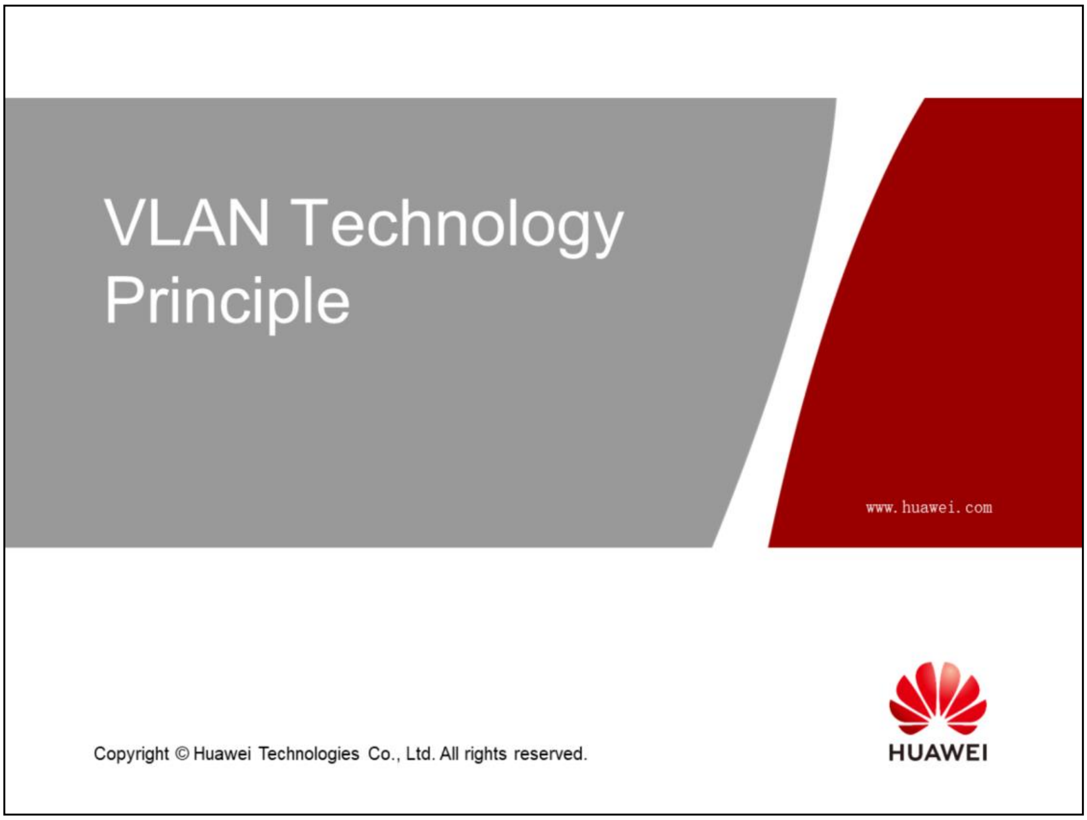
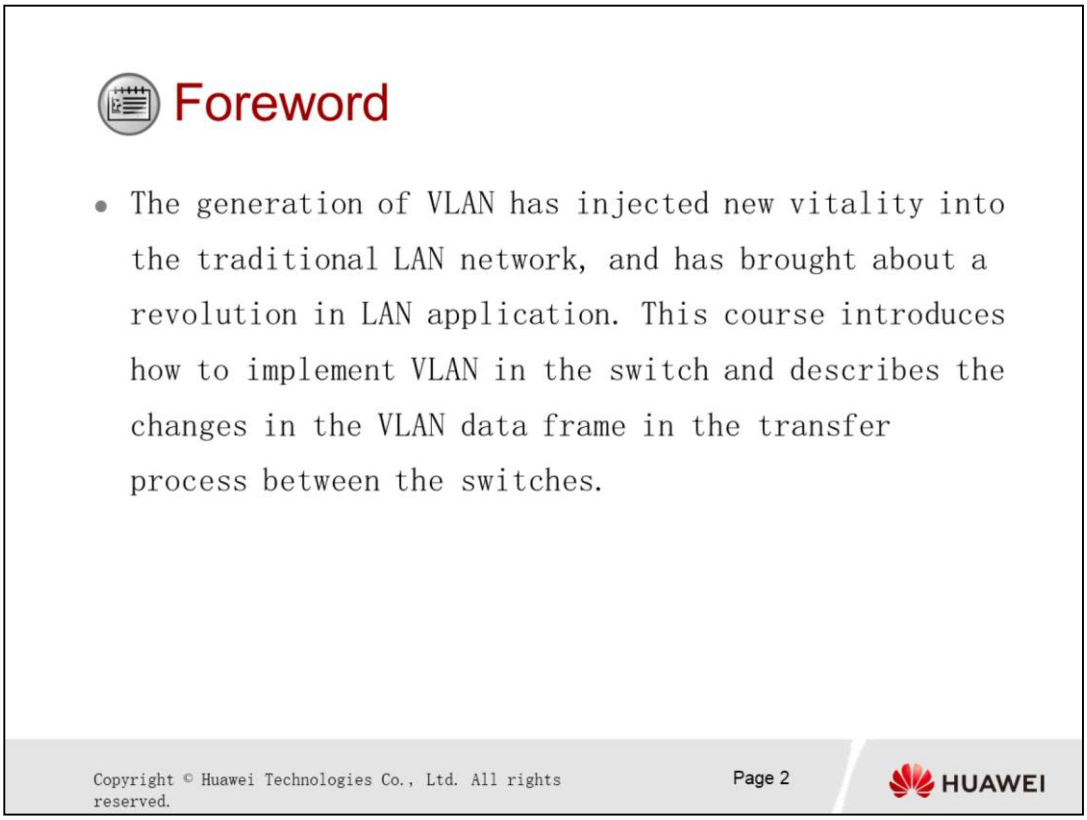


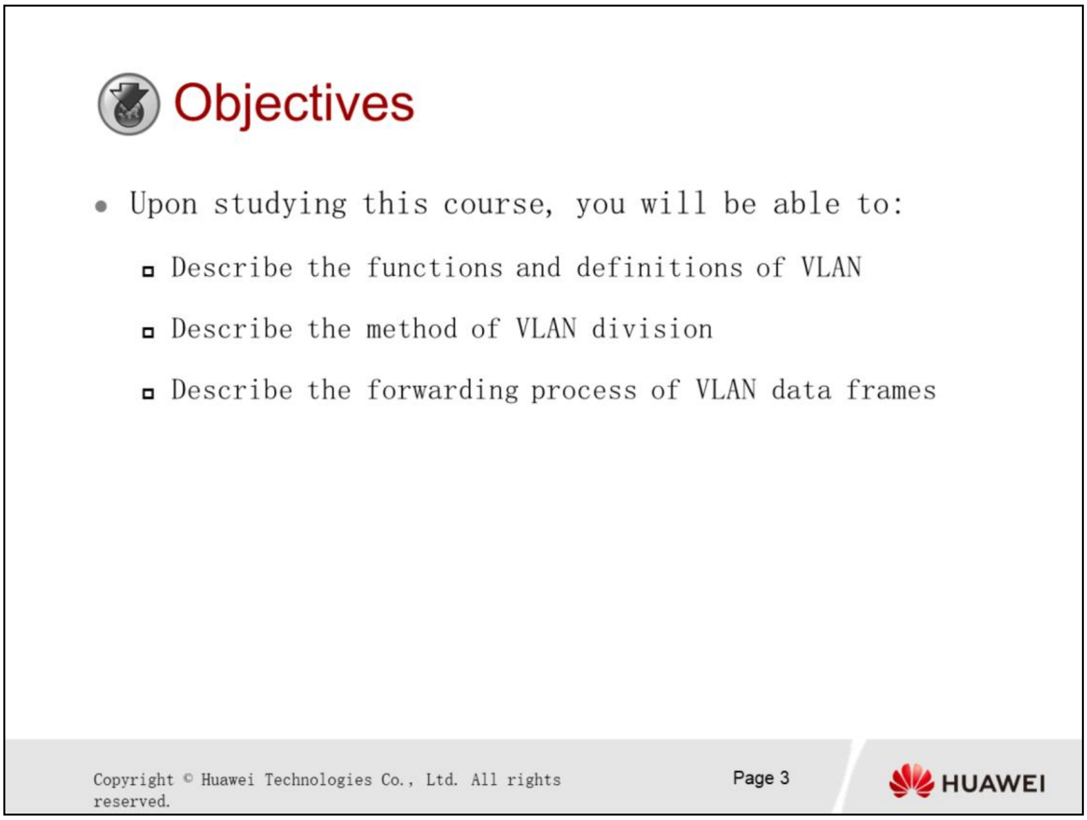
VLAN Technology Principle

www.huawei.com



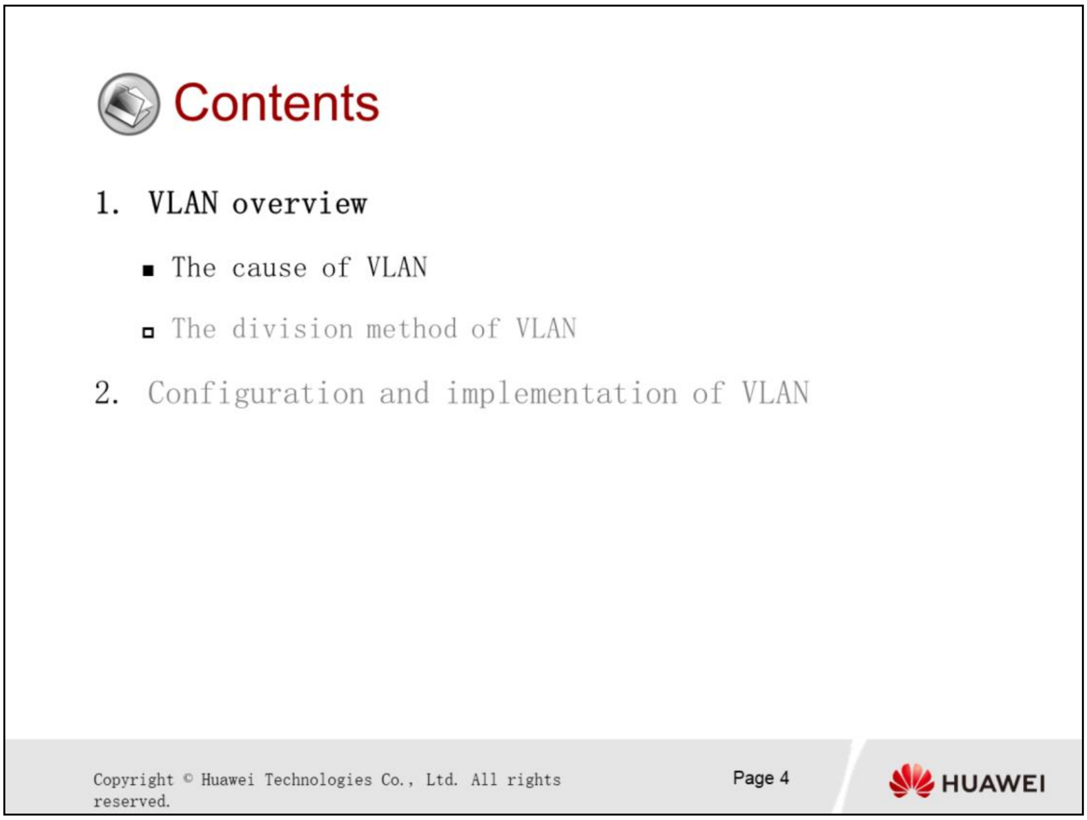
Foreword

- The generation of VLAN has injected new vitality into the traditional LAN network, and has brought about a revolution in LAN application. This course introduces how to implement VLAN in the switch and describes the changes in the VLAN data frame in the transfer process between the switches.



