VLAN Principles and Configuration

Foreword

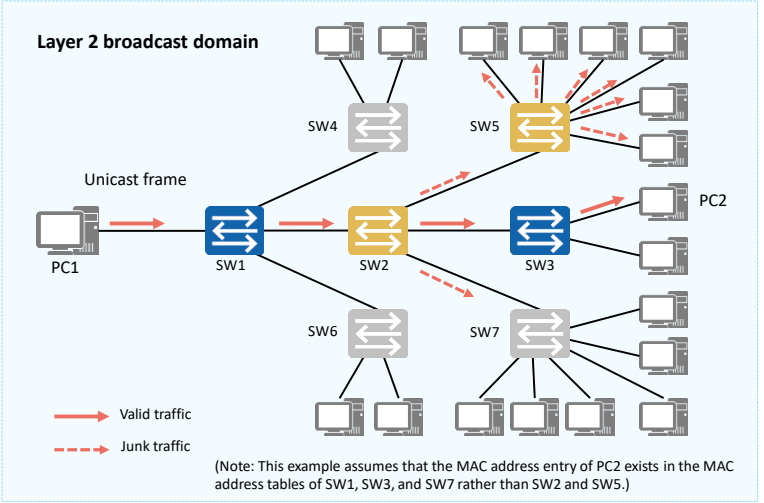
- Ethernet technology implements data communication over shared media based on carrier sense multiple access with collision detection (CSMA/CD). If there are a large number of PCs on the Ethernet, security risks and broadcast storms may occur, deteriorating network performance and even causing network breakdowns.
- The virtual local area network (VLAN) technology is therefore introduced to solve the preceding problem.
- This course describes basic VLAN principles, working principles of different Layer 2 interfaces, VLAN applications, data forwarding principles, and basic VLAN configuration methods.

Objectives

- On completion of this course, you will be able to:
  - Understand the background of the VLAN technology.
  - Identify the VLAN to which data belongs.
  - Master different VLAN assignment modes.
  - Describe how data communication is implemented through VLANs.
  - Master basic VLAN configuration methods.

Contents

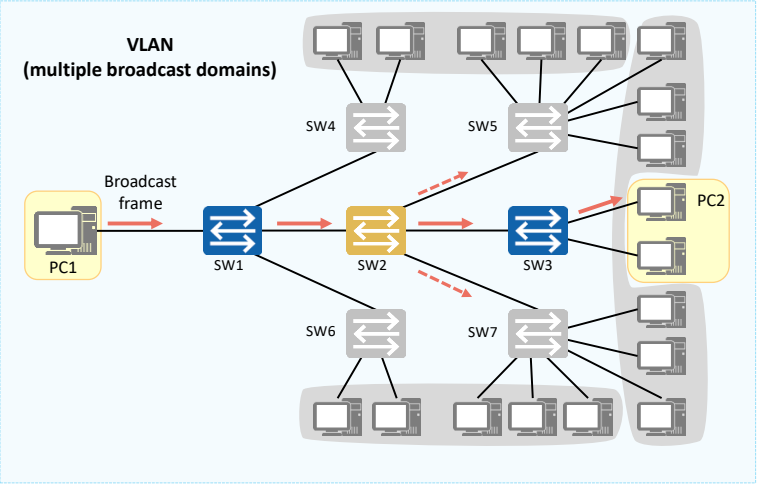
Issues Facing a Traditional Ethernet



- On a typical switching network,broadcast frames or unknown unicast frames sent by a PC are flooded in the entire broadcast domain.
- The larger the broadcast domain is, the more serious network security and junk traffic problems are.

- Broadcast domain:
  - The preceding figure shows a typical switching network with only PCs and switches. If PC1 sends a broadcast frame, the switches flood the frame on the network. As a result, all the other PCs receive the frame.
  - The range that broadcast frames can reach is called a Layer 2 broadcast domain (broadcast domain for short). A switching network is a broadcast domain.
- Network security and junk traffic problems:
  - Assume that PC1 sends a unicast frame to PC2. The MAC address entry of PC2 exists in the MAC address tables of SW1, SW3, and SW7 rather than SW2 and SW5. In this case, SW1 and SW3 forward the frame in point-to-point mode, SW7 discards the frame, and SW2 and SW5 flood the frame. As a result, although PC2 receives the unicast frame, other PCs on the network also receive the frame that should not be received.
- The larger the broadcast domain is, the more serious network security and junk traffic problems are.

VLAN



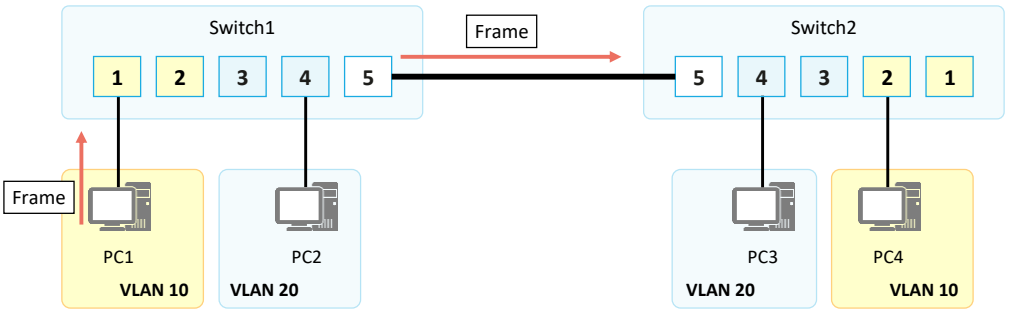
- The VLAN technology isolates broadcast domains.
- Characteristics:
  - Geographically independent.
  - Only devices in the same VLAN can directly communicate at Layer 2.

- The VLAN technology is introduced to solve the problems caused by large broadcast domains.
  - By deploying VLANs on switches, you can logically divide a large broadcast domain into several small broadcast domains. This effectively improves network security, lowers junk traffic, and reduces the number of required network resources.
- VLAN characteristics:
  - Each VLAN is a broadcast domain. Therefore, PCs in the same VLAN can directly communicate at Layer 2. PCs in different VLANs, by contrast, can only communicate at Layer 3 instead of directly communicating at Layer 2. In this way, broadcast packets are confined to a VLAN.
  - VLAN assignment is geographically independent.
- Advantages of the VLAN technology:
  - Allows flexible setup of virtual groups. With the VLAN technology, terminals in different geographical locations can be grouped together, simplifying network construction and maintenance.
  - Confines each broadcast domain to a single VLAN, conserving bandwidth and improving network processing capabilities.
  - Enhances LAN security. Frames in different VLANs are separately transmitted, so that PCs in a VLAN cannot directly communicate with those in another VLAN.
  - Improves network robustness. Faults in a VLAN do not affect PCs in other VLANs.
- Note: Layer 2 refers to the data link layer.

Contents

- This part describes VLAN principles from the following three aspects: VLAN identification, VLAN assignment, and VLAN frame processing on switches.

