VLAN Principles and Configuration

1 VLAN Principles and Configuration

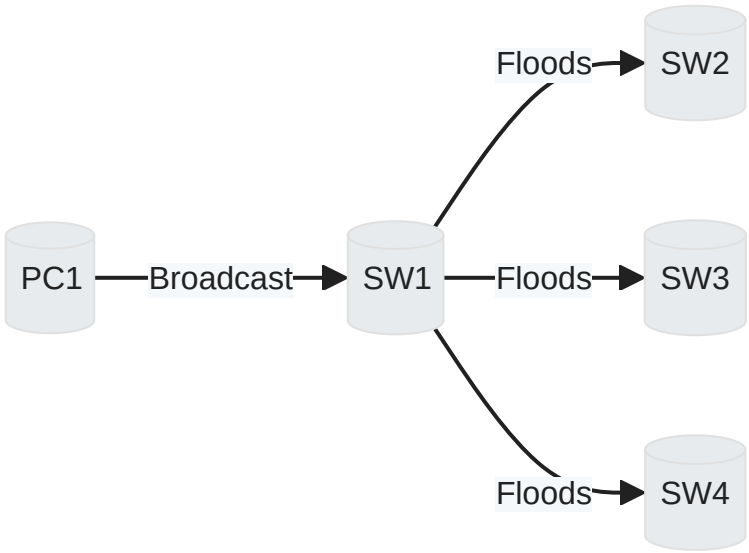
1.1 What Is VLAN

1.1.1 Broadcast Domains

> In a typical switching network, all devices receive broadcasts sent by any single device.

1.1.1.1 Issues with Large Broadcast Domains

- Increased **junk traffic** (unnecessary data packets that consume bandwidth).
- Higher potential for **network security** breaches.
- Reduced network efficiency due to too much broadcasts.



1.1.2 VLANs (Virtual Local Area Networks)

1.1.2.1 Purpose of VLANs

- To segment large broadcast domains into smaller ones.
- To improve **security**, reduce **junk traffic**, and Save network resources.

1.1.2.2 Characteristics of VLANs

- Each VLAN creates its own broadcast domain.
- Devices in the same VLAN can communicate at Layer 2; different VLANs require Layer 3 communication.
- VLAN assignments are geographically independent, allowing flexible network design.

1.1.2.3 Advantages of Using VLAN Technology

Advantage	Description
Flexible groups	Allows terminals in different locations to be part of the same network.
Bandwidth conservation	Limits broadcast traffic to within a single VLAN.
Enhanced security	Segregates traffic so that devices across VLANs cannot directly communicate at Layer 2.
Network robustness	Isolates faults within a single VLAN, preventing them from affecting other segments.

1.2 VLAN Principles

1.2.1 VLAN Identification

- **How VLANs are identified:** Through a 4-byte IEEE 802.1Q tag inserted into Ethernet frames.

> 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 Tag Components:**

Field	Description	Values
TPID	Identifies frame type	0x8100 for IEEE 802.1Q
PRI	Priority of frame (QoS)	0-7
CFI	Canonical format indicator	0 for Ethernet frames
VLAN ID	Identifies the VLAN	1 to 4094

> **Canonical format :** used for transmitting a MAC address in an Ethernet

> frame sends the least significant bit (rightmost bit) of each byte first.

> PCs cannot identify tagged frames and therefore can send or process only untagged frames. By contrast, all frames processed by switches are tagged ones

1.2.2 VLAN Assignment Methods

- **Interface-based:** Assigns based on switch interfaces.
- **MAC address-based:** Assigns based on source MAC addresses.
- **IP subnet-based:** Assigns based on source IP addresses/subnets.
- **Protocol-based:** Assigns based on frame protocol types.
- **Policy-based:** Uses a combination of methods.

1.2.2.1 Interface-Based VLAN Assignment

> - PVID (Port Default VLAN ID) is configured per switch interface.
> - Untagged frames received are assigned to the corresponding PVID.

Info

Default PVID is usually set to `1`. It must be reconfigured if PCs move to different ports.

1.2.2.2 MAC Address-Based VLAN Assignment

> A mapping table is maintained to assign VLANs based on source MAC addresses. This method allows port flexibility without needing reconfiguration.

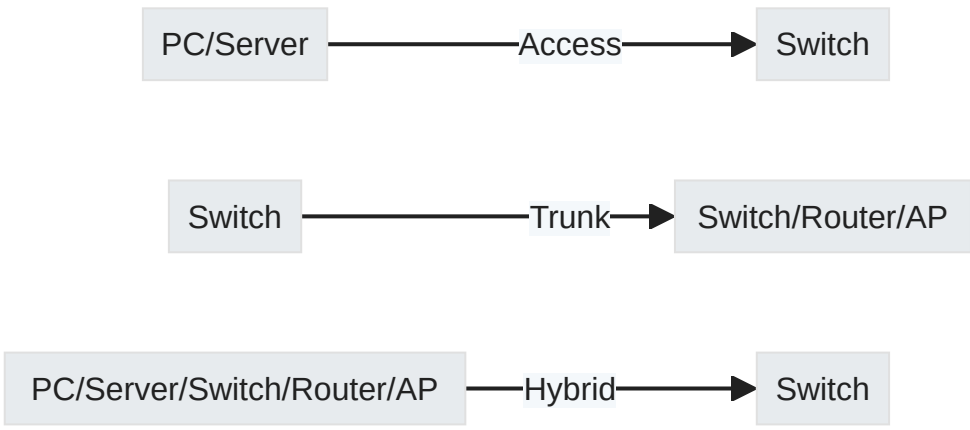
> ⚠ **Warning**
>
> Possible security risks due to potential MAC address spoofing.

