Contents

Configuring VLANs

About VLANs

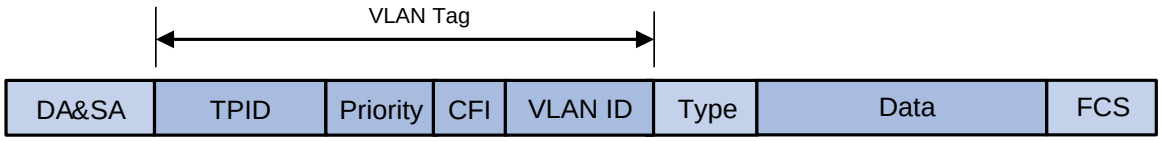
The Virtual Local Area Network (VLAN) technology divides a physical LAN into multiple logical LANs. It has the following benefits:

- **Security**—Hosts in the same VLAN can communicate with one another at Layer 2, but they are isolated from hosts in other VLANs at Layer 2.
- **Broadcast traffic isolation**—Each VLAN is a broadcast domain that limits the transmission of broadcast packets.
- **Flexibility**—A VLAN can be logically divided on a workgroup basis. Hosts in the same workgroup can be assigned to the same VLAN, regardless of their physical locations.

VLAN frame encapsulation

To identify Ethernet frames from different VLANs, IEEE 802.1Q inserts a four-byte VLAN tag between the destination and source MAC address (DA&SA) field and the Type field.

Figure 1 VLAN tag placement and format



A VLAN tag includes the following fields:

- **TPID**—16-bit tag protocol identifier that indicates whether a frame is VLAN-tagged. By default, the hexadecimal TPID value 8100 identifies a VLAN-tagged frame. A device vendor can set the TPID to a different value. For compatibility with a neighbor device, set the TPID value on the device to be the same as the neighbor device. For more information about setting the TPID value, see "Configuring QinQ."
- **Priority**—3-bit long, identifies the 802.1p priority of the frame. For more information, see *ACL and QoS Configuration Guide*.
- **CFI**—1-bit long canonical format indicator that indicates whether the MAC addresses are encapsulated in the standard format when packets are transmitted across different media. Available values include:
  - **0 (default)**—The MAC addresses are encapsulated in the standard format.
  - **1**—The MAC addresses are encapsulated in a non-standard format.

  This field is always set to 0 for Ethernet.
- **VLAN ID**—12-bit long, identifies the VLAN to which the frame belongs. The VLAN ID range is 0 to 4095. VLAN IDs 0 and 4095 are reserved, and VLAN IDs 1 to 4094 are user configurable.

The way a network device handles an incoming frame depends on whether the frame has a VLAN tag and the value of the VLAN tag (if any).

Ethernet supports encapsulation formats Ethernet II, 802.3/802.2 LLC, 802.3/802.2 SNAP, and 802.3 raw. The Ethernet II encapsulation format is used here. For information about the VLAN tag fields in other frame encapsulation formats, see related protocols and standards.

For a frame that has multiple VLAN tags, the device handles it according to its outermost VLAN tag and transmits its inner VLAN tags as the payload.

VLAN types

The following VLAN types are available:

- Port-based VLAN.
- MAC-based VLAN.
- IP subnet-based VLAN.
- Protocol-based VLAN.

If all these types of VLANs are configured on a port, the port processes packets in the following descending order of priority by default:

- MAC-based VLAN.
- IP subnet-based VLAN.
- Protocol-based VLAN.
- Port-based VLAN.

Port-based VLANs

Port-based VLANs group VLAN members by port. A port forwards packets from a VLAN only after it is assigned to the VLAN.

Port link type

You can set the link type of a port to access, trunk, or hybrid. The port link type determines whether the port can be assigned to multiple VLANs. The link types use the following VLAN tag handling methods:

- **Access**—An access port can forward packets only from one VLAN and send these packets untagged. An access port is typically used in the following conditions:
  - Connecting to a terminal device that does not support VLAN packets.
  - In scenarios that do not distinguish VLANs.
- **Trunk**—A trunk port can forward packets from multiple VLANs. Except packets from the port VLAN ID (PVID), packets sent out of a trunk port are VLAN-tagged. Ports connecting network devices are typically configured as trunk ports.
- **Hybrid**—A hybrid port can forward packets from multiple VLANs. The tagging status of the packets forwarded by a hybrid port depends on the port configuration. In one-to-two VLAN mapping, hybrid ports are used to remove SVLAN tags for downlink traffic. For more information about one-to-two VLAN mapping, see "Configuring VLAN mapping."

PVID

The PVID identifies the default VLAN of a port. Untagged packets received on a port are considered as the packets from the port PVID.

An access port can join only one VLAN. The VLAN to which the access port belongs is the PVID of the port. A trunk or hybrid port supports multiple VLANs and the PVID configuration.

How ports of different link types handle frames

Actions	Access	Trunk	Hybrid
In the inbound direction for an untagged frame	Tags the frame with the PVID tag.	• If the PVID is permitted on the port, tags the frame with the PVID tag. • If not, drops the frame.	
In the inbound direction for a tagged frame	• Receives the frame if its VLAN ID is the same as	• Receives the frame if its VLAN is permitted on the port. • Drops the frame if its VLAN is not permitted on the port.	

Actions	Access	Trunk	Hybrid
	the PVID. • Drops the frame if its VLAN ID is different from the PVID.		
In the outbound direction	Removes the VLAN tag and sends the frame.	• Removes the tag and sends the frame if the frame carries the PVID tag and the port belongs to the PVID. • Sends the frame without removing the tag if its VLAN is carried on the port but is different from the PVID.	Sends the frame if its VLAN is permitted on the port. The tagging status of the frame depends on the **`port hybrid vlan`** command configuration.

MAC-based VLANs

The MAC-based VLAN feature assigns hosts to a VLAN based on their MAC addresses. This feature is also called user-based VLAN because VLAN configuration remains the same regardless of a user's physical location.

Static MAC-based VLAN assignment

Use static MAC-based VLAN assignment in networks that have a small number of VLAN users. To configure static MAC-based VLAN assignment on a port, perform the following tasks:

1. Create MAC-to-VLAN entries.
2. Enable the MAC-based VLAN feature on the port.
3. Assign the port to the MAC-based VLAN.

A port configured with static MAC-based VLAN assignment processes a received frame as follows before sending the frame out:

- For an untagged frame, the port determines its VLAN ID in the following workflow:
  a. The port first performs a fuzzy match as follows:
     - Searches for the MAC-to-VLAN entries whose masks are not all Fs.
     - Performs a logical AND operation on the source MAC address and each of these masks.

       If an AND operation result matches the MAC address in a MAC-to-VLAN entry, the port tags the frame with the VLAN ID specific to this entry.

  b. If the fuzzy match fails, the port performs an exact match. It searches for MAC-to-VLAN entries whose masks are all Fs. If the source MAC address of the frame exactly matches the MAC address of a MAC-to-VLAN entry, the port tags the frame with the VLAN ID specific to this entry.

  c. If no matching VLAN ID is found, the port determines the VLAN for the packet by using the following matching order:
     - IP subnet-based VLAN.
     - Protocol-based VLAN.
     - Port-based VLAN.

     When a match is found, the port tags the packet with the matching VLAN ID.

- For a tagged frame, the port determines whether the VLAN ID of the frame is permitted on the port.
  - If the VLAN ID of the frame is permitted on the port, the port forwards the frame.
  - If the VLAN ID of the frame is not permitted on the port, the port drops the frame.

Dynamic MAC-based VLAN assignment

When you cannot determine the target MAC-based VLANs of a port, use dynamic MAC-based VLAN assignment on the port. To use dynamic MAC-based VLAN assignment, perform the following tasks:

1. Create MAC-to-VLAN entries.
2. Enable the MAC-based VLAN feature on the port.
3. Enable dynamic MAC-based VLAN assignment on the port.

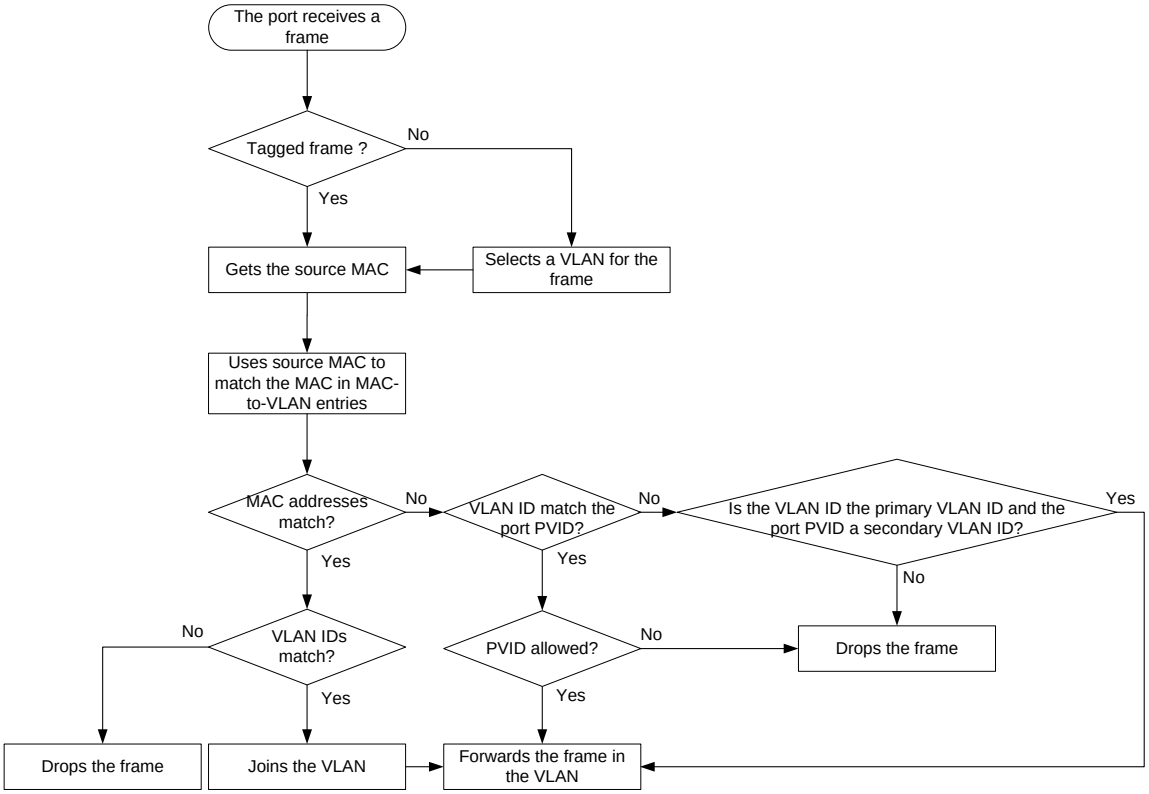
Dynamic MAC-based VLAN assignment uses the following workflow, as shown in Figure 2:

1. When a port receives a frame, it first determines whether the frame is tagged.
   - If the frame is tagged, the port gets the source MAC address of the frame.
   - If the frame is untagged, the port selects a VLAN for the frame by using the following matching order:
     - MAC-based VLAN (fuzzy and exact MAC address match).
     - IP subnet-based VLAN.
     - Protocol-based VLAN.
     - Port-based VLAN.

     After tagging the frame with the selected VLAN, the port gets the source MAC address of the frame.
2. The port uses the source MAC address and VLAN of the frame to match the MAC-to VLAN entries.
   - If the source MAC address of the frame exactly matches the MAC address in a MAC-to-VLAN entry, the port checks whether the VLAN ID of the frame matches the VLAN in the entry.
     - If the two VLAN IDs match, the port joins the VLAN and forwards the frame.
     - If the two VLAN IDs do not match, the port drops the frame.
   - If the source MAC address of the frame does not exactly match any MAC addresses in MAC-to-VLAN entries, the port checks whether the VLAN ID of the frame is its PVID.
     - If the VLAN ID of the frame is the PVID of the port, the port determines whether it allows the PVID.

       If the PVID is allowed, the port forwards the frame within the PVID. If the PVID is not allowed, the port drops the frame.
     - If the VLAN ID of the frame is not the PVID of the port, the port determines whether the VLAN ID is the primary VLAN ID and the port PVID is a secondary VLAN ID. If yes, the port forwards the frame. Otherwise, the port drops the frame.

Figure 2 Flowchart for processing a frame in dynamic MAC-based VLAN assignment



Server-assigned MAC-based VLAN

Use this feature with access authentication, such as MAC-based 802.1X authentication, to implement secure and flexible terminal access.

To implement server-assigned MAC-based VLAN, perform the following tasks:

1. Configure the server-assigned MAC-based VLAN feature on the access device.
2. Configure username-to-VLAN entries on the access authentication server.

When a user passes authentication of the access authentication server, the server assigns the authorization VLAN information for the user to the device. The device then performs the following operations:

1. Generates a MAC-to-VLAN entry by using the source MAC address of the user packet and the authorization VLAN information. The authorization VLAN is a MAC-based VLAN.

   The generated MAC-to-VLAN entry cannot conflict with the existing static MAC-to-VLAN entries. If a confliction exists, the dynamic MAC-to-VLAN entry cannot be generated.
2. Assigns the port that connects the user to the MAC-based VLAN.

When the user goes offline, the device automatically deletes the MAC-to-VLAN entry and removes the port from the MAC-based VLAN. For more information about 802.1X and MAC authentication, see *Security Configuration Guide*.

IP subnet-based VLANs

The IP subnet-based VLAN feature assigns untagged packets to VLANs based on their source IP addresses and subnet masks.

Use this feature when untagged packets from an IP subnet or IP address must be transmitted in a VLAN.

Protocol-based VLANs

The protocol-based VLAN feature assigns inbound packets to different VLANs based on their protocol types and encapsulation formats. The protocols available for VLAN assignment include IP, IPX, and AT. The encapsulation formats include Ethernet II, 802.3 raw, 802.2 LLC, and 802.2 SNAP.

This feature associates the available network service types with VLANs and facilitates network management and maintenance.

Layer 3 communication between VLANs

Hosts of different VLANs use VLAN interfaces to communicate at Layer 3. VLAN interfaces are virtual interfaces that do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface and assign an IP address to it. The VLAN interface acts as the gateway of the VLAN to forward packets destined for another IP subnet at Layer 3.

Protocols and standards

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

Restrictions: Hardware compatibility with VLAN

The S6861 switch series and the S6820 switch series do not support S-channel interface view, S-channel aggregate interface view, or S-channel bundle interface view.