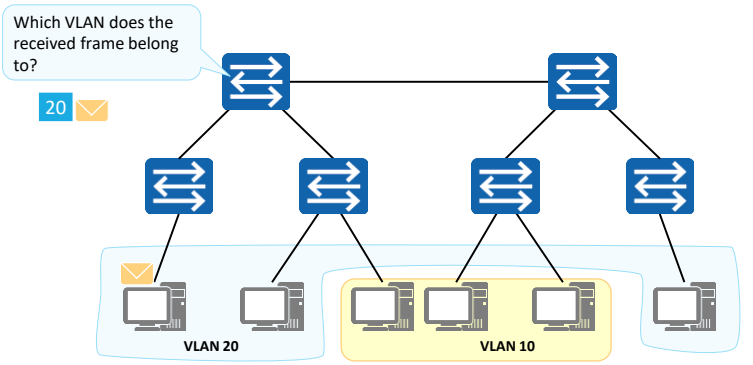
VLAN Implementation



- Switch1 and Switch2 belong to the network of the same enterprise. VLANs are planned for the network, with VLAN 10 for department A and VLAN 20 for department B. Employees in departments A and B are connected to both Switch1 and Switch2.
- Assume that a frame sent from PC1 reaches Switch2 through the link between Switch1 and Switch2. If no processing is implemented, Switch2 can neither identify the VLAN to which the frame belongs nor determine the local VLAN to which the frame should be sent.

VLAN Tag

- How does a switch identify the VLAN to which a received frame belongs?

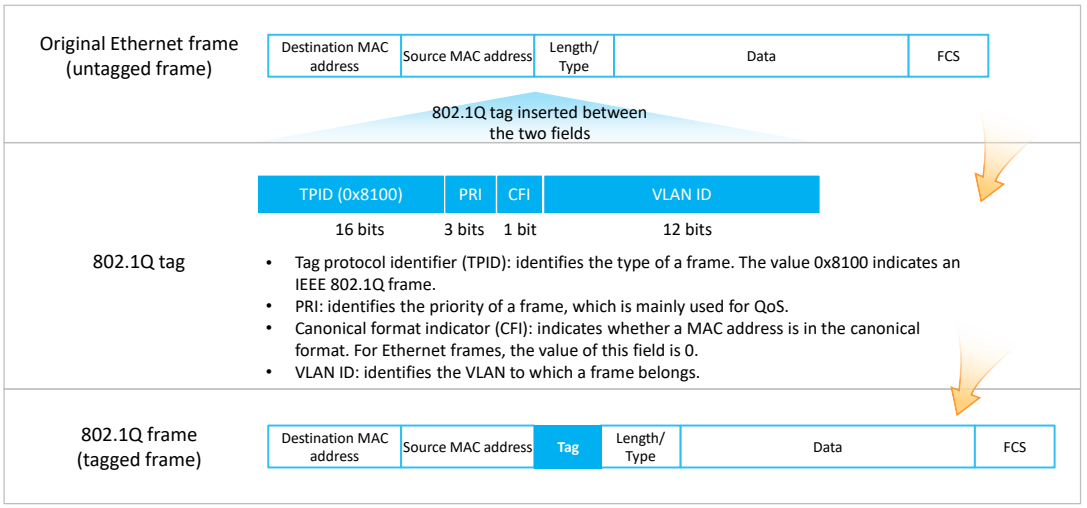


VLAN Tag

IEEE 802.1Q defines a 4-byte VLAN tag for Ethernet frames, enabling switches to identify the VLANs to which received frames belong.

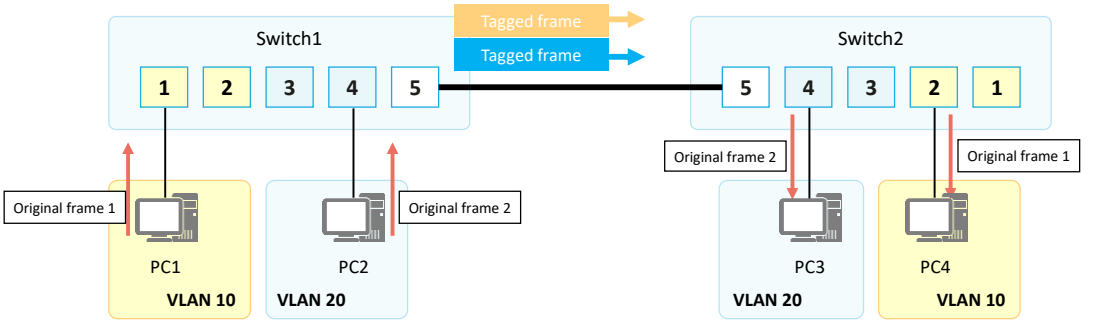
- As shown in the figure, after receiving a frame and identifying the VLAN to which the frame belongs, SW1 adds a VLAN tag to the frame to specify this VLAN. Then, after receiving the tagged frame sent from SW1, another switch, such as SW2, can easily identify the VLAN to which the frame belongs based on the VLAN tag.
- Frames with a 4-byte VLAN tag are called IEEE 802.1Q frames or VLAN frames.

VLAN Frame



- Ethernet frames in a VLAN are mainly classified into the following types:
  - Tagged frames: Ethernet frames for which a 4-byte VLAN tag is inserted between the source MAC address and length/type fields according to IEEE 802.1Q
  - Untagged frames: frames without a 4-byte VLAN tag
- Main fields in a VLAN frame:
  - TPID: a 16-bit field used to identify the type of a frame.
    - The value 0x8100 indicates an IEEE 802.1Q frame. A device that does not support 802.1Q discards 802.1Q frames.
    - Device vendors can define TPID values for devices. To enable a device to identify the non-802.1Q frames sent from another device, you can change the TPID on the device to be the same as that device.
  - PRI: a 3-bit field used to identify the priority of a frame. It is mainly used for QoS.
    - The value of this field is an integer ranging from 0 to 7. A larger value indicates a higher priority. If congestion occurs, a switch preferentially sends frames with the highest priority.

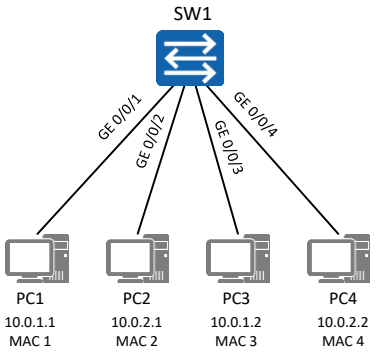
VLAN Implementation



- The link between Switch1 and Switch2 carries data of multiple VLANs. In this situation, a VLAN-based data tagging method is required to distinguish the frames of different VLANs.
- IEEE 802.1Q, often referred to as Dot1q, defines a system of VLAN tagging for Ethernet frames by inserting an 802.1Q tag into the frame header to carry VLAN information.

VLAN Assignment Methods

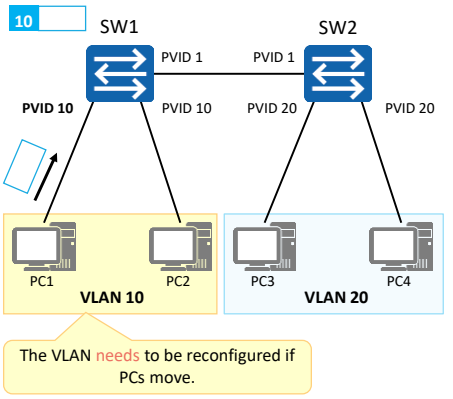
- How are VLANs assigned on a network?



VLAN Assignment Method	VLAN 10	VLAN 20
Interface-based assignment	GE 0/0/1 and GE 0/0/3	GE 0/0/2 and GE 0/0/4
MAC address-based assignment	MAC 1 and MAC 3	MAC 2 and MAC 4
IP subnet-based assignment	10.0.1.*	10.0.2.*
Protocol-based assignment	IP	IPv6
Policy-based assignment	10.0.1.* + GE 0/0/1 + MAC 1	10.0.2.* + GE 0/0/2 + MAC 2

- PCs send only untagged frames. After receiving such an untagged frame, a switch that supports the VLAN technology needs to assign the frame to a specific VLAN based on certain rules.
- Available VLAN assignment methods are as follows:
  - Interface-based assignment: assigns VLANs based on switch interfaces.
    - A network administrator preconfigures a port VLAN ID (PVID) for each switch interface. When an untagged frame arrives at an interface of a switch, the switch adds a tag carrying the PVID of the interface to the frame. The frame is then transmitted in the specified VLAN.
  - MAC address-based assignment: assigns VLANs based on the source MAC addresses of frames.
    - A network administrator preconfigures the mapping between MAC addresses and VLAN IDs. After receiving an untagged frame, a switch adds the VLAN tag mapping the source MAC address of the frame to the frame. The frame is then transmitted in the specified VLAN.