1.2.3 Layer 2 Ethernet Interface Types

1.2.3.1 Overview

- Ethernet interfaces on switches can be categorized into three main types:
  - Access
  - Trunk
  - Hybrid

> Each type is designed to handle VLAN tagging and forwarding in different scenarios.



1.2.3.2 Access Interface

- Connects endpoints like PCs or servers to a switch.
- Carries untagged frames.
- Belongs to one VLAN only.

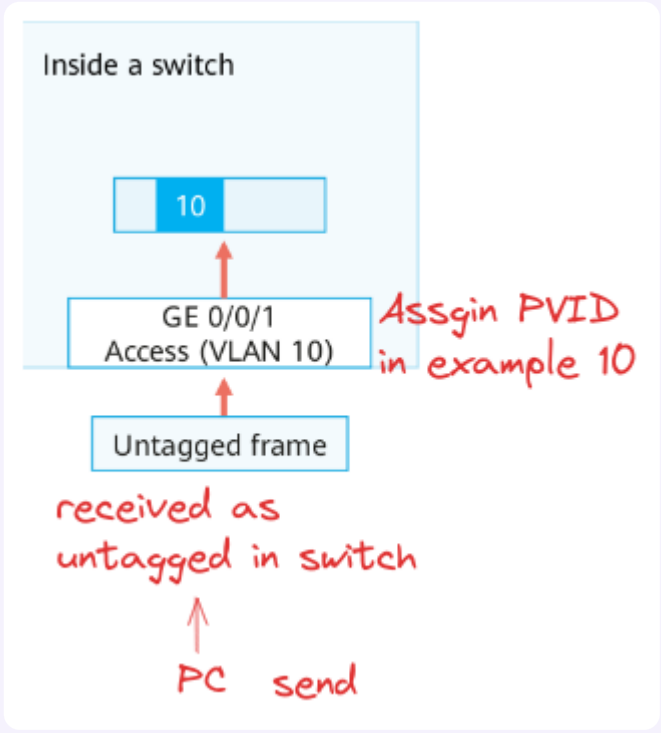
> Access interfaces are suitable for devices that do not recognize VLAN tags.

1.2.3.2.1 Frame Processing (Access)

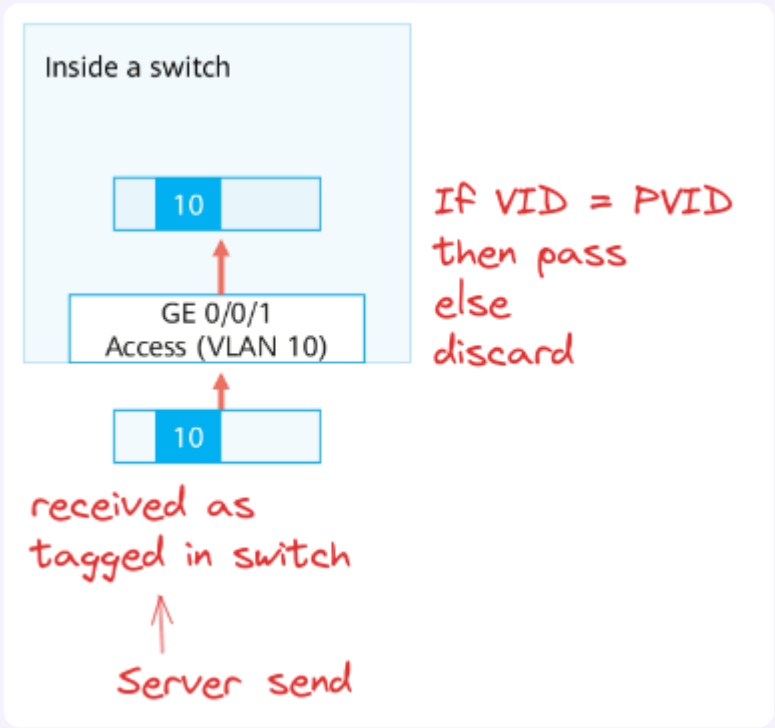
Action	Description
Receive (Untagged In)	If the incoming frame has no VLAN tag, the switch will assign it a default VLAN ID known as the Port VLAN ID (PVID).
Receive (Tagged In)	If the incoming frame has a VLAN tag, the switch will check if the tag's VLAN ID (VID) matches the PVID of that port. If they match, the frame is allowed; if not, it is discarded.
Send (Untagged Out)	When sending a frame out of an untagged port, it simply forwards the frame without any VLAN tag.
Send (Tagged Out)	When sending a frame out of a tagged port, if its VID matches the PVID of that port, the switch removes the tag before sending it out. If they don't match, then it discards the frame.

