy settings

Parameter	Default Value
forwarding-mode	VLAN+MAC

Procedure

- Configure VLAN+MAC forwarding.
You can configure a VLAN forwarding policy using two methods. Select an appropriate one as follows:
 - To configure a VLAN forwarding policy for a single VLAN, use the first method.
 - To configure the same forwarding policy for multiple VLANs with the same service profile parameters, use the second method (batch configuration using a service profile).
 - Method 1
 - a. In global configuration mode, run the **vlan forwarding** command.
 - Method 2
 - a. Run the **vlan service-profile** command to create a VLAN service profile and enter the VLAN service profile mode.
 - b. Run the **forwarding** command to configure a VLAN forwarding policy.
 - c. Run the **commit** command for the profile configuration to take effect.
 - d. Run the **quit** command to quit the VLAN service profile mode.
 - e. Run the **vlan bind service-profile** command to bind a VLAN to the VLAN service profile.
- Configure S-VLAN+C-VLAN forwarding.
 - a. Run the **vlan** command to add a VLAN.
 - b. Run the **vlan attrib** command to change the VLAN attribute to QinQ or stacking.
 - c. Run the **vlan forwarding** or **forwarding** command to configure a VLAN forwarding policy.
 - d. Run the **port vlan** command to associate upstream ports with S-VLANs and C-VLANs.
 - e. Run the **service-port** command to create a service port.

----End

Result

After the configuration, service flows can be created based on the configured VLANs and users connected to the MA5800 can ping the upstream equipment.

Example

Example: Configure the forwarding policy of VLAN 50 as S-VLAN+C-VLAN.

```
huawei(config)#vlan forwarding 50 vlan-connect
```

Example: Configure the forwarding policy of VLAN 65 as strict S-VLAN+C-VLAN. VLAN 73 indicates an enterprise VLAN on which MAC address learning is disabled.

```
huawei(config)#vlan 65 smart
huawei(config)#vlan attrib 65 stacking
huawei(config)#vlan service-profile profile-id 200
huawei(config-vlan-srvprof-200)#mac-address learning fabric disable
huawei(config-vlan-srvprof-200)#forwarding vlan-connect
huawei(config-vlan-srvprof-200)#commit
huawei(config-vlan-srvprof-200)#quit
huawei(config)#vlan bind service-profile 65 profile-id 200
huawei(config)#port vlan 65 inner-vlan-list 73 0/9 0
huawei(config)#service-port 100 uplink-port 0/9/0 vlan 65 eth 0/2/1 multi-service user-vlan 73 rx-cttr
10 tx-cttr 10
```

10.6 Layer 2 User Bridging

Layer 2 user bridging implements Layer 2 data exchange among users under the same MA5800.

10.6.1 Layer 2 User Bridging Overview

Users under the same MA5800 are isolated at Layer 2, but QinQ service deployment requires users communicate with each other at Layer 2. Therefore, QinQ services can be deployed only between different MA5800s.

If users in the same IP network segment on the same MA5800 need to exchange data, upstream equipment should support ARP proxy to implement Layer 3 data forwarding.