Configuring a VLAN

Restrictions and guidelines

- As the system default VLAN, VLAN 1 cannot be created or deleted.
- Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

VLAN configuration tasks at a glance

To configure VLANs, perform the following tasks:

1. Creating VLANs
2. (Optional.) Enabling packet dropping in the VLAN

Creating VLANs

1. Enter system view.
   `system-view`
2. Create one or multiple VLANs.
   - Create a VLAN and enter its view.
     `vlan` *`vlan-id`*
   - Create multiple VLANs and enter VLAN view.

Create VLANs.

vlan { *vlan-id-list* | **all** }

Enter VLAN view.

vlan *vlan-id*

By default, only the system default VLAN (VLAN 1) exists.

3. (Optional.) Set a name for the VLAN.

   name *text*

   By default, the name of a VLAN is **VLAN** *vlan-id.* The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the name of VLAN 100 is **VLAN 0100**.

4. (Optional.) Configure the description for the VLAN.

   description *text*

   By default, the description of a VLAN is **VLAN** *vlan-id.* The *vlan-id* argument specifies the VLAN ID in a four-digit format. If the VLAN ID has fewer than four digits, leading zeros are added. For example, the default description of VLAN 100 is **VLAN 0100**.

Enabling packet dropping in the VLAN

About packet dropping in the VLAN

This feature enables the device to drop packets (including protocol packets) forwarded by the software in a VLAN. To drop all packets that are received and transmitted in the VLAN, you must configure a QoS policy. For more information about configuring QoS policies, see QoS configuration in *ACL and QoS Configuration Guide*.

Procedure

1. Enter system view.

   system-view

2. Enter VLAN view.

   vlan *vlan-id*

3. Enable packet dropping in the VLAN.

   block outbound

   By default, packet dropping is disabled in a VLAN.

Configuring port-based VLANs

Restrictions and guidelines for port-based VLANs

- When you use the **undo vlan** command to delete the PVID of a port, either of the following events occurs depending on the port link type:
  - For an access port, the PVID of the port changes to VLAN 1.
  - For a hybrid or trunk port, the PVID setting of the port does not change.

  You can use a nonexistent VLAN as the PVID for a hybrid or trunk port, but not for an access port.
- As a best practice, set the same PVID for a local port and its peer.
- To prevent a port from dropping untagged packets or PVID-tagged packets, assign the port to its PVID.

Assigning an access port to a VLAN

About assigning an access port to a VLAN

You can assign an access port to a VLAN in VLAN view or interface view.

Assigning one or multiple access ports to a VLAN in VLAN view

1. Enter system view.
   system-view
2. Enter VLAN view.
   vlan *vlan-id*
3. Assign one or multiple access ports to the VLAN.
   port *interface-list*
   By default, all ports belong to VLAN 1.

Assigning an access port to a VLAN in interface view

1. Enter system view.
   system-view
2. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter Layer 2 aggregate interface view.
     interface bridge-aggregation *interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*
   - Enter S-channel aggregate interface view.
     interface schannel-aggregation *interface-number*:*channel-id*
   - Enter S-channel bundle interface view.
     interface schannel-bundle *interface-number*
3. Set the port link type to access.
   port link-type access
   By default, all ports are access ports.
4. Assign the access port to a VLAN.
   port access vlan *vlan-id*
   By default, all access ports belong to VLAN 1.

Assigning a trunk port to a VLAN

About assigning a trunk port to a VLAN

A trunk port supports multiple VLANs. You can assign it to a VLAN in interface view.

Restrictions and guidelines

To change the link type of a port from trunk to hybrid, set the link type to access first.

To enable a trunk port to transmit packets from its PVID, you must assign the trunk port to the PVID by using the **port trunk permit vlan** command.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter Layer 2 aggregate interface view.
     interface bridge-aggregation *interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*
   - Enter S-channel aggregate interface view.
     interface schannel-aggregation *interface-number*:*channel-id*
   - Enter S-channel bundle interface view.
     interface schannel-bundle *interface-number*
3. Set the port link type to trunk.
   port link-type trunk
   By default, all ports are access ports.
4. Assign the trunk port to the specified VLANs.
   port trunk permit vlan { *vlan-id-list* | **all** }
   By default, a trunk port permits only VLAN 1.
5. (Optional.) Set the PVID for the trunk port.
   port trunk pvid vlan *vlan-id*
   The default setting is VLAN 1.

Assigning a hybrid port to a VLAN

About assigning a hybrid port to a VLAN

A hybrid port supports multiple VLANs. You can assign it to the specified VLANs in interface view. Make sure the VLANs have been created.

Restrictions and guidelines

To change the link type of a port from trunk to hybrid, set the link type to access first.

To enable a hybrid port to transmit packets from its PVID, you must assign the hybrid port to the PVID by using the **port hybrid vlan** command.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter Layer 2 aggregate interface view.
     interface bridge-aggregation *interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*

- Enter S-channel aggregate interface view.
  interface schannel-aggregation *interface-number*:*channel-id*
- Enter S-channel bundle interface view.
  interface schannel-bundle *interface-number*

3. Set the port link type to hybrid.
   port link-type hybrid
   By default, all ports are access ports.
4. Assign the hybrid port to the specified VLANs.
   port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }
   By default, the hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
5. (Optional.) Set the PVID for the hybrid port.
   port hybrid pvid vlan *vlan-id*
   By default, the PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

Configuring MAC-based VLANs

Restrictions and guidelines for MAC-based VLANs

- MAC-based VLANs are available only on hybrid ports.
- Do not configure a VLAN as both a super VLAN and a MAC-based VLAN.
- The MAC-based VLAN feature is mainly configured on downlink ports of user access devices. Do not use this feature with link aggregation.

Configuring static MAC-based VLAN assignment

1. Enter system view.
   system-view
2. Create a MAC-to-VLAN entry.
   mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1p** *priority*]
   By default, no MAC-to-VLAN entries exist.
3. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*
   - Enter S-channel aggregate interface view.
     interface schannel-aggregation *interface-number*:*channel-id*
4. Set the port link type to hybrid.
   port link-type hybrid
   By default, all ports are access ports.
5. Assign the hybrid port to the MAC-based VLANs.
   port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.

6. Enable the MAC-based VLAN feature.

   mac-vlan enable

   By default, this feature is disabled.

7. (Optional.) Configure the system to assign VLANs based on the MAC address preferentially.

   vlan precedence mac-vlan

   By default, the system assigns VLANs based on the MAC address preferentially when both the MAC-based VLAN and IP subnet-based VLAN are configured on a port.

Configuring dynamic MAC-based VLAN assignment

About dynamic MAC-based VLAN assignment

For successful dynamic MAC-based VLAN assignment, use static VLANs when you create MAC-to-VLAN entries.

When a port joins a VLAN specified in the MAC-to-VLAN entry, one of the following events occurs depending on the port configuration:

- If the port has not been configured to allow packets from the VLAN to pass through, the port joins the VLAN as an untagged member.
- If the port has been configured to allow packets from the VLAN to pass through, the port configuration remains the same.

The 802.1p priority of the VLAN in a MAC-to-VLAN entry determines the transmission priority of the matching packets.

Restrictions and guidelines

- If you configure both static and dynamic MAC-based VLAN assignments on a port, dynamic MAC-based VLAN assignment takes effect.
- As a best practice to ensure correct operation of 802.1X and MAC authentication, do not use dynamic MAC-based VLAN assignment with 802.1X or MAC authentication.
- As a best practice, do not both configure dynamic MAC-based VLAN assignment and disable MAC address learning on a port. If the two features are configured together on a port, the port forwards only packets exactly matching the MAC-to-VLAN entries and drops inexactly matching packets.
- As a best practice, do not configure both dynamic MAC-based VLAN assignment and the MAC learning limit on a port.

  If the two features are configured together on a port and the port learns the configured maximum number of MAC address entries, the port processes packets as follows:

  - Forwards only packets matching the MAC address entries learnt by the port.
  - Drops unmatching packets.
- As a best practice, do not use dynamic MAC-based VLAN assignment with MSTP. In MSTP mode, if a port is blocked in the MSTI of its target VLAN, the port drops the received packets instead of delivering them to the CPU. As a result, the port will not be dynamically assigned to the target VLAN.
- As a best practice, do not use dynamic MAC-based VLAN assignment with PVST. In PVST mode, if the target VLAN of a port is not permitted on the port, the port is placed in blocked state. The port drops the received packets instead of delivering them to the CPU. As a result, the port will not be dynamically assigned to the target VLAN.
- As a best practice, do not configure both dynamic MAC-based VLAN assignment and automatic voice VLAN assignment mode on a port. They can have a negative impact on each other.

Procedure

1. Enter system view.
   system-view
2. Create a MAC-to-VLAN entry.
   mac-vlan mac-address *mac-address* **vlan** *vlan-id* [**dot1p** *priority*]
   By default, no MAC-to-VLAN entries exist.
3. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*
   - Enter S-channel aggregate interface view.
     interface schannel-aggregation *interface-number*:*channel-id*
4. Set the port link type to hybrid.
   port link-type hybrid
   By default, all ports are access ports.
5. Enable the MAC-based VLAN feature.
   mac-vlan enable
   By default, MAC-based VLAN is disabled.
6. Enable dynamic MAC-based VLAN assignment.
   mac-vlan trigger enable
   By default, dynamic MAC-based VLAN assignment is disabled.
   The VLAN assignment for a port is triggered only when the source MAC address of its receiving packet exactly matches the MAC address in a MAC-to-VLAN entry.
7. (Optional.) Configure the system to assign VLANs based on the MAC address preferentially.
   vlan precedence mac-vlan
   By default, the system assigns VLANs based on the MAC address preferentially when both the MAC-based VLAN and IP subnet-based VLAN are configured on a port.
8. (Optional.) Disable the port from forwarding packets that fail the exact MAC address match in its PVID.
   port pvid forbidden
   By default, when a port receives packets whose source MAC addresses fail the exact match, the port forwards them in its PVID.

Configuring server-assigned MAC-based VLAN

1. Enter system view.
   system-view
2. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*
   - Enter S-channel aggregate interface view.
     interface schannel-aggregation *interface-number*:*channel-id*

3. Set the port link type to hybrid.
   port link-type hybrid
   By default, all ports are access ports.
4. Assign the hybrid port to the MAC-based VLANs.
   port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }
   By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
5. Enable the MAC-based VLAN feature.
   mac-vlan enable
   By default, MAC-based VLAN is disabled.
6. Configure 802.1X or MAC authentication.
   For more information, see *Security Command Reference*.

Configuring IP subnet-based VLANs

Restrictions and guidelines

This feature is available only on hybrid ports, and it processes only untagged packets.

Procedure

1. Enter system view.
   system-view
2. Enter VLAN view.
   vlan *vlan-id*
3. Associate the VLAN with an IP subnet or IP address.
   ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]
   By default, a VLAN is not associated with an IP subnet or IP address.
   A multicast subnet or a multicast address cannot be associated with a VLAN.
4. Return to system view.
   quit
5. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter Layer 2 aggregate interface view.
     interface bridge-aggregation *interface-number*
6. Set the port link type to hybrid.
   port link-type hybrid
   By default, all ports are access ports.
7. Assign the hybrid port to the specified IP subnet-based VLANs.
   port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }
   By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.
8. Associate the hybrid port with the specified IP subnet-based VLAN.
   port hybrid ip-subnet-vlan vlan *vlan-id*
   By default, a hybrid port is not associated with a subnet-based VLAN.

Configuring protocol-based VLANs

About protocol-based VLANs

A protocol-based VLAN has one or multiple protocol templates. A protocol template defines a protocol type and an encapsulation format as the match criteria to match inbound packets. Each protocol template has a unique index in the protocol-based VLAN. All protocol templates in a protocol-based VLAN have the same VLAN ID.

For a port to assign inbound packets to protocol-based VLANs, perform the following tasks:

- Assign the port to the protocol-based VLANs.
- Associate the port with the protocol templates of the protocol-based VLANs.

When an untagged packet arrives at the port, the port processes the packet as follows:

- If the protocol type and encapsulation format in the packet match a protocol template, the port tags the packet with the VLAN tag specific to the protocol template.
- If no protocol templates are matched, the port tags the packet with its PVID.

Restrictions and guidelines

The voice VLAN in automatic mode processes only tagged voice traffic. Do not configure a VLAN as both a protocol-based VLAN and a voice VLAN.

Procedure

1. Enter system view.

   system-view

2. Enter VLAN view.

   vlan *vlan-id*

3. Associate the VLAN with a protocol template.

   protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }

   By default, a VLAN is not associated with a protocol template.

4. Exit VLAN view.

   quit

5. Enter interface view.
   - Enter Layer 2 Ethernet interface view.

     interface *interface-type interface-number*
   - Enter Layer 2 aggregate interface view.

     interface bridge-aggregation *interface-number*

6. Set the port link type to hybrid.

   port link-type hybrid

   By default, all ports are access ports.

7. Assign the hybrid port to the specified protocol-based VLANs.

   port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

   By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**.

8. Associate the hybrid port with the specified protocol-based VLAN.

   port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

By default, a hybrid port is not associated with a protocol-based VLAN.

Configuring a VLAN group

About a VLAN group

A VLAN group includes a set of VLANs.

On an authentication server, a VLAN group name represents a group of authorization VLANs. When an 802.1X or MAC authentication user passes authentication, the authentication server assigns a VLAN group name to the device. The device then uses the received VLAN group name to match the locally configured VLAN group names. If a match is found, the device selects a VLAN from the group and assigns the VLAN to the user. For more information about 802.1X and MAC authentication, see *Security Configuration Guide*.

Procedure

1. Enter system view.
   `system-view`
2. Create a VLAN group and enter its view.
   `vlan-group` *`group-name`*
3. Add VLANs to the VLAN group.
   `vlan-list` *`vlan-id-list`*
   By default, no VLANs exist in a VLAN group.
   You can add multiple VLAN lists to a VLAN group.

Configuring VLAN interfaces

Restrictions and guidelines

- You cannot create VLAN interfaces for sub-VLANs. For more information about sub-VLANs, see "Configuring super VLANs."
- You cannot create VLAN interfaces for secondary VLANs that have the following characteristics:
  - Associated with the same primary VLAN.
  - Enabled with Layer 3 communication in VLAN interface view of the primary VLAN interface.

  For more information about secondary VLANs, see "Configuring private VLAN."

VLAN interfaces configuration tasks at a glance

To configure VLAN interfaces, perform the following tasks:

1. Creating a VLAN interface
2. (Optional.) Specifying a traffic processing slot for the VLAN interface
3. (Optional.) Restoring the default settings for the VLAN interface

Prerequisites

Before you create a VLAN interface for a VLAN, create the VLAN first.