Example

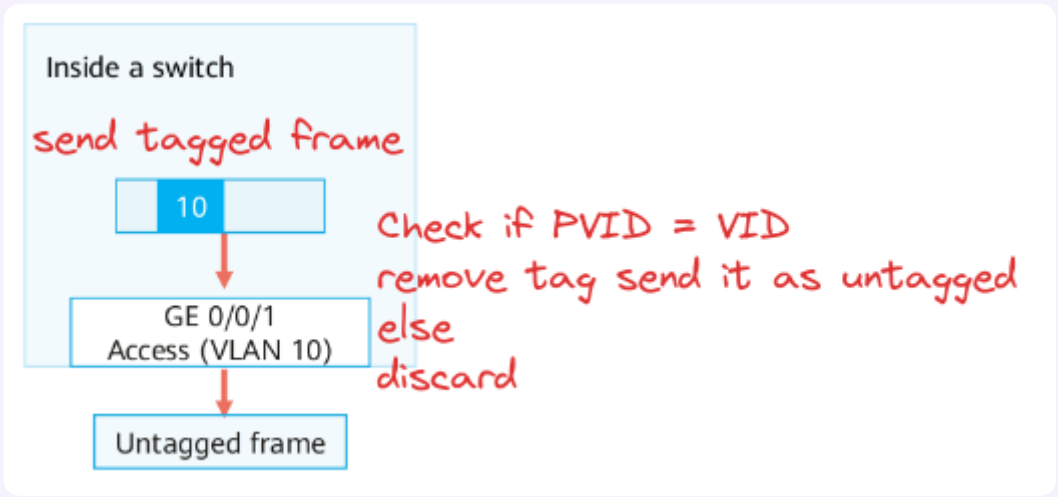
- **Receive (Untagged In):** A computer without VLAN configuration sends data to the switch, which assigns it to the default VLAN (PVID).



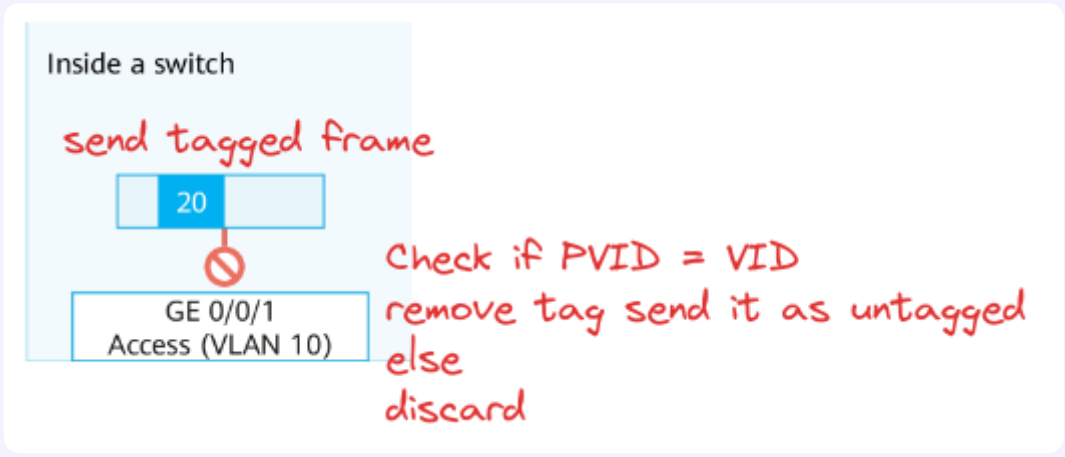
- **Receive (Tagged In):** A server sends data with a VLAN tag, and the switch checks if the tag matches the port's settings before accepting it.



- **Send (Untagged Out):** The switch sends data to a device like a printer that doesn't understand VLAN tags, so it removes any tag.(if the VID match the PVID)



- **Send (Tagged Out):** The switch forwards data with a VLAN tag to another switch, but removes the tag if that port is set to send untagged traffic only.



> **PVID** stands for Port VLAN ID: The default VLAN ID assigned to untagged frames that arrive on a port.
> **VID** stands for VLAN ID: The identifier for each Virtual Local Area Network.

1.2.3.3 Trunk Interface

- Connects switches or supports devices like routers that handle tagged frames.
- Carries multiple tagged VLANs using 802.1Q.

- Configured with a permitted VLAN list.