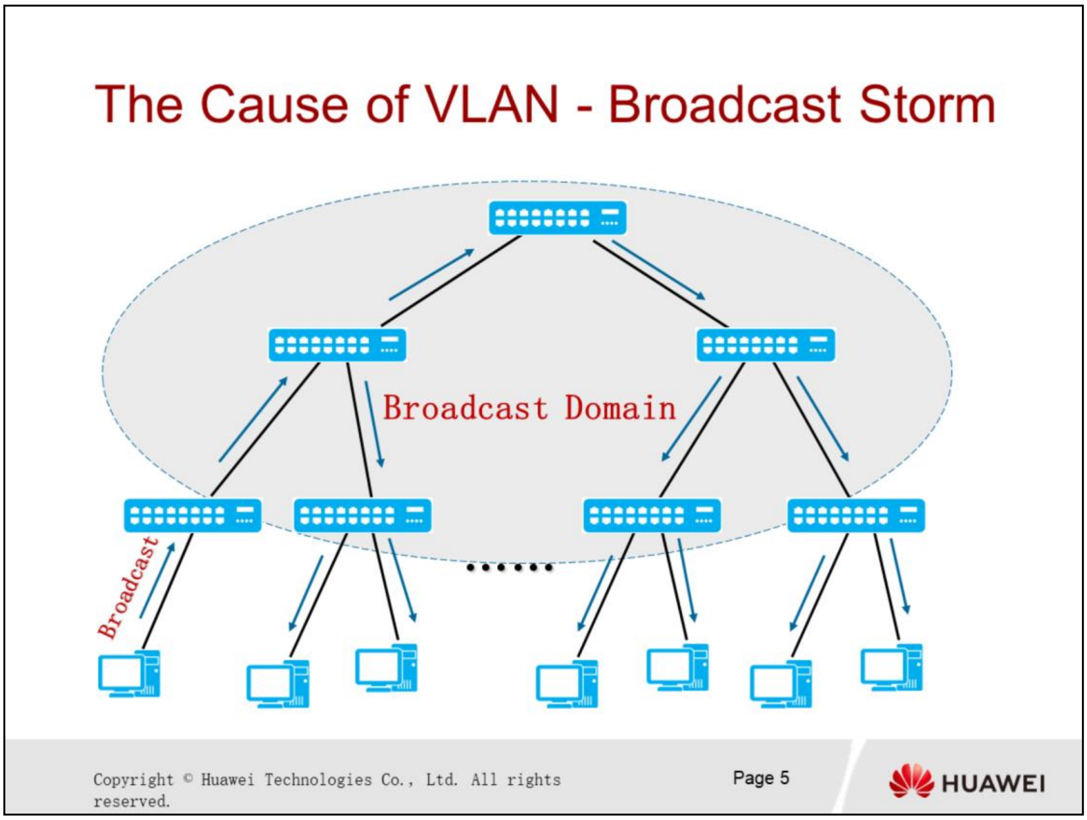
Objectives

- Upon studying this course, you will be able to:
  - Describe the functions and definitions of VLAN
  - Describe the method of VLAN division
  - Describe the forwarding process of VLAN data frames



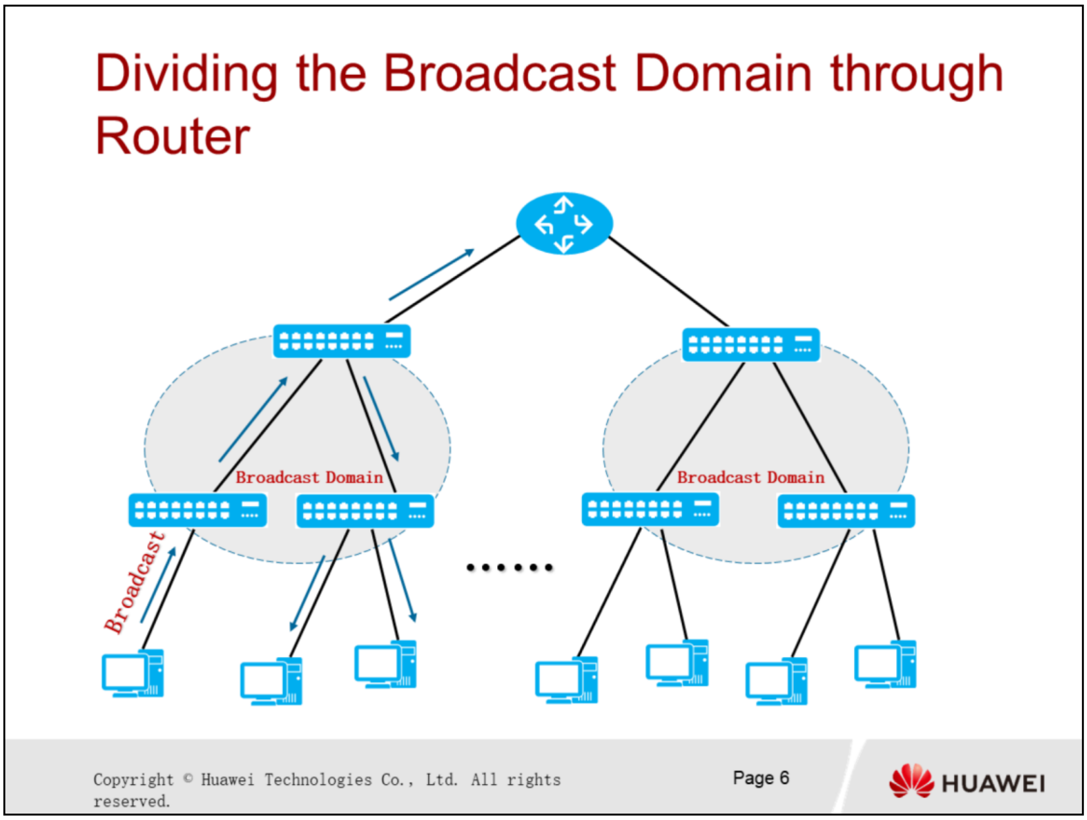
Contents

1. VLAN overview
   - ■ The cause of VLAN
   - □ The division method of VLAN
2. Configuration and implementation of VLAN



The Cause of VLAN - Broadcast Storm

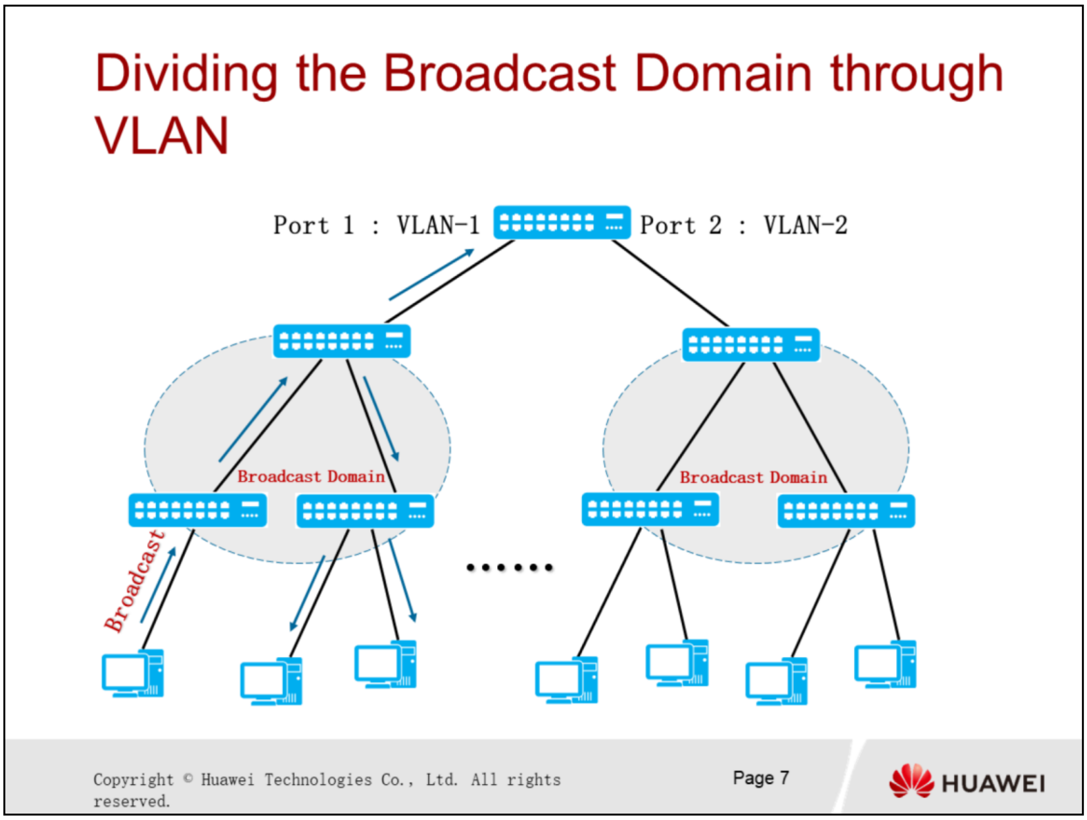
- Traditional LAN uses HUB, HUB has only one bus, and a bus is a collision domain. Therefore, the traditional LAN is a flat network, and a LAN belongs to the same conflict domain. Any packet sent by a host will be received by all other machines in the same conflict domain. Later, the network bridge (two layer switch) is used instead of the hub (HUB). Each port can be regarded as a single bus, and the conflict domain is restricted to each port, which greatly improves the efficiency of the network sending unicast packet and greatly improves the performance of the layer 2 network. If a host sends a broadcast packet, the device can also receive the broadcast information. We usually call the area that the broadcast packet can reach as a broadcast domain. When the bridge is transmitting the broadcast packet, it will still copy the broadcast packets and send them to the various corners of the network. With the expansion of network scale, more and more broadcast packets are in the network, and more and more network resources are occupied by the broadcast packet, which seriously affects the network performance. This is the problem of the so-called broadcast storm.
- Because of the working principle limitation of the layer two network, the bridge is powerless for the broadcast storm problem. In order to improve the efficiency of the network, we usually need to segment the network: divide a large broadcast domain into several small broadcast domains.