Creating a VLAN interface

1. Enter system view.
   system-view
2. Create a VLAN interface and enter its view.
   interface vlan-interface *interface-number*
3. Assign an IP address to the VLAN interface.
   ip address *ip-address* { *mask* | *mask-length* } [**sub**]
   By default, no IP address is assigned to a VLAN interface.
4. (Optional.) Configure the description for the VLAN interface.
   description *text*
   The default setting is the VLAN interface name. For example, **Vlan-interface1 Interface**.
5. (Optional.) Set the MTU for the VLAN interface.
   mtu *size*
   By default, the MTU of a VLAN interface is 1500 bytes.
6. (Optional.) Set a MAC address for the VLAN interface.
   mac-address *mac-address*
   By default, no MAC addresses are set for a VLAN interface.
7. (Optional.) Set the expected bandwidth for the interface.
   bandwidth *bandwidth-value*
   By default, the expected bandwidth (in kbps) is the interface baud rate divided by 1000.
8. Bring up the VLAN interface.
   undo shutdown
   By default, a VLAN interface is not manually shut down. The status of the VLAN interface depends on the status of member ports of the VLAN.

Specifying a traffic processing slot for the VLAN interface

About traffic processing slot

Specify a traffic processing slot for a VLAN interface if all traffic on the VLAN interface must be processed on the same slot.

Procedure

1. Enter system view.
   system-view
2. Enter a VLAN interface view.
   interface vlan-interface *interface-number*
3. Specify a traffic processing slot for the VLAN interface.
   service slot *slot-number*
   By default, no traffic processing slot is specified for the VLAN interface.

Restoring the default settings for the VLAN interface

Restrictions and guidelines

CAUTION:

This feature might interrupt ongoing network services. Make sure you are fully aware of the impact of this feature when you use it on a live network.

This feature might fail to restore the default settings for some commands for reasons such as command dependencies or system restrictions. Use the **display this** command in interface view to identify these commands, and then use their **undo** forms or follow the command reference to restore their default settings. If your restoration attempt still fails, follow the error message instructions to resolve the problem.

Procedure

1. Enter system view.
   system-view
2. Enter a VLAN interface view.
   interface vlan-interface *interface-number*
3. Restore the default settings for the VLAN interface.
   default

Display and maintenance commands for VLANs

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display VLAN interface information.	**display interface** [**vlan-interface** [*interface-number*]] [**brief** [**description** | **down**]]
Display information about IP subnet-based VLANs that are associated with the specified ports.	**display ip-subnet-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
Display information about IP subnet-based VLANs.	**display ip-subnet-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
Display hybrid ports or trunk ports on the device.	**display port** { **hybrid** | **trunk** }
Display information about protocol-based VLANs that are associated with the specified ports.	**display protocol-vlan interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }
Display information about protocol-based VLANs.	**display protocol-vlan vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }
Display VLAN information.	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]
Display brief VLAN information.	**display vlan brief**
Display VLAN group information.	**display vlan-group** [*group-name*]

Task	Command
Clear statistics on a VLAN interface.	**reset counters interface** [**vlan-interface** [*interface-number*]]
Display MAC-to-VLAN entries.	**display mac-vlan** { **all** | **dynamic** | **mac-address** *mac-address* [**mask** *mac-mask*] | **static** | **vlan** *vlan-id* }
Display all ports that are enabled with the MAC-based VLAN feature.	**display mac-vlan interface**

VLAN configuration examples

Example: Configuring port-based VLANs

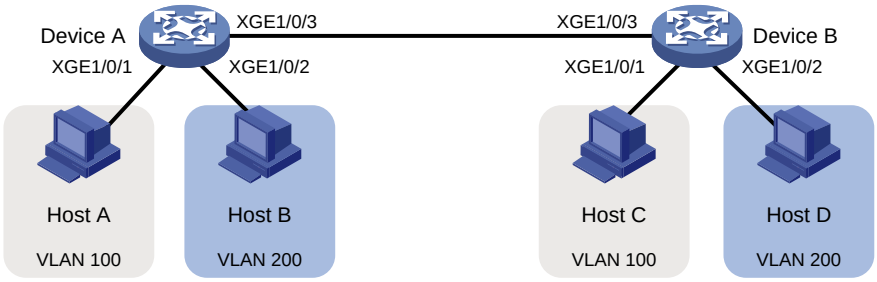
Network configuration

As shown in Figure 3:

- Host A and Host C belong to Department A. VLAN 100 is assigned to Department A.
- Host B and Host D belong to Department B. VLAN 200 is assigned to Department B.

Configure port-based VLANs so that only hosts in the same department can communicate with each other.

Figure 3 Network diagram



Procedure

1. Configure Device A:

   # Create VLAN 100, and assign Ten-GigabitEthernet 1/0/1 to VLAN 100.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] port ten-gigabitethernet 1/0/1
   [DeviceA-vlan100] quit
   ```

   # Create VLAN 200, and assign Ten-GigabitEthernet 1/0/2 to VLAN 200.

   ```
   [DeviceA] vlan 200
   [DeviceA-vlan200] port ten-gigabitethernet 1/0/2
   [DeviceA-vlan200] quit
   ```

   # Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and assign the port to VLANs 100 and 200.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/3
   [DeviceA-Ten-GigabitEthernet1/0/3] port link-type trunk
   [DeviceA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 100 200
   ```

```
Please wait... Done.
```

2. Configure Device B in the same way Device A is configured. (Details not shown.)
3. Configure hosts:
   a. Configure Host A and Host C to be on the same IP subnet. For example, 192.168.100.0/24.
   b. Configure Host B and Host D to be on the same IP subnet. For example, 192.168.200.0/24.

Verifying the configuration

Verify that Host A and Host C can ping each other, but they both fail to ping Host B and Host D. (Details not shown.)

Verify that Host B and Host D can ping each other, but they both fail to ping Host A and Host C. (Details not shown.)

Verify that VLANs 100 and 200 are correctly configured on Device A.

```
[DeviceA-Ten-GigabitEthernet1/0/3] display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    Ten-GigabitEthernet1/0/3
 Untagged ports:
    Ten-GigabitEthernet1/0/1
[DeviceA-Ten-GigabitEthernet1/0/3] display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    Ten-GigabitEthernet1/0/3
 Untagged ports:
    Ten-GigabitEthernet1/0/2
```

Example: Configuring MAC-based VLANs

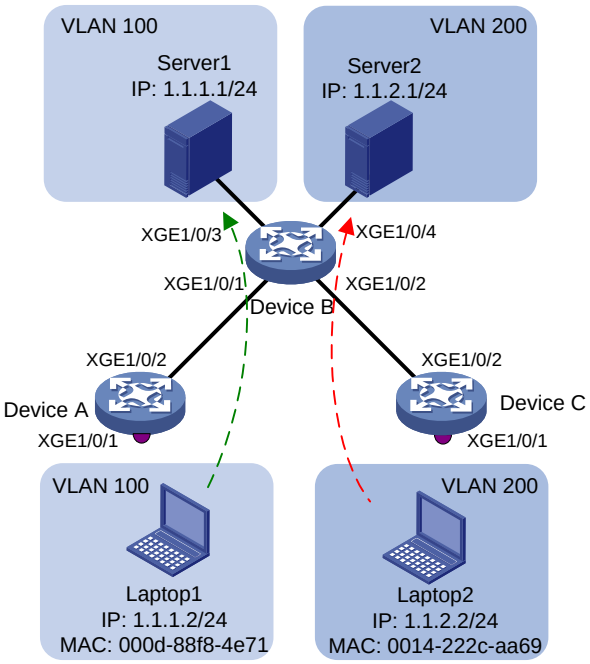
Network configuration

As shown in Figure 4:

- Ten-GigabitEthernet 1/0/1 of Device A and Device C are each connected to a meeting room. Laptop 1 and Laptop 2 are used for meetings and might be used in either of the two meeting rooms.
- One department uses VLAN 100 and owns Laptop 1. The other department uses VLAN 200 and owns Laptop 2.

Configure MAC-based VLANs, so that Laptop 1 and Laptop 2 can access Server 1 and Server 2, respectively, no matter which meeting room they are used in.

Figure 4 Network diagram



Procedure

1. Configure Device A:

   # Create VLANs 100 and 200.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 100
   [DeviceA-vlan100] quit
   [DeviceA] vlan 200
   [DeviceA-vlan200] quit
   ```

   # Associate the MAC addresses of Laptop 1 and Laptop 2 with VLANs 100 and 200, respectively.

   ```
   [DeviceA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
   [DeviceA] mac-vlan mac-address 0014-222c-aa69 vlan 200
   ```

   # Configure Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
   [DeviceA-Ten-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
   ```

   # Enable the MAC-based VLAN feature on Ten-GigabitEthernet 1/0/1.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/1] mac-vlan enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Configure the uplink port (Ten-GigabitEthernet 1/0/2) as a trunk port, and assign it to VLANs 100 and 200.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-type trunk
   [DeviceA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 200
   [DeviceA-Ten-GigabitEthernet1/0/2] quit
   ```

2. Configure Device B:

   # Create VLAN 100, and assign Ten-GigabitEthernet 1/0/3 to VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port ten-gigabitethernet 1/0/3
[DeviceB-vlan100] quit
```

Create VLAN 200 and assign Ten-GigabitEthernet 1/0/4 to VLAN 200.

```
[DeviceB] vlan 200
[DeviceB-vlan200] port ten-gigabitethernet 1/0/4
[DeviceB-vlan200] quit
```

Configure Ten-GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLANs 100 and 200.

```
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[DeviceB-Ten-GigabitEthernet1/0/1] quit
```

Configure Ten-GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLANs 100 and 200.

```
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

3. Configure Device C in the same way as the Device A is configured. (Details not shown.)

Verifying the configuration

Verify that Laptop 1 can access only Server 1, and Laptop 2 can access only Server 2. (Details not shown.)

Verify the MAC-to-VLAN entries on Device A and Device C, for example, on Device A.

```
[DeviceA] display mac-vlan all
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC address      Mask             VLAN ID  Priority    State
  000d-88f8-4e71   ffff-ffff-ffff   100       0          S
  0014-222c-aa69   ffff-ffff-ffff   200       0          S

  Total MAC VLAN address count: 2
```

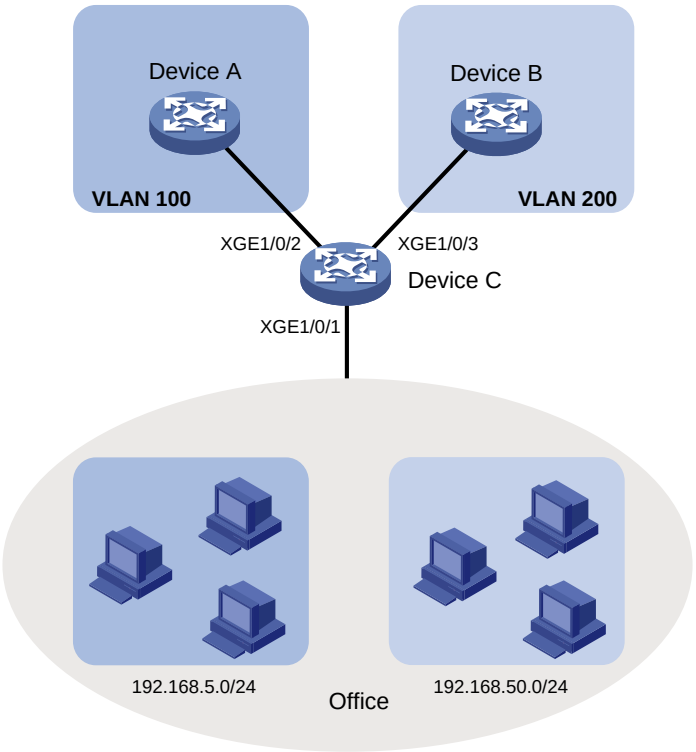
Example: Configuring IP subnet-based VLANs

Network configuration

As shown in Figure 5, the hosts in the office belong to different IP subnets.

Configure Device C to transmit packets from 192.168.5.0/24 and 192.168.50.0/24 in VLANs 100 and 200, respectively.

Figure 5 Network diagram



Procedure

1. Configure Device C:

Associate IP subnet 192.168.5.0/24 with VLAN 100.

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0
[DeviceC-vlan100] quit
```

Associate IP subnet 192.168.50.0/24 with VLAN 200.

```
[DeviceC] vlan 200
[DeviceC-vlan200] ip-subnet-vlan ip 192.168.50.0 255.255.255.0
[DeviceC-vlan200] quit
```

Configure Ten-GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLAN 100 as a tagged VLAN member.

```
[DeviceC] interface ten-gigabitethernet 1/0/2
[DeviceC-Ten-GigabitEthernet1/0/2] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/2] port hybrid vlan 100 tagged
[DeviceC-Ten-GigabitEthernet1/0/2] quit
```

Configure Ten-GigabitEthernet 1/0/3 as a hybrid port, and assign it to VLAN 200 as a tagged VLAN member.

```
[DeviceC] interface ten-gigabitethernet 1/0/3
[DeviceC-Ten-GigabitEthernet1/0/3] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/3] port hybrid vlan 200 tagged
[DeviceC-Ten-GigabitEthernet1/0/3] quit
```

Configure Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.

```
[DeviceC] interface ten-gigabitethernet 1/0/1
[DeviceC-Ten-GigabitEthernet1/0/1] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Associate Ten-GigabitEthernet 1/0/1 with the IP subnet-based VLANs 100 and 200.

```
[DeviceC-Ten-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
[DeviceC-Ten-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
[DeviceC-Ten-GigabitEthernet1/0/1] quit
```

2. Configure Device A and Device B to forward packets from VLANs 100 and 200, respectively. (Details not shown.)

Verifying the configuration

Verify the IP subnet-based VLAN configuration on Device C.

```
[DeviceC] display ip-subnet-vlan vlan all
 VLAN ID: 100
  Subnet index      IP address      Subnet mask
  0                 192.168.5.0     255.255.255.0

 VLAN ID: 200
  Subnet index      IP address      Subnet mask
  0                 192.168.50.0    255.255.255.0
```

Verify the IP subnet-based VLAN configuration on Ten-GigabitEthernet 1/0/1 of Device C.