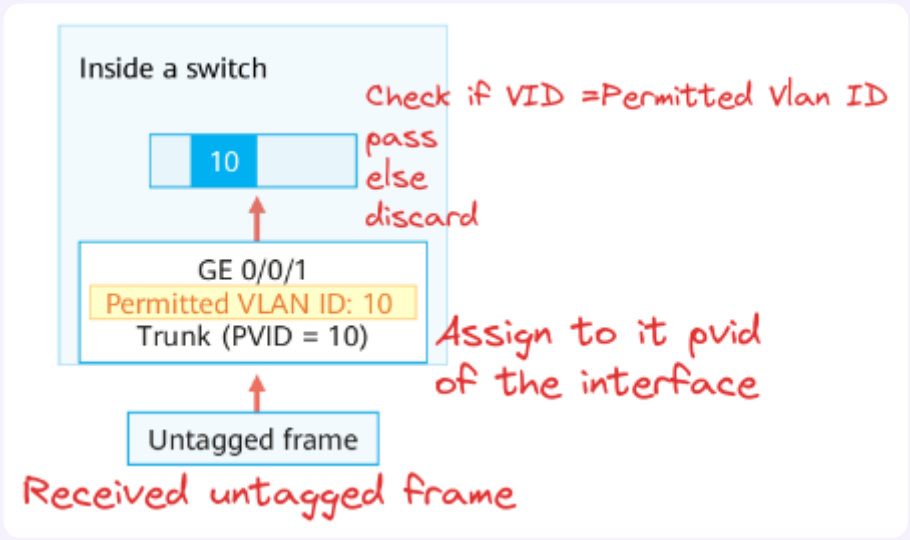
> Only allows frames if their VLAN ID is within the permitted list.

1.2.3.3.1 Frame Processing (Trunk)

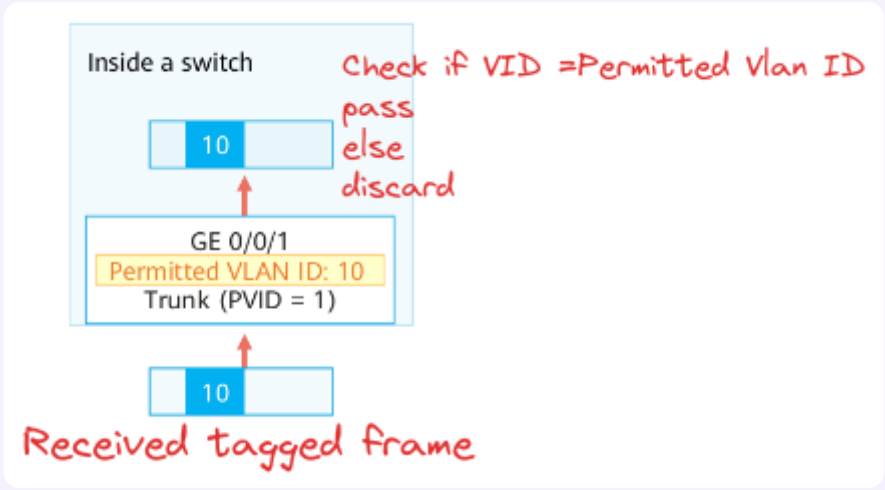
Action	Description
Receive (Untagged In)	Add a VLAN tag using the port's default VLAN ID (PVID) to untagged incoming frames. Decide to allow or block when the VID is in the list of VLAN IDs
Receive (Tagged In)	Check if incoming tagged frames are allowed on that port when the VID is in the list of VLAN IDs
Send (Untagged Out)	If the frame's VLAN ID matches the port's PVID, remove the VLAN tag before sending; otherwise, send as is (still tagged).
Send (Tagged Out)	Send tagged frames out of the port if their VLAN ID is permitted on that port. Frames with disallowed VLAN IDs are discarded.

Example

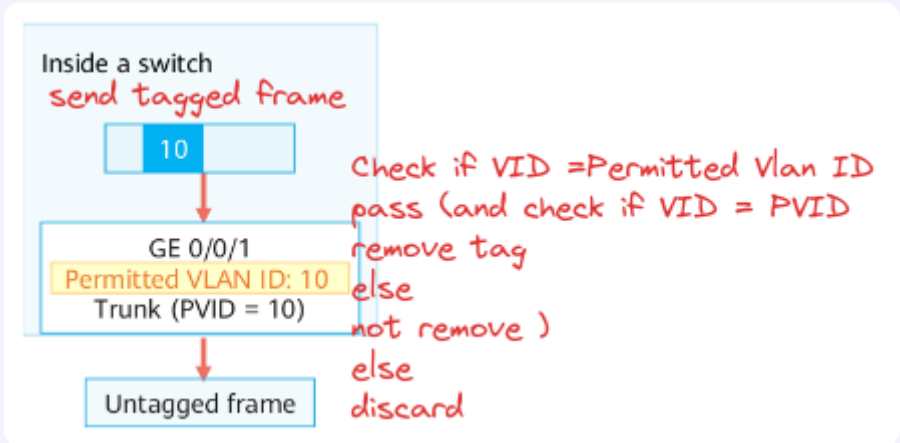
- **Receive (Untagged In):** A computer without VLAN configuration sends data to the switch, which adds the appropriate VLAN tag based on the switch port's (PVID).