Interface-based VLAN Assignment



Interface-based VLAN Assignment

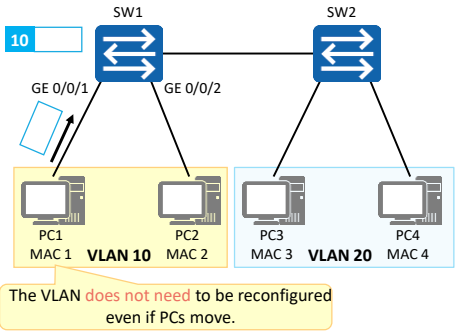
- **Principles**
  - VLANs are assigned based on interfaces.
  - A network administrator preconfigures a PVID for each switch interface and assigns each interface to a VLAN corresponding to the PVID.
  - After an interface receives an untagged frame, the switch adds a tag carrying the PVID of the interface to the frame. The frame is then transmitted in the specified VLAN.
- **Port Default VLAN ID: PVID**
  - Default VLAN ID for an interface
  - Value range: 1–4094

- Assignment rules:
  - VLAN IDs are configured on physical interfaces of a switch. All PC-sent untagged frames arriving at a physical interface are assigned to the VLAN corresponding to the PVID configured for the interface.
- Characteristics:
  - VLAN assignment is simple, intuitive, and easy to implement. Currently, it is the most widely used VLAN assignment method.
  - If the switch interface to which a PC is connected changes, the VLAN to which frames sent from the PC to the interface are assigned may also change.
- Port Default VLAN ID: PVID
  - A PVID needs to be configured for each switch interface. All untagged frames arriving at an interface are assigned to the VLAN corresponding to the PVID configured for the interface.
  - The default PVID is 1.

MAC Address-based VLAN Assignment

Mapping Between MAC Addresses and VLAN IDs on SW1

MAC Address	VLAN ID
MAC 1	10
MAC 2	10
...	...

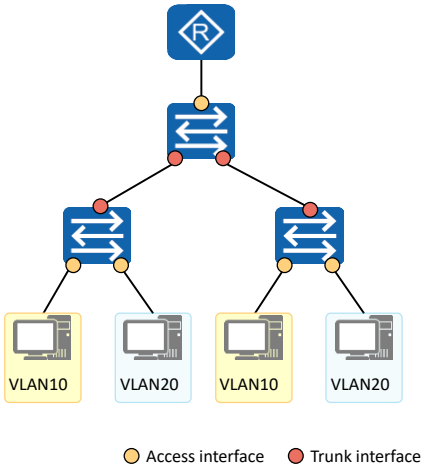


MAC Address-based VLAN Assignment

- **Principles**
  - VLANs are assigned based on the source MAC addresses of frames.
  - A network administrator preconfigures the mapping between MAC addresses and VLAN IDs.
  - After receiving an untagged frame, a switch adds the VLAN tag mapping the source MAC address of the frame to the frame. The frame is then transmitted in the specified VLAN.
- **Mapping table**
  - Records the mapping between MAC addresses and VLAN IDs.

- Assignment rules:
  - Each switch maintains a table recording the mapping between MAC addresses and VLAN IDs. After receiving a PC-sent untagged frame, a switch analyzes the source MAC address of the frame, searches the mapping table for the VLAN ID mapping the MAC address, and assigns the frame to the corresponding VLAN according to the mapping.
- Characteristics:
  - This assignment method is a bit complex but more flexible.
  - If the switch interface to which a PC is connected changes, the VLAN to which frames sent from the PC to the interface are assigned remains unchanged because the PC's MAC address does not change.
  - However, as malicious PCs can easily forge MAC addresses, this assignment method is prone to security risks.

Layer 2 Ethernet Interface Types



Interface Types

- **Access interface**

  An access interface is used to connect a switch to a terminal, such as a PC or server. In general, the NICs on such a terminal receive and send only untagged frames. An access interface can be added to only one VLAN.

- **Trunk interface**

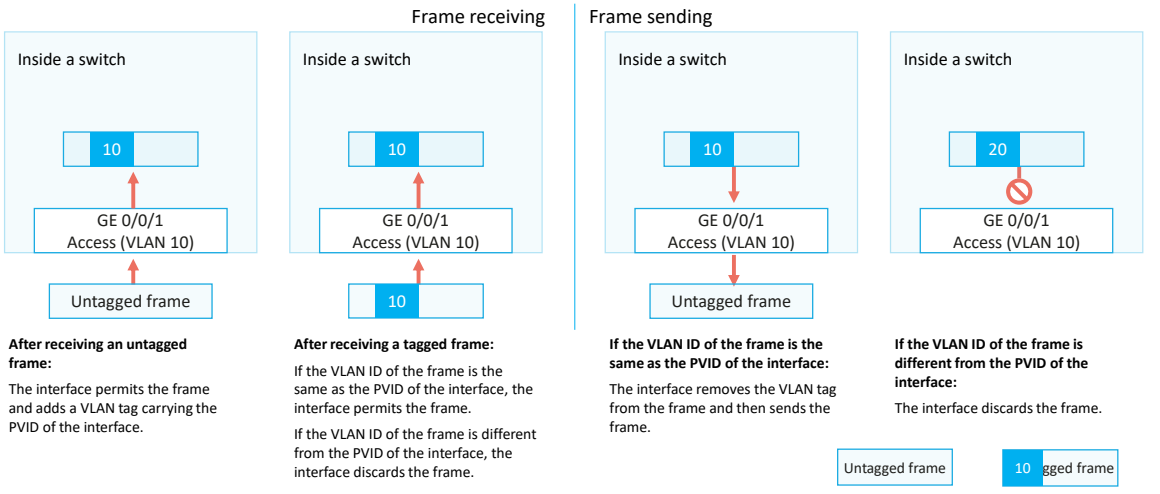
  A trunk interface allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag. This type of interface is used to connect a switch to another switch or a sub-interface on a device, such as a router or firewall.

- **Hybrid interface**

  Similar to a trunk interface, a hybrid interface also allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag. You can determine whether to allow a hybrid interface to carry VLAN tags when sending the frames of one or more VLANs.

