Contents

1 Configuring VLAN

1.1 Introduction

1.1.1 Overview

A virtual local area network (VLAN) is a logical network created by dividing a physical network. Every VLAN has an independent broadcast domain, and different VLANs are isolated on layer 2 (L2). Devices on different VLANs can implement communication through layer 3 (L3) devices or L3 interfaces.

1.1.2 Background and Functions

1. Background

The earliest local area network (LAN) adopts a bus structure, and STAs on the bus belong to the same contention domain. Bridges and L2 switches can isolate STAs onto different ports and control packet forwarding to isolate the contention domain. All ports of L2 switches belong to the same broadcast domain. When a switch receives a frame with an unknown destination address, the switch broadcasts this frame to all ports in the broadcast domain other than the source port. After receiving a reply from a port that matches the destination address, the switch learns the new MAC address based on the source address in the reply packet. This is the basic working mode of the switch.

If the network scale is enlarged, the increasing broadcast packets waste bandwidth. In addition, each STA in the broadcast domain can receive broadcast packets in the entire LAN. If users capture these packets using a packet capture tool, the content in the packets may be intercepted, which affects information security.

Routers communicate based on L3 IP addresses, and different subnets belong to different broadcast domains. This dampens the forwarding of broadcast packets. However, high forwarding performance of routers depends on central processing units (CPUs), and requires a high cost. Therefore, routers are usually used as egresses between LANs and wide area networks (WANs). Based on the concept of router subnet, a VLAN is developed.

2. Functions

You can divide a physical LAN into multiple VLANs by using different division methods so as to isolate broadcast domains, which saves bandwidth and enhances LAN security.

3. Features

- L2 isolation

  A VLAN shares the same attributes with a common physical LAN except the restriction on physical location. Every VLAN has an independent broadcast domain. If no switch virtual interface (SVI) is configured for VLANs, the VLANs are mutually isolated on L2. Users in different VLANs cannot communicate with each other. L2 unicast, broadcast and multicast frames are forwarded and transmitted in the same VLAN without entering other VLANs.

- L3 interconnection

In an L3 switch, each VLAN corresponds to an SVI and the SVI functions as a VLAN gateway to implement L3 communication between VLANs.

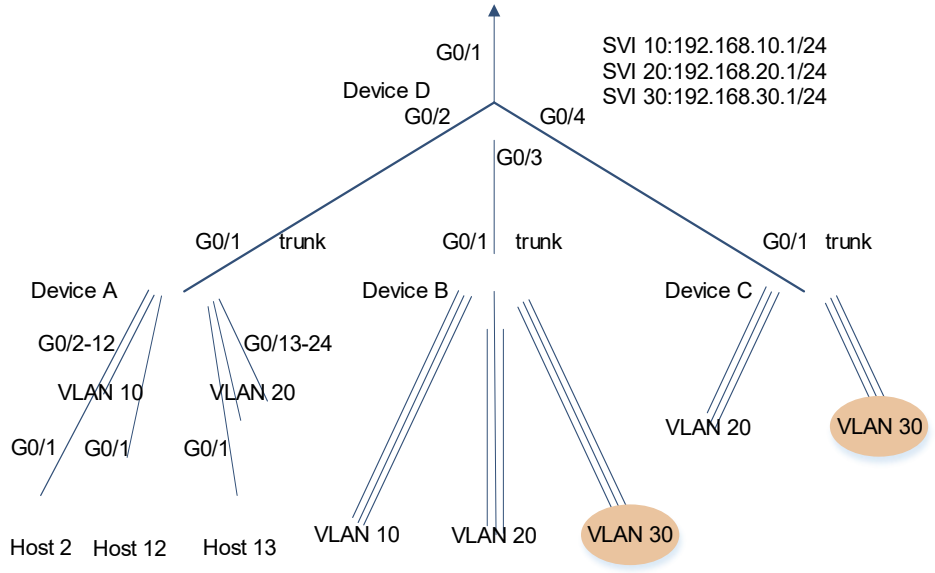
4. Application

As shown in Figure 1-1, VLANs are created on Device A, Device B, and Device C, and the LAN is divided into VLAN10, VLAN20, and VLAN30. The VLANs are mutually isolated on L2.

A port is defined as a VLAN member. All STAs connected to the port are a part of the VLAN. To change the VLAN of a user, modify the VLAN configuration of the port without adjusting the physical position of the user.

On the core device Device D, configure three VLANs, configure the ports to be connected to Device A, Device B, and Device C as trunk ports, and specify an allowed VLAN list. Three SVIs are configured as gateway interfaces of IP subnets corresponding to the three VLANs, and IP addresses are configured accordingly. The three VLANs enable subnet interconnection based on the IP forwarding capability of the L3 core device.

Figure 1-1 Typical Scenario

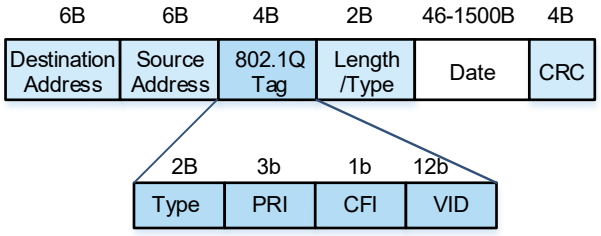


1.1.3 Frame Format

Based on IEEE 802.1Q, a 4-byte 802.1Q tag is inserted between the source MAC address field and protocol type field of an Ethernet frame, as shown in Figure 1-1. The VLAN ID (VID) field in the tag is used to represent the VLAN where the frame comes from. Not all devices identify tagged 802.1Q frames. Therefore, Ethernet frames can be tagged or untagged in the VLAN.

- Type: two bytes. The value **0X8100** indicates 802.1Q frames. Devices not supporting 802.1Q discard these frames upon receiving them.
- PRI: three bits. It indicates the L2 priority and corresponds to the Class of Service (CoS) priority of the Quality of Service (QoS). The value range is from 0 to 7. A larger value indicates a higher priority.
- CFI: one bit. It differentiates among Ethernet frames, Fiber Distributed Data Interface (FDDI) frames, and token ring network frames. The value **0** indicates Ethernet frames.
- VID: 12 bits. It indicates the ID of a VLAN to which packets belong. The value range is from 1 to 4094, and the value **0** and **4095** are reserved.

Figure 1-1 802.1Q Frame Format



This product complies with IEEE 802.1Q and supports a maximum of 4094 VLANs. The value range of the VLAN ID is from 1 to 4094. VLAN 1 is a default VLAN that does not need to be created and cannot be deleted. Other VLANs can be created and deleted. When you create a VLAN, the system returns a VLAN creation failure message if hardware resources are insufficient.

1.1.4 Port Types and Link Types

Ports can be classified into L2 interfaces and L3 interfaces. Only L2 interfaces can be added to VLANs. Table 1-1 lists different types of VLAN ports. You can configure the type of a VLAN port to determine the types of frames supported by the port, the number of VLANs supported by the port, and whether packets to be forwarded by the port carry the tag field.

Table 1-1 Port Types

Port Type	Function
Access port	An access port must belong to one VLAN. Therefore, only frames from this VLAN can pass the port. This VLAN is referred to as access VLAN, which is a native VLAN and also an allowed VLAN. All access ports belong to VLAN 1 by default. The frames sent from the access port do not carry tags. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the access VLAN and adds the access VLAN ID to the frame.
Trunk port	A trunk port has one native VLAN and multiple allowed VLANs. The native VLAN is VLAN 1 by default. The allowed VLANs are all VLANs (1 to 4094) of the local device. Therefore, the trunk port can forward frames of all VLANs. The frames forwarded by the trunk port from the native VLAN do not carry tags and the frames forwarded by the trunk port from allowed VLANs carry tags. Note that the trunk ports of a link must be configured with the same native VLAN.
Uplink port	An uplink port has one native VLAN and several allowed VLANs. The native VLAN is VLAN 1 by default. The allowed VLANs are all VLANs (1 to 4094) of the local device. Therefore, the uplink port can forward frames of all VLANs. Frames sent by the uplink port are tagged. In a QinQ scenario, frames sent by a Provider Edge (PE) device port connected to a public network must carry tags. Therefore, the port must be configured as an uplink port. A Customer Edge (CE) device port connected to the PE device can also be configured as an