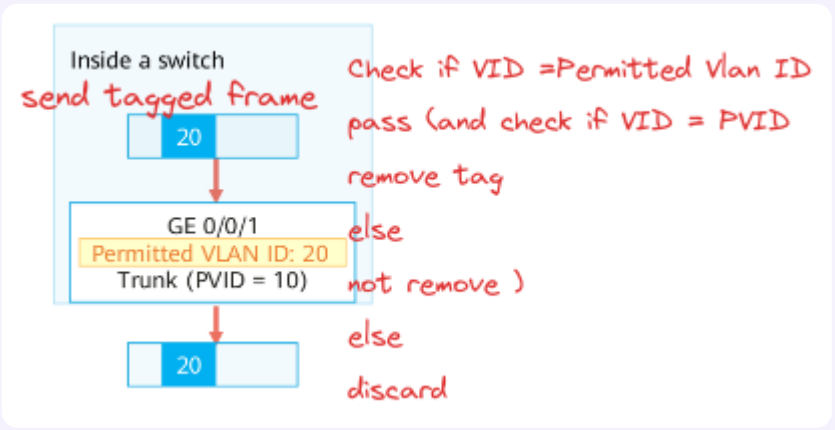
- **Receive (Tagged In):** A server sends data with a VLAN tag, and the switch checks if it should accept frames on that VLAN.



- **Send (Untagged Out):** The switch forwards data to a printer without a VLAN tag because the printer doesn't understand VLANs.



- **Send (Tagged Out):** The switch sends data with a VLAN tag to another switch that manages traffic for multiple VLANs.



1.2.3.4 Hybrid Interface

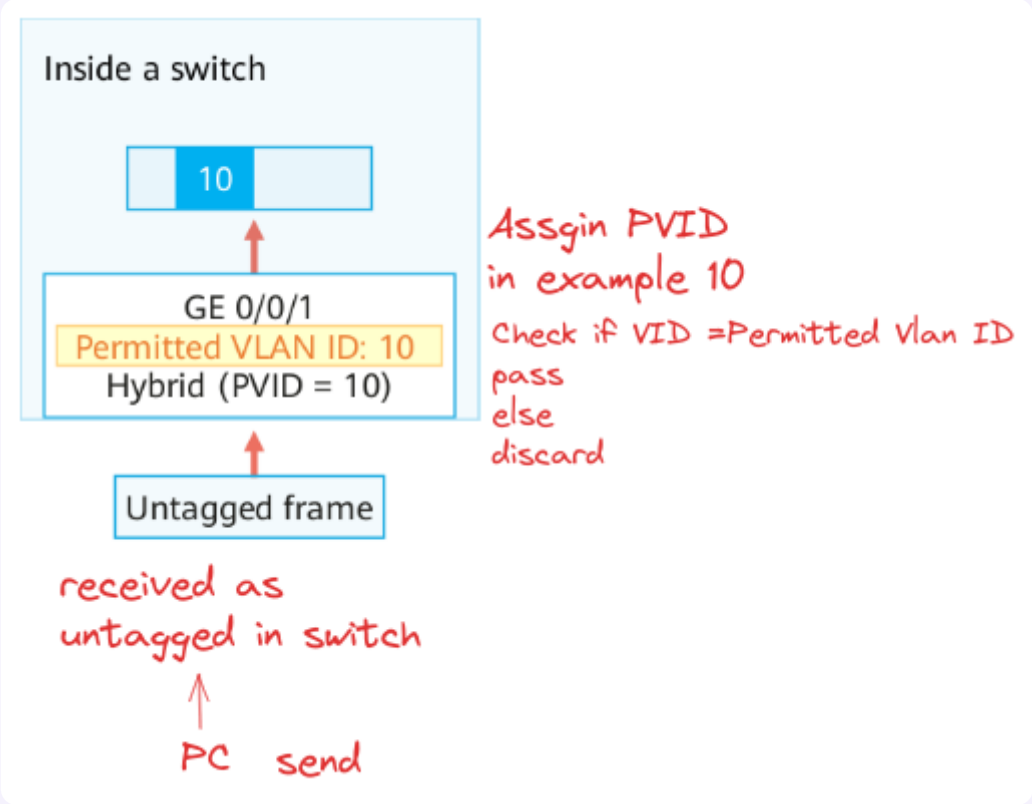
- Combines features of both access and trunk interfaces.
- Supports both tagged and untagged traffic across multiple VLANs.
- Configured with separate lists for tagged and untagged VLAN IDs.