```
[DeviceC] display ip-subnet-vlan interface ten-gigabitethernet 1/0/1
 Interface: Ten-GigabitEthernet1/0/1
  VLAN ID   Subnet index    IP address       Subnet mask       Status
  100       0               192.168.5.0      255.255.255.0     Active
  200       0               192.168.50.0     255.255.255.0     Active
```

Example: Configuring protocol-based VLANs

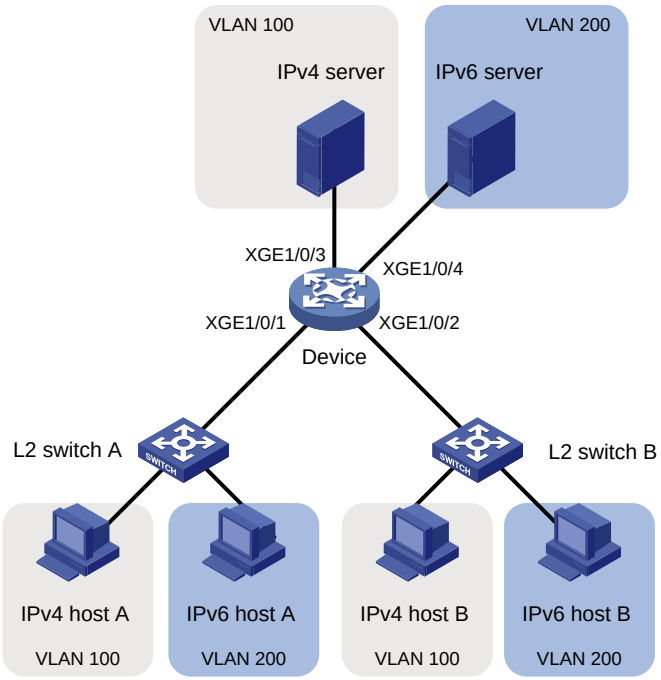
Network configuration

As shown in Figure 6:

- The majority of hosts in a lab environment run the IPv4 protocol.
- The other hosts run the IPv6 protocol for teaching purposes.

To isolate IPv4 and IPv6 traffic at Layer 2, configure protocol-based VLANs to associate the IPv4 and ARP protocols with VLAN 100, and associate the IPv6 protocol with VLAN 200.

Figure 6 Network diagram



Procedure

In this example, L2 Switch A and L2 Switch B use the factory configuration.

1. Configure Device:

Create VLAN 100, and configure the description for VLAN 100 as **protocol VLAN for IPv4**.

```
<Device> system-view
[Device] vlan 100
[Device-vlan100] description protocol VLAN for IPv4
```

Assign Ten-GigabitEthernet 1/0/3 to VLAN 100.

```
[Device-vlan100] port ten-gigabitethernet 1/0/3
[Device-vlan100] quit
```

Create VLAN 200, and configure the description for VLAN 200 as **protocol VLAN for IPv6**.

```
[Device] vlan 200
[Device-vlan200] description protocol VLAN for IPv6
```

Assign Ten-GigabitEthernet 1/0/4 to VLAN 200.

```
[Device-vlan200] port ten-gigabitethernet 1/0/4
```

Configure VLAN 200 as a protocol-based VLAN, and create an IPv6 protocol template with the index 1 for VLAN 200.

```
[Device-vlan200] protocol-vlan 1 ipv6
[Device-vlan200] quit
```

Configure VLAN 100 as a protocol-based VLAN. Create an IPv4 protocol template with the index 1, and create an ARP protocol template with the index 2. (In Ethernet II encapsulation, the protocol type ID for ARP is 0806 in hexadecimal notation.)

```
[Device] vlan 100
[Device-vlan100] protocol-vlan 1 ipv4
[Device-vlan100] protocol-vlan 2 mode ethernetii etype 0806
[Device-vlan100] quit
```

Configure Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port link-type hybrid
[Device-Ten-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Associate Ten-GigabitEthernet 1/0/1 with the IPv4 and ARP protocol templates of VLAN 100 and the IPv6 protocol template of VLAN 200.

```
[Device-Ten-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 1 to 2
[Device-Ten-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 1
[Device-Ten-GigabitEthernet1/0/1] quit
```

Configure Ten-GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLANs 100 and 200 as an untagged VLAN member.

```
[Device] interface ten-gigabitethernet 1/0/2
[Device-Ten-GigabitEthernet1/0/2] port link-type hybrid
[Device-Ten-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged
```

Associate Ten-GigabitEthernet 1/0/2 with the IPv4 and ARP protocol templates of VLAN 100 and the IPv6 protocol template of VLAN 200.

```
[Device-Ten-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 1 to 2
[Device-Ten-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 1
[Device-Ten-GigabitEthernet1/0/2] quit
```

2. Configure hosts and servers:
   a. Configure IPv4 Host A, IPv4 Host B, and IPv4 server to be on the same network segment (192.168.100.0/24, for example). (Details not shown.)
   b. Configure IPv6 Host A, IPv6 Host B, and IPv6 server to be on the same network segment (2001::1/64, for example). (Details not shown.)

Verifying the configuration

1. Verify the following:
   - The hosts and the server in VLAN 100 can successfully ping one another. (Details not shown.)
   - The hosts and the server in VLAN 200 can successfully ping one another. (Details not shown.)
   - The hosts or the server in VLAN 100 cannot ping the hosts or server in VLAN 200. (Details not shown.)
2. Verify the protocol-based VLAN configuration:

Display protocol-based VLANs on Device.

```
[Device] display protocol-vlan vlan all
 VLAN ID: 100
  Protocol index  Protocol type
  1               IPv4
  2               Ethernet II Etype 0x0806

 VLAN ID: 200
  Protocol index  Protocol type
  1               IPv6
```

Display protocol-based VLANs on the ports of Device.

```
[Device] display protocol-vlan interface all
 Interface: Ten-GigabitEthernet1/0/1
  VLAN ID  Protocol index  Protocol type            Status
```

```
 100      1               IPv4                       Active
 100      2               Ethernet II Etype 0x0806   Active
 200      1               IPv6                       Active

Interface: Ten-GigabitEthernet 1/0/2
 VLAN ID  Protocol index  Protocol type              Status
 100      1               IPv4                       Active
 100      2               Ethernet II Etype 0x0806   Active
 200      1               IPv6                       Active
```

Configuring super VLANs

About super VLANs

Hosts in a VLAN typically use IP addresses in the same subnet. For Layer 3 interoperability with other VLANs, you can create a VLAN interface for the VLAN and assign an IP address to it. This requires a large number of IP addresses.

The super VLAN feature was introduced to save IP addresses. A super VLAN is associated with multiple sub-VLANs. These sub-VLANs use the VLAN interface of the super VLAN (also known as a super VLAN interface) as the gateway for Layer 3 communication.

You can create a VLAN interface for a super VLAN and assign an IP address to it. However, you cannot create a VLAN interface for a sub-VLAN. You can assign a physical port to a sub-VLAN, but you cannot assign a physical port to a super VLAN. Sub-VLANs are isolated at Layer 2.

To enable Layer 3 communication between sub-VLANs, perform the following tasks:

1. Create a super VLAN and the VLAN interface for the super VLAN.
2. Enable local proxy ARP or ND on the super VLAN interface as follows:
   - In an IPv4 network, enable local proxy ARP on the super VLAN interface. The super VLAN can then process ARP requests and replies sent from the sub-VLANs.
   - In an IPv6 network, enable local proxy ND on the super VLAN interface. The super VLAN can then process the NS and NA messages sent from the sub-VLANs.

Restrictions and guidelines: Super VLAN configuration

- The VLAN of a MAC address-to-VLAN entry cannot be configured as a super VLAN.
- A VLAN cannot be configured as both a super VLAN and a guest VLAN, Auth-Fail VLAN, or critical VLAN. For more information about guest VLANs, Auth-Fail VLANs, and critical VLANs, see *Security Configuration Guide*.
- A VLAN cannot be configured as both a super VLAN and a sub-VLAN.
- Layer 2 multicast configuration for super VLANs does not take effect because they do not have physical ports.

Super VLAN tasks at a glance

To configure a super VLAN, perform the following tasks:

1. Creating a sub-VLAN
2. Configuring a super VLAN
3. Configuring a super VLAN interface

Creating a sub-VLAN

1. Enter system view.

   `system-view`
2. Create a sub-VLAN.

vlan *vlan-id-list*

By default, only the system default VLAN (VLAN 1) exists.

Configuring a super VLAN

1. Enter system view.
   system-view
2. Enter VLAN view.
   vlan *vlan-id*
3. Configure the VLAN as a super VLAN.
   supervlan
   By default, a VLAN is not a super VLAN.
4. Associate the super VLAN with the sub-VLANs.
   subvlan *vlan-id-list*
   Make sure the sub-VLANs already exist before associating them with a super VLAN.

Configuring a super VLAN interface

Restrictions and guidelines

As a best practice, do not configure VRRP for a super VLAN interface because the configuration affects network performance. For more information about VRRP, see *High Availability Configuration Guide*.

Procedure

1. Enter system view.
   system-view
2. Create a VLAN interface and enter its view.
   interface vlan-interface *interface-number*
   The value for the *interface-number* argument must be the super VLAN ID.
3. Configure an IP address for the super VLAN interface.
   IPv4:
   ip address *ip-address* { *mask-length* | *mask* } [**sub**]
   IPv6:
   ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }
   By default, no IP address is configured for a VLAN interface.
4. Configure Layer 3 communication between sub-VLANs by enabling local proxy ARP or ND.
   IPv4:
   local-proxy-arp enable
   By default:
   - Sub-VLANs cannot communicate with each other at Layer 3.
   - Local proxy ARP is disabled.

   For more information about local proxy ARP, see *Layer 3—IP Services Configuration Guide*.
   IPv6:
   local-proxy-nd enable
   By default:

- Sub-VLANs cannot communicate with each other at Layer 3.
- Local proxy ND is disabled.

For more information about local proxy ND, see *Layer 3—IP Services Configuration Guide*.

Display and maintenance commands for super VLANs

Execute **display** commands in any view.

Task	Command
Display information about super VLANs and their associated sub-VLANs.	**display supervlan** [*supervlan-id*]

Super VLAN configuration examples

Example: Configuring a super VLAN

Network configuration

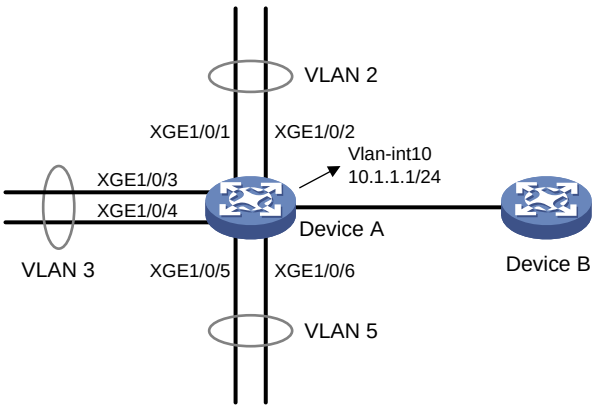
As shown in Figure 7:

- Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 are in VLAN 2.
- Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 are in VLAN 3.
- Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 1/0/6 are in VLAN 5.

To save IP addresses and enable sub-VLANs to be isolated at Layer 2 but interoperable at Layer 3, perform the following tasks:

- Create a super VLAN and assign an IP address to its VLAN interface.
- Associate the super VLAN with VLANs 2, 3, and 5.

Figure 7 Network diagram



Procedure

Create VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
```

```
[DeviceA-vlan10] quit
```

Create VLAN-interface 10, and assign IP address 10.1.1.1/24 to it.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
```

Enable local proxy ARP.

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

Create VLAN 2, and assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to the VLAN.

```
[DeviceA] vlan 2
[DeviceA-vlan2] port ten-gigabitethernet 1/0/1 ten-gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Create VLAN 3, and assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to the VLAN.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port ten-gigabitethernet 1/0/3 ten-gigabitethernet 1/0/4
[DeviceA-vlan3] quit
```

Create VLAN 5, and assign Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 1/0/6 to the VLAN.

```
[DeviceA] vlan 5
[DeviceA-vlan5] port ten-gigabitethernet 1/0/5 ten-gigabitethernet 1/0/6
[DeviceA-vlan5] quit
```

Configure VLAN 10 as a super VLAN, and associate sub-VLANs 2, 3, and 5 with the super VLAN.

```
[DeviceA] vlan 10
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] subvlan 2 3 5
[DeviceA-vlan10] quit
[DeviceA] quit
```

Verifying the configuration

Display information about super VLAN 10 and its associated sub-VLANs.

```
<DeviceA> display supervlan
 Super VLAN ID: 10
 Sub-VLAN ID: 2-3 5
 VLAN ID: 10
 VLAN type: Static
 It is a super VLAN.
 Route interface: Configured
 Ipv4 address: 10.1.1.1
 Ipv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports: None
 VLAN ID: 2
 VLAN type: Static
 It is a sub VLAN.
 Route interface: Configured
 Ipv4 address: 10.1.1.1
 Ipv4 subnet mask: 255.255.255.0
```