Port Type	Function
	uplink port. For more information, see *QinQ*.
Hybrid port	A hybrid port has one native VLAN and multiple allowed VLANs. The allowed VLANs can be classified into tagged VLANs and untagged VLANs. The native VLAN is VLAN 1 by default. The allowed VLANs can be classified into untagged VLAN 1 and tagged VLANs 2 to 4094. Therefore, the hybrid port can forward frames of all VLANs. The frames forwarded by the hybrid port from a tagged VLAN carry tags, and the frames forwarded by the hybrid port from an untagged VLAN do not carry tags. The frames forwarded by the hybrid port from the native VLAN must not carry tags, because the native VLAN is an untagged VLAN. The MAC VLAN function applies to only untagged VLANs on the hybrid port. Therefore, the hybrid port can be used as an interface to connect to STAs in MAC VLAN scenarios. For more information, see *MAC VLAN*.
Dot1q-tunnel port	A Dot1q-tunnel port has one native VLAN and several allowed VLANs. The allowed VLANs can be classified into tagged VLANs and untagged VLANs. The native VLAN is VLAN 1 by default, and the allowed VLAN is untagged VLAN 1. If QinQ is enabled, the PE port connected to the user network encapsulates an outer VLAN tag to user packets and then transmits the packets in the operator network. The PE port must be configured as a Dot1q-tunnel port and the VLAN on the operator network must be configured as the native VLAN of the Dot1q-tunnel port. If packets are encapsulated using the basic QinQ method, the PE port uses the native VLAN ID as the VLAN ID of the outer VLAN tag. To ensure uplink and downlink packet transmission, the native VLAN must be added to the untagged VLAN allowed list of the Dot1q-tunnel port. For more information, see *QinQ*.

VLAN links include access links and trunk links.

- An access link connects STAs to a switch port. Generally, the STA hardware cannot identify frames that carry VLAN tags. Therefore, the frames transmitted between the STAs and access ports are untagged frames. The access port and hybrid port can be connected by the access link. Some STAs can identify frames that carry VLAN tags. The actual product prevails.
- A trunk link can bear data of different VLANs. You must ensure that the devices connected by the trunk link can identify the VLAN of frames transmitted on the trunk link. The trunk port, uplink port, and Dot1q-tunnel port can be connected by the trunk link only. The hybrid port can be connected by both the trunk link and the access link. To transmit untagged frames from the native VLAN on the trunk link, ensure that the native VLAN configuration on the peer device is consistent with that on the local device.

1.1.5 Principles

1. Frame Processing Rules

- Frame receiving rule

  When detecting an incoming untagged frame, if the port regards that the frame comes from the native VLAN, the port receives the packet, and identifies the frame as one from the native VLAN.

When detecting a tagged frame, the port receives the packet if the port allows the VLAN identified by the tag. Otherwise, the port discards the packet.

- Frame forwarding rule

  An L2 switch can forward packets to only ports that match allowed VLANs (other than the source port).

  An L3 switch can determine an egress VLAN by querying the routing table in software and forward packets to a port that allows the egress VLAN.

- Frame sending rule

  After packets are forwarded in the switch, the switch determines whether to add tags to the packets based on the VLAN type (tagged VLAN or untagged VLAN).

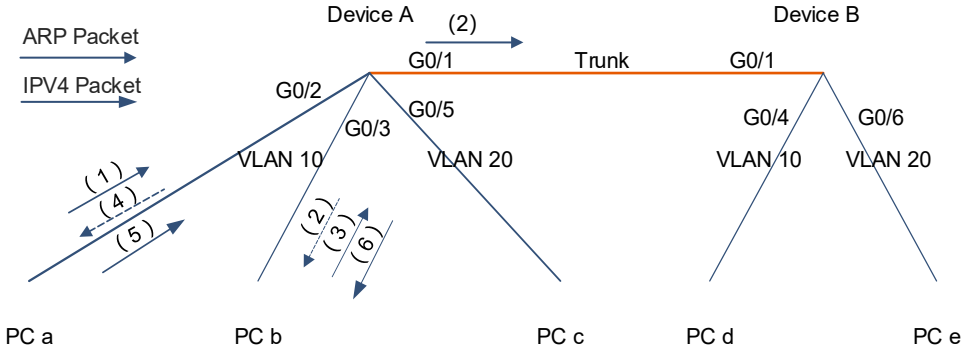
Table 1-1 Port Examples

Port	Mode	Native VLAN	Allowed VLAN List	Allowed VLAN Type
Gi 0/0	Access	10	10	10 (untagged)
Gi 0/1	Trunk	10	10, 20, 30	10 (untagged), 20 (tagged), and 30 (tagged)
Gi 0/2	Hybrid	20	10, 20, 30	20 (untagged), 10 (tagged), and 30 (tagged)
Gi 0/3	Uplink	30	20, 30	30 (tagged) and 20 (tagged)

As described in Table 1-1, when GigabitEthernet 0/0 receives an untagged frame or a frame with a VLAN 10 tag, it forwards the frame to GigabitEthernet 0/1 and GigabitEthernet 0/2 that allow VLAN 10. The VLAN 10 frame sent to GigabitEthernet 0/1 is untagged, and the VLAN 10 frame sent to GigabitEthernet 0/2 is tagged. When GigabitEthernet 0/3 receives a frame with a VLAN 30 tag, it forwards the frame to GigabitEthernet 0/1 and GigabitEthernet 0/2 that allow VLAN 30. The VLAN 30 frame sent to GigabitEthernet 0/1 is tagged, and the VLAN 30 frame sent to GigabitEthernet 0/2 is untagged.

2. Intra-VLAN Communication Within One Device

Figure 1-1 Example of Intra-VLAN Communication Within One Device



As shown in Figure 1-1, the mappings between ports and VLANs on Device A are as follows:

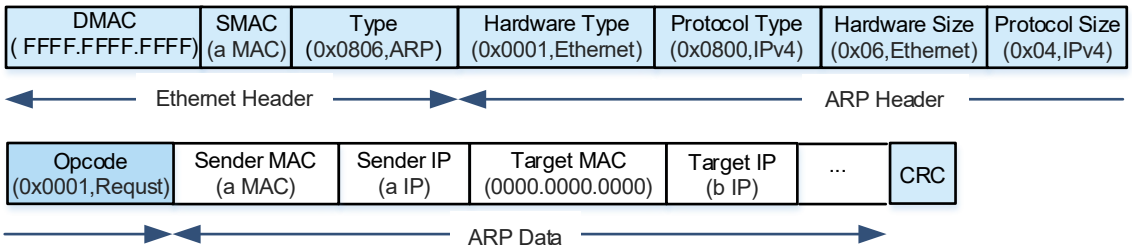
```
VLAN      Name       Status     Ports
10        VLAN10     STATIC     Gi0/1, Gi0/2, Gi0/3
20        VLAN20     STATIC     Gi0/1, Gi0/5
```

PC a and PC b belong to VLAN 10. Their communication procedure is as follows:

(1) To communicate with PC b (1.1.10.3/24), PC a (1.1.10.2/24) first determines that it is in the same subnet as PC b and queries the Address Resolution Protocol (ARP) table for the MAC address corresponding to the IP address of PC b. If PC a finds the MAC address of PC b, go to step (5) . If PC a does not find the MAC address of PC b, PC a sends an ARP request packet encapsulated in an Ethernet broadcast frame to PC b, as shown in Figure 1-2.

```
Protocol       Address                 Age(min)     Hardware          Type
Internet       1.1.10.3                 0                             arpa
```

Figure 1-2 ARP Request Packet Sent by PC a for Requesting MAC Address of PC b



Upon receiving the ARP request packet of PC a from GigabitEthernet 0/2 (as shown in Figure 1-2), if Device A finds that the packet is untagged, it determines that the packet comes from VLAN 10 and receives the packet. Device A learns the source IP address in the packet, and enters the mapping among the IP address, MAC address, port, and VLAN of PC a into the ARP table.

```
Protocol      Address     Age(min)     Hardware         Type    Interface
Internet      1.1.10.2     0            a MAC            arpa    Gi0/2
```

Device A enters the mapping among the VLAN, MAC address, and port of PC a into the dynamic MAC address table.

```
Vlan          MAC Address        Type           Interface
10            a MAC              Dynamic        Gi0/2
```

(2) Device A searches for the port that allows VLAN 10, and broadcasts the ARP request to GigabitEthernet 0/1 and GigabitEthernet 0/3.