Dividing the Broadcast Domain through Router

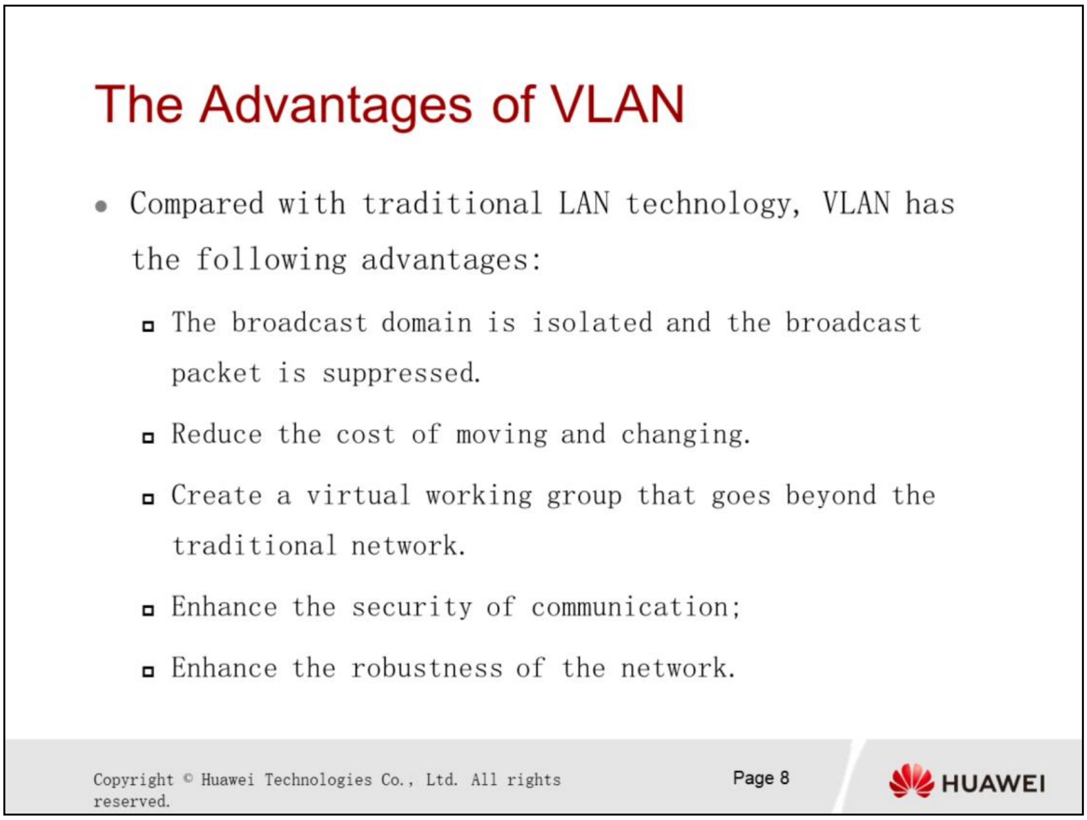
HUAWEI

- In the past, LAN was often segmented through a router, the transmission range of the broadcast message is greatly reduced. This scheme solves the problem of broadcast storm, but the router separate the network on the network layer, the network planning is complex, it is not flexible on networking, and the difficulty of management and maintenance is greatly increased. As an alternative LAN segmentation method, the virtual LAN is introduced into the network solution to solve the problems of large-scale layer two network environment.



Dividing the Broadcast Domain through VLAN

- The Virtual Local Area Network (VLAN) technology logically divides a physical LAN into multiple VLANs (broadcast domains). As a result, hosts within the same VLAN can communicate directly, while hosts in different VLANs cannot. In this manner, messages are broadcast in each VLAN, inter-VLAN communication is restricted, and network security is enhanced.

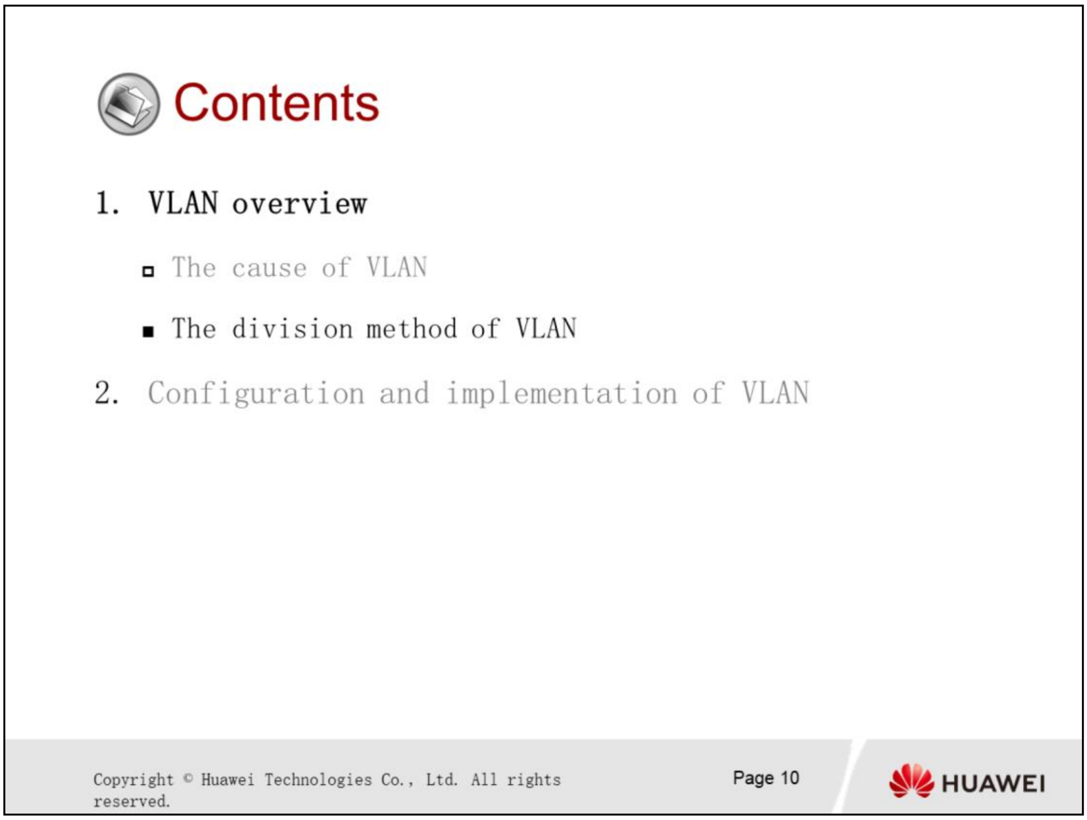


The Advantages of VLAN

- Compared with traditional LAN technology, VLAN has the following advantages:
  - The broadcast domain is isolated and the broadcast packet is suppressed.
  - Reduce the cost of moving and changing.
  - Create a virtual working group that goes beyond the traditional network.
  - Enhance the security of communication;
  - Enhance the robustness of the network.

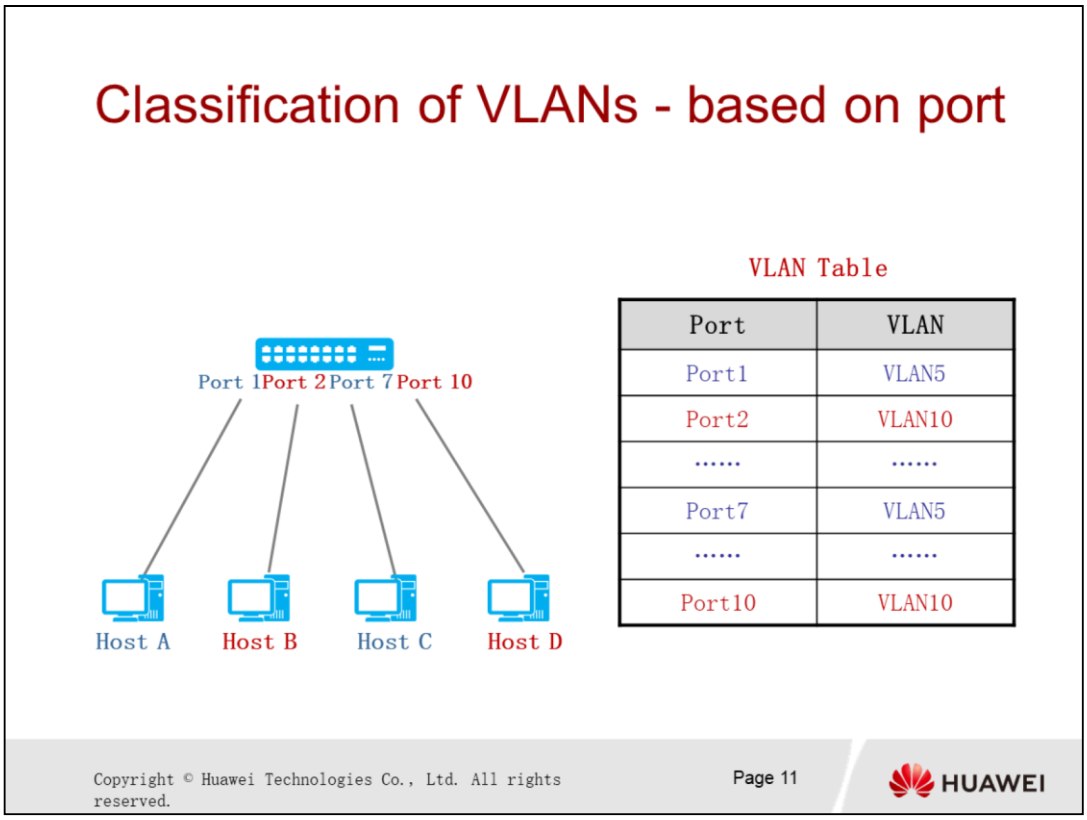
Page 8

- Compared with the traditional LAN, VLAN has the following advantages:
- Limit the broadcast packet to improve the utilization of bandwidth:
  - The performance degradation problem caused by broadcast storm is effectively solved. A VLAN forms a small broadcast domain, and the same VLAN member is in the broadcast domain identified by the VLAN, then when a packet has no routing, the switch will only send the packet to all other ports that belong to the VLAN, not all the ports of the switch, so that the packet is limited within a VLAN. To a certain extent, the bandwidth can be saved.
- Reduce the cost of movement and change:
  - The dynamic management network, that is, when a user moves from one position to another, his network attributes do not need to be reconfigured, but dynamic. This dynamic management network brings great benefits to both the network manager and the user. One user, wherever he goes, can access the network without changing configurations. The prospect of access to the network without any modification is very promising. Of course, not all VLAN definition methods can do this.