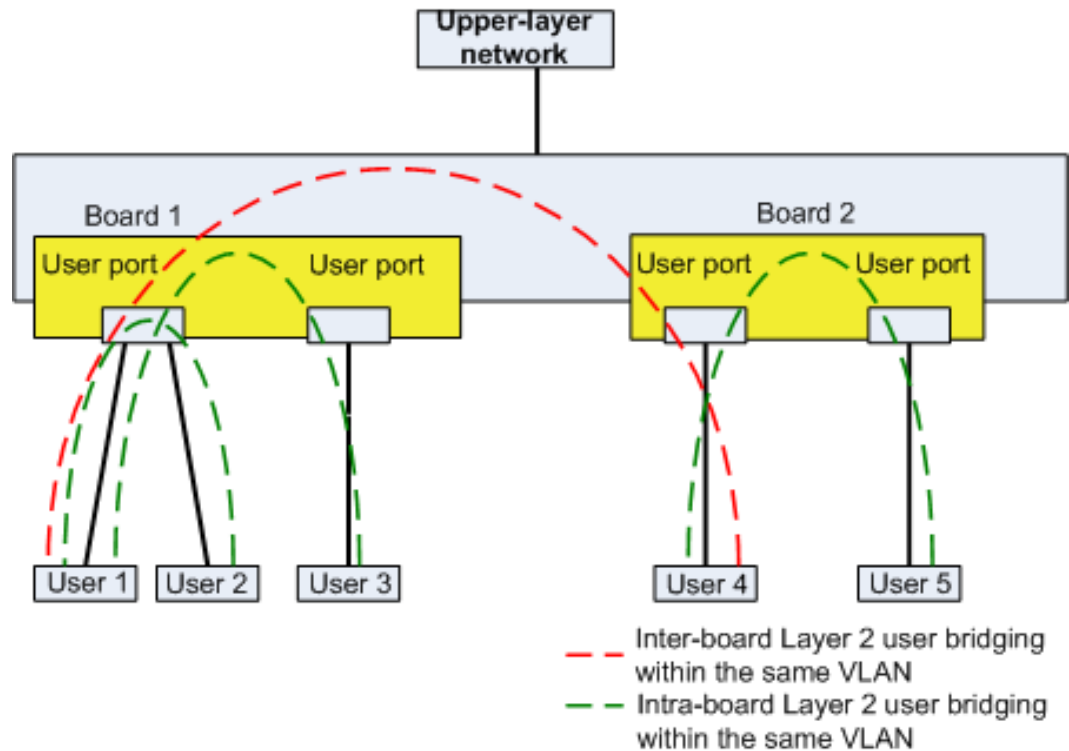
The Layer 2 user bridging feature addresses the preceding issues. After Layer 2 user bridging is enabled, users under the same MA5800 can exchange data at Layer 2.

10.6.2 Layer 2 User Bridging Principles

OLT supports VLAN-based Layer 2 user bridging.

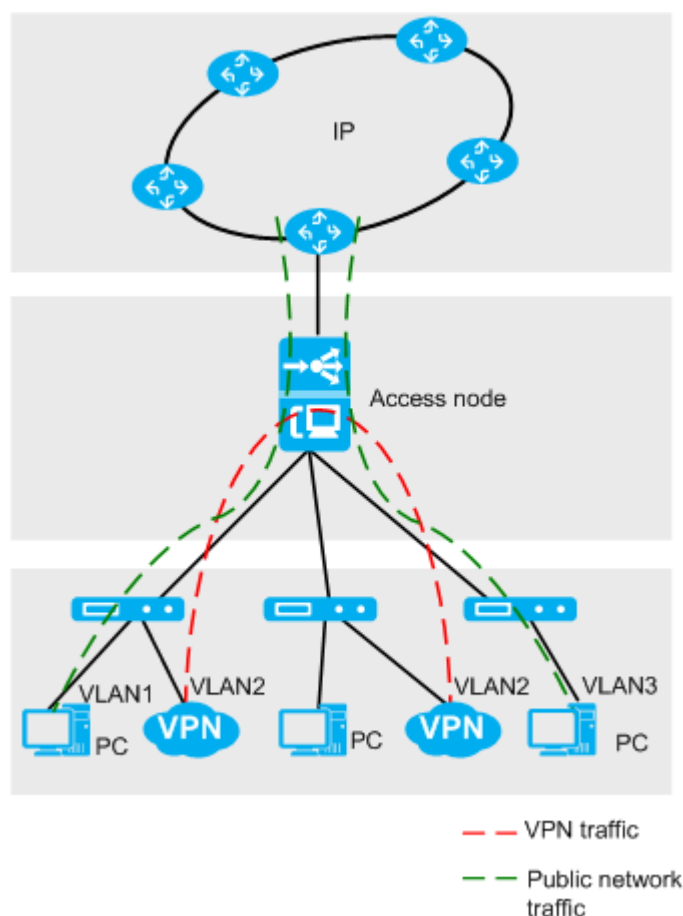
VLAN-based Layer 2 User Bridging

Figure 10-30 VLAN-based Layer 2 user bridging model



As shown in [Figure 10-30](#), the following functions are implemented on the MA5800 after Layer 2 user bridging is enabled on a VLAN.