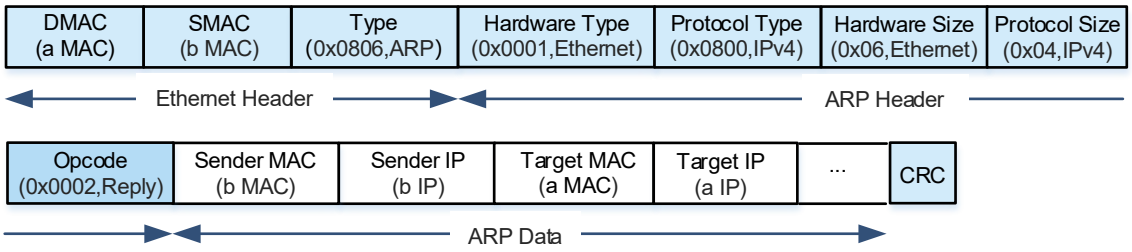
```
VLAN      Name        Status      Ports
10        VLAN10      STATIC      Gi0/1, Gi0/2, Gi0/3
20        VLAN20      STATIC      Gi0/1, Gi0/5
```

PC b receives the ARP request (as shown in Figure 1-2) of PC a from GigabitEthernet 0/3, learns the mapping between the IP address and MAC address of PC a, and enters the mapping into the ARP table.

```
Protocol  Address       Age(min)     Hardware         Type
Internet  1.1.10.2      0            a MAC            arpa
```

(3) If PC b finds that the destination IP address in the ARP request matches its own IP address, it sends an ARP reply to PC a in unicast mode (as shown in Figure 1-1).

Figure 1-1 ARP Reply Packet Sent by PC b to PC a



Upon receiving the ARP reply (as shown in Figure 1-1) of PC b from GigabitEthernet 0/3, Device A learns the source IP address and enters the mapping among the IP address, MAC address, port, and VLAN of PC b into the ARP table.

```
Protocol  Address      Age(min)    Hardware        Type   Interface
Internet  1.1.10.2      1           a MAC           arpa   Gi0/2
Internet  1.1.10.3      0           b MAC           arpa   Gi0/3
```

Device A enters the mapping among the VLAN, MAC address, and port of PC b into the dynamic MAC address table.

```
Vlan          MAC Address       Type          Interface
10            a MAC             Dynamic       Gi0/2
10            b MAC             Dynamic       Gi0/3
```

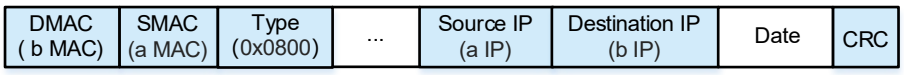
(4) Device A queries the MAC address table, hits the MAC address of PC a, and forwards the ARP reply of PC b to GigabitEthernet 0/2.

PC a receives the ARP reply (as shown in Figure 1-1) of PC b from GigabitEthernet 0/2, learns the mapping between the IP address and MAC address of PC b, and enters the mapping into the ARP table.

(5) PC a finds the MAC address of PC b in the ARP table, generates a packet with the MAC address of PC b as the destination MAC address and the MAC address of PC a as the source MAC address, and sends the packet to PC b (as shown in Figure 1-1).

```
Protocol      Address             Age(min)    Hardware       Type
Internet      1.1.10.3              0         b MAC          arpa
```

Figure 1-1 IPv4 Packet Sent from PC a to PC b



(6) Upon receiving the packet from PC a, Device A refreshes the MAC address table based on the source IP address of PC a, queries the MAC address table to hit the destination MAC address of PC b, and forwards the packet to GigabitEthernet 0/3 (as shown in Figure 1-1).

3. Inter-VLAN Communication

Devices from different VLANs may need to communicate with each other. The VLAN broadcast domains are isolated on L2. Therefore, the devices from different VLANs can communicate with each other by using an L3 device, for example, by using a routing device for relay. This method requires router ports. A routing module can be added to the L2 switch to form an L3 switch.

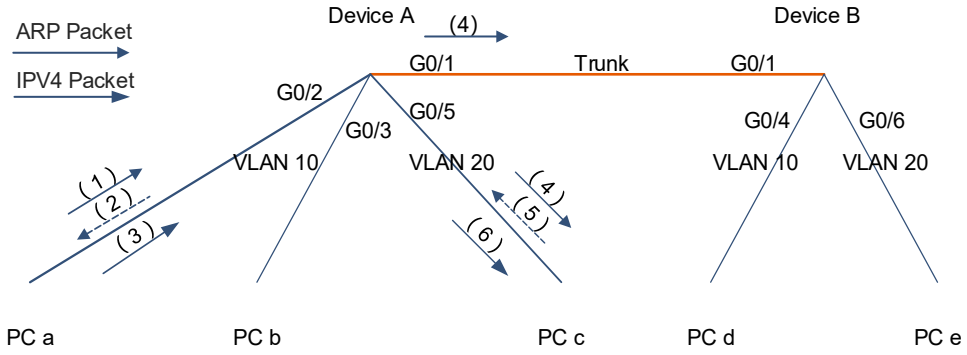
On the L3 switch, one VLAN corresponds to one SVI. The L3 switch takes the SVI as an independent interface, creates an ARP entry for the interface, and records the mapping between the IP address and MAC address of the SVI.

A STA in each VLAN uses the IP address of an SVI corresponding to this VLAN as the default gateway. When the STA in the VLAN tries to communicate with an STA in another VLAN, the STA queries the MAC address of the gateway, and then forwards a packet to the gateway.

When the L3 switch receives the packet whose MAC address matches the SVI, the switch enables L3 forwarding. If the L3 switch does not know the MAC address of the destination host, the L3 switch queries the routing table in the software, determines the egress VLAN of the destination host, and sends an ARP request in the egress VLAN. Upon obtaining an ARP reply from the destination host, the L3 switch learns the IP address, MAC address, port, and VLAN of the destination host, updates the L3 routing table, replaces the source MAC address in the packet with the MAC address of the gateway and the destination MAC address with the MAC address of the destination host, and forwards the packet to the destination host. Later, when the L3 switch receives packets with the same destination MAC address, the L3 switch directly queries the L3 routing table, replaces the source and destination MAC addresses, and forwards the packets.

As shown in Figure 1-1, PC a belongs to VLAN 10 and PC c belongs to VLAN 20. Their communication is implemented across the VLANs.

Figure 1-1 Example of Inter-VLAN Communication



The mappings between ports and VLANs on Device A are as follows:

```
VLAN      Name        Status      Ports
10        VLAN10      STATIC      Gi0/1, Gi0/2, Gi0/3
20        VLAN20      STATIC      Gi0/1, Gi0/5
```

After an SVI is created, the switch generates the mappings of IP addresses to MAC addresses. The gateway MAC address is the MAC address of Device A.

```
VLAN      IP Address                  Hardware Address
10        1.1.10.1                     g MAC
20        1.1.20.1                     g MAC
```

A direct route to L3 SVI is generated.

```
C         1.1.10.0/24 is directly connected, VLAN 10
C         1.1.20.0/24 is directly connected, VLAN 20
```

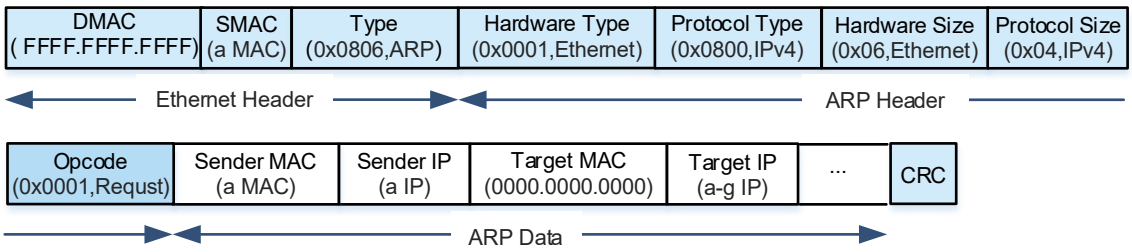
PC a and PC b belong to different VLANs. Their communication procedure is as follows:

(1) To communicate with PC c (1.1.20.5/24), PC a (1.1.10.2/24) first determines that they are in different subnets and queries the ARP table for the gateway MAC address corresponding to the gateway IP address (1.1.10.1/24) of PC a. If PC a finds the MAC address of the gateway, go to step (3). If PC a does not find the MAC address of the gateway, it sends an ARP request packet encapsulated in an Ethernet broadcast frame to the gateway, as shown in Figure 1-2.

```
Protocol  Address       Age(min)     Hardware        Type
```

```
Internet  1.1.10.1      0                              arpa
```

Figure 1-2 ARP Request Packet Sent by PC a for Requesting MAC Address of the Gateway



Upon receiving the ARP request packet of PC a from GigabitEthernet 0/2 (as shown in Figure 1-2), if Device A finds that the packet is untagged, it determines that the packet comes from VLAN 10 and receives the packet.

Device A learns the source IP address in the packet, and enters the mapping among the IP address, MAC address, port, and VLAN of PC a into the ARP table.

```
Protocol  Address      Age(min)    Hardware        Type   Interface
Internet  1.1.10.2     0           a MAC           arpa   Gi0/2
```

Device A enters the mapping among the VLAN, MAC address, and port of PC a into the dynamic MAC address table.