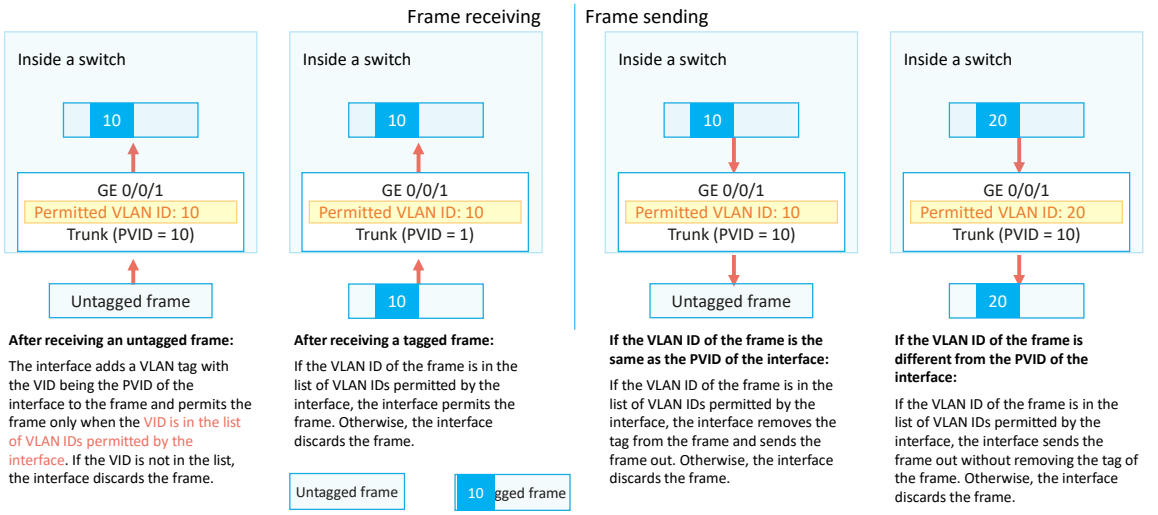
- The interface-based VLAN assignment method varies according to the switch interface type.
- Access interface
  - An access interface often connects to a terminal (such as a PC or server) that cannot identify VLAN tags, or is used when VLANs do not need to be differentiated.
- Trunk interface
  - A trunk interface often connects to a switch, router, AP, or voice terminal that can receive and send both tagged and untagged frames.
- Hybrid interface
  - A hybrid interface can connect to a user terminal (such as a PC or server) that cannot identify VLAN tags or to a switch, router, AP, or voice terminal that can receive and send both tagged and untagged frames.
  - By default, hybrid interfaces are used on Huawei devices.

Access Interface



- How do switch interfaces process tagged and untagged frames? First, let's have a look at access interfaces.
- Characteristics of access interfaces:
  - An access interface permits only frames whose VLAN ID is the same as the PVID of the interface.
- Frame receiving through an access interface:
  - After receiving an untagged frame, the access interface adds a tag with the VID being the PVID of the interface to the frame and then floods, forwards, or discards the tagged frame.
  - After receiving a tagged frame, the access interface checks whether the VID in the tag of the frame is the same as the PVID. If they are the same, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.
- Frame sending through an access interface:
  - After receiving a tagged frame sent from another interface on the same switch, the access interface checks whether the VID in the tag of the frame is the same as the PVID.
    - If they are the same, the interface removes the tag from the frame and sends the untagged frame out.
    - Otherwise, the interface directly discards the tagged frame.

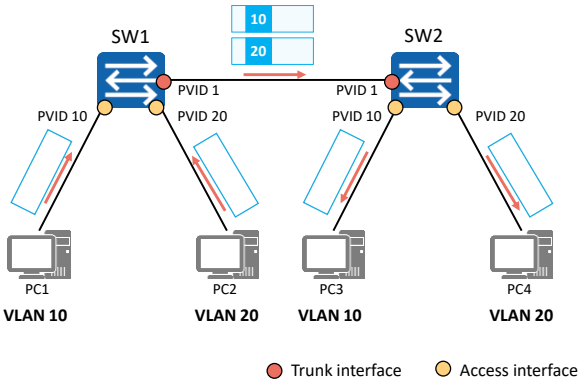
Trunk interface



- For a trunk interface, you need to configure not only a PVID but also a list of VLAN IDs permitted by the interface. By default, VLAN 1 exists in the list.
- Characteristics of trunk interfaces:
  - A trunk interface allows only frames whose VLAN IDs are in the list of VLAN IDs permitted by the interface to pass through.
  - It allows tagged frames from multiple VLANs but untagged frames from only one VLAN to pass through.
- Frame receiving through a trunk interface:
  - After receiving an untagged frame, the trunk interface adds a tag with the VID being the PVID of the interface to the frame and then checks whether the VID is in the list of VLAN IDs permitted by the interface. If the VID is in the list, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.
  - After receiving a tagged frame, the trunk interface checks whether the VID in the tag of the frame is in the list of VLAN IDs permitted by the interface. If the VID is in the list, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.

Example for Frame Processing on Access and Trunk Interfaces

- Describe how inter-PC access is implemented in this example.

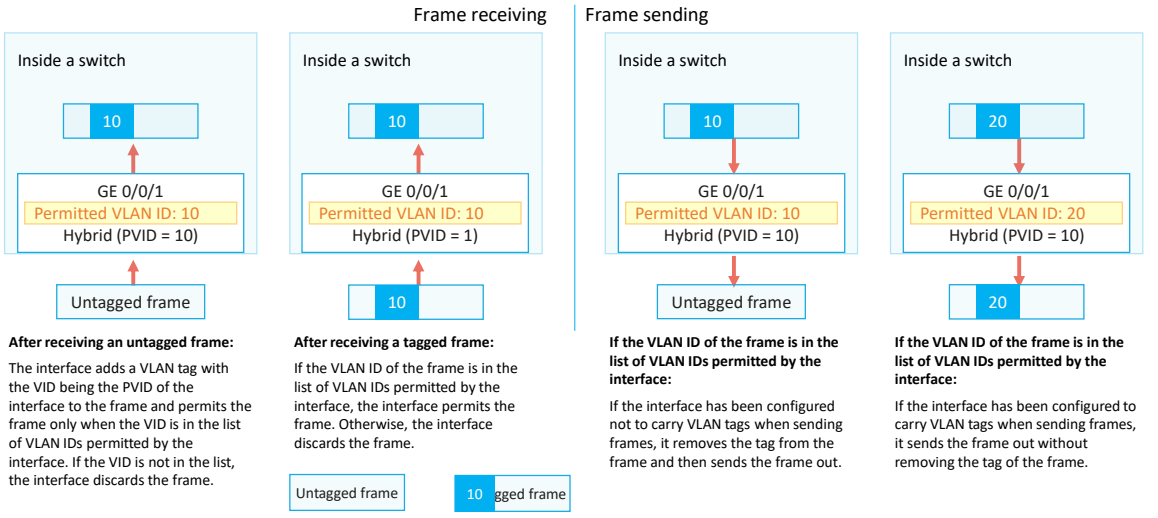


Trunk Interfaces on SW1 and SW2

List of Permitted VLAN IDs	
VLAN ID	1
	10
	20

- In this example, SW1 and SW2 connect to PCs through access interfaces. PVIDs are configured for the interfaces, as shown in the figure. SW1 and SW2 are connected through trunk interfaces whose PVIDs are all set to 1. The table lists the VLAN IDs permitted by the trunk interfaces.
- Describe how inter-PC access is implemented in this example.

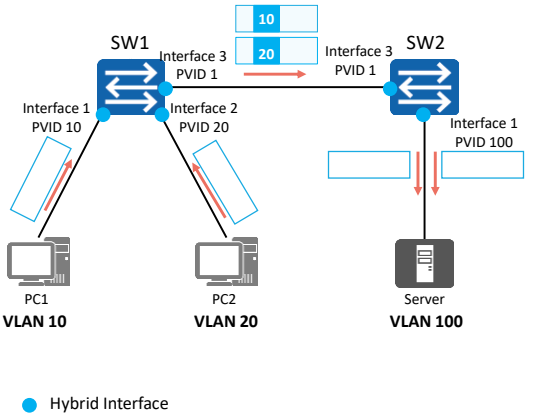
Hybrid Interface



- For a hybrid interface, you need to configure not only a PVID but also two lists of VLAN IDs permitted by the interface: one untagged VLAN ID list and one tagged VLAN ID list. By default, VLAN 1 is in the untagged VLAN ID list. Frames from all the VLANs in the two lists are allowed to pass through the hybrid interface.
- Characteristics of hybrid interfaces:
  - A hybrid interface allows only frames whose VLAN IDs are in the lists of VLAN IDs permitted by the interface to pass through.
  - It allows tagged frames from multiple VLANs to pass through. Frames sent out from a hybrid interface can be either tagged or untagged, depending on the VLAN configuration.
  - Different from a trunk interface, a hybrid interface allows untagged frames from multiple VLANs to pass through.