Contents

1. VLAN overview
   - The cause of VLAN
   - The division method of VLAN
2. Configuration and implementation of VLAN

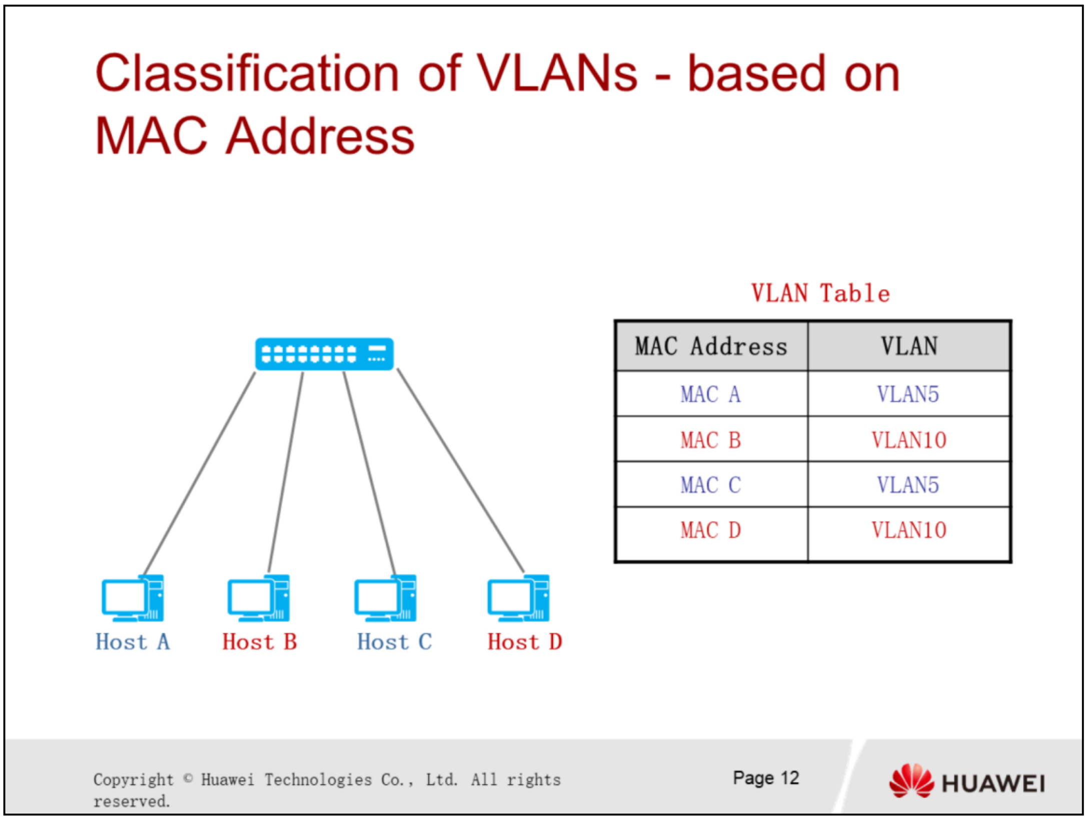


Classification of VLANs - based on port

VLAN Table

Port	VLAN
Port1	VLAN5
Port2	VLAN10
......	......
Port7	VLAN5
......	......
Port10	VLAN10

- In this mode, VLANs are classified based on the port numbers on a switching device. The network administrator configures a port default VLAN ID (PVID), that is, the default VLAN ID, for each port on the switching device. That is, a port belongs to a VLAN by default. When a data frame reaches a port, it is marked with the PVID if the data frame carries no VLAN tag and the port is configured with a PVID. If the data frame carries a VLAN tag, the switching device will not add a VLAN tag to the data frame even if the port is configured with a PVID.
- Different types of ports process VLAN frames in different manners.
- Advantages: It is simple to define VLAN members.
- Disadvantages: VLANs must be re-configured when VLAN members change locations.

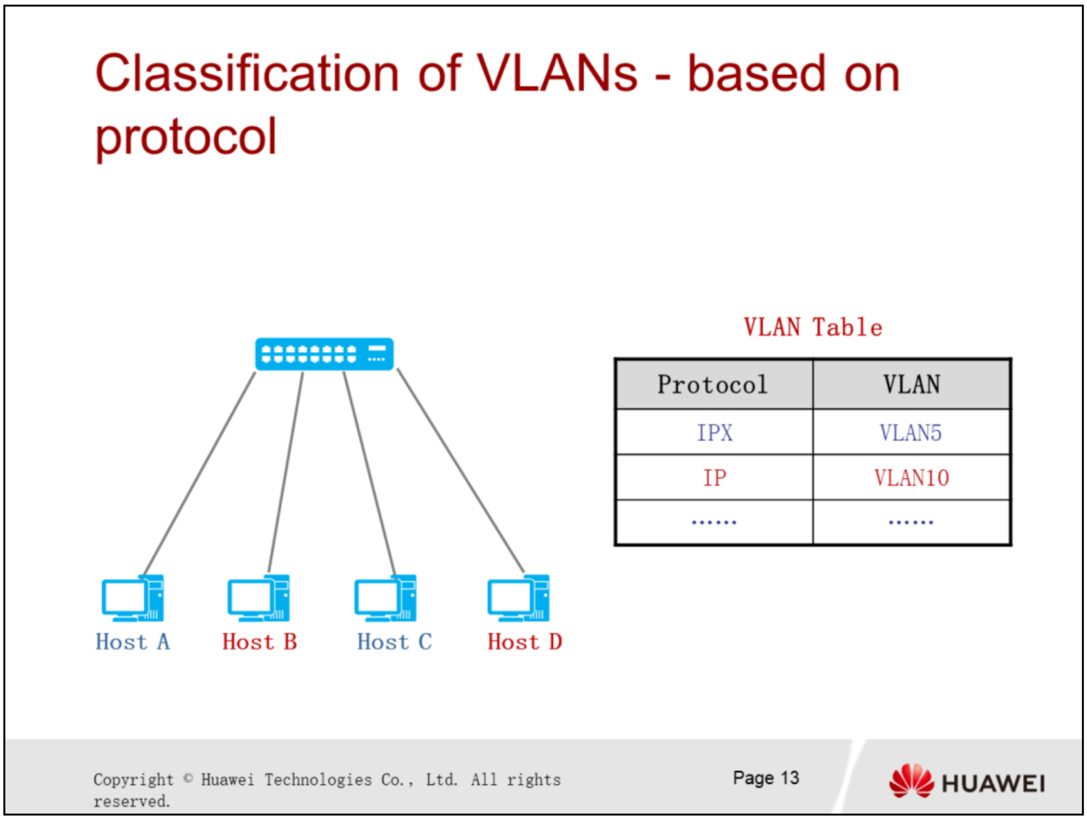


Classification of VLANs - based on MAC Address

VLAN Table

MAC Address	VLAN
MAC A	VLAN5
MAC B	VLAN10
MAC C	VLAN5
MAC D	VLAN10

- In this mode, VLANs are classified based on the MAC addresses of network interface cards (NICs). The network administrator configures the mappings between MAC addresses and VLAN IDs. In this case, when a switching device receives an untagged packet, it searches the MAC-VLAN table for a VLAN tag to be added to the packet according to the MAC address of the packet.
- Advantages: When the physical locations of users change, you do not need to re-configure VLANs for the users. This improves the security of users and increases the flexibility of user access.
- Disadvantages: This mode is applicable to only a simple networking environment where the NIC seldom changes.In addition, all members on the network must be pre-defined.

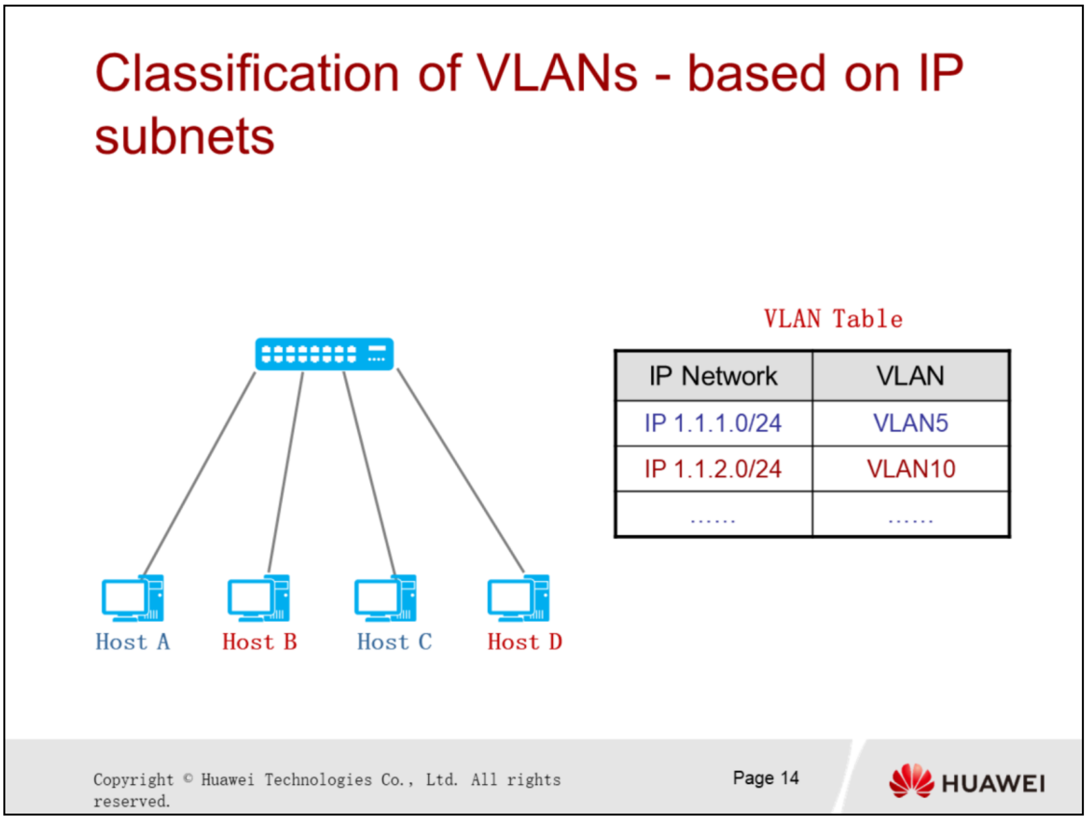


Classification of VLANs - based on protocol

VLAN Table

Protocol	VLAN
IPX	VLAN5
IP	VLAN10
......	......