1.2.3.4.1 Frame Processing (Hybrid)

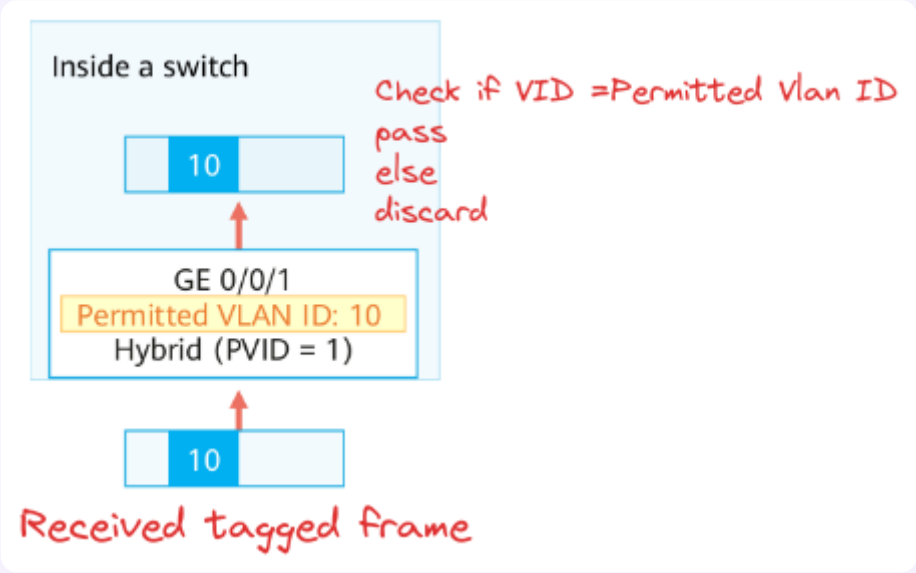
Action	Description
Receive (Untagged In)	When a frame without a VLAN tag arrives, the switch adds the default VLAN ID (PVID) to it. The frame's Acceptance is then determined when the VID is in the list of VLAN IDs otherwise discard
Receive (Tagged In)	If the VLAN ID of the frame is in the list of VLAN IDs permitted by the interface, the interface permits the frame. Otherwise, the interface discards the frame.
Send (Untagged Out)	If an interface allows a frame's VLAN ID and is set to not use VLAN tags, it will remove the tag before sending the frame.
Send (Tagged Out)	If the frame's VLAN ID is allowed by the interface and the interface is set to keep VLAN tags, then it sends the frame with its tag Whole.

Example

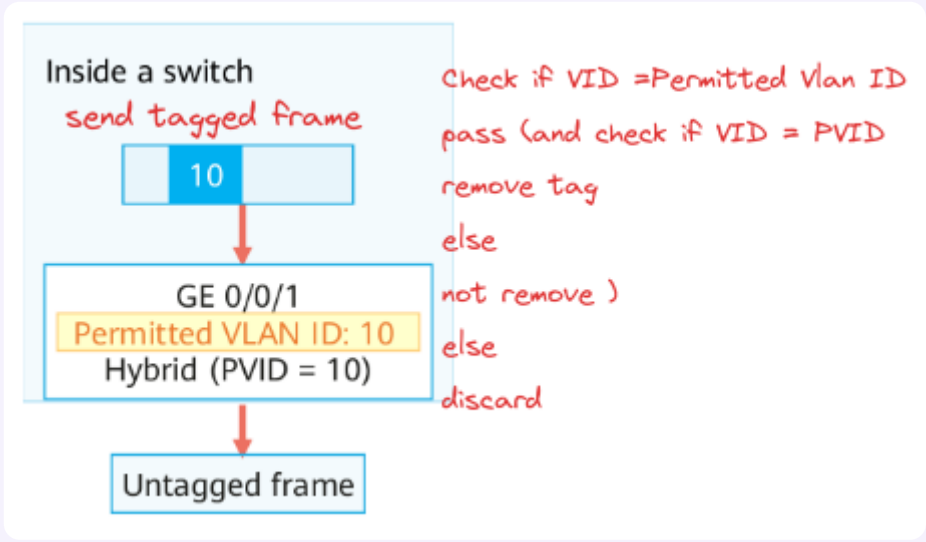
- **Receive (Untagged In):** A computer sends data without a VLAN tag, and the switch assigns its default VLAN to the data before processing.



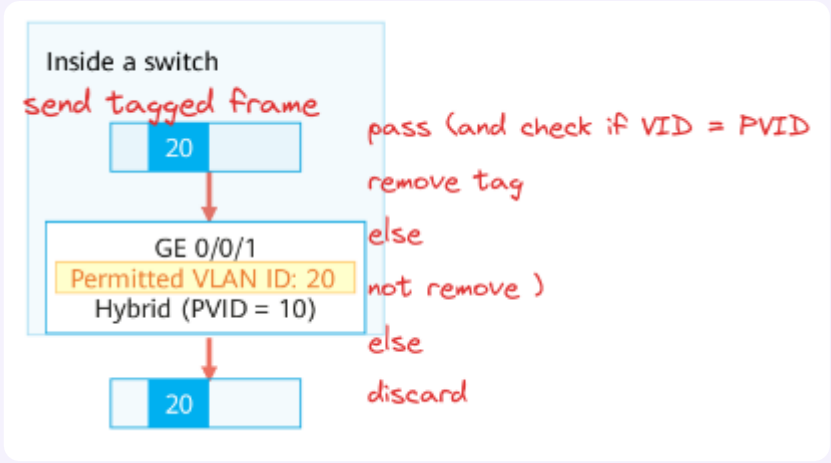
- **Receive (Tagged In):** A printer sends data with a VLAN tag, and the switch checks if it's allowed on that network; if not, the data is discarded.