Example for Frame Processing on Hybrid Interfaces

- Describe how PCs access the server in this example.



List of VLAN IDs Permitted by Interfaces on SW1

Interface 1	
Untagged	
VLAN ID	1
	10
	100

Interface 2	
Untagged	
VLAN ID	1
	20
	100

Interface 3	
Tagged	
VLAN ID	10
	10
	100

List of VLAN IDs Permitted by Interfaces on SW2

Interface 1	
Untagged	
VLAN ID	1
	10
	20
	100

Interface 3	
Tagged	
VLAN ID	10
	20
	100

- In this example, SW1 and SW2 connect to PCs through hybrid interfaces. The two switches are connected also through this type of interface. PVIDs are configured for the interfaces, as shown in the figure. The tables list the VLAN IDs permitted by the interfaces.
- Describe how PCs access the server in this example.

Summary

Access Interface	Trunk Interface	Hybrid Interface
Frame receiving ▫ Untagged frame: adds a tag with the VID being the PVID of the interface and permits the frame. ▫ Tagged frame: checks whether the VID in the tag of the frame is the same as the PVID of the interface. If they are the same, permits the frame; otherwise, discards the frame.	Frame receiving ▫ Untagged frame: adds a tag with the VID being the PVID of the interface and checks whether the VID is in the list of permitted VLAN IDs. If yes, permits the frame. If not, discards it. ▫ Tagged frame: checks whether the VID is in the list of permitted VLAN IDs. If yes, permits the frame. If not, discards it.	Frame receiving ▫ Untagged frame: adds a tag with the VID being the PVID of the interface and checks whether the VID is in the list of permitted VLAN IDs. If yes, permits the frame. If not, discards it. ▫ Tagged frame: checks whether the VID is in the list of permitted VLAN IDs. If yes, permits the frame. If not, discards it.
Frame sending ▫ Checks whether the VID in the tag of the frame is the same as the PVID of the interface. If they are the same, removes the tag and sends the frame out; otherwise, discards the frame.	Frame sending ▫ If the VID is in the list of permitted VLAN IDs and the same as the PVID of the interface, removes the tag and sends the frame out. ▫ If the VID is in the list of permitted VLAN IDs but different from the PVID of the interface, sends the frame out without removing the tag. ▫ If the VID is not in the list of permitted VLAN IDs, discards the frame.	Frame sending ▫ If the VID is not in the list of permitted VLAN IDs, discards the frame. ▫ If the VID is in the untagged VLAN ID list, removes the tag and sends the frame out. ▫ If the VID is in the tagged VLAN ID list, sends the frame out without removing the tag.

- The processes of adding and removing VLAN tags on interfaces are as follows:
  - Frame receiving:
    - After receiving an untagged frame, access, trunk, and hybrid interfaces all add a VLAN tag to the frame. Then, trunk and hybrid interfaces determine whether to permit the frame based on the VID of the frame (the frame is permitted only when the VID is a permitted VLAN ID), whereas an access interface permits the frame unconditionally.
    - After receiving a tagged frame, an access interface permits the frame only when the VID in the tag of the frame is the same as the PVID configured for the interface, while trunk and hybrid interfaces permit the frame only when the VID in the tag of the frame is in the list of permitted VLANs.
  - Frame sending:
    - Access interface: directly removes VLAN tags from frames before sending the frames.
    - Trunk interface: removes VLAN tags from frames only when the VIDs in the tags are the same as the PVID of the interface.
    - Hybrid interface: determines whether to remove VLAN tags from frames based on the interface configuration.
- Frames sent by an access interface are all untagged. On a trunk interface, only frames of one VLAN are sent without tags, and frames of other VLANs are all sent with tags. On a hybrid interface, you can specify the VLANs of which frames are sent with or without tags.

Contents

VLAN Planning

- **VLAN assignment rules**
  - By service: voice, video, and data VLANs
  - By department: e.g. VLANs for engineering, marketing, and financing departments
  - By application: e.g. VLANs for servers, offices, and classrooms
- **Tips for VLAN assignment**

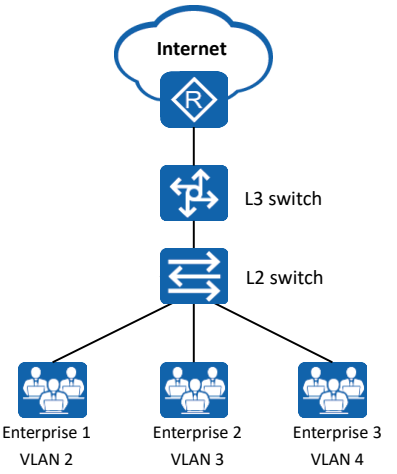
  VLAN IDs can be randomly assigned within the supported range. To improve VLAN ID continuity, you can associate VLAN IDs with subnets during VLAN assignment.
- **Example for VLAN planning**
  - Assume that there are three buildings: administrative building with offices, classrooms, and financing sections, teaching building with offices and classrooms, and office building with offices and financing sections. Each building has one access switch, and the core switch is deployed in the administrative building.
  - The following table describes the VLAN plan.

VLAN ID	IP Address Segment	Description
1	X.16.10.0/24	VLAN to which office users belong
2	X.16.20.0/24	VLAN to which the users of the financing department belong
3	X.16.30.0/24	VLAN to which classroom users belong
100	Y.16.100.0/24	VLAN to which the device management function belongs

- You are advised to assign consecutive VLAN IDs to ensure proper use of VLAN resources. The most common method is interface-based VLAN assignment.

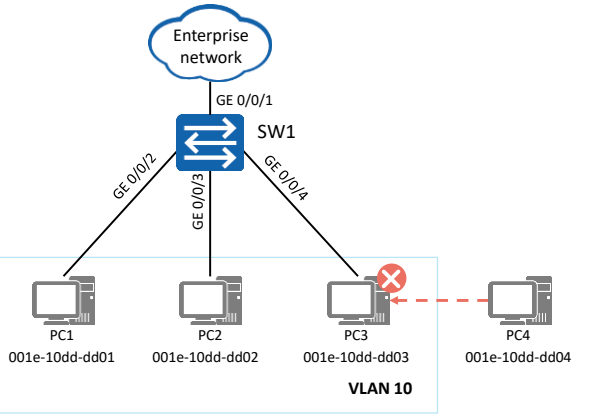
Interface-based VLAN Assignment

- Applicable scenario:
  - There are multiple enterprises in a building. These enterprises share network resources to reduce costs. Networks of the enterprises connect to different interfaces of the same Layer 2 switch and access the Internet through the same egress device.
- VLAN assignment:
  - To isolate the services of different enterprises and ensure service security, assign interfaces connected to the enterprises' networks to different VLANs. In this way, each enterprise has an independent network, and each VLAN works as a virtual work group.



MAC Address-based VLAN Assignment

- Applicable scenario:
  - The network administrator of an enterprise assigns PCs in the same department to the same VLAN. To improve information security, the enterprise requires that only employees in the specified department be allowed to access specific network resources.
- VLAN assignment:
  - To meet the preceding requirement, configure MAC address-based VLAN assignment on SW1, preventing new PCs connected to the network from accessing the network resources.