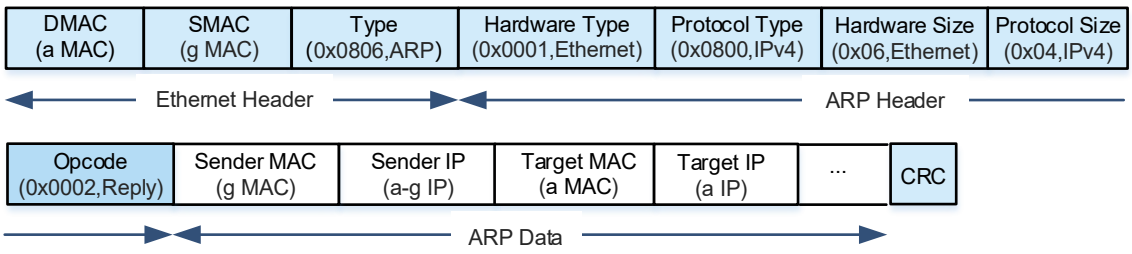
```
Vlan          MAC Address       Type          Interface
10            a MAC             Dynamic       Gi0/2
```

The preceding information constitutes the content of an L3 routing table. The routing table cannot be queried but its content is reflected in the ARP table and MAC address table.

```
VLAN      IP Address        Hardware          Interface
10        1.1.10.2          a MAC             Gi0/2
```

(2) If Device A finds that the packet is an ARP packet and the destination IP address in the packet is the IP address of the SVI corresponding to VLAN 10 of this device, it returns an ARP reply in unicast mode and forwards the reply packet through GigabitEthernet 0/2. The reply packet (as shown in Figure 1-1) includes the IP address and MAC address of SVI 10.

Figure 1-1 ARP Reply Packet Sent by the Gateway to PC a

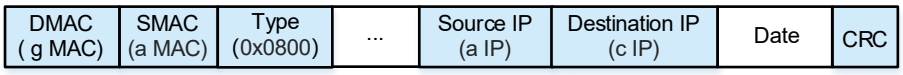


Upon receiving the ARP reply, PC a learns the MAC address corresponding to the IP address of the SVI 10 gateway and updates the ARP table of PC a.

(3) If PC a finds the MAC address of the gateway in the ARP table, it generates a packet with the gateway MAC address as the destination MAC address and the MAC address of PC a as the source MAC address, encapsulates the packet in an Ethernet frame (as shown in Figure 1-1), and forwards the packet to the gateway.

```
Protocol  Address      Age(min)    Hardware        Type
Internet  1.1.10.1     0           g MAC           arpa
```

Figure 1-1 IPv4 Packet Sent by PC a to PC c



(4) Upon receiving the packet of PC a from GigabitEthernet 0/2 (as shown in Figure 1-1), Device A refreshes the MAC address entry of PC a. If Device A finds that the packet is untagged, it determines that the packet comes from VLAN 10. The destination MAC address (gateway MAC address) is the MAC address of the local device. Therefore, the packet must be forwarded at L3. If Device A finds the MAC address of PC c corresponding to the IP address of PC c, go to step (6) . If Device A does not find this MAC address, it forwards the packet to the CPU for processing.

```
VLAN      IP Address         Hardware Address          Port
10        1.1.10.2           a MAC                     Gi0/2
          1.1.20.5
```

The CPU queries the routing table in the software, and finds that the packet matches a direct route to 1.1.20.0/24, with the egress VLAN being VLAN 20.

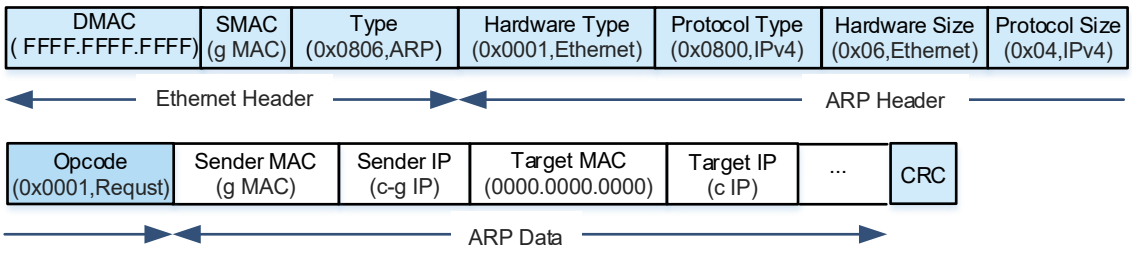
```
Connected    1.1.20.0/24 is directly connected, VLAN 20
```

The CPU continues to query the ARP table for the MAC address corresponding to the IP address of PC c, but the query fails.

```
Protocol  Address      Age(min)    Hardware     Type    Interface
Internet  1.1.20.5      0                       arpa
```

Device A broadcasts the ARP request (as shown in Figure 1-1) in the egress VLAN (VLAN 20) to request the MAC address of PC c. In this case, the IP address of the gateway is the address of the SVI in VLAN 20, that is, the gateway IP address (1.1.20.1/24) of PC c.

Figure 1-1 ARP Request Packet Sent by the Gateway for Requesting MAC Address of PC c



The ARP request is sent from GigabitEthernet 0/1 and GigabitEthernet 0/5 that allow VLAN 20.

```
VLAN      Name         Status      Ports
```

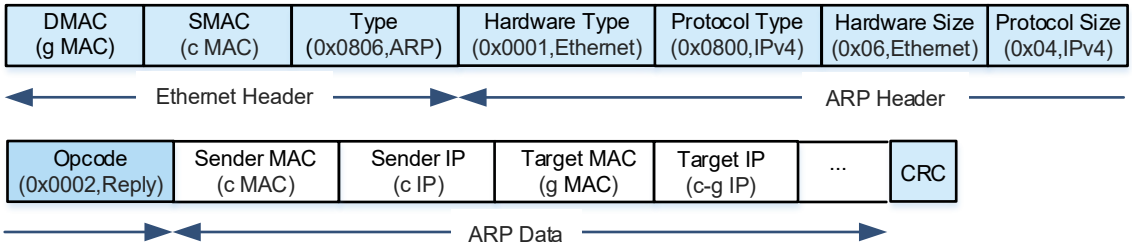
```
10        VLAN10      STATIC      Gi0/1, Gi0/2, Gi0/3
20        VLAN20      STATIC      Gi0/1, Gi0/5
```

PC c receives the ARP request (as shown in Figure 1-1) of Device A from GigabitEthernet 0/5, learns the mapping between the gateway IP address and gateway MAC address in VLAN 20 on Device A, and enters the mapping into the ARP table.

```
Protocol  Address       Age(min)     Hardware        Type
Internet  1.1.20.1      0            g MAC           arpa
```

(5) If PC c finds that the destination IP address in the ARP request matches its own IP address, it sends an ARP reply packet in unicast mode (as shown in Figure 1-1).

Figure 1-1 ARP Reply Packet Sent by PC c to the Gateway



Upon receiving the ARP reply (as shown in Figure 1-1) of PC c, Device A learns the mapping among the IP address, MAC address, port, and VLAN of PC c, and enters the mapping into the ARP table.

```
Protocol  Address       Age(min)     Hardware        Type    Interface
Internet  1.1.10.2          1          a MAC         arpa    Gi0/2
Internet  1.1.20.5          0          c MAC         arpa    Gi0/5
```

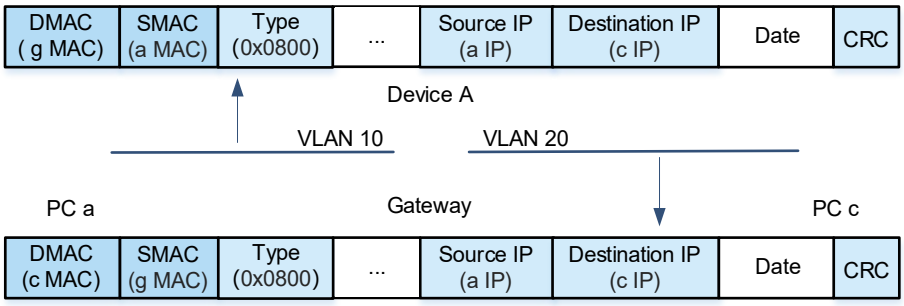
Device A enters the information about PC c into the dynamic MAC address table.

```
Vlan          MAC Address        Type           Interface
10            a MAC              Dynamic        Gi0/2
20            c MAC              Dynamic        Gi0/5
```

(6) If Device A finds the MAC address of PC c, it replaces the MAC address of PC a with the gateway MAC address and the gateway MAC address with the MAC address of PC c, and forwards the packet of PC a to PC c (as shown in Figure 1-1).

```
VLAN      IP Address         Hardware           Port
10        1.1.10.2           a MAC              Gi0/2
20        1.1.20.5           c MAC              Gi0/5
```

Figure 1-1 Packet Forwarded by the Gateway



PC c receives this packet (as shown in Figure 1-1) from GigabitEthernet 0/5, learns the mapping between the IP address of PC a and the gateway MAC address, and enters the mapping into the ARP table.