- VLAN IDs are allocated to packets received on an interface according to the protocol (suite) type and encapsulation format of the packets. The network administrator configures the mappings between types of protocols and VLAN IDs.
- This classification of VLANs is barely ised today.



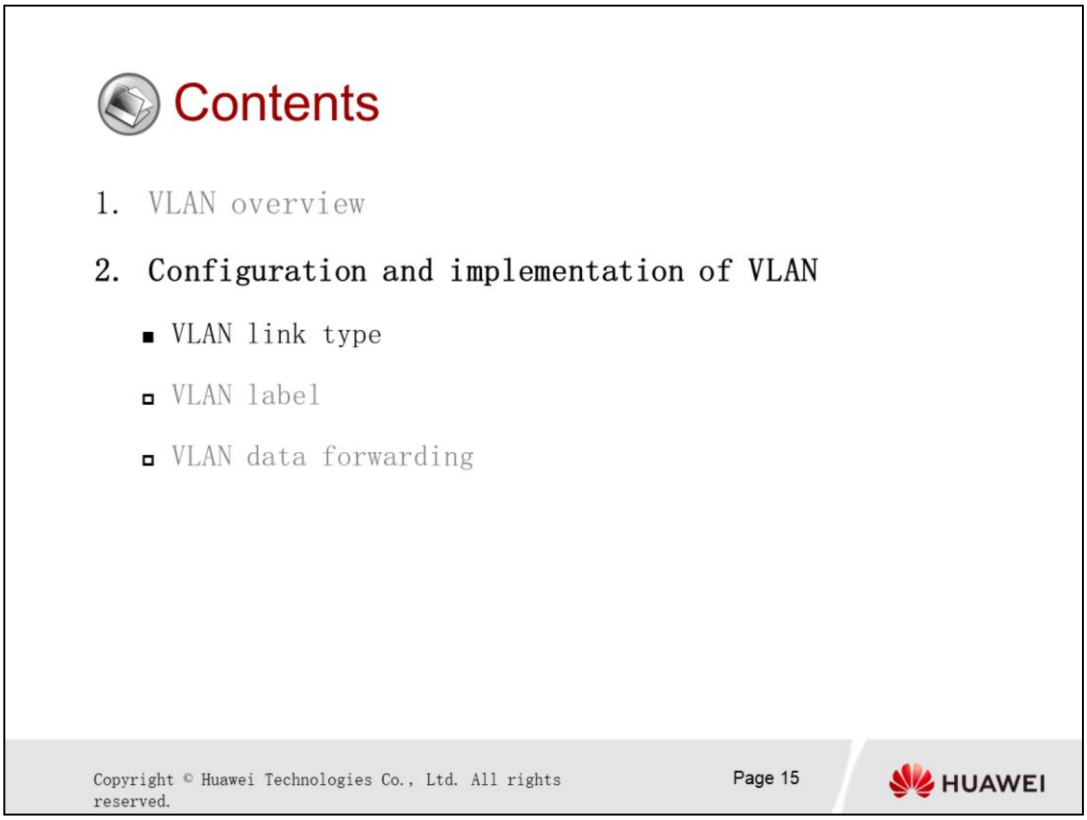
Classification of VLANs - based on IP subnets

VLAN Table

IP Network	VLAN
IP 1.1.1.0/24	VLAN5
IP 1.1.2.0/24	VLAN10
……	……

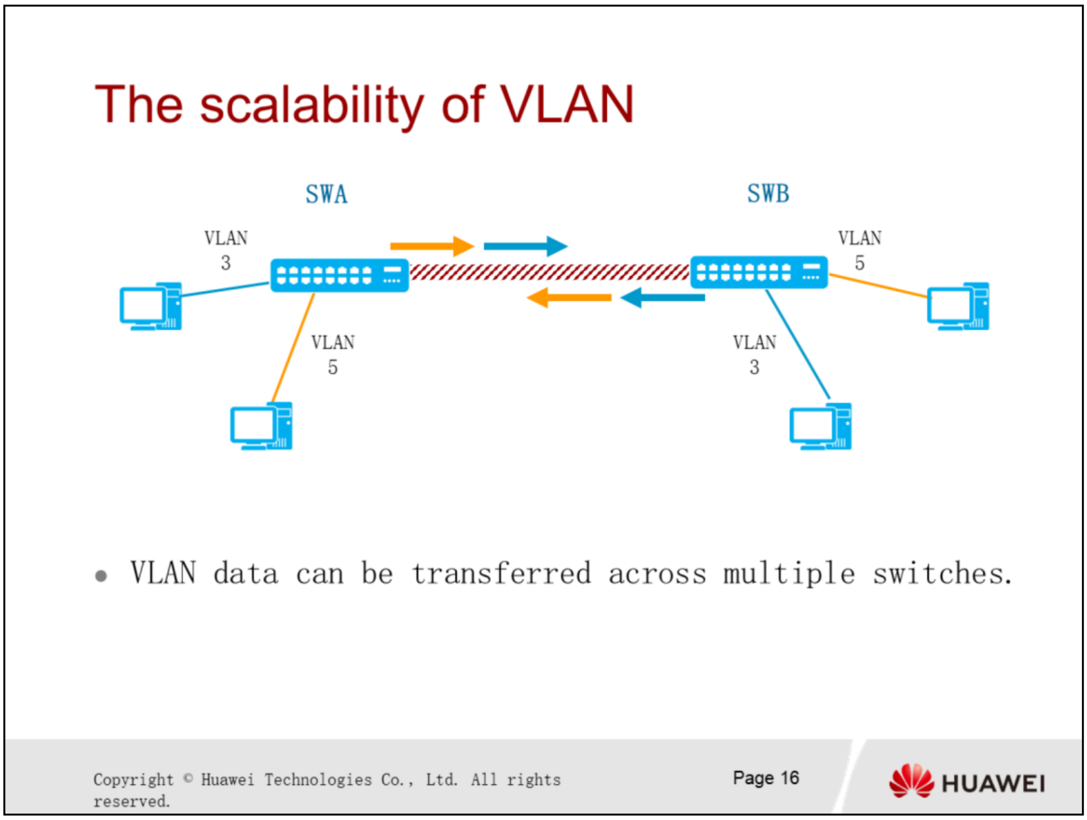
Page 14

- When receiving an untagged packet, a switching device adds a VLAN tag to the packet based on the IP address of the packet.
- Advantages: Packets sent from specific network segments or IP addresses are transmitted in specific VLANs. This decreases burden on the network administrator and facilitates management.
- Disadvantages: This mode is applicable to the networking environment where users are distributed in an orderly manner and multiple users are on the same network segment.



Contents

1. VLAN overview
2. Configuration and implementation of VLAN
   - VLAN link type
   - VLAN label
   - VLAN data forwarding

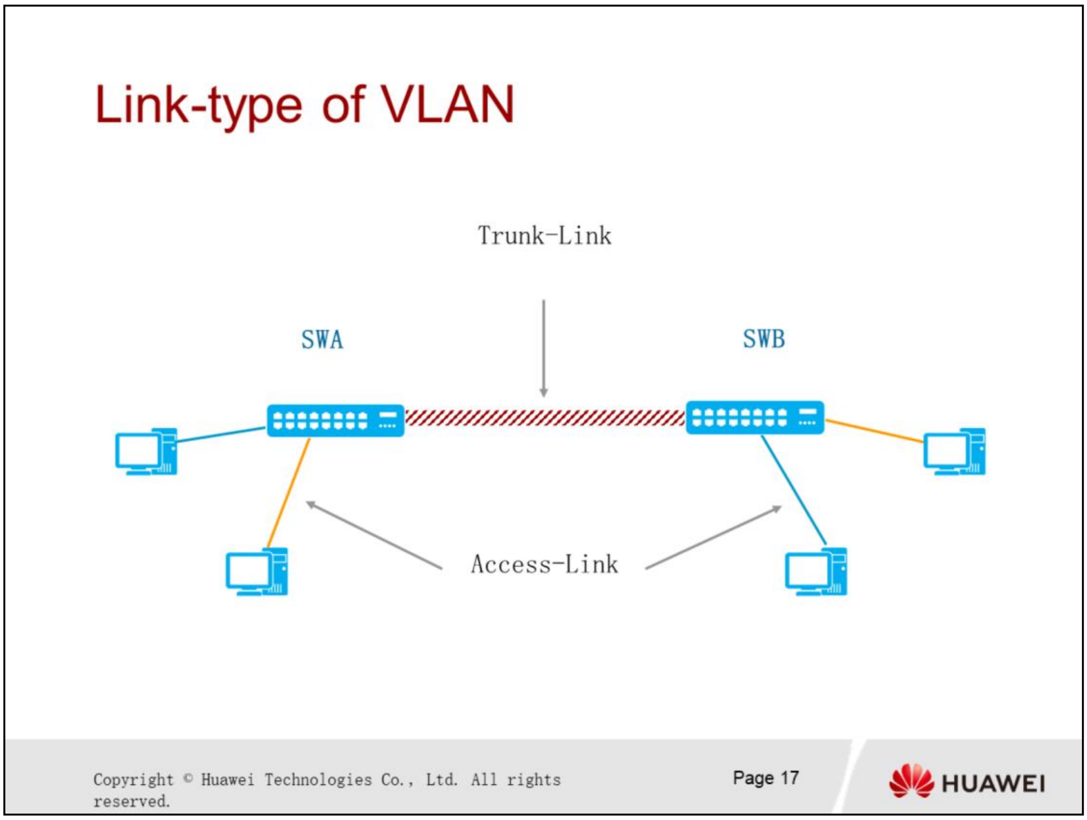


The scalability of VLAN

- VLAN data can be transferred across multiple switches.

Page 16

- VLAN information can be transmitted across multiple switches to related switches.
- All VLAN-3 data in the above figure can be communicated through intermediate transition switches, so as the data of VLAN-5.