Contents

Basic VLAN Configuration Commands

1. Create one or more VLANs.

[Huawei] **vlan** *vlan-id*

This command creates a VLAN and displays the VLAN view. If the VLAN to be created already exists, this command directly displays the VLAN view.

- The value of *vlan-id* is an integer ranging from 1 to 4094.

[Huawei] **vlan batch** { *vlan-id1* [**to** *vlan-id2*] }

This command creates VLANs in a batch. In this command:

- **batch**: creates VLANs in a batch.
- *vlan-id1*: specifies a start VLAN ID.
- *vlan-id2*: specifies an end VLAN ID.

- The **vlan** command creates a VLAN and displays the VLAN view. If the VLAN to be created already exists, this command directly displays the VLAN view.
- The **undo vlan** command deletes a VLAN.
- By default, all interfaces are added to the default VLAN with the ID of 1.
- Commands:
  - **vlan** *vlan-id*
    - *vlan-id*: specifies a VLAN ID. The value is an integer ranging from 1 to 4094.
  - **vlan batch** { *vlan-id1* [**to** v*lan-id2*] }
    - **batch**: creates VLANs in a batch.
    - *vlan-id1* [**to** v*lan-id2*]: specifies the IDs of VLANs to be created in a batch.
      - *vlan-id1*: specifies a start VLAN ID.
      - *vlan-id2*: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*. The two parameters work together to define a VLAN range.
    - If you do not specify **to** v*lan-id2*, the command creates only one VLAN with the ID being specified using *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.

Basic Access Interface Configuration Commands

1. Set the link type of an interface.

   [Huawei-GigabitEthernet0/0/1] **port link-type access**

   In the interface view, set the link type of the interface to access.

2. Configure a default VLAN for the access interface.

   [Huawei-GigabitEthernet0/0/1] **port default vlan** *vlan-id*

   In the interface view, configure a default VLAN for the interface and add the interface to the VLAN.
   - *vlan-id:* specifies an ID for the default VLAN. The value is an integer ranging from 1 to 4094.

Basic Trunk Interface Configuration Commands

1. Set the link type of an interface.

   [Huawei-GigabitEthernet0/0/1] **port link-type trunk**

   In the interface view, set the link type of the interface to trunk.

2. Add the trunk interface to specified VLANs.

   [Huawei-GigabitEthernet0/0/1] **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }

   In the interface view, add the trunk interface to specified VLANs.

3. (Optional) Configure a default VLAN for the trunk interface.

   [Huawei-GigabitEthernet0/0/1] **port trunk pvid vlan** *vlan-id*

   In the interface view, configure a default VLAN for the trunk interface.

- Command: **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] | **all** }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the IDs of VLANs to which a trunk interface needs to be added.
    - *vlan-id1*: specifies a start VLAN ID.
    - *vlan-id2*: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.
  - **all**: adds a trunk interface to all VLANs.
- The **port trunk pvid vlan** *vlan-id* command configures a default VLAN for a trunk interface.
  - *vlan-id*: specifies the ID of the default VLAN to be created for a trunk interface. The value is an integer ranging from 1 to 4094.

Basic Hybrid Interface Configuration Commands

1. Set the link type of an interface.

   [Huawei-GigabitEthernet0/0/1] **port link-type hybrid**

   In the interface view, set the link type of the interface to hybrid.

2. Add the hybrid interface to specified VLANs.

   [Huawei-GigabitEthernet0/0/1] **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }

   In the interface view, add the hybrid interface to specified VLANs in untagged mode.

   [Huawei-GigabitEthernet0/0/1] **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }

   In the interface view, add the hybrid interface to specified VLANs in tagged mode.

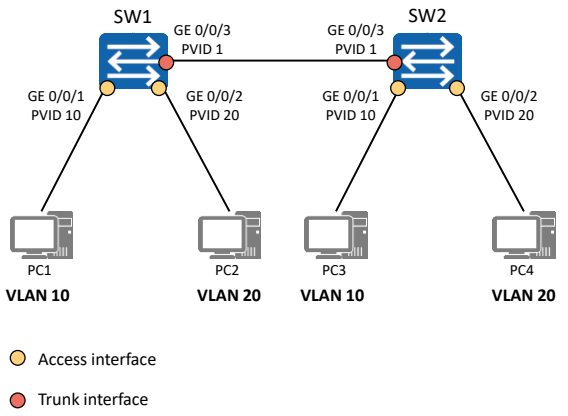
3. (Optional) Configure a default VLAN for the hybrid interface.

   [Huawei-GigabitEthernet0/0/1] **port hybrid pvid vlan** *vlan-id*

   In the interface view, configure a default VLAN for the hybrid interface.

- Command: **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the IDs of VLANs to which a hybrid interface needs to be added.
    - *vlan-id1*: specifies a start VLAN ID.
    - vlan-id2: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.
  - **all**: adds a hybrid interface to all VLANs.
- Command: **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the IDs of VLANs to which a hybrid interface needs to be added.
    - *vlan-id1*: specifies a start VLAN ID.
    - vlan-id2: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.
  - **all**: adds a hybrid interface to all VLANs.
- The **port hybrid pvid vlan** *vlan-id* command configures a default VLAN for a hybrid interface.
  - *vlan-id*: specifies the ID of the default VLAN to be created for a hybrid interface. The value is an integer ranging from 1 to 4094.

Case1:Configuring Interface-based VLAN Assignment

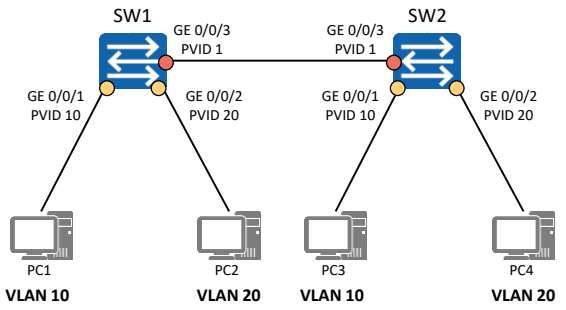


- Networking requirements:
  - On the network shown in the left figure, the switches (SW1 and SW2) of an enterprise are connected to multiple PCs, and PCs with the same services access the network using different devices. To ensure communication security, the enterprise requires that only PCs with the same service can directly communicate.
  - To meet this requirement, configure interface-based VLAN assignment on the switches and add interfaces connected to PCs with the same service to the same VLAN. In this way, PCs in different VLANs cannot directly communicate at Layer 2, but PCs in the same VLAN can directly communicate.

Configuration roadmap:

- Create VLANs and add interfaces connected to PCs to the VLANs to isolate Layer 2 traffic between PCs with different services.
- Configure interface types and specify permitted VLANs for SW1 and SW2 to allow PCs with the same service to communicate through SW1 and SW2.

Creating VLANs

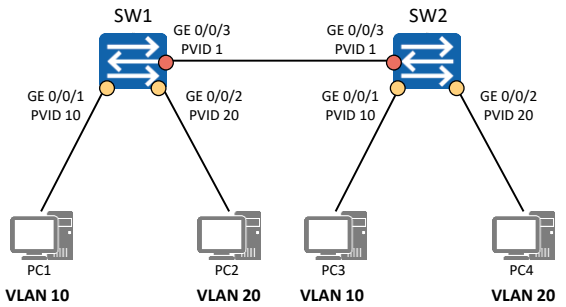


Create VLANs.

```
[SW1] vlan 10
[SW1-vlan10] quit
[SW1] vlan 20
[SW1-vlan20] quit
```

```
[SW2] vlan batch 10 20
```

Configuring Access and Trunk Interfaces



Configure access interfaces and add the interfaces to corresponding VLANs.

```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
```

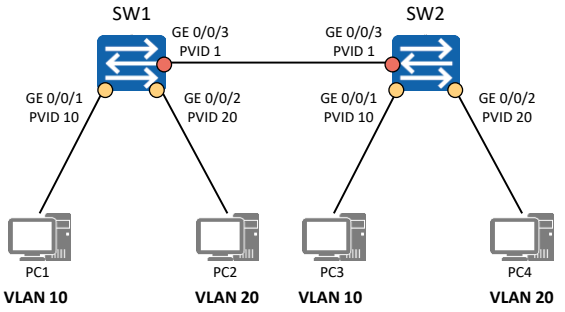
```
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1] vlan 20
[SW1-vlan20] port GigabitEthernet0/0/2
[SW1-vlan20] quit
```

Configure a trunk interface and specify a list of VLAN IDs permitted by the interface.

```
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk pvid vlan 1
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
```

Note: The configuration on SW2 is similar to that on SW1.