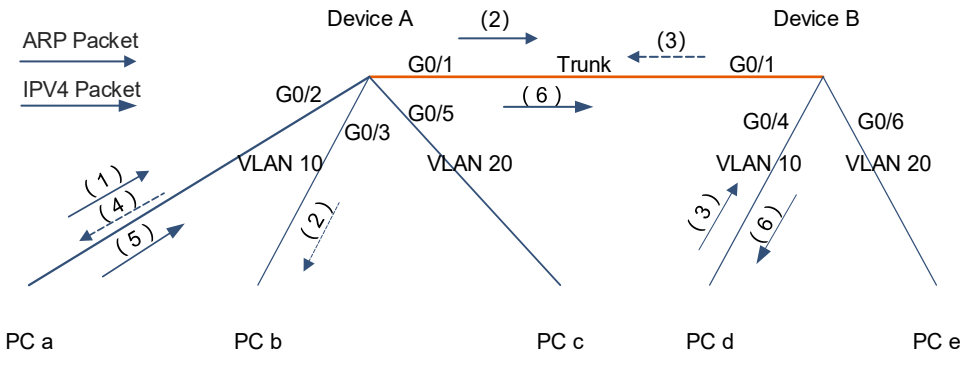
```
Protocol  Address      Age(min)    Hardware        Type
Internet  1.1.20.1        1        g MAC           arpa
Internet  1.1.10.2        0        g MAC           arpa
```

Later, when PC c sends the packet to PC a, it can query the gateway MAC address corresponding to the IP address of PC a, and encapsulate the packet for PC a by using the gateway MAC address as the destination MAC address.

4. Intra-VLAN Communication Across Devices

Ports on different devices can be assigned to the same VLAN. As shown in Figure 1-1, one port between two devices must allow packets from different VLANs to pass through, so that two PCs in the same VLAN can communicate across the devices. This interconnection port must be configured as a trunk port. PC a is connected to VLAN 10 through Device A, and PC d is connected to VLAN 10 through Device B. Device A and Device B are connected through the trunk port. The communication between PC a and PC d is intra-VLAN communication across devices.

Figure 1-1 Example of Intra-VLAN Communication Across Devices



The mappings between ports and VLANs on Device A are as follows:

```
Device A  VLAN     Name        Status     Ports
10                 VLAN10      STATIC     Gi0/1, Gi0/2, Gi0/3
20                 VLAN20      STATIC     Gi0/1, Gi0/5
```

The port configurations of Device A are as follows:

```
Device A Interface    Switchport   Mode     Access  Native   VLAN lists
```

```
Gi0/1                enabled      trunk            10       10,20
Gi0/2-Gi0/3          enabled      access    10               10
Gi0/5                enabled      access    20               20
```

The mappings between ports and VLANs on Device B are as follows:

```
Device B VLAN     Name       Status     Ports
10                VLAN10     STATIC     Gi0/1, Gi0/4
20                VLAN20     STATIC     Gi0/1, Gi0/6
```

The port configurations of Device B are as follows:

```
Device B Interface    Switchport   Mode     Access  Native   VLAN lists
Gi0/1                  enabled     trunk             10       10,20
Gi0/4                  enabled     access    10              10
Gi0/6                  enabled     access    20              20
```

The procedure of intra-VLAN communication across devices is similar to the procedure of intra-VLAN communication within one device, except for the following:

- When Device A sends a packet through the trunk port GigabitEthernet 0/1, if the packet comes from the native VLAN (for example, the packet is sent by PC a to PC d in VLAN 10), the packet is untagged; or if the packet comes from an allowed VLAN (for example, the packet is sent by PC c to PC e in VLAN 20), the packet is tagged.
- When Device B receives the packet through the trunk port GigabitEthernet 0/1, if the packet is untagged (for example, the packet is sent by PC a to PC d in VLAN 10), Device B determines that the packet comes from the native VLAN (VLAN 10). If the native VLAN is also an allowed VLAN (VLAN 10 or VLAN 20), Device B allows the packet to pass through. If the native VLAN is not an allowed VLAN, Device B does not allow the packet to pass through. If the packet is tagged (for example, the packet is sent by PC c to PC e in VLAN 20), Device B checks whether the packet comes from an allowed VLAN (VLAN 10 or VLAN 20). If yes, Device B receives the packet. Otherwise, Device B discards the packet.

1.1.6 VLAN Assignment Methods

- Port-based assignment

Port-based VLAN assignment is the most basic VLAN assignment method. After the administrator configures a port with a Port Default VLAN ID (PVID), the port is assigned to a VLAN. The VLAN ID range is from 1 to 4094. In case of no VLAN assignment, all ports are assigned to VLAN 1 by default.

- Super VLAN

Super VLAN is also referred to as VLAN aggregation, which aggregates multiple VLANs into one IP address segment. Only one IP address is assigned to a super VLAN that contains multiple sub VLANs, and this saves address resources and facilitates network management. A VLAN accessible by an STA is subject only to an access port of the STA. That is, the STA is assigned to a VLAN based on the STA's access port. For more information, see *Super VLAN*.

- Private VLAN

Private VLAN is a technology that can divide an L2 broadcast domain of a VLAN into multiple sub domains, and each sub domain is composed of one private VLAN pair: primary VLAN and secondary VLAN. This technology can increase the number of users that can be supported by an operator network and reduce waste of IP address resources. A VLAN accessible by an STA is subject only to an access port of the STA. That is, the STA is assigned to a VLAN based on the STA's access port. For more information, see *Private VLAN*.

- MAC VLAN

MAC VLAN is a MAC address-based VLAN assignment method. When an STA is physically relocated, it can re-access the network from another device and there is no need to reconfigure a VLAN for the access port. If different STAs access the network from the same port, they can be assigned to different VLANs based on their MAC addresses. This method belongs to packet content-based VLAN assignment. Generally, this function is used with the 802.1x VLAN delivery function to ensure secure and flexible access of 802.1x STAs. For more information, see *MAC VLAN*.

- Voice VLAN

A voice VLAN is a VLAN dedicated for voice data streams of users. With this technology, data streams and voice streams are transmitted in the data VLAN and the voice VLAN, respectively, to prevent mutual interference between voice calls and service packets. This function identifies voice data and assigns the voice data to the voice VLAN. This method belongs to packet content-based VLAN assignment. For more information, see *Voice VLAN*.

- Protocol VLAN

Protocol VLAN is a VLAN assignment technology based on the protocol type or IP subnet in packets. The service types supported in a network are bound to VLANs to facilitate management and maintenance. This method belongs to packet content-based VLAN assignment. For more information, see *Protocol VLAN*.

1.1.7 Protocols and Standards

IEEE 802.1Q: IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks

1.2 Restrictions and Guidelines

Before you configure a port type or add the port to a VLAN, ensure that the port is an L2 interface. You can run the **switchport** command to configure an interface as an L2 interface. You can run the **no switchport** command to configure an interface as an L3 interface.

1.3 Configuration Task Summary

VLAN configuration includes the following tasks:

(1) Configuring VLAN

a Creating and Configuring VLAN

b (Optional) Configuring VLAN Name

c (Optional) Configuring L3 SVI of VLAN

(2) Configuring a port type and adding ports to a VLAN by performing at least one of the following configuration tasks:

- Configuring Access Port
- Configuring Trunk Port
- Configuring Uplink Port
- Configuring Hybrid Port

1.4 Configuring VLAN

1.4.1 Overview

This section describes how to create a VLAN, configure the VLAN, and enter the VLAN configuration mode.

1.4.2 Restrictions and Guidelines

In case of insufficient hardware resources, the system returns information on VLAN creation failure.

1.4.3 Configuration Tasks

VLAN configuration includes the following tasks:

(1) Creating and Configuring VLAN

(2) (Optional) Configuring VLAN Name

(3) (Optional) Configuring L3 SVI of VLAN

1.4.4 Creating and Configuring VLAN

1. Overview

You can create a VLAN or enter the VLAN configuration mode.

A VLAN is identified based on a VLAN ID, and the VLAN ID range is from 1 to 4094. VLAN 1 is created automatically and cannot be deleted. VLANs 2 to 4094 can be created, deleted, and edited.