```
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:   None
Untagged ports:
   Ten-GigabitEthernet1/0/1
   Ten-GigabitEthernet1/0/2
VLAN ID: 3
VLAN type: Static
It is a sub VLAN.
Route interface: Configured
Ipv4 address: 10.1.1.1
Ipv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
   Ten-GigabitEthernet1/0/3
   Ten-GigabitEthernet1/0/4
VLAN ID: 5
VLAN type: Static
It is a sub VLAN.
Route interface: Configured
Ipv4 address: 10.1.1.1
Ipv4 subnet mask: 255.255.255.0
Description: VLAN 0005
Name: VLAN 0005
Tagged ports:   None
Untagged ports:
   Ten-GigabitEthernet1/0/5
   Ten-GigabitEthernet1/0/6
```

Configuring private VLAN

About private VLAN

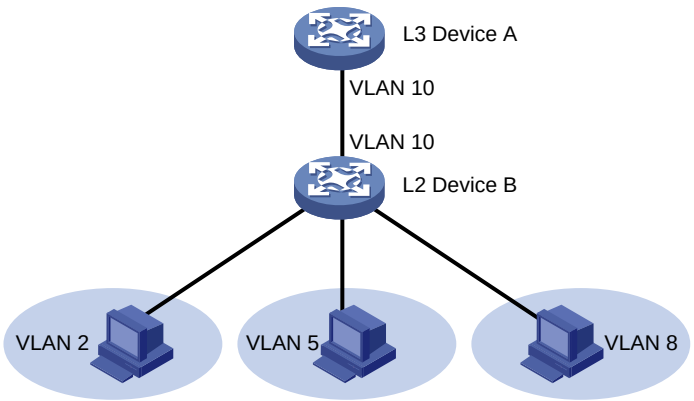
VLAN technology provides a method for isolating traffic from customers. At the access layer of a network, customer traffic must be isolated for security or accounting purposes. If VLANs are assigned on a per-user basis, a large number of VLANs will be required.

The private VLAN feature saves VLAN resources. It uses a two-tier VLAN structure as follows:

- **Primary VLAN**—Used for connecting the upstream device. A primary VLAN can be associated with multiple secondary VLANs. The upstream device identifies only the primary VLAN.
- **Secondary VLANs**—Used for connecting users. Secondary VLANs are isolated at Layer 2. To implement Layer 3 communication between secondary VLANs associated with the primary VLAN, enable local proxy ARP or ND on the upstream device (for example, L3 Device A in Figure 8).

As shown in Figure 8, the private VLAN feature is enabled on L2 Device B. VLAN 10 is the primary VLAN. VLANs 2, 5, and 8 are secondary VLANs that are associated with VLAN 10. L3 Device A is only aware of VLAN 10.

Figure 8 Private VLAN example



If the private VLAN feature is configured on a Layer 3 device, use one of the following methods on the Layer 3 device to enable Layer 3 communication. Layer 3 communication might be required between secondary VLANs that are associated with the same primary VLAN, or between secondary VLANs and other networks.

- Method 1:
  - **a.** Create VLAN interfaces for the secondary VLANs.
  - **b.** Assign IP addresses to the secondary VLAN interfaces.
- Method 2:
  - **a.** Enable Layer 3 communication between the secondary VLANs that are associated with the primary VLAN.
  - **b.** Create the VLAN interface for the primary VLAN and assign an IP address to it. (Do not create secondary VLAN interfaces if you use this method.)
  - **c.** Enable local proxy ARP or ND on the primary VLAN interface.

Restrictions and guidelines: Private VLAN configuration

- Make sure the following requirements are met:
  - For a promiscuous port:
    - The primary VLAN is the PVID of the port.
    - The port is an untagged member of the primary VLAN and secondary VLANs.
  - For a host port:
    - The PVID of the port is a secondary VLAN.
    - The port is an untagged member of the primary VLAN and the secondary VLAN.
  - A trunk promiscuous or trunk secondary port must be a tagged member of the primary VLANs and the secondary VLANs.
- VLAN 1 (system default VLAN) does not support the private VLAN configuration.

Private VLAN tasks at a glance

To configure a private VLAN, perform the following tasks:

1. Creating a primary VLAN
2. Creating secondary VLANs
3. Associating the primary VLAN with secondary VLANs
4. Configuring the uplink port
5. Configuring a downlink port
6. (Optional.) Configuring Layer 3 communication for secondary VLANs

Creating a primary VLAN

1. Enter system view.
   system-view
2. Create a VLAN and enter VLAN view.
   vlan *vlan-id*
3. Configure the VLAN as a primary VLAN.
   private-vlan primary
   By default, a VLAN is not a primary VLAN.

Creating secondary VLANs

1. Enter system view.
   system-view
2. Create one or multiple secondary VLANs.
   vlan { *vlan-id-list* | **all** }

Associating the primary VLAN with secondary VLANs

1. Enter system view.
   system-view
2. Create enter VLAN view of the primary VLAN.
   vlan *vlan-id*
3. Associate the primary VLAN with the secondary VLANs.
   private-vlan secondary *vlan-id-list*
   By default, a primary VLAN is not associated with any secondary VLANs.

Configuring the uplink port

About the uplink port

Configure the uplink port (for example, the port connecting L2 Device B to L3 Device A in Figure 8) as follows:

- If the port allows only one primary VLAN, configure the port as a promiscuous port of the primary VLAN. The promiscuous port can be automatically assigned to the primary VLAN and its associated secondary VLANs.
- If the port allows multiple primary VLANs, configure the port as a trunk promiscuous port of the primary VLANs. The trunk promiscuous port can be automatically assigned to the primary VLANs and their associated secondary VLANs.

Procedure

1. Enter system view.
   system-view
2. Enter interface view of the uplink port.
   interface *interface-type interface-number*
3. Configure the uplink port as a promiscuous or trunk promiscuous port of the specified VLANs.
   - Configure the uplink port as a promiscuous port of the specified VLAN.
     port private-vlan *vlan-id* **promiscuous**
   - Configure the uplink port as a trunk promiscuous port of the specified VLANs.
     port private-vlan *vlan-id-list* **trunk promiscuous**

   By default, a port is not a promiscuous or trunk promiscuous port of any VLANs.

Configuring a downlink port

About the downlink port

Configure a downlink port as follows:

- If a downlink port allows only one secondary VLAN (for example, the port connecting L2 Device B to a host in Figure 8), configure the port as a host port. The host port can be automatically assigned to the secondary VLAN and its associated primary VLAN.
- If a downlink port allows multiple secondary VLANs, configure the port as a trunk secondary port. The trunk secondary port can be automatically assigned to the secondary VLANs and their associated primary VLANs.

Procedure

1. Enter system view.
   system-view
2. Enter interface view of the downlink port.
   interface *interface-type interface-number*
3. Assign the downlink port to secondary VLANs.
   a. Set the link type of the port.
      port link-type { **access** | **hybrid | trunk** }
   b. Assign the access port to the specified VLAN.
      port access vlan *vlan-id*
   c. Assign the trunk port to the specified VLANs.
      port trunk permit vlan { *vlan-id-list* | **all** }
   d. Assign the hybrid port to the specified VLANs.
      port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

   Select substep b, c, or d depending on the port link type.
4. Configure the downlink port as a host or trunk secondary port.
   - Configure the downlink port as a host port.
     port private-vlan host
   - Configure the downlink port as a trunk secondary port of the specified VLANs.
     port private-vlan *vlan-id-list* **trunk secondary**

   By default, a port is not a host or trunk secondary port.
5. Return to system view.
   quit
6. Enter VLAN view of a secondary VLAN.
   vlan *vlan-id*
7. (Optional.) Enable Layer 2 communication for ports in the same secondary VLAN. Choose one command as needed:
   undo private-vlan isolated
   private-vlan community
   By default, ports in the same secondary VLAN can communicate with each other at Layer 2.

Configuring Layer 3 communication for secondary VLANs

1. Enter system view.
   system-view
2. Enter VLAN interface view of the primary VLAN interface.
   interface vlan-interface *interface-number*
3. Enable Layer 3 communication between secondary VLANs that are associated with the primary VLAN.
   private-vlan secondary *vlan-id-list*
   By default, secondary VLANs cannot communicate with each other at Layer 3.
4. Assign an IP address to the primary VLAN interface.

IPv4:

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

IPv6:

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

By default, no IP address is configured for a VLAN interface.

5. Enable local proxy ARP or ND.

   IPv4:

   local-proxy-arp enable

   By default, local proxy ARP is disabled.

   For more information about local proxy ARP, see *Layer 3—IP Services Configuration Guide*.

   IPv6:

   local-proxy-nd enable

   By default, local proxy ND is disabled.

   For more information about local proxy ND, see *Layer 3—IP Services Configuration Guide*.

Display and maintenance commands for the private VLAN

Execute **display** commands in any view.

Task	Command
Display information about primary VLANs and the secondary VLANs associated with each primary VLAN.	**display private-vlan** [*primary-vlan-id*]

Private VLAN configuration examples

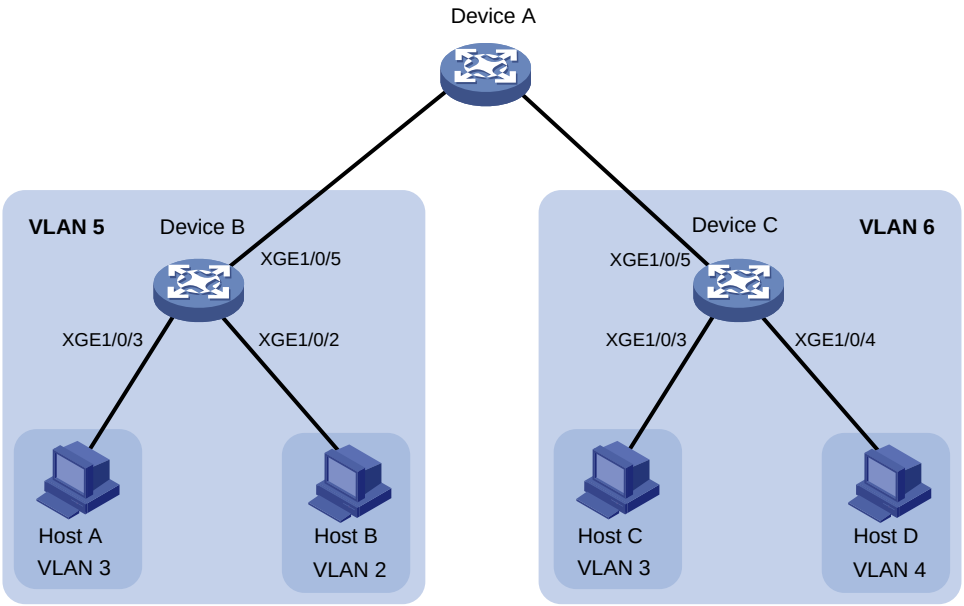
Example: Configuring promiscuous ports

Network configuration

As shown in Figure 9, configure the private VLAN feature to meet the following requirements:

- On Device B, VLAN 5 is a primary VLAN that is associated with secondary VLANs 2 and 3. Ten-GigabitEthernet 1/0/5 is in VLAN 5. Ten-GigabitEthernet 1/0/2 is in VLAN 2. Ten-GigabitEthernet 1/0/3 is in VLAN 3.
- On Device C, VLAN 6 is a primary VLAN that is associated with secondary VLANs 3 and 4. Ten-GigabitEthernet 1/0/5 is in VLAN 6. Ten-GigabitEthernet 1/0/3 is in VLAN 3. Ten-GigabitEthernet 1/0/4 is in VLAN 4.
- Device A is aware of only VLAN 5 on Device B and VLAN 6 on Device C.

Figure 9 Network diagram



Procedure

This example describes the configurations on Device B and Device C.

1. Configure Device B:

Configure VLAN 5 as a primary VLAN.

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan primary
[DeviceB-vlan5] quit
```

Create VLANs 2 and 3.

```
[DeviceB] vlan 2 to 3
```

Associate secondary VLANs 2 and 3 with primary VLAN 5.

```
[DeviceB] vlan 5
[DeviceB-vlan5] private-vlan secondary 2 to 3
[DeviceB-vlan5] quit
```

Configure the uplink port (Ten-GigabitEthernet 1/0/5) as a promiscuous port of VLAN 5.

```
[DeviceB] interface ten-gigabitethernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] port private-vlan 5 promiscuous
[DeviceB-Ten-GigabitEthernet1/0/5] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.

```
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-Ten-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.

```
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-Ten-GigabitEthernet1/0/3] port private-vlan host
```

```
[DeviceB-Ten-GigabitEthernet1/0/3] quit
```

2. Configure Device C:

Configure VLAN 6 as a primary VLAN.

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC–vlan6] private-vlan primary
[DeviceC–vlan6] quit
```

Create VLANs 3 and 4.

```
[DeviceC] vlan 3 to 4
```

Associate secondary VLANs 3 and 4 with primary VLAN 6.

```
[DeviceC] vlan 6
[DeviceC-vlan6] private-vlan secondary 3 to 4
[DeviceC-vlan6] quit
```

Configure the uplink port (Ten-GigabitEthernet 1/0/5) as a promiscuous port of VLAN 6.

```
[DeviceC] interface ten-gigabitethernet 1/0/5
[DeviceC-Ten-GigabitEthernet1/0/5] port private-vlan 6 promiscuous
[DeviceC-Ten-GigabitEthernet1/0/5] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.

```
[DeviceC] interface ten-gigabitethernet 1/0/3
[DeviceC-Ten-GigabitEthernet1/0/3] port access vlan 3
[DeviceC-Ten-GigabitEthernet1/0/3] port private-vlan host
[DeviceC-Ten-GigabitEthernet1/0/3] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/4 to VLAN 4, and configure the port as a host port.

```
[DeviceC] interface ten-gigabitethernet 1/0/4
[DeviceC-Ten-GigabitEthernet1/0/4] port access vlan 4
[DeviceC-Ten-GigabitEthernet1/0/4] port private-vlan host
[DeviceC-Ten-GigabitEthernet1/0/4] quit
```

Verifying the configuration

Verify the private VLAN configurations on the devices, for example, on Device B.