- Inter-board user bridging: bridging among ports on different boards, for example, users 1, 2, and 3 can exchange data with users 4 and 5
- Intra-board user bridging:
 - Bridging among different users under the same port, for example, users 1 and 2 can exchange data with each other
 - Bridging among users under different ports on the same board, for example, users 1, 2, and 3 can exchange data
 - Bridging among different ports on the same board, for example, users 4 and 5 can exchange data with each other

Figure 10-31 VLAN-based user bridging network

As shown in [Figure 10-31](#), on one MA5800, Layer 2 bridging is implemented among enterprise private line users (VPN represented by the red line) but is not implemented among some common access users (represented by the green line). Services are classified by VLAN. VLAN 2 is a QinQ VLAN for carrying enterprise private line services. Enable Layer 2 user bridging on VLAN 2 so that private line users on the same MA5800 can exchange data.

10.6.3 Configuring VLAN-based Layer 2 User Bridging

Default Setting

By default, Layer 2 user bridging based on VLAN service profiles is disabled.

Procedure

- Step 1** In global configuration mode, run the **vlan service-profile** command to enter the VLAN service profile mode.
- Step 2** Run the **user-bridging** command to enable Layer 2 user bridging on a VLAN service profile.
- Step 3** Run the **commit** command for the settings to take effect.

Step 4 Go back to the global configuration mode and run the **vlan bind service-profile** command to bind a VLAN to the VLAN service profile.

 NOTE

- If the VLAN has been bound to the VLAN service profile, you do not need to bind the VLAN again.
- When the users of the same OLT are configured with Layer 2 intercommunication in the VLAN domain and do not need to communicate with users of other networks outside the OLT, you do not need to configure the VLAN tag on the upstream port.

----End

Result

If you run the **display vlan service-profile** command, **User-bridging** is **enable** for the VLAN service profile. Then, under the MA5800, users in the same VLAN with Layer 2 user bridging enabled can be pinged with each other

Example

Example: VLAN 10 is the S-VLAN for enterprise private line services. The VLAN is bound to VLAN service profile 3. Run the following commands to enable Layer 2 user bridging on VLAN 10 so that users in the VLAN on the same MA5800 can communicate with each other at Layer 2.

```
huawei(config)#vlan service-profile profile-id 3
huawei(config-vlan-srvprof-3)#user-bridging enable
huawei(config-vlan-srvprof-3)#commit
huawei(config-vlan-srvprof-3)#quit
```

ONU1 and ONU2 are deployed in enterprise branches and connect to the OLT through aggregation links. ONU1 and ONU2 can communicate with each other at Layer 2. The upstream port of the OLT is 0/9/0, the VLAN ID of the L2 intercommunication service is 300, and the GEM Port ID is 12. Create a VLAN service profile, enable the VLAN Layer 2 intercommunication function, and configure the protocol transparent transmission attributes related to the Layer 2 intercommunication service.

```
huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/9 0
huawei(config)#traffic table ip index 10 cir 102400 priority user-cos 4 priority-policy tag-in-package
huawei(config)#service-port 301 vlan 300 gpon 0/2/0 ont 1 gemport 12 multi-service user-vlan 300 rx-
cttr 10 tx-cttr 10
huawei(config)#service-port 302 vlan 300 gpon 0/2/1 ont 2 gemport 12 multi-service user-vlan 300 rx-
cttr 10 tx-cttr 10
huawei(config)#vlan service-profile profile-id 1
huawei(config-vlan-srvprof-1)#user-bridging enable // Mandatory
huawei(config-vlan-srvprof-1)#bpd tunnel enable
huawei(config-vlan-srvprof-1)#ospf tunnel enable
huawei(config)#vlan bind service-profile 300 profile-id 1
```