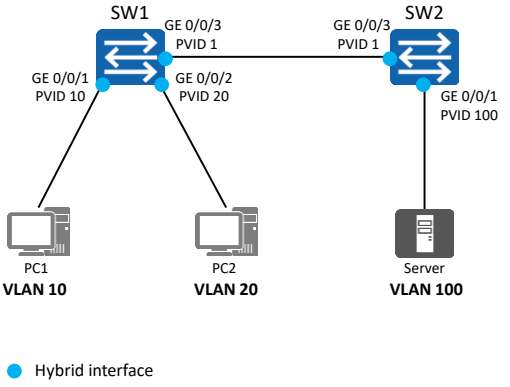
Verifying the Configuration




```
[SW1]display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;         D: Down;                TG: Tagged;    UT: Untagged;
MP: Vlan-mapping;                      ST: Vlan-stacking;
#: ProtocolTransparent-vlan;  *: Management-vlan;
--------------------------------------------------------------------------------
VID        Type        Ports
--------------------------------------------------------------------------------
1          common      UT:GE0/0/3(U)                    .....
10         common      UT:GE0/0/1(U)
                       TG:GE0/0/3(U)
20         common      UT:GE0/0/2(U)
                       TG:GE0/0/3(U)
.....
```


- Command: The **display vlan** command displays VLAN information.
- Command output:
  - **Tagged/Untagged**: Interfaces are manually added to VLANs in tagged or untagged mode.
  - **VID** or **VLAN ID**: VLAN ID.
  - **Type** or **VLAN Type**: VLAN type. The value **common** indicates a common VLAN.
  - **Ports**: interfaces added to VLANs.

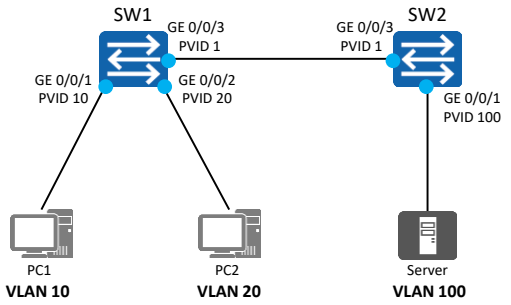
Case2:Configuring Interface-based VLAN Assignment



- Networking requirements:
  - On the network shown in the left figure, the switches (SW1 and SW2) of an enterprise are connected to multiple PCs, and PCs in different departments need to access the server of the enterprise. To ensure communication security, the enterprise requires that PCs in different departments cannot directly communicate.
  - To meet this requirement, configure interface-based VLAN assignment and hybrid interfaces on the switches to enable PCs in different departments to access the server but disable them from directly communicating at Layer 2.

- Configuration roadmap:
  - Create VLANs and add interfaces connected to PCs to the VLANs to isolate Layer 2 traffic between PCs with different services.
  - Configure interface types and specify permitted VLANs for SW1 and SW2 to allow PCs to communicate with the server through SW1 and SW2.

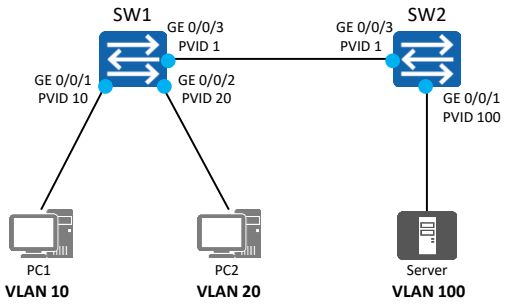
Configuring Hybrid Interfaces (1)



SW1 configuration:

```
[SW1] vlan batch 10 20 100
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SW1-GigabitEthernet0/0/1] port hybrid untagged vlan 10 100
[SW1-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type hybrid
[SW1-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[SW1-GigabitEthernet0/0/2] port hybrid untagged vlan 20 100
[SW1-GigabitEthernet0/0/2] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type hybrid
[SW1-GigabitEthernet0/0/3] port hybrid tagged vlan 10 20 100
```

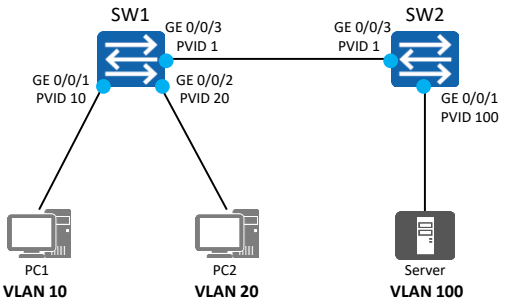
Configuring Hybrid Interfaces (2)



SW2 configuration:

```
[SW2] vlan batch 10 20 100
[SW2] interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1] port link-type hybrid
[SW2-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SW2-GigabitEthernet0/0/1] port hybrid untagged vlan 10  20 100
[SW2-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3] port link-type hybrid
[SW2-GigabitEthernet0/0/3] port hybrid tagged vlan 10 20 100
```

Verifying the Configuration




```
[SW1]display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;                TG: Tagged;    UT: Untagged;
MP: Vlan-mapping;                      ST: Vlan-stacking;
#: ProtocolTransparent-vlan;  *: Management-vlan;
--------------------------------------------------------------------------------
VID         Type        Ports
--------------------------------------------------------------------------------
1           common      UT:GE0/0/1(U)     GE0/0/2(U)     GE0/0/3(U) .....
10          common      UT:GE0/0/1(U)
                        TG:GE0/0/3(U)
20          common      UT:GE0/0/2(U)
                        TG:GE0/0/3(U)
100         common      UT:GE0/0/1(U)     GE0/0/2(U)
                        TG:GE0/0/3(U)
.....
```

Basic VLAN Configuration Commands

1. Associate a MAC address with a VLAN.

   [Huawei-vlan10] **mac-vlan mac-address** *mac-address* [*mac-address-mask* | *mac-address-mask-length*]

   This command associates a MAC address with a VLAN.
   - *mac-address*: specifies the MAC address to be associated with a VLAN. The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits, such as 00e0 or fc01. If an H contains less than four digits, the left-most digits are padded with zeros. For example, e0 is displayed as 00e0. The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or any multicast address.
   - *mac-address-mask*: specifies the mask of a MAC address. The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
   - *mac-address-mask-length*: specifies the mask length of a MAC address. The value is an integer ranging from 1 to 48.