```
[DeviceB] display private-vlan
 Primary VLAN ID: 5
 Secondary VLAN ID: 2-3

 VLAN ID: 5
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0005
 Name: VLAN 0005
 Tagged ports:   None
 Untagged ports:
    Ten-GigabitEthernet1/0/2
    Ten-GigabitEthernet1/0/3
    Ten-GigabitEthernet1/0/5
```

```
VLAN ID: 2
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:   None
Untagged ports:
   Ten-GigabitEthernet1/0/2
   Ten-GigabitEthernet1/0/5

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged Ports:   None
Untagged Ports:
   Ten-GigabitEthernet1/0/3
   Ten-GigabitEthernet1/0/5
```

The output shows that:

- The promiscuous port (Ten-GigabitEthernet 1/0/5) is an untagged member of primary VLAN 5 and secondary VLANs 2 and 3.
- Host port Ten-GigabitEthernet 1/0/2 is an untagged member of primary VLAN 5 and secondary VLAN 2.
- Host port Ten-GigabitEthernet 1/0/3 is an untagged member of primary VLAN 5 and secondary VLAN 3.

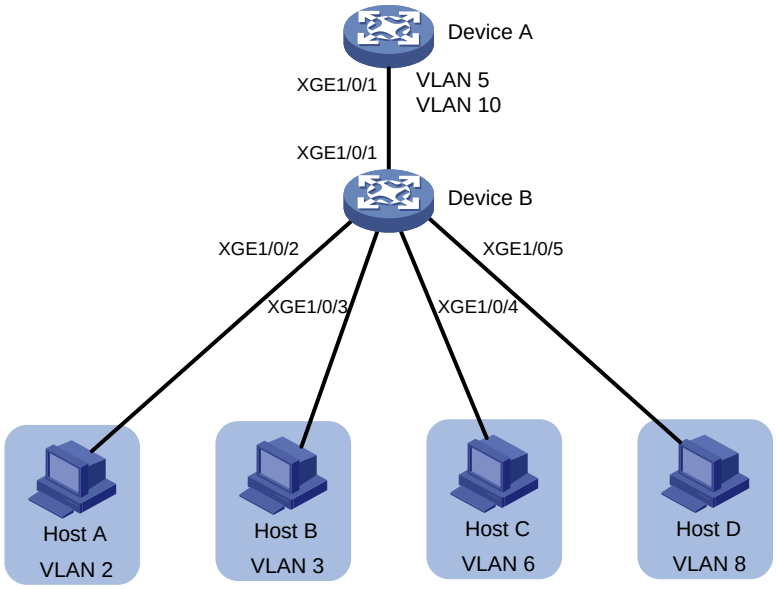
Example: Configuring trunk promiscuous ports

Network configuration

As shown in Figure 10, configure the private VLAN feature to meet the following requirements:

- VLANs 5 and 10 are primary VLANs on Device B. The uplink port (Ten-GigabitEthernet 1/0/1) on Device B permits the packets from VLANs 5 and 10 to pass through tagged.
- On Device B, downlink port Ten-GigabitEthernet 1/0/2 permits secondary VLAN 2. Downlink port Ten-GigabitEthernet 1/0/3 permits secondary VLAN 3. Secondary VLANs 2 and 3 are associated with primary VLAN 5.
- On Device B, downlink port Ten-GigabitEthernet 1/0/4 permits secondary VLAN 6. Downlink port Ten-GigabitEthernet 1/0/5 permits secondary VLAN 8. Secondary VLANs 6 and 8 are associated with primary VLAN 10.
- Device A is aware of only VLANs 5 and 10 on Device B.

Figure 10 Network diagram



Procedure

1. Configure Device B:

   # Configure VLANs 5 and 10 as primary VLANs.

   ```
   <DeviceB> system-view
   [DeviceB] vlan 5
   [DeviceB-vlan5] private-vlan primary
   [DeviceB-vlan5] quit
   [DeviceB] vlan 10
   [DeviceB-vlan10] private-vlan primary
   [DeviceB-vlan10] quit
   ```

   # Create VLANs 2, 3, 6, and 8.

   ```
   [DeviceB] vlan 2 to 3
   [DeviceB] vlan 6
   [DeviceB-vlan6] quit
   [DeviceB] vlan 8
   [DeviceB-vlan8] quit
   ```

   # Associate secondary VLANs 2 and 3 with primary VLAN 5.

   ```
   [DeviceB] vlan 5
   [DeviceB-vlan5] private-vlan secondary 2 to 3
   [DeviceB-vlan5] quit
   ```

   # Associate secondary VLANs 6 and 8 with primary VLAN 10.

   ```
   [DeviceB] vlan 10
   [DeviceB-vlan10] private-vlan secondary 6 8
   [DeviceB-vlan10] quit
   ```

   # Configure the uplink port (Ten-GigabitEthernet 1/0/1) as a trunk promiscuous port of VLANs 5 and 10.

   ```
   [DeviceB] interface ten-gigabitethernet 1/0/1
   [DeviceB-Ten-GigabitEthernet1/0/1] port private-vlan 5 10 trunk promiscuous
   [DeviceB-Ten-GigabitEthernet1/0/1] quit
   ```

Assign downlink port Ten-GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.

```
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port access vlan 2
[DeviceB-Ten-GigabitEthernet1/0/2] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.

```
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port access vlan 3
[DeviceB-Ten-GigabitEthernet1/0/3] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/3] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/4 to VLAN 6, and configure the port as a host port.

```
[DeviceB] interface ten-gigabitethernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] port access vlan 6
[DeviceB-Ten-GigabitEthernet1/0/4] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/4] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/5 to VLAN 8, and configure the port as a host port.

```
[DeviceB] interface ten-gigabitethernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] port access vlan 8
[DeviceB-Ten-GigabitEthernet1/0/5] port private-vlan host
[DeviceB-Ten-GigabitEthernet1/0/5] quit
```

2. Configure Device A:

Create VLANs 5 and 10.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

Configure Ten-GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLANs 5 and 10 as a tagged VLAN member.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
[DeviceA-Ten-GigabitEthernet1/0/1] port hybrid vlan 5 10 tagged
[DeviceA-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify the primary VLAN configurations on Device B. The following output uses primary VLAN 5 as an example.

```
[DeviceB] display private-vlan 5
 Primary VLAN ID: 5
 Secondary VLAN ID: 2-3

 VLAN ID: 5
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0005
```

```
Name: VLAN 0005
Tagged ports:
    Ten-GigabitEthernet1/0/1
Untagged ports:
    Ten-GigabitEthernet1/0/2
    Ten-GigabitEthernet1/0/3

VLAN ID: 2
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:
    Ten-GigabitEthernet1/0/1
Untagged ports:
    Ten-GigabitEthernet1/0/2

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:
    Ten-GigabitEthernet1/0/1
Untagged ports:
    Ten-GigabitEthernet1/0/3
```

The output shows that:

- The trunk promiscuous port (Ten-GigabitEthernet 1/0/1) is a tagged member of primary VLAN 5 and secondary VLANs 2 and 3.
- Host port Ten-GigabitEthernet 1/0/2 is an untagged member of primary VLAN 5 and secondary VLAN 2.
- Host port Ten-GigabitEthernet 1/0/3 is an untagged member of primary VLAN 5 and secondary VLAN 3.

Example: Configuring trunk promiscuous and trunk secondary ports

Network configuration

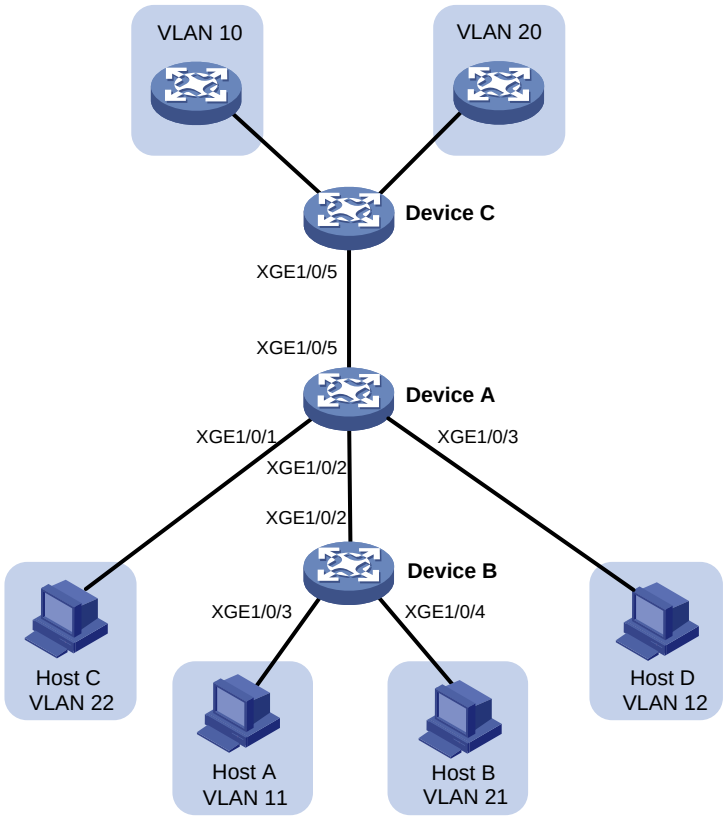
As shown in Figure 11, configure the private VLAN feature to meet the following requirements:

- VLANs 10 and 20 are primary VLANs on Device A. The uplink port (Ten-GigabitEthernet 1/0/5) on Device A permits the packets from VLANs 10 and 20 to pass through tagged.
- VLANs 11, 12, 21, and 22 are secondary VLANs on Device A.
  - Downlink port Ten-GigabitEthernet 1/0/2 permits the packets from secondary VLANs 11 and 21 to pass through tagged.
  - Downlink port Ten-GigabitEthernet 1/0/1 permits secondary VLAN 22.

- Downlink port Ten-GigabitEthernet 1/0/3 permits secondary VLAN 12.

- Secondary VLANs 11 and 12 are associated with primary VLAN 10.
- Secondary VLANs 21 and 22 are associated with primary VLAN 20.

Figure 11 Network diagram



Procedure

1. Configure Device A:

Configure VLANs 10 and 20 as primary VLANs.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan primary
[DeviceA-vlan20] quit
```

Create VLANs 11, 12, 21, and 22.

```
[DeviceA] vlan 11 to 12
[DeviceA] vlan 21 to 22
```

Associate secondary VLANs 11 and 12 with primary VLAN 10.

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan secondary 11 12
[DeviceA-vlan10] quit
```

Associate secondary VLANs 21 and 22 with primary VLAN 20.

```
[DeviceA] vlan 20
[DeviceA-vlan20] private-vlan secondary 21 22
```

```
[DeviceA-vlan20] quit
```

Configure the uplink port (Ten-GigabitEthernet 1/0/5) as a trunk promiscuous port of VLANs 10 and 20.

```
[DeviceA] interface ten-gigabitethernet 1/0/5
[DeviceA-Ten-GigabitEthernet1/0/5] port private-vlan 10 20 trunk promiscuous
[DeviceA-Ten-GigabitEthernet1/0/5] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/1 to VLAN 22 and configure the port as a host port.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port access vlan 22
[DeviceA-Ten-GigabitEthernet1/0/1] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/1] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 12 and configure the port as a host port.

```
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port access vlan 12
[DeviceA-Ten-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/3] quit
```

Configure downlink port Ten-GigabitEthernet 1/0/2 as a trunk secondary port of VLANs 11 and 21.

```
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port private-vlan 11 21 trunk secondary
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

2. Configure Device B:

Create VLANs 11 and 21.

```
<DeviceB> system-view
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 21
[DeviceB-vlan21] quit
```

Configure Ten-GigabitEthernet 1/0/2 as a hybrid port, and assign it to VLANs 11 and 21 as a tagged VLAN member.

```
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-type hybrid
[DeviceB-Ten-GigabitEthernet1/0/2] port hybrid vlan 11 21 tagged
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

Assign Ten-GigabitEthernet 1/0/3 to VLAN 11.

```
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port access vlan 11
[DeviceB-Ten-GigabitEthernet1/0/3] quit
```

Assign Ten-GigabitEthernet 1/0/4 to VLAN 21.

```
[DeviceB] interface ten-gigabitethernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] port access vlan 21
[DeviceB-Ten-GigabitEthernet1/0/4] quit
```

3. Configure Device C:

Create VLANs 10 and 20.

```
<DeviceC> system-view
[DeviceC] vlan 10
```

```
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
```

Configure Ten-GigabitEthernet 1/0/5 as a hybrid port, and assign it to VLANs 10 and 20 as a tagged VLAN member.

```
[DeviceC] interface ten-gigabitethernet 1/0/5
[DeviceC-Ten-GigabitEthernet1/0/5] port link-type hybrid
[DeviceC-Ten-GigabitEthernet1/0/5] port hybrid vlan 10 20 tagged
[DeviceC-Ten-GigabitEthernet1/0/5] quit
```

Verifying the configuration

Verify the primary VLAN configurations on Device A. The following output uses primary VLAN 10 as an example.

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 11-12

 VLAN ID: 10
 VLAN type: Static
 Private-vlan type: Primary
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:
    Ten-GigabitEthernet1/0/2
    Ten-GigabitEthernet1/0/5
 Untagged ports:
    Ten-GigabitEthernet1/0/3

 VLAN ID: 11
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0011
 Name: VLAN 0011
 Tagged ports:
    Ten-GigabitEthernet1/0/2
    Ten-GigabitEthernet1/0/5
 Untagged ports: None

 VLAN ID: 12
 VLAN type: Static
 Private-vlan type: Secondary
 Route interface: Not configured
 Description: VLAN 0012
 Name: VLAN 0012
 Tagged ports:
    Ten-GigabitEthernet1/0/5
 Untagged ports:
```

```
    Ten-GigabitEthernet1/0/3
```

The output shows that:

- The trunk promiscuous port (Ten-GigabitEthernet 1/0/5) is a tagged member of primary VLAN 10 and secondary VLANs 11 and 12.
- The trunk secondary port (Ten-GigabitEthernet 1/0/2) is a tagged member of primary VLAN 10 and secondary VLAN 11.
- The host port (Ten-GigabitEthernet 1/0/3) is an untagged member of primary VLAN 10 and secondary VLAN 12.

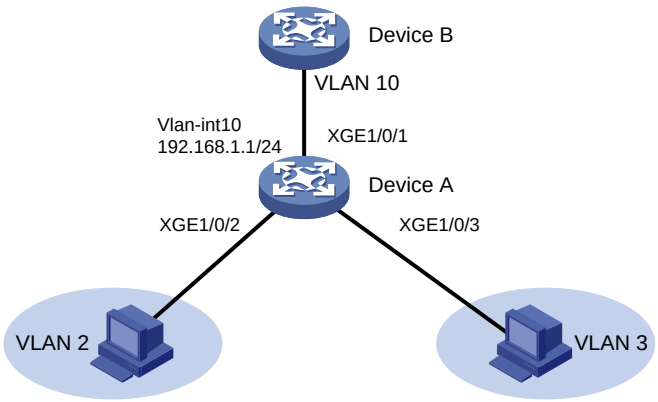
Example: Configuring Layer 3 communication for secondary VLANs

Network configuration

As shown in Figure 12, configure the private VLAN feature to meet the following requirements:

- Primary VLAN 10 on Device A is associated with secondary VLANs 2 and 3. The IP address of VLAN-interface 10 is 192.168.1.1/24.
- Ten-GigabitEthernet 1/0/1 belongs to VLAN 10. Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/3 belong to VLAN 2 and VLAN 3, respectively.
- Secondary VLANs are isolated at Layer 2 but interoperable at Layer 3.

Figure 12 Network diagram



Procedure

Create VLAN 10 and configure it as a primary VLAN.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] quit
```

Create VLANs 2 and 3.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

Associate primary VLAN 10 with secondary VLANs 2 and 3.

```
[DeviceA] vlan 10
[DeviceA-vlan10] private-vlan primary
[DeviceA-vlan10] private-vlan secondary 2 3
[DeviceA-vlan10] quit
```

Configure the uplink port (Ten-GigabitEthernet 1/0/1) as a promiscuous port of VLAN 10.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
[DeviceA-Ten-GigabitEthernet1/0/1] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/2 to VLAN 2, and configure the port as a host port.

```
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port access vlan 2
[DeviceA-Ten-GigabitEthernet1/0/2] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

Assign downlink port Ten-GigabitEthernet 1/0/3 to VLAN 3, and configure the port as a host port.

```
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port access vlan 3
[DeviceA-Ten-GigabitEthernet1/0/3] port private-vlan host
[DeviceA-Ten-GigabitEthernet1/0/3] quit
```

Enable Layer 3 communication between secondary VLANs 2 and 3 that are associated with primary VLAN 10.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] private-vlan secondary 2 3
```

Assign IP address 192.168.1.1/24 to VLAN-interface 10.