Link-type of VLAN

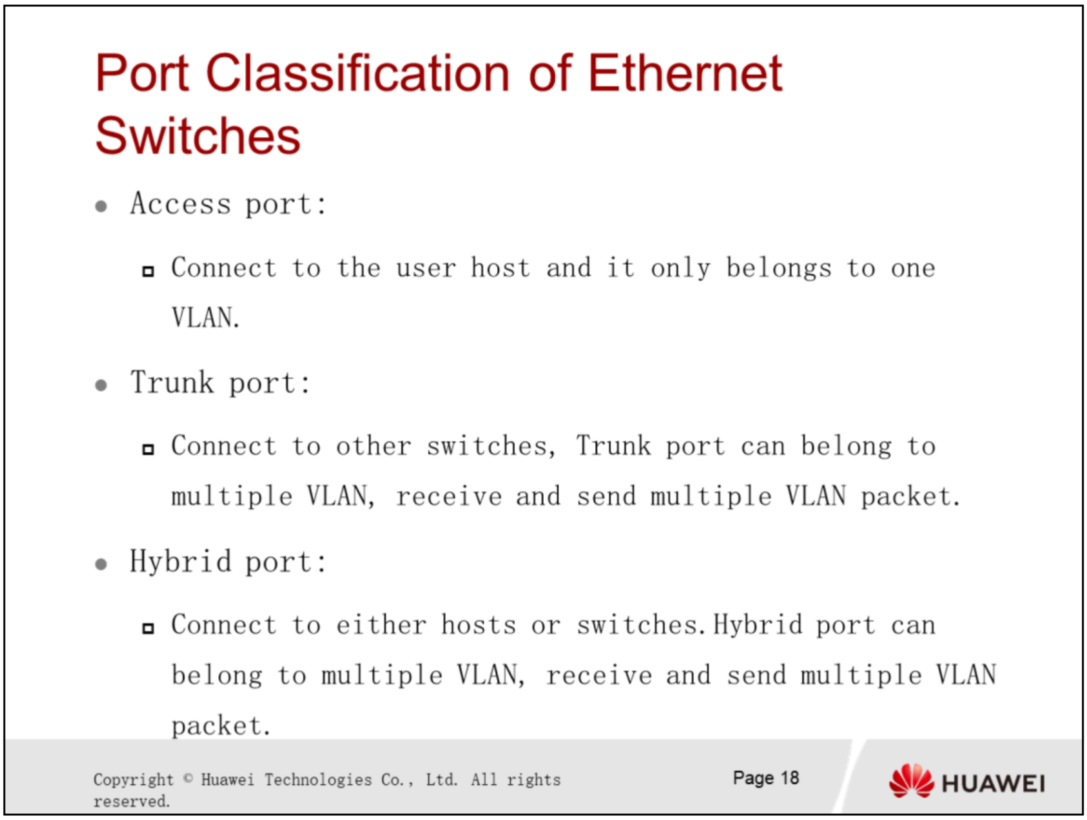
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Page 17

HUAWEI

- The access link refers to the link between a host and a switch. Usually, hosts do not need to know which VLAN they belong to, and the host hardware does not necessarily support frames with VLAN tags. The frames that the host requires to send and receive are frames that are not marked.
- The access link belongs to a specific port, which belongs to one VLAN. This port can not directly receive information from other VLAN, nor can it send packets to other VLAN directly. The information of different VLAN must be processed through layer 3 so that it can be forwarded to this port.
- Trunk links are links that can carry multiple VLAN data. Trunk links are usually used for interconnection between switches or for connections between switches and routers.
- When a data frame is transmitted on a trunk link, the switch must identify the VLAN of the data frame. IEEE 802.1Q defines the VLAN frame format, all the frames transmitted on the trunk link are tagged frames. Through these tags, the switch can determine which frames belong to which VLAN.
- Unlike access links, the trunk links are used to carry VLAN data between different devices (such as switches and routers, switches and switches), so the trunk links belong to no specific VLAN. By configuring, the trunk link can carry all the VLAN data, or it can be configured to transmit only the specified VLAN data.
- Although the trunk link does not belong to any specific VLAN, it can

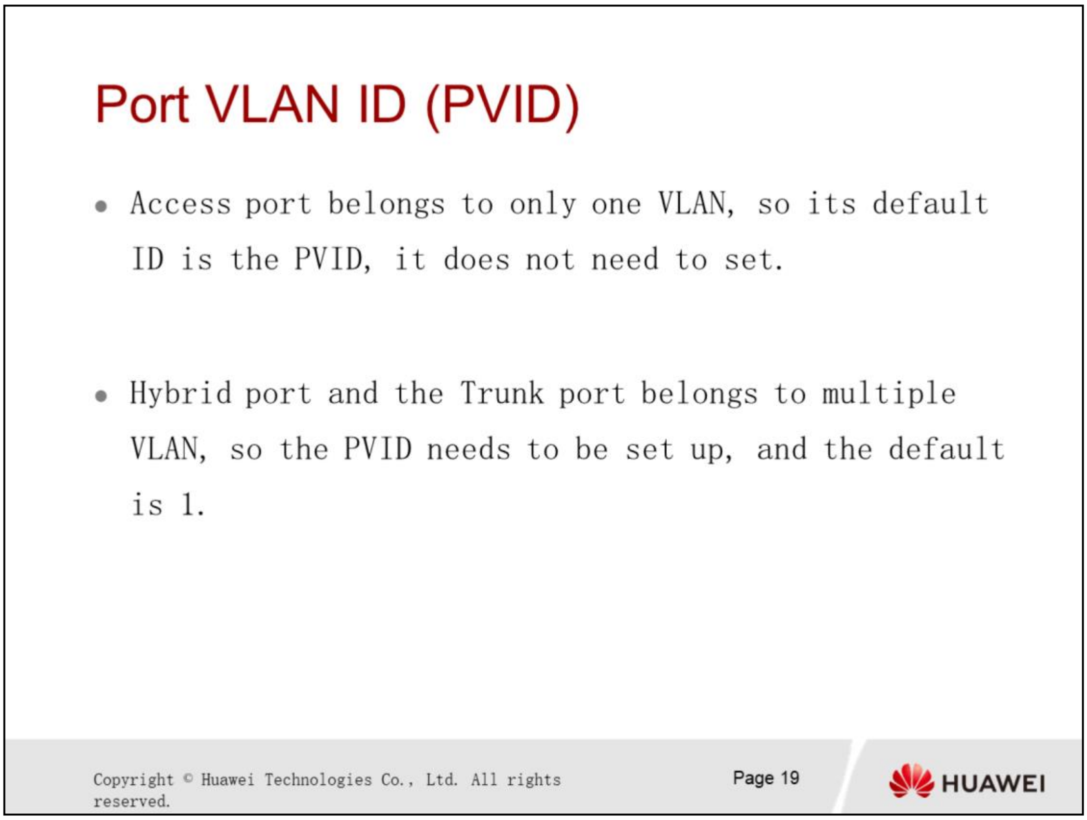
configure a PVID(port VLAN ID). When there is untagged frame transmitting on the trunk link, the switch will add PVID as VLAN tag to the frame, then handles it.



Port Classification of Ethernet Switches

- Access port:
  - Connect to the user host and it only belongs to one VLAN.
- Trunk port:
  - Connect to other switches, Trunk port can belong to multiple VLAN, receive and send multiple VLAN packet.
- Hybrid port:
  - Connect to either hosts or switches.Hybrid port can belong to multiple VLAN, receive and send multiple VLAN packet.

- The difference between the Hybrid port and the Trunk port is that the hybrid port allows multiple VLAN packets to be untagged, while the trunk port only allows the default VLAN packet to be untagged. On the same switch, hybrid port and trunk port can not coexist.

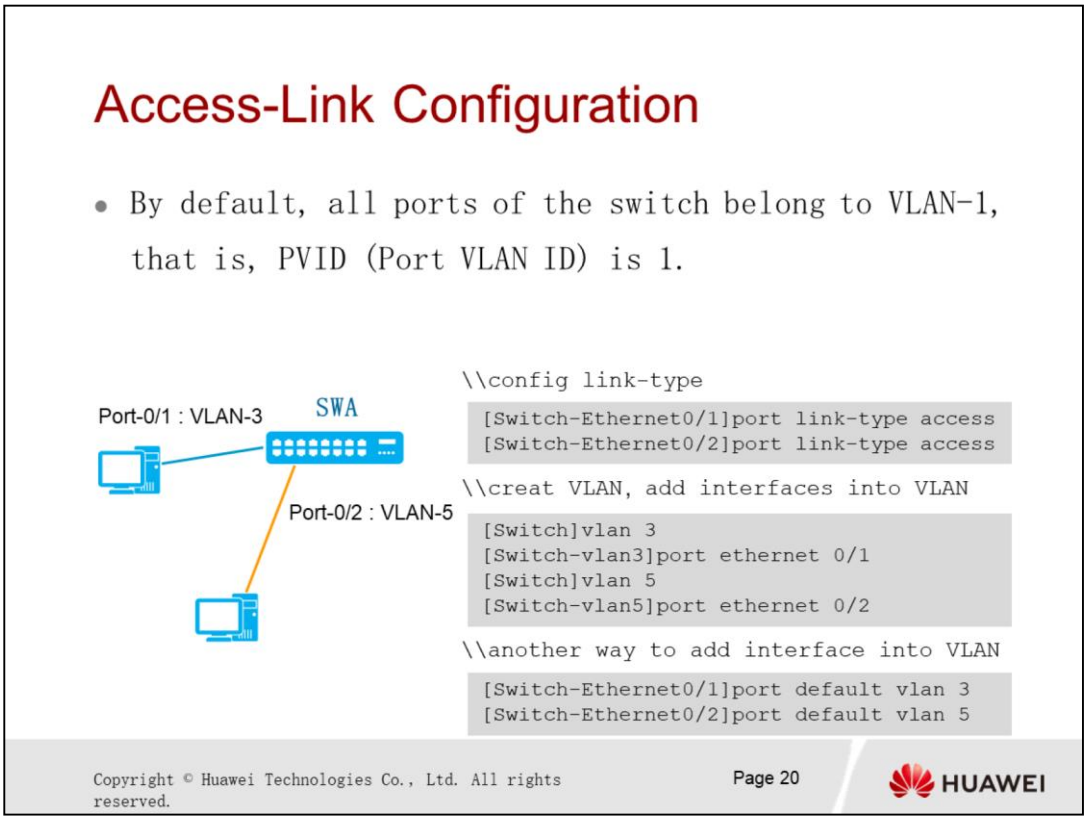


Port VLAN ID (PVID)

- Access port belongs to only one VLAN, so its default ID is the PVID, it does not need to set.

- Hybrid port and the Trunk port belongs to multiple VLAN, so the PVID needs to be set up, and the default is 1.

- All the default ports belong to VLAN 1, and VLAN 1 is the default VLAN, which can neither be created nor deleted.