2. Restrictions and Guidelines

- In case of insufficient hardware resources, the system returns information on VLAN creation failure.
- You can run the **no vlan** *vlan-id* command to delete a common VLAN. VLANs such as VLAN 1, VLANs with SVIs configured, and private VLANs cannot be deleted.
- To delete a VLAN with a created SVI, run the **no interface vlan** *vlan-id* command to delete the SVI and then the **no vlan** *vlan-id* command to delete the VLAN.

3. Prerequisites

Check VLAN and its VLAN status. If you enter a new VLAN ID, a corresponding VLAN is created. If you enter an existing VLAN ID, the system enters the configuration mode of the corresponding VLAN, and you can modify the VLAN settings.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a VLAN and enter the VLAN configuration mode.

vlan *vlan-id*

Only VLAN 1 exists by default.

1.4.5 Configuring VLAN Name

1. Overview

You can name a VLAN.

2. Restrictions and Guidelines

- You cannot rename a VLAN the same as the default name of another VLAN.
- To restore the VLAN name to a default value, run the **no name** command.

3. Prerequisites

The VLAN name must be unique.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN configuration mode.

vlan *vlan-id*

(4) Configure a VLAN name.

name *vlan-name*

The name of a VLAN is its VLAN ID by default. For example, the name of VLAN 4 is VLAN0004.

1.4.6 Configuring L3 SVI of VLAN

1. Overview

You can create an L3 SVI of a VLAN and enter the SVI configuration mode. Configure an IP address for the SVI so that devices in the VLAN can communicate at L3.

2. Restrictions and Guidelines

- You cannot create SVIs for sub VLANs of a super VLAN or secondary VLANs of a private VLAN.
- To delete a VLAN with a created SVI, run the **no interface vlan** *vlan-id* command to delete the SVI and then the **no vlan** *vlan-id* command to delete the VLAN.

3. Prerequisites

Create a VLAN.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an SVI of a VLAN and enter the SVI configuration mode.

interface vlan *vlan-id*

No SVI is configured for a VLAN by default.

(4) (Optional) Configure an IP address and a mask for the VLAN gateway.

ip address *ip-address mask*

No IP address is configured for an SVI by default.

1.5 Configuring Access Port

1.5.1 Overview

You can define the type of an interface as L2 access port and add the interface to a VLAN.

1.5.2 Restrictions and Guidelines

- When you run the **switchport access vlan** *vlan-id* command to configure a VLAN for an access port, if you add the access port to an inexistent VLAN, the VLAN is automatically created. You can run the **no switchport access vlan** command to restore the VLAN for the access port to VLAN 1.
- The **add interface** { *interface-type interface-number* | **range** *interface-type interface-range* } command has the same execution effect as that of the **switchport access vlan** *vlan-id* command. You can run the **no add interface** { *interface-type interface-number* | **range** *interface-type interface-range* } command to restore the VLAN (other than VLAN 1) of a specified access port to VLAN 1.
- This command is available to access ports only. If you configure the command multiple times, the last command prevails.

1.5.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure one interface as an access port or a group of interfaces as access ports.

a Enter the configuration mode corresponding to the interface or the group of interfaces.

interface { *interface-type interface-number* | **range** *interface-type interface-range* }

b Configure the L2 interface as an access port.

switchport mode access

The L2 interface mode is **access** by default.

c Return to the global configuration mode.

exit

(4) (Optional) Add the interface or the group of interfaces to a VLAN. Select a method to configure the interface or the group of interfaces.

- Create a VLAN, and add the interface or the group of interfaces to the VLAN in VLAN configuration mode. Run the following commands in sequence:

  vlan *vlan-id*

  Only VLAN 1 exists by default.

  add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  An access port belongs to VLAN 1 by default.

- Add the interface or the group of interfaces to a VLAN (which can be automatically created) in interface configuration mode. Run the following commands in sequence:

  interface { *interface-type interface-number* | **range** *interface-type interface-range* }

  switchport access vlan *vlan-id*

  An access port belongs to VLAN 1 by default.

1.6 Configuring Trunk Port

1.6.1 Overview

A trunk link can transmit traffic of multiple VLANs. To enable a port to transmit traffic of multiple VLANs, you can configure the port as a trunk port.

You can configure a common Ethernet L2 interface or an aggregation port (AP) as a trunk port. For more information about AP, see *Link Aggregation Port*.

L2 switch ports have two key attributes, native VLAN and allowed VLAN. A trunk port has one native VLAN and several allowed VLANs.

- Native VLAN: When the trunk port receives an untagged packet or a priority packet, the trunk port considers that the packet comes from the native VLAN of this port. Packets of the native VLAN sent by the trunk port are untagged. When you configure a trunk link, ensure that the trunk ports of the link are bound to the same native VLAN.
- Allowed VLAN: When the trunk port receives a tagged packet, it determines whether the packet comes from an allowed VLAN of this port. If yes, the trunk port receives the packet. Otherwise, the trunk port discards the packet. Packets of an allowed VLAN sent by the trunk port are tagged.

1.6.2 Restrictions and Guidelines

- Before you configure the native VLAN and allowed VLANs for the trunk port, create these VLANs first. *When you* set the native VLAN to an inexistent VLAN, this VLAN is not created automatically.
- *vlan-list* can contain one or more VLANs. VLAN IDs are separated by commas (,). Continuous VLAN IDs are represented by connecting the first and the last VLAN IDs with a hyphen (-), for example, 3, 10-20, and 22.

  all: Indicates that the allowed VLAN list includes all supported VLANs.

  add *vlan-list*: Adds a specified VLAN to the allowed VLAN list.

  remove *vlan-list*: Removes a specified VLAN from the allowed VLAN list.

  except *vlan-list*: Adds all VLANs other than a specified VLANs to the allowed VLAN list.

only *vlan-list* : Adds only a specified VLAN to the allowed VLAN list and remove all the other VLANs from the list.

- The native VLAN of an interface can be excluded from the allowed VLAN list for this interface. In this case, traffic of the native VLAN cannot pass through this interface.
- You can run the **no switchport mode** command to restore the trunk port to an access port.

  You can run the **no switchport trunk native vlan** command to restore the native VLAN of the trunk port to a default value.

  You can run the **no switchport trunk allowed vlan** command to restore the allowed VLANs of the trunk port to default values.

1.6.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.6.4 Procedure

(1) Create a VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create one VLAN or a group of VLANs as the native VLAN and allowed VLANs of the trunk port.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the interface as a trunk port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the L2 interface as a trunk port.

switchport mode trunk

The L2 interface mode is **access** by default.

(3) (Optional) Configure a native VLAN for the trunk port.

switchport trunk native vlan *vlan-id*

The native VLAN of the trunk port is VLAN 1 by default.

(4) (Optional) Configure an allowed VLAN list for the trunk port.

switchport trunk allowed vlan { **all** | { **add** | **remove** | **except** | **only** } *vlan-list* }

The allowed VLANs of the trunk port are VLANs 1 to 4094 by default.

1.7 Configuring Uplink Port

1.7.1 Overview

You can configure an interface as an uplink port to transmit only tagged frames of multiple VLANs. An uplink port has one native VLAN and several allowed VLANs.

The uplink port is generally used in QinQ scenarios as an interface for a PE to connect to a public network.

- Native VLAN: When the uplink port receives an untagged packet or a priority packet, the uplink port considers that the packet comes from the native VLAN of this port. Different from the trunk port, packets of the native VLAN sent by the uplink port are tagged.
- Allowed VLAN: When the uplink port receives a tagged packet, it determines whether the packet comes from the native VLAN of this port. If yes, the uplink port receives the packet. Otherwise, the uplink port discards the packet. Packets of the allowed VLANs sent by the uplink port are tagged.

1.7.2 Restrictions and Guidelines

- Before you configure the native VLAN and allowed VLANs for the uplink port, create these VLANs first.
- You can run the **no switchport mode** command to restore the uplink port to an access port.
- You can run the **no switchport trunk native vlan** command to restore the native VLAN of the uplink port to a default value.
- You can run the **no switchport trunk allowed vlan** command to restore the allowed VLANs of the uplink port to default values.
- You can run the **show vlan** [**id** *vlan-id*] and **show interface switchport** commands to check whether the configurations take effect.

1.7.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.7.4 Procedure

(1) Create a VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create one VLAN or a group of VLANs as the native VLAN and allowed VLANs of the uplink port.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the interface as an uplink port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the L2 interface as an uplink port.

switchport mode uplink

The L2 interface mode is **access** by default.

(3) (Optional) Configure a native VLAN for the uplink port.

switchport trunk native vlan *vlan-id*

The native VLAN of the uplink port is VLAN 1 by default.