```
[DeviceA-Vlan-interface10] ip address 192.168.1.1 255.255.255.0
```

Enable local proxy ARP on VLAN-interface 10.

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

Verifying the configuration

Display the configuration of primary VLAN 10.

```
[DeviceA] display private-vlan 10
 Primary VLAN ID: 10
 Secondary VLAN ID: 2-3

 VLAN ID: 10
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Ten-GigabitEthernet1/0/1
    Ten-GigabitEthernet1/0/2
    Ten-GigabitEthernet1/0/3

 VLAN ID: 2
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Configured
```

```
IPv4 address: 192.168.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:   None
Untagged ports:
   Ten-GigabitEthernet1/0/1
   Ten-GigabitEthernet1/0/2

VLAN ID: 3
VLAN type: Static
Private VLAN type: Secondary
Route interface: Configured
IPv4 address: 192.168.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
Untagged ports:
   Ten-GigabitEthernet1/0/1
   Ten-GigabitEthernet1/0/3
```

The **Route interface** field in the output is **Configured**, indicating that secondary VLANs 2 and 3 are interoperable at Layer 3.

Configuring voice VLANs

About voice VLANs

A voice VLAN is used for transmitting voice traffic. The device can configure QoS parameters for voice packets to ensure higher transmission priority of the voice packets.

Common voice devices include IP phones and integrated access devices (IADs). This chapter uses IP phones as an example.

Working mechanism

When an IP phone accesses a device, the device performs the following operations:

1. Identifies the IP phone in the network and obtains the MAC address of the IP phone.
2. Advertises the voice VLAN information to the IP phone.

After receiving the voice VLAN information, the IP phone performs automatic configuration. Voice packets sent from the IP phone can then be transmitted within the voice VLAN.

Methods of identifying IP phones

Devices can use the OUI addresses or LLDP to identify IP phones.

Identifying IP phones through OUI addresses

A device identifies voice packets based on their source MAC addresses. A packet whose source MAC address complies with an Organizationally Unique Identifier (OUI) address of the device is regarded as a voice packet.

You can use system default OUI addresses (see Table 1) or configure OUI addresses for the device. You can manually remove or add the system default OUI addresses.

Table 1 Default OUI addresses

Number	OUI address	Vendor
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	000f-e200-0000	H3C Aolynk phone
5	0060-b900-0000	Philips/NEC phone
6	00d0-1e00-0000	Pingtel phone
7	00e0-7500-0000	Polycom phone
8	00e0-bb00-0000	3Com phone

Typically, an OUI address refers to the first 24 bits of a MAC address (in binary notation) and is a globally unique identifier that IEEE assigns to a vendor. However, OUI addresses in this chapter are addresses that the system uses to identify voice packets. They are the logical AND results of the *mac-address* and *oui-mask* arguments in the **voice-vlan mac-address** command.

Automatically identifying IP phones through LLDP

If IP phones support LLDP, configure LLDP for automatic IP phone discovery on the device. The device can then automatically discover the peer through LLDP, and exchange LLDP TLVs with the peer.

If the LLDP System Capabilities TLV received on a port indicates that the peer can act as a telephone, the device performs the following operations:

1. Sends an LLDP TLV with the voice VLAN configuration to the peer.
2. Assigns the receiving port to the voice VLAN.
3. Increases the transmission priority of the voice packets sent from the IP phone.
4. Adds the MAC address of the IP phone to the MAC address table to ensure that the IP phone can pass authentication.

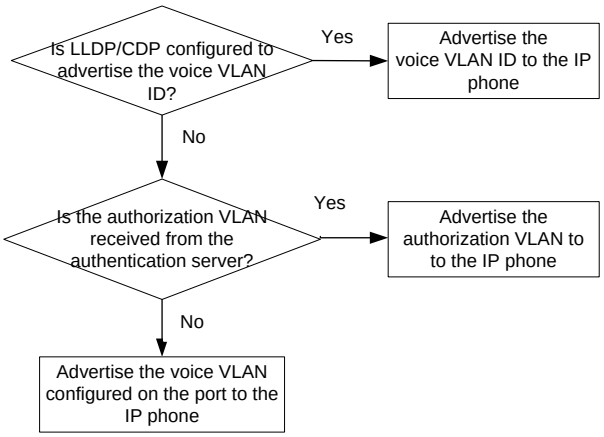
Use LLDP instead of the OUI list to identify IP phones if the network has more IP phone categories than the maximum number of OUI addresses supported on the device. LLDP has higher priority than the OUI list.

For more information about LLDP, see "Configuring LLDP."

Advertising the voice VLAN information to IP phones

Figure 13 shows the workflow of advertising the voice VLAN information to IP phones.

Figure 13 Workflow of advertising the voice VLAN information to IP phones



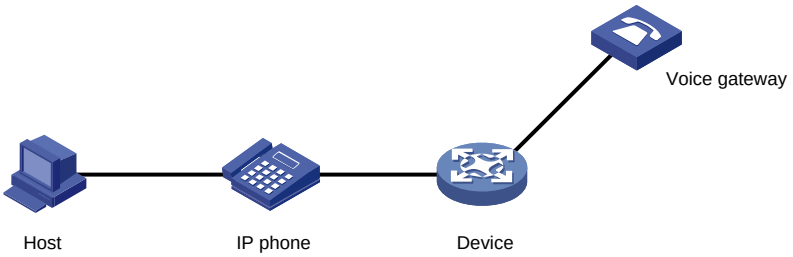
IP phone access methods

Connecting the host and the IP phone in series

As shown in Figure 14, the host is connected to the IP phone, and the IP phone is connected to the device. In this scenario, the following requirements must be met:

- The host and the IP phone use different VLANs.
- The IP phone is able to send out VLAN-tagged packets, so that the device can differentiate traffic from the host and the IP phone.
- The port connecting to the IP phone forwards packets from the voice VLAN and the PVID.

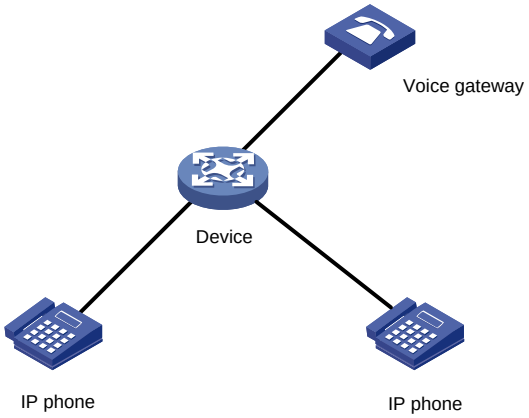
Figure 14 Connecting the host and IP phone in series



Connecting the IP phone to the device

As shown in Figure 15, IP phones are connected to the device without the presence of the host. Use this connection method when IP phones sends out untagged voice packets. In this scenario, you must configure the voice VLAN as the PVID of the access port of the IP phone, and configure the port to forward the packets from the PVID.

Figure 15 Connecting the IP phone to the device



Voice VLAN assignment modes

A port can be assigned to a voice VLAN automatically or manually.

Automatic mode

Use automatic mode when PCs and IP phones are connected in series to access the network through the device, as shown in Figure 14. Ports on the device transmit both voice traffic and data traffic.

When an IP phone is powered on, it sends out protocol packets. After receiving these protocol packets, the device uses the source MAC address of the protocol packets to match its OUI addresses. If the match succeeds, the device performs the following operations:

- Assigns the receiving port of the protocol packets to the voice VLAN.
- Issues ACL rules to set the packet precedence.
- Starts the voice VLAN aging timer.

If no voice packet is received from the port before the aging timer expires, the device will remove the port from the voice VLAN. The aging timer is also configurable.

When the IP phone reboots, the port is reassigned to the voice VLAN to ensure the correct operation of the existing voice connections. The reassignment occurs automatically without being triggered by voice traffic as long as the voice VLAN operates correctly.

Manual mode

Use manual mode when only IP phones access the network through the device, as shown in Figure 15. In this mode, ports are assigned to a voice VLAN that transmits voice traffic exclusively. No data traffic affects the voice traffic transmission.

You must manually assign the port that connects to the IP phone to a voice VLAN. The device uses the source MAC address of the received voice packets to match its OUI addresses. If the match succeeds, the device issues ACL rules to set the packet precedence.

To remove the port from the voice VLAN, you must manually remove it.

Cooperation of voice VLAN assignment modes and IP phones

Some IP phones send out VLAN-tagged packets, and others send out only untagged packets. For correct packet processing, ports of different link types must meet specific configuration requirements in different voice VLAN assignment modes.

If an IP phone sends out tagged voice traffic, and its access port is configured with 802.1X authentication, guest VLAN, Auth-Fail VLAN, or critical VLAN, VLAN IDs must be different for the following VLANs:

- Voice VLAN.
- PVID of the access port.
- 802.1X guest, Auth-Fail, or critical VLAN.

If an IP phone sends out untagged voice traffic, the PVID of the access port must be the voice VLAN. In this scenario, 802.1X authentication is not supported.

Access ports do not transmit tagged packets.

Configuration requirements for transmitting tagged voice traffic

Port link type	Voice VLAN assignment mode	Configuration requirements
Trunk	Automatic	The PVID of the port cannot be the voice VLAN.
	Manual	The PVID of the port cannot be the voice VLAN. The port must forward packets from the voice VLAN.
Hybrid	Automatic	The PVID of the port cannot be the voice VLAN.
	Manual	The PVID of the port cannot be the voice VLAN. The port must forward packets from the voice VLAN with VLAN tags.

Configuration requirements for transmitting untagged voice traffic

When IP phones send out untagged packets, you must set the voice VLAN assignment mode to manual.

Table 2 Configuration requirements for ports in manual mode to support untagged voice traffic

Port link type	Configuration requirements
Access	The voice VLAN must be the PVID of the port.
Trunk	The voice VLAN must be the PVID of the port.

Port link type	Configuration requirements
	The port must forward packets from the voice VLAN.
Hybrid	The voice VLAN must be the PVID of the port. The port must forward packets from the voice VLAN without VLAN tags.

Security mode and normal mode of voice VLANs

Depending on the filtering mechanisms to incoming packets, a voice VLAN-enabled port can operate in one of the following modes:

- **Normal mode**—The port receives voice-VLAN-tagged packets and forwards them in the voice VLAN without examining their MAC addresses. If the PVID of the port is the voice VLAN and the port operates in manual VLAN assignment mode, the port forwards all the received untagged packets in the voice VLAN.

  In this mode, voice VLANs are vulnerable to traffic attacks. Malicious users might send a large number of forged voice-VLAN-tagged or untagged packets to affect voice communication.
- **Security mode**—The port uses the source MAC addresses of voice packets to match the OUI addresses of the device. Packets that fail the match will be dropped.

In a safe network, you can configure the voice VLANs to operate in normal mode. This mode reduces system resource consumption in source MAC address checking.

In either mode, the device modifies the transmission priority only for voice VLAN packets whose source MAC addresses match OUI addresses of the device.

As a best practice, do not transmit both voice traffic and non-voice traffic in a voice VLAN. If you must transmit different traffic in a voice VLAN, make sure the voice VLAN security mode is disabled.

Table 3 Packet processing on a voice VLAN-enabled port in normal or security mode

Voice VLAN mode	Packet type	Packet processing
Normal	• Untagged packets • Packets with the voice VLAN tags	The port does not examine their source MAC addresses. Both voice traffic and non-voice traffic can be transmitted in the voice VLAN.
	Packets with other VLAN tags	The port forwards or drops them depending on whether the port permits packets from these VLANs to pass through.
Security	• Untagged packets • Packets with the voice VLAN tags	• If the source MAC address of a packet matches an OUI address on the device, the packet is forwarded in the voice VLAN. • If the source MAC address of a packet does not match an OUI address on the device, the packet is dropped.
	Packets with other VLAN tags	The port forwards or drops them depending on whether the port permits packets from these VLANs to pass through.

Restrictions: Hardware compatibility with voice VLAN

The S6861 switch series and the S6820 switch series do not support S-channel interface view or S-channel aggregate interface view.

Restrictions and guidelines: Voice VLAN configuration

The aging timer of a voice VLAN starts only when the dynamic MAC address entry of the voice VLAN ages out. The aging period for the voice VLAN equals the sum of the voice VLAN aging timer and the aging timer for its dynamic MAC address entry. For more information about the aging timer for dynamic MAC address entries, see "Configuring the MAC address table."

As a best practice, do not both configure voice VLAN and disable MAC address learning on a port. If the two features are configured together on a port, the port forwards only packets exactly matching the OUI addresses and drops inexactly matching packets.

As a best practice, do not configure both voice VLAN and the MAC learning limit on a port. If the two features are configured together on a port and the port learns the configured maximum number of MAC address entries, the port processes packets as follows:

- Forwards only packets matching the MAC address entries learnt by the port and OUI addresses.
- Drops unmatching packets.

Voice VLAN tasks at a glance

To configure a voice VLAN, perform the following tasks:

1. Configuring the QoS priority settings for voice traffic
2. Use one of the following methods:
   - Configuring a port to operate in automatic voice VLAN assignment mode
   - Configuring a port to operate in manual voice VLAN assignment mode
3. (Optional.) Enabling LLDP for automatic IP phone discovery
4. (Optional.) Use one of the following methods:
   - Configuring LLDP to advertise a voice VLAN
   - Configuring CDP to advertise a voice VLAN

Configuring the QoS priority settings for voice traffic

About the QoS priority settings for voice traffic

The QoS priority settings carried in voice traffic include the CoS and DSCP values. You can configure the device to modify the QoS priority settings for voice traffic.

Restrictions and guidelines

You cannot configure the QoS priority settings on a voice VLAN-enabled port. Before you configure the QoS priority settings for voice traffic on a port, you must disable the voice VLAN feature on it.

If you execute the **`voice-vlan qos`** and **`voice-vlan qos trust`** commands multiple times, the most recent configuration takes effect.

Procedure

1. Enter system view.

   `system-view`
2. Enter interface view.

- Enter Layer 2 Ethernet interface view.
  interface *interface-type interface-number*
- Enter S-channel interface view.
  interface s-channel *interface-number.channel-id*
- Enter S-channel aggregate interface view.
  interface schannel-aggregation *interface-number*:*channel-id*

3. Configure QoS priority settings for incoming voice VLAN packets.
   - Configure the port to trust the QoS priority settings.
     voice-vlan qos trust
   - Configure the port to modify the CoS and DSCP values.
     voice-vlan qos *cos-value dscp-value*

   By default, a port modifies the CoS and DSCP values for voice VLAN packets to 6 and 46, respectively.

   If a port trusts the QoS priority settings in incoming voice VLAN packets, the port does not modify their CoS and DSCP values.

Configuring voice VLAN assignment modes for a port

Configuring a port to operate in automatic voice VLAN assignment mode

Restrictions and guidelines

- Do not configure a VLAN as both a voice VLAN and a protocol-based VLAN.
  - A voice VLAN in automatic mode on a hybrid port processes only tagged incoming voice traffic.
  - A protocol-based VLAN on a hybrid port processes only untagged incoming packets. For more information about protocol-based VLANs, see "Configuring protocol-based VLANs."
- As a best practice, do not use this mode with MSTP. In MSTP mode, if a port is blocked in the MSTI of the target voice VLAN, the port drops the received packets instead of delivering them to the CPU. As a result, the port will not be dynamically assigned to the voice VLAN.
- As a best practice, do not use this mode with PVST. In PVST mode, if the target voice VLAN is not permitted on a port, the port is placed in blocked state. The port drops the received packets instead of delivering them to the CPU. As a result, the port will not be dynamically assigned to the voice VLAN.
- As a best practice, do not configure both dynamic MAC-based VLAN assignment and automatic voice VLAN assignment mode on a port. They can have a negative impact on each other.

Procedure

1. Enter system view.
   system-view
2. (Optional.) Set the voice VLAN aging timer.
   voice-vlan aging *minutes*

   By default, the aging timer of a voice VLAN is 1440 minutes.

   The voice VLAN aging timer takes effect only on ports in automatic voice VLAN assignment mode.

3. (Optional.) Enable the voice VLAN security mode.
   voice-vlan security enable
   By default, the voice VLAN security mode is enabled.
4. (Optional.) Add an OUI address for voice packet identification.
   voice-vlan mac-address *oui* **mask** *oui-mask* [**description** *text*]
   By default, system default OUI addresses exist. For more information, see Table 1.
5. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*
   - Enter S-channel aggregate interface view.
     interface schannel-aggregation *interface-number*:*channel-id*
6. Configure the link type of the port.
   - **port link-type trunk**
   - **port link-type hybrid**
7. Configure the port to operate in automatic voice VLAN assignment mode.
   voice-vlan mode auto
   By default, the automatic voice VLAN assignment mode is enabled.
8. Enable the voice VLAN feature on the port.
   voice-vlan *vlan-id* **enable**
   By default, the voice VLAN feature is disabled.
   Before you execute this command, make sure the specified VLAN already exists.

Configuring a port to operate in manual voice VLAN assignment mode

Restrictions and guidelines

- You can configure different voice VLANs for different ports on the same device. Make sure the following requirements are met:
  - One port can be configured with only one voice VLAN.
  - Voice VLANs must be existing static VLANs.
- Do not enable voice VLAN on the member ports of a link aggregation group. For more information about link aggregation, see "Configuring Ethernet link aggregation."
- To make a voice VLAN take effect on a port operating in manual mode, you must manually assign the port to the voice VLAN.

Procedure

1. Enter system view.
   system-view
2. (Optional.) Enable the voice VLAN security mode.
   voice-vlan security enable
   By default, the voice VLAN security mode is enabled.
3. (Optional.) Add an OUI address for voice packet identification.
   voice-vlan mac-address *oui* **mask** *oui-mask* [**description** *text*]

By default, system default OUI addresses exist. For more information, see Table 1.

4. Enter interface view.
   - Enter Layer 2 Ethernet interface view.
     interface *interface-type interface-number*
   - Enter S-channel interface view.
     interface s-channel *interface-number.channel-id*
   - Enter S-channel aggregate interface view.
     interface schannel-aggregation *interface-number*:*channel-id*
5. Configure the port to operate in manual voice VLAN assignment mode.
   undo voice-vlan mode auto
   By default, a port operates in automatic voice VLAN assignment mode.
6. Assign the access, trunk, or hybrid port to the voice VLAN.
   - For the access port, see "Assigning an access port to a VLAN."
   - For the trunk port, see "Assigning a trunk port to a VLAN."
   - For the hybrid port, see "Assigning a hybrid port to a VLAN."

   After you assign an access port to the voice VLAN, the voice VLAN becomes the PVID of the port.
7. (Optional.) Configure the voice VLAN as the PVID of the trunk or hybrid port.
   - For the trunk port, see "Assigning a trunk port to a VLAN."
   - For the hybrid port, see "Assigning a hybrid port to a VLAN."

   This step is required for untagged incoming voice traffic and prohibited for tagged incoming voice traffic.
8. Enable the voice VLAN feature on the port.
   voice-vlan *vlan-id* **enable**
   By default, the voice VLAN feature is disabled.
   Before you execute this command, make sure the specified VLAN already exists.

Enabling LLDP for automatic IP phone discovery

Restrictions and guidelines

- Before you enable this feature, enable LLDP both globally and on access ports.
- Use this feature only with the automatic voice VLAN assignment mode.
- Do not use this feature together with CDP compatibility.
- After you enable this feature on the device, each port of the device can be connected to a maximum of five IP phones.

Procedure

1. Enter system view.
   system-view
2. Enable LLDP for automatic IP phone discovery.
   voice-vlan track lldp
   By default, this feature is disabled.

Configuring LLDP or CDP to advertise a voice VLAN

Configuring LLDP to advertise a voice VLAN

About configuring LLDP to advertise a voice VLAN

For IP phones that support LLDP, the device advertises the voice VLAN information to the IP phones through the LLDP-MED TLVs.

Prerequisites

Before you configure this feature, enable LLDP both globally and on access ports.

Procedure

1. Enter system view.
   system-view
2. Enter Layer 2 Ethernet interface view.
   interface *interface-type interface-number*
3. Configure an advertised voice VLAN ID.
   lldp tlv-enable med-tlv network-policy *vlan-id*

   By default, no advertised voice VLAN ID is configured.

   For more information about the command, see *Layer 2—LAN Switching Command Reference*.
4. (Optional.) Display the voice VLAN advertised by LLDP.
   display lldp local-information

   For more information about the command, see *Layer 2—LAN Switching Command Reference*.

Configuring CDP to advertise a voice VLAN

About configuring CDP to advertise a voice VLAN

If an IP phone supports CDP but does not support LLDP, it will send out CDP packets to the device to request the voice VLAN ID. If the IP phone does not receive the voice VLAN ID within a time period, it will send out untagged packets. The device cannot differentiate untagged voice packets from other types of packets.

You can configure CDP compatibility on the device to enable it to perform the following operations:

- Receive and identify CDP packets from the IP phone.
- Send CDP packets to the IP phone. The voice VLAN information is carried in the CDP packets.

After receiving the advertised VLAN information, the IP phone performs automatic voice VLAN configuration. Packets from the IP phone will be transmitted in the dedicated voice VLAN.

LLDP packets sent from the device carry the priority information. CDP packets sent from the device do not carry the priority information.

Prerequisites

Before you configure this feature, enable LLDP globally and on access ports.

Procedure

1. Enter system view.
   system-view

2. Enable CDP compatibility.
   lldp compliance cdp
   By default, CDP compatibility is disabled.
3. Enter Layer 2 Ethernet interface view.
   interface *interface-type interface-number*
4. Configure CDP-compatible LLDP to operate in TxRx mode.
   lldp compliance admin-status cdp txrx
   By default, CDP-compatible LLDP operates in Disable mode.
5. Configure an advertised voice VLAN ID.
   cdp voice-vlan *vlan-id*
   By default, no advertised voice VLAN ID is configured.
   For more information about the command, see *Layer 2—LAN Switching Command Reference*.

Display and maintenance commands for voice VLANs

Execute **display** commands in any view.

Task	Command
Display OUI addresses on a device.	**display voice-vlan mac-address**
Display the voice VLAN state.	**display voice-vlan state**

Voice VLAN configuration examples

Example: Configuring automatic voice VLAN assignment mode

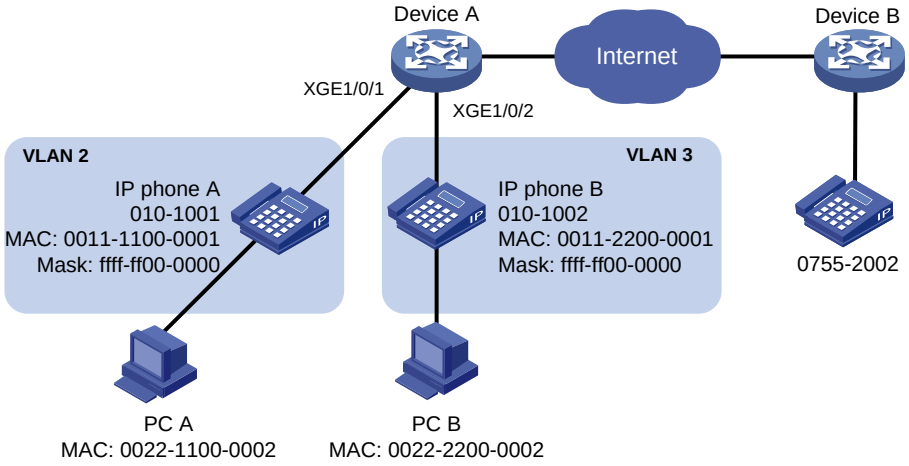
Network configuration

As shown in Figure 16, Device A transmits traffic from IP phones and hosts.

For correct voice traffic transmission, perform the following tasks on Device A:

- Configure voice VLANs 2 and 3 to transmit voice packets from IP phone A and IP phone B, respectively.
- Configure Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to operate in automatic voice VLAN assignment mode.
- Add MAC addresses of IP phones A and B to the device for voice packet identification. The mask of the two MAC addresses is FFFF-FF00-0000.
- Set an aging timer for voice VLANs.

Figure 16 Network diagram



Procedure

1. Configure voice VLANs:

   # Create VLANs 2 and 3.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 2 to 3
   ```