Access-Link Configuration

- By default, all ports of the switch belong to VLAN-1, that is, PVID (Port VLAN ID) is 1.

\\config link-type

```
[Switch-Ethernet0/1]port link-type access
[Switch-Ethernet0/2]port link-type access
```

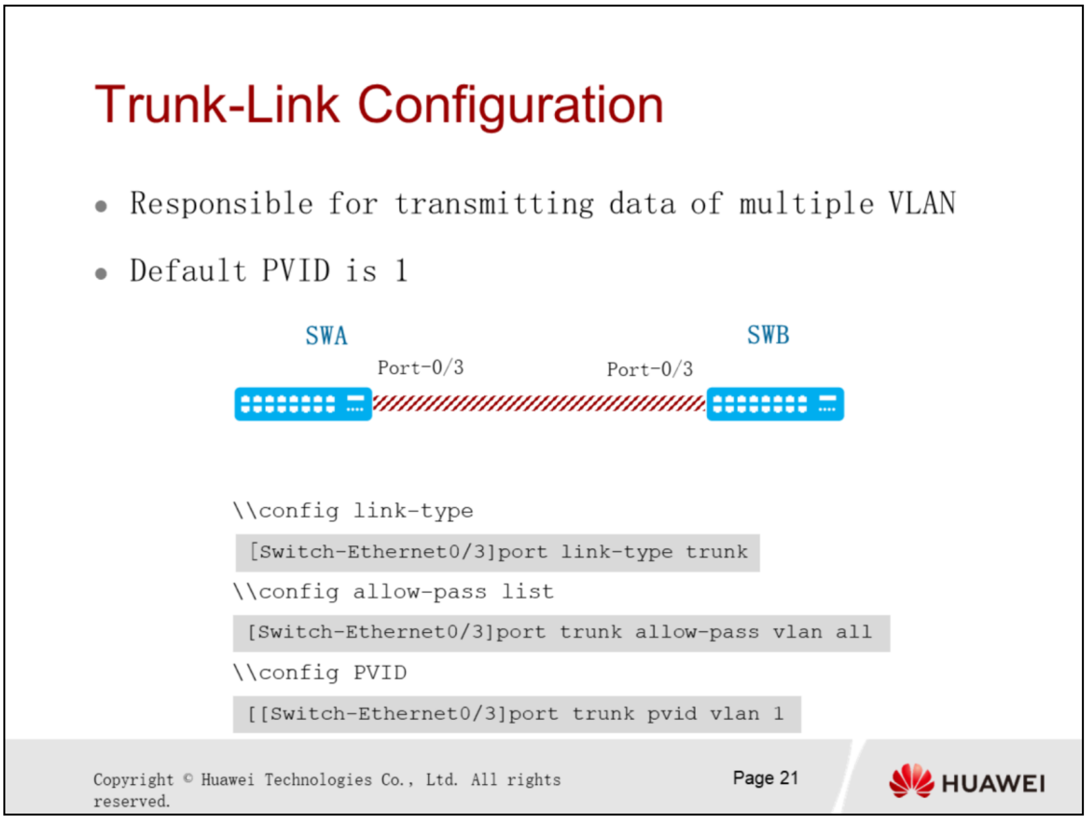
\\creat VLAN, add interfaces into VLAN

```
[Switch]vlan 3
[Switch-vlan3]port ethernet 0/1
[Switch]vlan 5
[Switch-vlan5]port ethernet 0/2
```

\\another way to add interface into VLAN

```
[Switch-Ethernet0/1]port default vlan 3
[Switch-Ethernet0/2]port default vlan 5
```

- All ports of 802.1Q based switches belong to VLAN-1, so they call VLAN-1 the default VLAN.
- Here is a new term called PVID, the full name called Port VLAN ID, which represents the VLAN of the port. In the Access port, the value of PVID represents the VLAN that the port belongs to, such as PVID = 100, that is, the port is divided into VLAN100.



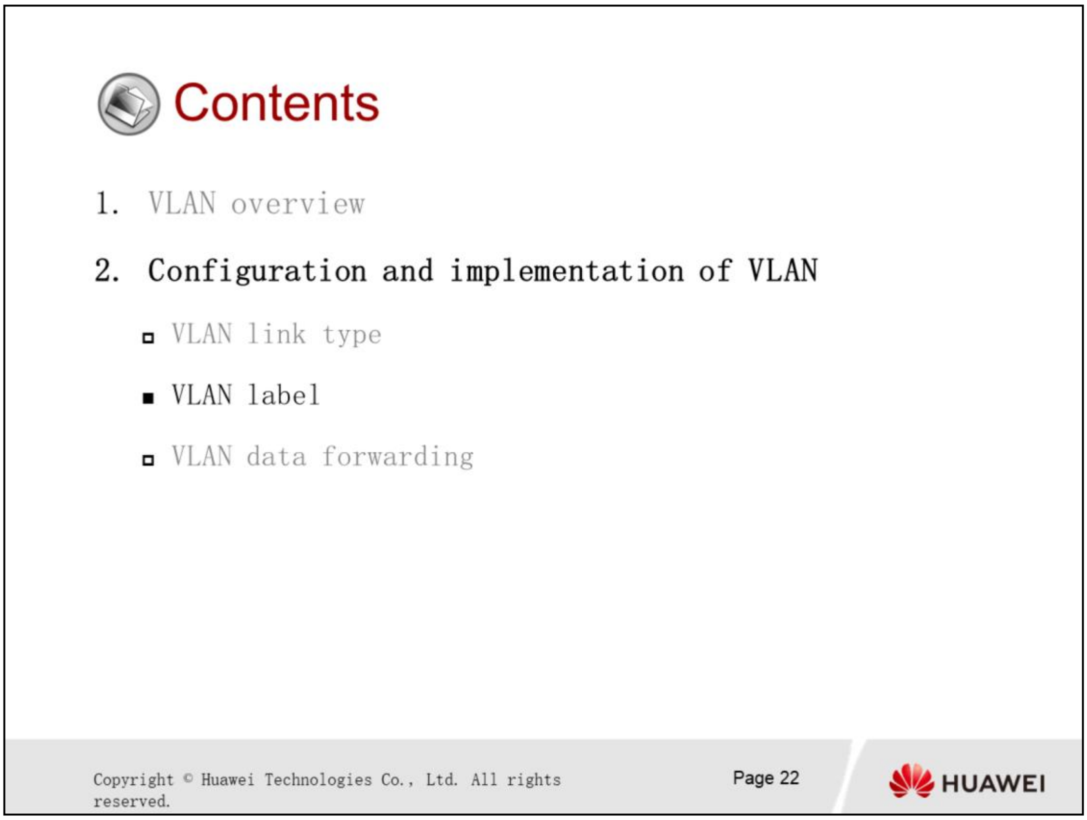
Trunk-Link Configuration

- Responsible for transmitting data of multiple VLAN
- Default PVID is 1

SWA
Port-0/3
Port-0/3
SWB

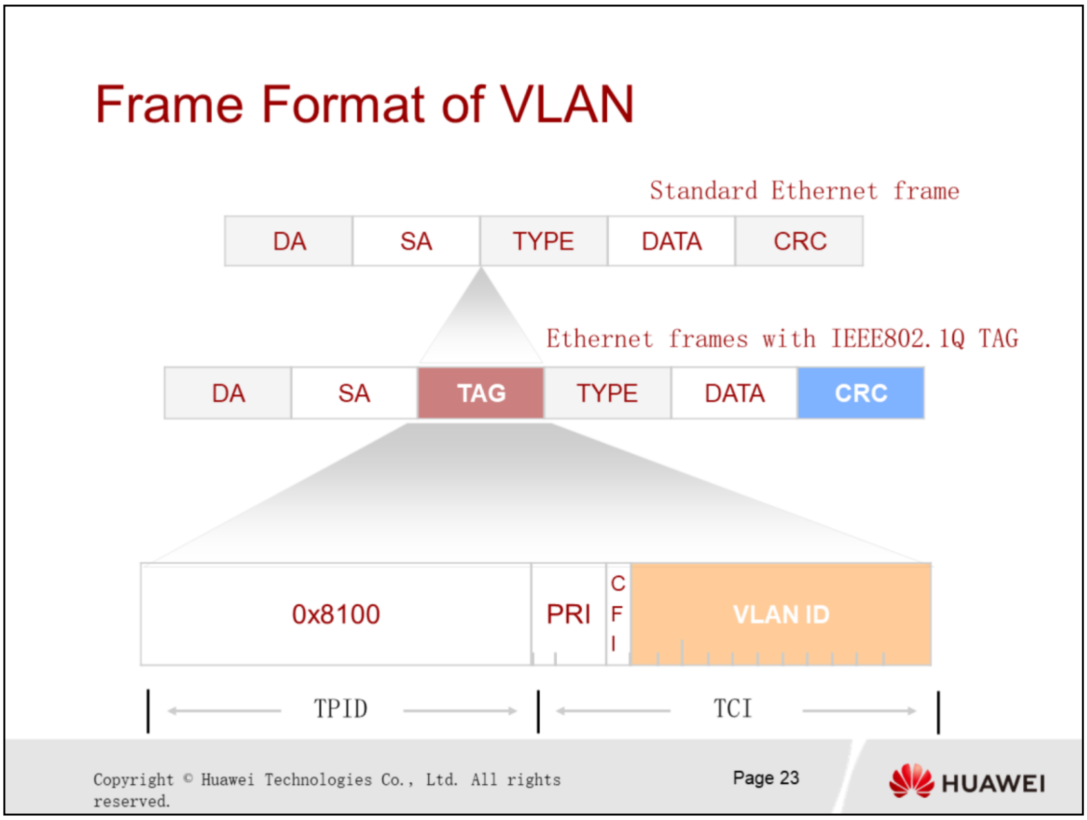
```
\\config link-type
[Switch-Ethernet0/3]port link-type trunk
\\config allow-pass list
[Switch-Ethernet0/3]port trunk allow-pass vlan all
\\config PVID
[[Switch-Ethernet0/3]port trunk pvid vlan 1
```

- Trunk port is responsible for forwarding multiple VLAN data frames between switches, use command “port trunk allow-pass vlan [VID]” to allow the data frames with a specific VLAN to pass.
- Here is a command ″port trunk PVID VLAN [VID]″ to change the PVID value of the Trunk port, and the meaning of the Trunk port PVID value is different from the Access port PVID. For Access port, it represents a VLAN belongs to the port, but for Trunk port, it represents the default VLAN value.