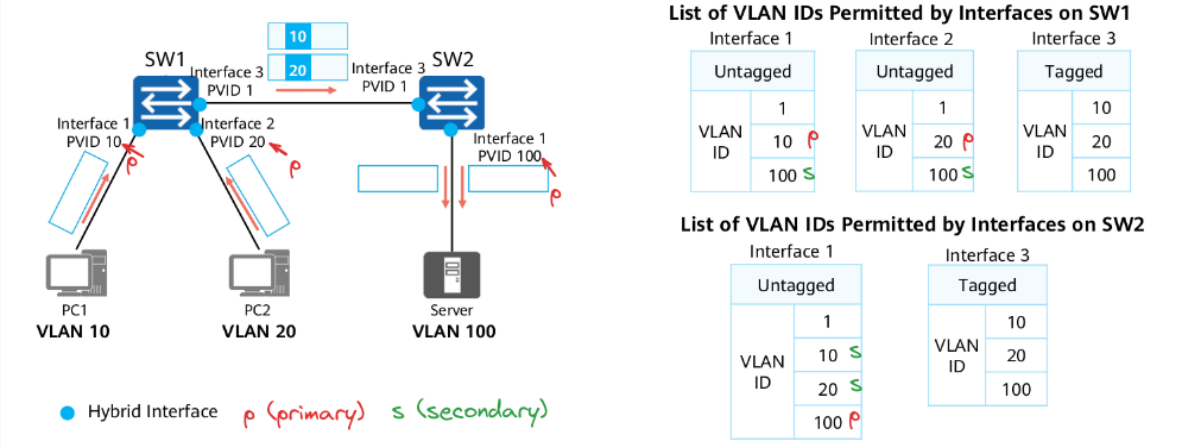


- **Send (Untagged Out):** A switch sends data to an older printer that doesn't understand VLAN tags, so it removes the tag before sending.



- **Send (Tagged Out):** A switch forwards data with its VLAN tag intact to another switch that also manages VLANs.