   # Set the voice VLAN aging timer to 30 minutes.

   ```
   [DeviceA] voice-vlan aging 30
   ```

   # Enable security mode for voice VLANs.

   ```
   [DeviceA] voice-vlan security enable
   ```

   # Add MAC addresses of IP phones A and B to the device with mask FFFF-FF00-0000.

   ```
   [DeviceA] voice-vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP phone A
   [DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP phone B
   ```

2. Configure Ten-GigabitEthernet 1/0/1:

   # Configure Ten-GigabitEthernet 1/0/1 as a hybrid port.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
   ```

   # Configure Ten-GigabitEthernet 1/0/1 to operate in automatic voice VLAN assignment mode.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/1] voice-vlan mode auto
   ```

   # Enable voice VLAN on Ten-GigabitEthernet 1/0/1 and configure VLAN 2 as the voice VLAN for it.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/1] voice-vlan 2 enable
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   ```

3. Configure Ten-GigabitEthernet 1/0/2:

   # Configure Ten-GigabitEthernet 1/0/2 as a hybrid port.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/2
   [DeviceA-Ten-GigabitEthernet1/0/2] port link-type hybrid
   ```

   # Configure Ten-GigabitEthernet 1/0/2 to operate in automatic voice VLAN assignment mode.

   ```
   [DeviceA-Ten-GigabitEthernet1/0/2] voice-vlan mode auto
   ```

   # Enable voice VLAN on Ten-GigabitEthernet 1/0/2 and configure VLAN 3 as the voice VLAN for it.

```
[DeviceA-Ten-GigabitEthernet1/0/2] voice-vlan 3 enable
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Display the OUI addresses supported on Device A.

```
[DeviceA] display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-1100-0000  ffff-ff00-0000  IP phone A
0011-2200-0000  ffff-ff00-0000  IP phone B
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Display the voice VLAN state.

```
[DeviceA] display voice-vlan state
 Current voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 30 minutes
 Voice VLAN enabled ports and their modes:
 Port                      VLAN        Mode        CoS         DSCP
 XGE1/0/1                  2           Auto        6           46
 XGE1/0/2                  3           Auto        6           46
```

Example: Configuring manual voice VLAN assignment mode

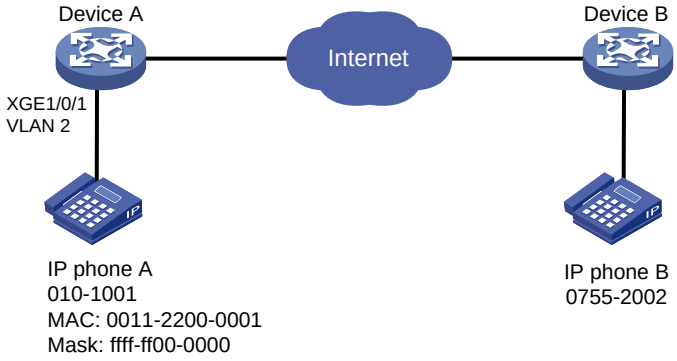
Network configuration

As shown in Figure 17, IP phone A send untagged voice traffic.

To enable Ten-GigabitEthernet 1/0/1 to transmit only voice packets, perform the following tasks on Device A:

- Create VLAN 2. This VLAN will be used as a voice VLAN.
- Configure Ten-GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode and add it to VLAN 2.
- Add the OUI address of IP phone A to the OUI list of Device A.

Figure 17 Network diagram



Procedure

Enable security mode for voice VLANs.

```
<DeviceA> system-view
[DeviceA] voice-vlan security enable
```

Add MAC address 0011-2200-0001 with mask FFFF-FF00-0000.

```
[DeviceA] voice-vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description test
```

Create VLAN 2.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

Configure Ten-GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] undo voice-vlan mode auto
```

Configure Ten-GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-Ten-GigabitEthernet1/0/1] port link-type hybrid
```

Set the PVID of Ten-GigabitEthernet 1/0/1 to VLAN 2.

```
[DeviceA-Ten-GigabitEthernet1/0/1] port hybrid pvid vlan 2
```

Assign Ten-GigabitEthernet 1/0/1 to VLAN 2 as an untagged VLAN member.

```
[DeviceA-Ten-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

Enable voice VLAN and configure VLAN 2 as the voice VLAN on Ten-GigabitEthernet 1/0/1.

```
[DeviceA-Ten-GigabitEthernet1/0/1] voice-vlan 2 enable
[DeviceA-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display the OUI addresses supported on Device A.

```
[DeviceA] display voice-vlan mac-address
OUI Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-2200-0000  ffff-ff00-0000  test
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Display the voice VLAN state.

```
[DeviceA] display voice-vlan state
 Current voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 XGE1/0/1                    2           Manual      6           46
```