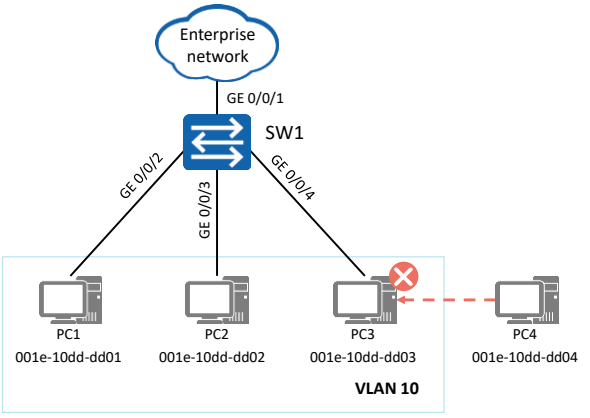
2. Enable MAC address-based VLAN assignment on an interface.

   [Huawei-GigabitEthernet0/0/1] **mac-vlan enable**

   This command enables MAC address-based VLAN assignment on an interface.

- Command: **mac-vlan mac-address** *mac-address* [*mac-address-mask* | *mac-address-mask-length*]
  - *mac-address*: specifies the MAC address to be associated with a VLAN.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits, such as 00e0 or fc01. If an H contains less than four digits, the left-most digits are padded with zeros. For example, e0 is displayed as 00e0.
    - The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or any multicast address.
  - *mac-address-mask*: specifies the mask of a MAC address.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
  - *mac-address-mask-length*: specifies the mask length of a MAC address.
    - The value is an integer ranging from 1 to 48.
- The **mac-vlan enable** command enables MAC address-based VLAN assignment on an interface.

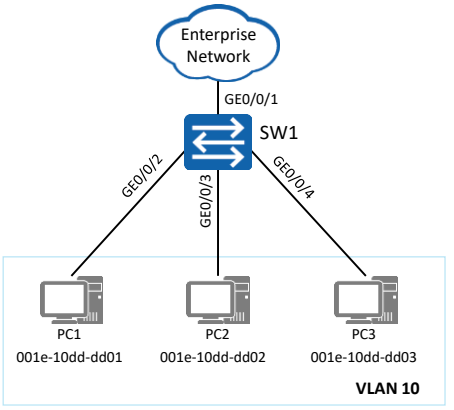
Example for Configuring MAC Address-based VLAN Assignment



- Networking requirements:
  - The network administrator of an enterprise assigns PCs in the same department to the same VLAN. To improve information security, the enterprise requires that only employees in the department be allowed to access the network resources of the enterprise.
  - PCs 1 through 3 belong to the same department. According to the enterprise' requirement, only the three PCs can access the enterprise network through SW1.
  - To meet this requirement, configure MAC address-based VLAN assignment and associate the MAC addresses of the three PCs with the specified VLAN.

- Configuration roadmap:
  - Create a VLAN, for example, VLAN 10.
  - Add Ethernet interfaces on SW1 to the VLAN.
  - Associate the MAC addresses of PCs 1 through 3 with the VLAN.

Creating a VLAN and Associating MAC Addresses with the VLAN



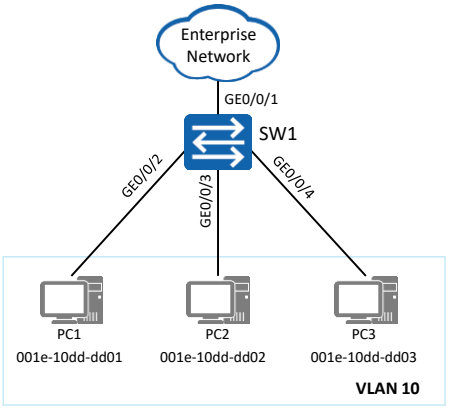
Create a VLAN.

```
[SW1] vlan 10
[SW1-vlan10] quit
```

Associate MAC addresses with the VLAN.

```
[SW1] vlan 10
[SW1-vlan10] mac-vlan mac-address 001e-10dd-dd01 [SW1-vlan10]
mac-vlan mac-address 001e-10dd-dd02 [SW1-vlan10] mac-vlan
mac-address 001e-10dd-dd03 [SW1-vlan10] quit
```

Adding Interfaces to the VLAN and Enabling MAC Address-based VLAN Assignment



Add interfaces to the VLAN.

```
[SW1] interface gigabitethernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid tagged vlan 10

[SW1] interface gigabitethernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type hybrid
[SW1-GigabitEthernet0/0/2] port hybrid untagged vlan 10
```

Enable MAC address-based VLAN assignment on the specified interface.

```
[SW1] interface gigabitethernet 0/0/2
[SW1-GigabitEthernet0/0/2] mac-vlan enable
[SW1-GigabitEthernet0/0/2] quit
```

Note: The configuration of GE 0/0/3 and GE 0/0/4 is similar to that of GE 0/0/2.

- On access and trunk interfaces, MAC address-based VLAN assignment can be used only when the MAC address-based VLAN is the same as the PVID. It is recommended that MAC address-based VLAN assignment be configured on hybrid interfaces.

Verifying the Configuration

```
[SW1]display vlan
The total number of vlans is : 2
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;    UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;  *: Management-vlan;
--------------------------------------------------------------------------------
VID        Type        Ports
--------------------------------------------------------------------------------
1          common      UT:GE0/0/1(U)              GE0/0/2(U)    GE0/0/3(U) .....
10         common      UT:GE0/0/2(U)              GE0/0/3(U)    GE0/0/4(U)
                       TG:GE0/0/1(U)
.....
```

```
[SW1]display mac-vlan mac-address all
--------------------------------------------------------------------------------
MAC Address  MASK           VLAN       Priority
--------------------------------------------------------------------------------
001e-10dd-dd01               ffff-ffff-ffff  10         0
001e-10dd-dd02               ffff-ffff-ffff  10         0
001e-10dd-dd03               ffff-ffff-ffff  10         0

Total MAC VLAN address count: 3
```


- Command: The **display mac-vlan** { **mac-address** { **all** | *mac-address* [*mac-address-mask* | *mac-address-mask-length*] } | **vlan** *vlan-id* } command displays the configuration of MAC address-based VLAN assignment.
  - **all**: displays all VLANs associated with MAC addresses.
  - **mac-address** *mac-address*: displays the VLAN associated with a specified MAC address.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
  - *mac-address-mask*: specifies the mask of a MAC address.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
  - *mac-address-mask-length*: specifies the mask length of a MAC address.
    - The value is an integer ranging from 1 to 48.
  - **vlan** *vlan-id*: specifies a VLAN ID.
    - The value is an integer ranging from 1 to 4094.
- Command output:
  - **MAC Address**: MAC address
  - **MASK**: mask of a MAC address
  - **VLAN**: ID of the VLAN associated with a MAC address
  - **Priority**: 802.1p priority of the VLAN associated with a MAC address

Quiz

1. (Multiple) Which of the following statements about the VLAN technology are incorrect? ( )
   A. The VLAN technology can isolate a large collision domain into several small collision domains.
   B. The VLAN technology can isolate a large Layer 2 broadcast domain into several small Layer 2 broadcast domains.
   C. PCs in different VLANs cannot communicate.
   D. PCs in the same VLAN can communicate at Layer 2.
2. If the PVID of a trunk interface is 5 and the port trunk allow-pass vlan 2 3 command is run on the interface, which VLANs' frames can be transmitted through the trunk interface?

1. AC
2. After the **port trunk allow-pass vlan 2 3** command is run, the frames of VLAN 5 cannot be transmitted through the trunk interface. By default, the frames of VLAN 1 can be transmitted through the trunk interface. Therefore, the frames of VLANs 1 through 3 can all be transmitted through the interface.

Summary

- This course describes the VLAN technology, including the functions, identification, assignment, data exchange, planning, application, and basic configuration of VLANs.
- The VLAN technology can divide a physical LAN into multiple broadcast domains so that network devices in the same VLAN can directly communicate at Layer 2, while devices in different VLANs cannot.


Thank You
www.huawei.com