(4) (Optional) Configure an allowed VLAN list for the uplink port.

switchport trunk allowed vlan { **all** | { **add** | **remove** | **except** | **only** } *vlan-list* }

The allowed VLANs of the uplink port are VLANs 1 to 4094 by default.

1.8 Configuring Hybrid Port

1.8.1 Overview

You can configure an interface as a hybrid port to transmit traffic of multiple VLANs. The hybrid port is used in MAC VLANs and connected to an access link. A hybrid port has one native VLAN and several allowed VLANs.

- Native VLAN: The native VLAN of a hybrid port is VLAN 1 by default. When the hybrid port receives an untagged packet or a priority packet, the hybrid port considers that the packet comes from the native VLAN of this port. Packets of the native VLAN sent by the hybrid port are untagged.
- Allowed VLAN: The allowed VLANs of the hybrid port are VLANs 1 to 4094 by default. When the hybrid port receives a tagged packet, it determines whether the packet comes from an allowed VLAN of this port. If yes, the hybrid port receives the packet. Otherwise, the hybrid port discards the packet. Different from the trunk port, the hybrid port can send tagged or untagged packets of the allowed VLANs (other than the native VLAN) based on configurations.

1.8.2 Restrictions and Guidelines

- Before you configure the native VLAN and allowed VLANs for the hybrid port, create these VLANs first.
- You can run the **no switchport mode** command to restore the hybrid port to an access port.
- You can run the **no switchport hybrid native vlan** command to restore the native VLAN of the hybrid port to a default value.
- You can run the **no switchport hybrid allowed vlan** command to restore the allowed VLANs of the hybrid port to default values.
- You can run the **show vlan** [**id** *vlan-id*] and **show interface switchport** commands to check whether the configurations take effect.

1.8.3 Prerequisites

The interface to be configured must be an L2 interface. You can run the **show interface switchport** command to query the interface type. If the **Switchport** field corresponding to the interface is set to **enabled**, this

interface is an L2 interface. Otherwise, this interface is an L3 interface. You should run the **switchport** command to configure the interface as an L2 interface and then set the default interface mode to **access**.

1.8.4 Procedure

(1) Create a VLAN.

a Enter the privileged EXEC mode.

enable

b Enter the global configuration mode.

configure terminal

c Create one VLAN or a group of VLANs as the native VLAN and allowed VLANs of the hybrid port.

vlan { *vlan-id* | **range** *vlan-range* }

Only VLAN 1 exists by default.

d Return to the global configuration mode.

exit

(2) Configure the interface as a hybrid port.

a Enter the interface configuration mode.

interface *interface-type interface-number*

b Configure the L2 interface as a hybrid port.

switchport mode hybrid

The L2 interface mode is **access** by default.

(3) Configure a native VLAN for the hybrid port.

switchport hybrid native vlan *vlan-id*

The native VLAN of the hybrid port is VLAN 1 by default.

(4) Configure an allowed VLAN list for the hybrid port.

switchport hybrid allowed vlan { [**add**] **tagged** | [**add**] **untagged** | **only tagged** | **remove** } *vlan-list*

By default, the allowed VLANs of the hybrid port are tagged VLANs 2 to 4094 and untagged VLAN 1.

1.9 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

This section also describes the **debug** command used for outputting debugging information.

Caution

System resources are occupied when debugging information is output. Therefore, disable the debugging function immediately after use.

You can run the **clear** commands to clear information.

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
show vlan [**id** *vlan-id*]	Displays VLAN configurations.
show interface switchport	Displays configurations of switch ports.
debug bridge vlan	Enables the debug function of a VLAN.

1.10 Configuration Examples

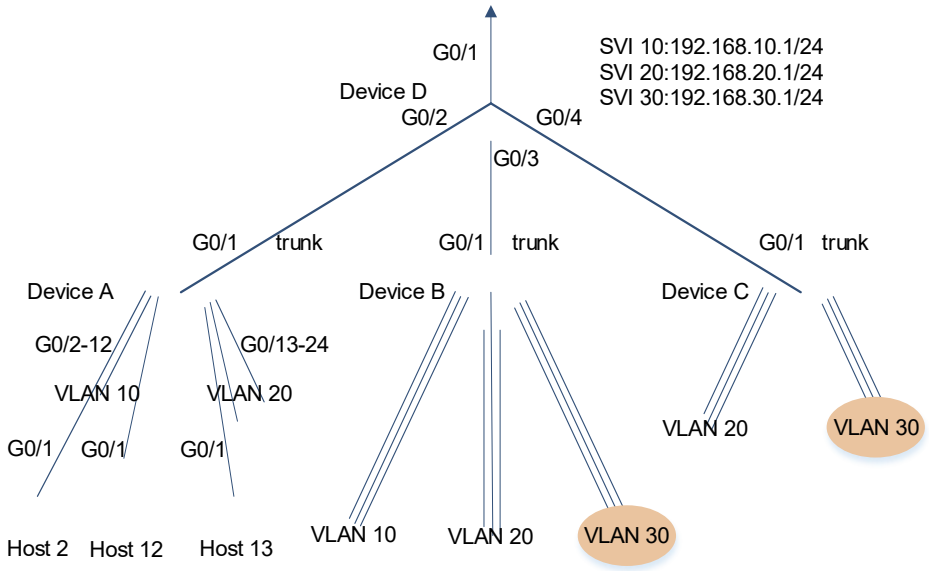
1.10.1 Configuring L2 Isolation and L3 Interconnection of VLAN

1. Requirements

The LAN of a user needs to be divided into VLAN 10, VLAN 20 and VLAN 30 to realize L2 isolation. The three VLANs correspond to the IP subnets 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, respectively, and these VLANs implement subnet interconnection based on the IP forwarding capability of L3 core switches.

2. Topology

Figure 1-1 Typical Scenario



3. Notes

The following describes the configuration procedure by using Device D and Device A as examples:

- On the L3 core device Device D, configure the three VLANs, configure the ports for connecting Device A,

Device B, and Device C as trunk ports, and specify an allowed VLAN list to realize L2 isolation.

- Configure three SVIs on Device D, which are used as the gateway interfaces of the IP subnets corresponding to the three VLANs. Configure the IP addresses for these SVIs. Configure a default gateway for hosts based on the VLANs of the hosts.
- Create the VLANs separately on the three access devices, assign an access port for each VLAN, and configure the ports for connecting Device D as trunk ports.

4. Procedure

(1) Create and configure VLANs.

Create VLANs on Device D and rename VLAN 10.

```
DeviceD> enable
DeviceD# configure terminal
DeviceD(config)# vlan 10
DeviceD(config-vlan)# name office
DeviceD(config-vlan)# vlan range 20,30
DeviceD(config-vlan-range)# exit
```

Create VLANs on Devices A, B and C. The following example describes how to configure Device A. For the configuration of Devices B and C, see the configuration procedure of Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# vlan rang 10,20
DeviceA(config-vlan-range)# exit
```

(2) Configure IP addresses for the L3 SVIs of the VLANs on Device D.

```
DeviceD(config)# interface vlan 10
DeviceD(config-if-VLAN 10)# ip address 192.168.10.1 255.255.255.0
DeviceD(config-if-VLAN 10)# interface vlan 20
DeviceD(config-if-VLAN 20)# ip address 192.168.20.1 255.255.255.0
DeviceD(config-if-VLAN 20)# interface vlan 30
DeviceD(config-if-VLAN 30)# ip address 192.168.30.1 255.255.255.0
DeviceD(config-if-VLAN 30)# exit
```

(3) Configure specific types of ports and add the ports to the VLANs.

Configure the downlink port of Device D as a trunk port and configure an allowed VLAN list for the port.

```
DeviceD(config)# interface range gigabitethernet 0/2-4
DeviceD(config-if-range)# switchport
DeviceD(config-if-range)# switchport mode trunk
DeviceD(config-if-range)# exit
DeviceD(config)# interface gigabitethernet 0/2
DeviceD(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan remove
1-4094
DeviceD(config-if-GigabitEthernet 0/2)# switchport trunk allowed vlan add
10,20
DeviceD(config-if-GigabitEthernet 0/2)# interface gigabitethernet 0/3
```

```
DeviceD(config-if-GigabitEthernet 0/3)# switchport trunk allowed vlan only
10,20,30
DeviceD(config-if-GigabitEthernet 0/3)# interface gigabitethernet 0/4
DeviceD(config-if-GigabitEthernet 0/4)# switchport trunk allowed vlan only
20,30
DeviceD(config-if-GigabitEthernet 0/4)# end
DeviceD# write
```

Configure the uplink port of the access device as a trunk port. If you do not configure an allowed VLAN list for the port, the port allows packets of all VLANs to pass through by default. The following example describes how to configure Device A. For the configuration of Devices B and C, see the configuration procedure of Device A.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# switchport mode trunk
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure the downlink port of the access device as an access port and add the port to a specified VLAN. The following example describes how to configure Device A. For the configuration of Devices B and C, see the configuration procedure of Device A.