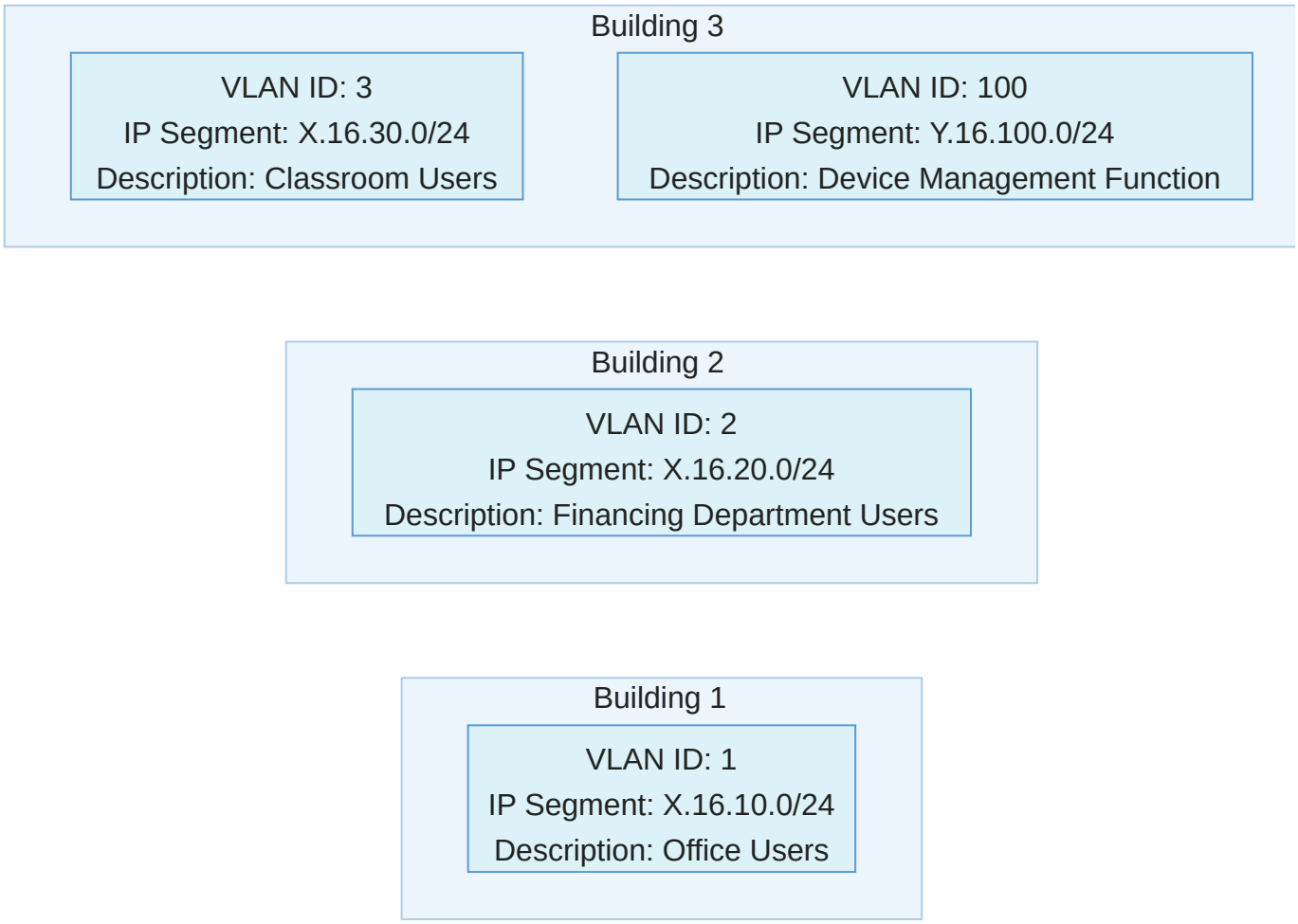
1.3 VLAN Applications

> **Tip**
>
> - **By Service**
>   - `Voice`, `Video`, and `Data` services should have separate VLANs to enhance performance and security.
> - **By Department**
>   - Departments such as `Engineering`, `Marketing`, and `Financing` should have distinct VLANs for data segmentation.
> - **By Application**
>   - Applications or areas such as `Servers`, `Offices`, and `Classrooms` can be grouped into dedicated VLANs.

1.3.1 Example of VLAN Planning

VLAN ID	IP Address Segment	Description
1	X.16.10.0/24	Office Users
2	X.16.20.0/24	Financing Department Users
3	X.16.30.0/24	Classroom Users
100	Y.16.100.0/24	Device Management Function

> **Scenario:** Three buildings with different sections assigned to specific VLANs based on purpose and location.



> In this scenario, each building is connected through its respective access switch to the core switch located in the administrative building.

1.4 VLAN Configuration Examples

1.4.1 Basic Commands

1.4.1.1 Creating VLANs

- `[Huawei] vlan <vlan-id>` : Create a single VLAN.
- `[Huawei] vlan batch <vlan-id1> [to <vlan-id2>]` : Create multiple VLANs in a batch.

> VLAN IDs range from 1 to 4094.

> By default, all interfaces are added to the default VLAN with the ID of 1.

1.4.1.2 Deleting VLANs

- `[Huawei] undo vlan <vlan-id>` : Delete a specific VLAN.

1.4.1.3 Display VLANS

- Display current VLANS: `[Huawei] display vlan`

```
[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)
.....
```

1.4.2 Interface-based VLAN Assignment

1.4.2.1 Access Interface Configuration

- `[Huawei-GigabitEthernet0/0/1] port link-type access` : set the link type of the interface to access.
- `[Huawei-GigabitEthernet0/0/1] port default vlan <vlan-id>` : configure a default VLAN for the interface

1.4.2.2 Trunk Interface Configuration

- `[Huawei-GigabitEthernet0/0/1] port link-type trunk` : set the link type of the interface to trunk.
- `[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan { <vlan-id1> to <vlan-id2> } || all` : add the trunk interface to specified VLANs.
- `[Huawei-GigabitEthernet0/0/1] port trunk pvid vlan <vlan-id>` : configure a default VLAN for the trunk interface.

1.4.2.3 Hybrid Interface Configuration

- `[Huawei-GigabitEthernet0/0/1] port link-type hybrid` : set the link type of the interface to hybrid.
- `[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan { <vlan-id1> to <vlan-id2> } || all` : dd the hybrid interface to specified VLANs in untagged mode.
- `[Huawei-GigabitEthernet0/0/1] port hybrid tagged vlan { <vlan-id1> to <vlan-id2> } || all` : add the hybrid interface to specified VLANs in tagged mode.
- `[Huawei-GigabitEthernet0/0/1] port hybrid pvid vlan <vlan-id>` : configure a default VLAN for the hybrid interface.

1.4.3 MAC Address-based VLAN Assignment

1.4.3.1 Associating MAC with a VLAN

- `[Huawei-vlan10] mac-vlan mac-address <mac-address> <mac-address-mask> || <mac-address-mask-length>` : Associate MAC address with a specific VLAN.

> - **mac-address:** 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.

1.4.3.2 Enabling MAC-based Assignment on an Interface

- `[Huawei-GigabitEthernet0/0/1] mac-vlan enable` : Enable MAC address-based assignment on an interface.

1.4.3.3 Display MAC-VLAN

- Display MAC-VLAN associations: `[Huawei] display mac-vlan mac-address all`

```
[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
```