```
DeviceA(config)# interface range gigabitethernet 0/2-12
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode access
DeviceA(config-if-range)# switchport access vlan 10
DeviceA(config-if-range)# interface range gigabitethernet 0/13-24
DeviceA(config-if-range)# switchport
DeviceA(config-if-range)# switchport mode access
DeviceA(config-if-range)# switchport access vlan 20
DeviceA(config-if-range)# end
DeviceA# write
```

5. Verification

(1) Run the **show vlan** [**id** *vlan-id*] command on Device D to display VLAN information, including the VLAN ID, name, status and ports.

```
DeviceD# show vlan
VLAN  Name        Status                Ports
---- --------  --------   --------------------------------
   1 VLAN0001   STATIC     Gi0/1, Gi0/5, Gi0/6, Gi0/7
                           Gi0/8, Gi0/9, Gi0/10, Gi0/11
                           Gi0/12, Gi0/13, Gi0/14, Gi0/15
                           Gi0/16, Gi0/17, Gi0/18, Gi0/19
                           Gi0/20, Gi0/21, Gi0/22, Gi0/23
                           Gi0/24
  10 office    STATIC      Gi0/2, Gi0/3
  20 VLAN0020  STATIC      Gi0/2, Gi0/3, Gi0/4
  30 VLAN0030  STATIC      Gi0/3, Gi0/4
```

(2) Check the port configuration and port status.

Run the **show interface switchport** command on Device D to display the VLAN status of ports.

```
DeviceD# show interface gigabitethernet 0/2 switchport
Interface                        Switchport Mode      Access Native Protected
VLAN lists
-------------------------------- ---------- --------- ------ ------ ---------
--
GigabitEthernet 0/2              enabled    TRUNK     1      1       Disabled
10,20

DeviceD# show interface switchport
Interface                        Switchport Mode      Access Native Protected
VLAN lists
-------------------------------- ---------- --------- ------ ------ ---------
--
GigabitEthernet 0/2              enabled    TRUNK     1      1       Disabled
10,20
GigabitEthernet 0/3              enabled    TRUNK     1      1       Disabled
10,20,30
GigabitEthernet 0/4              enabled    TRUNK     1      1       Disabled
20,30
```

Run the **show interface description** command on Device D to check whether the port status is up.

```
DeviceD# show interface description
Interface                                Status   Administrative Description
---------------------------------------- -------- -------------- -----------
GigabitEthernet 0/2                      up       up
GigabitEthernet 0/3                      up       up
GigabitEthernet 0/4                      up       up

VLAN 10                                  up       up
VLAN 20                                  up       up
VLAN 30                                  up       up
```

(3) Run the **show ip route** command on Device D to display the direct route information of SVIs.

Packets whose destination IP address matches 192.168.10.0/24 are forwarded to VLAN 10. Packets whose destination IP address matches 192.168.20.0/24 are forwarded to VLAN 20. Packets whose destination IP address matches 192.168.30.0/24 are forwarded to VLAN 30.

```
DeviceD# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, EV - BGP EVPN, A - Arp to host
        LA - Local aggregate route
        * - candidate default

Gateway of last resort is no set
```

```
…
C     192.168.10.0/24 is directly connected, VLAN 10
C     192.168.10.1/32 is local host.
C     192.168.20.0/24 is directly connected, VLAN 20
C     192.168.20.1/32 is local host.
C     192.168.30.0/24 is directly connected, VLAN 30
C     192.168.30.1/32 is local host.
```

Ping the SVI address of a VLAN (for example, VLAN 10) on Device D.

```
DeviceD# ping 192.168.10.1
Sending 5, 100-byte ICMP Echoes to 192.168.10.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

(4) The following example describes how to ping Hosts 2, 12, and 13.

Configure the default gateway of Host 2 in VLAN 10 as 192.168.10.1, the IP address of the port as 192.168.10.2, and the mask as 255.255.255.0.

```
Host2> enable
Host2# configure terminal
Host2(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1
Host2(config)# interface gigabitethernet 0/1
Host2(config-if-GigabitEthernet 0/1)# no switchport
Host2(config-if-GigabitEthernet 0/1)# ip address 192.168.10.2 255.255.255.0
```

Configure the default gateway of Host 12 in VLAN 10 as 192.168.10.1, the IP address of the port as 192.168.10.12, and the mask as 255.255.255.0.

```
Host2> enable
Host2# configure terminal
Host2(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1
Host2(config)# interface gigabitethernet 0/1
Host2(config-if-GigabitEthernet 0/1)# no switchport
Host2(config-if-GigabitEthernet 0/1)# ip address 192.168.10.12 255.255.255.0
```

Configure the default gateway of Host 13 in VLAN 20 as 192.168.20.1, the IP address of the port as 192.168.20.13, and the mask as 255.255.255.0.

```
Host13> enable
Host13# configure terminal
Host13(config)# ip route 0.0.0.0 0.0.0.0 192.168.20.1
Host13(config)# interface gigabitethernet 0/1
Host13(config-if-GigabitEthernet 0/1)# no switchport
Host13(config-if-GigabitEthernet 0/1)# ip address 192.168.20.13 255.255.255.0
```

Run the **show ip route** command on the hosts to display the default gateway. The default gateway must be configured on the transmit and receive ends. Inter-VLAN communication fails to be implemented if either end is not configured with the default gateway. Take Host 2 as an example. Due to the default route S*0.0.0.0/0 [1/0] via 192.168.10.1, a host sends a packet to the gateway 192.168.10.1 when the host tries to communicate across VLANs.

```
Host2# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, EV - BGP EVPN, A - Arp to host
        LA - Local aggregate route
        * - candidate default

Gateway of last resort is 192.168.10.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.168.10.1
C     192.168.10.0/24 is directly connected, GigabitEthernet 0/1
C     192.168.10.2/32 is local host.
```

Ping the IP address of a host (for example, Host 2) on Device D.

```
DeviceD# ping 192.168.10.2
Sending 5, 100-byte ICMP Echoes to 192.168.10.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms.
```

Hosts in the same VLAN (for example, VLAN 10) can ping each other.

```
Host2# ping 192.168.10.12
Sending 5, 100-byte ICMP Echoes to 192.168.10.12, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms.
```

Hosts in different VLANs can also ping each other. If you delete the IP address of an SVI on Device D or delete the default gateway on a host, hosts in different VLANs cannot ping each other.

```
Host2# ping 192.168.20.13
Sending 5, 100-byte ICMP Echoes to 192.168.10.3, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms.
```

6. Configuration Files

- Device D configuration file

```
vlan 10
 name office
vlan range 1,20,30

interface GigabitEthernet 0/2
 switchport mode trunk
 switchport trunk allowed vlan only 10,20
interface GigabitEthernet 0/3
```

```
 switchport mode trunk
 switchport trunk allowed vlan only 10,20,30
interface GigabitEthernet 0/4
 switchport mode trunk
 switchport trunk allowed vlan only 20,30

interface VLAN 10
 ip address 192.168.10.1 255.255.255.0
interface VLAN 20
 ip address 192.168.20.1 255.255.255.0
interface VLAN 30
 ip address 192.168.30.1 255.255.255.0
```

- Device A configuration file. Similar configurations of ports are represented by ellipsis (...). For the configuration of Devices B and C, see the Device A configuration procedure.

```
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 10
…
interface GigabitEthernet 0/12
 switchport access vlan 10
!
interface GigabitEthernet 0/13
 switchport access vlan 20
…
interface GigabitEthernet 0/24
 switchport access vlan 20
```

7. Common Errors

- If no IP address is configured for a gateway (SVI), or no default gateway is configured for an STA, or either the transmit or receive end is not configured with the default gateway, STAs in different VLANs cannot ping each other.
- If connected trunk ports have different native VLANs, data communication may fail.
- If interfaces connected to STAs are not configured as access ports, data communication may fail.
- If only one VLAN needs to be configured for a trunk port but the default allowed VLAN of the trunk port is not deleted after the VLAN creation command is run, the configuration result is inconsistent with the configuration plan.
- A trunk port on a vendor's device needs to receive only tagged frames and discard untagged packets. If the trunk port of the local device sends untagged packets of the native VLAN, the packets may be discarded. In this case, configure the connection port on the local device as an uplink port so that packets sent by this port are tagged.