Contents

1. VLAN overview
2. Configuration and implementation of VLAN
   - VLAN link type
   - VLAN label
   - VLAN data forwarding



Frame Format of VLAN

Standard Ethernet frame

DA SA TYPE DATA CRC

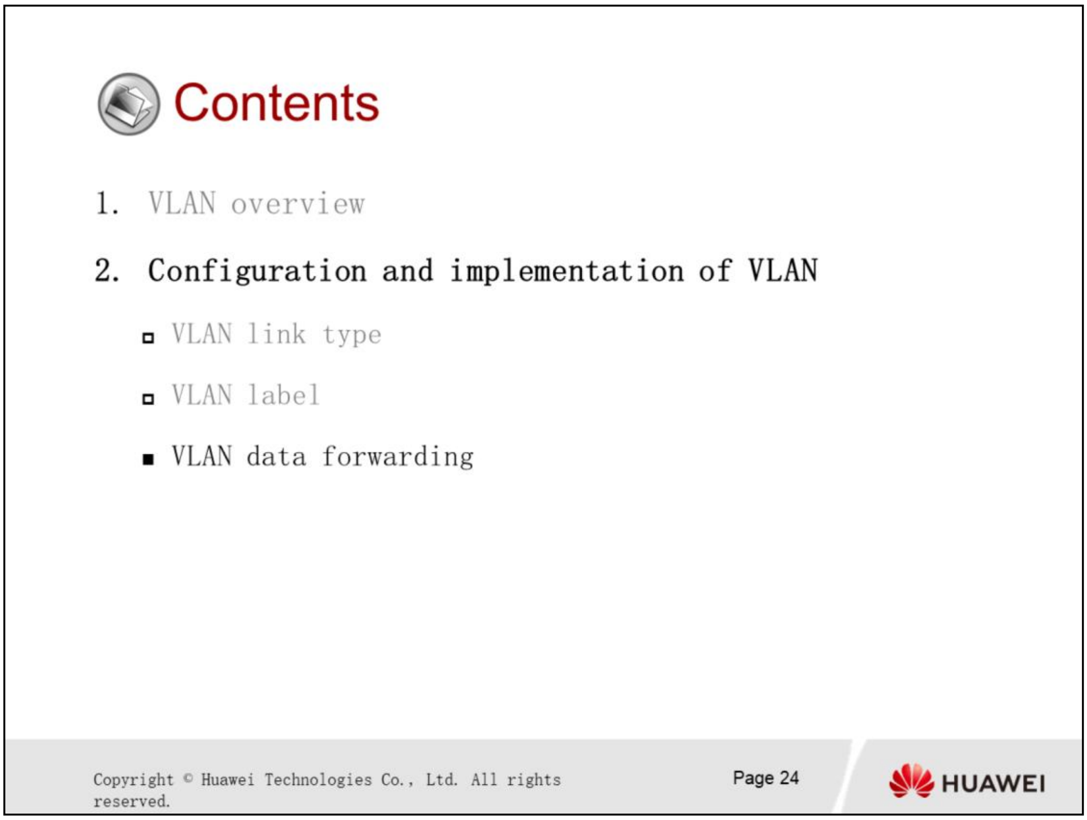
Ethernet frames with IEEE802.1Q TAG

DA SA TAG TYPE DATA CRC

0x8100 PRI CFI VLAN ID

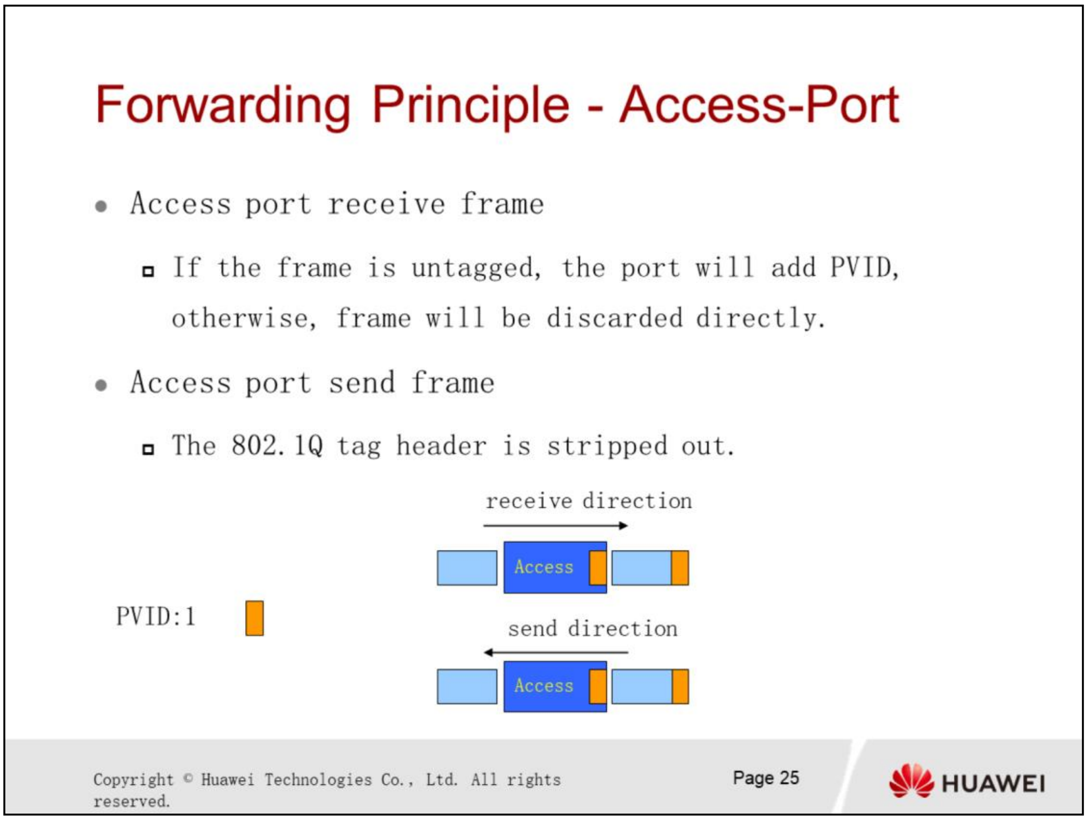
TPID TCI

- The four byte 802.1Q tag header contains 2 byte label protocol identifier (TPID) and 2 byte label control information (TCI).
- TPID (Tag Protocol Identifier) is a new type defined by IEEE, indicating that it is a frame with 802.1Q tag. TPID contains a fixed value 0x8100.
- TCI is a control information of frames. It contains the following elements:
    - Priority: the 3 bits indicate the priority of the frame. There are 8 kinds of priorities, 0-7. The IEEE 802.1Q standard uses these three bits information.
    - The value of Canonical Format Indicator (CFI):CFI set to 0 means it’ s a standard format and 1 means non-standard format.
    - VLAN Identified (VLAN ID): This is a 12 bit domain, indicating the ID of VLAN, range from 0 to 4095, a total of 4096, and the actual range is 1-4094. Each packet sent by the switch supports the 802.1Q protocol will contain the domain to indicate which VLAN belongs to.
- In an switched network environment, there are two formats of Ethernet frames: some frames are not labeled with these four bytes, called untagged frame, and some frames are added to the four bytes, called the tagged frame.



Contents

1. VLAN overview
2. Configuration and implementation of VLAN
   - VLAN link type
   - VLAN label
   - VLAN data forwarding

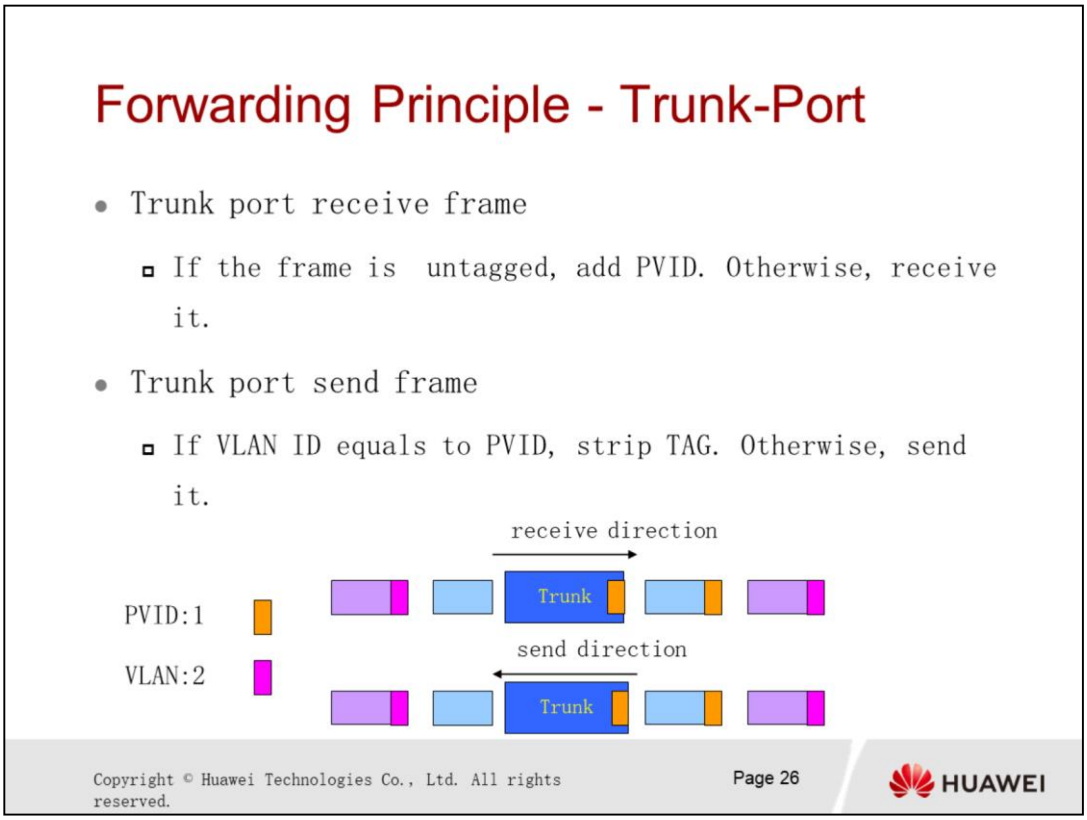


Forwarding Principle - Access-Port

- Access port receive frame
  - If the frame is untagged, the port will add PVID, otherwise, frame will be discarded directly.
- Access port send frame
  - The 802.1Q tag header is stripped out.

HUAWEI

- Access port receive frame
  - If the frame is untagged, the port will add PVID, otherwise, frame will be discarded directly.
- Access port send frame
  - The 802.1Q tag header is stripped out, and the frame that been sent is an ordinary Ethernet frame.



Forwarding Principle - Trunk-Port

- Trunk port receive frame
  - If the frame is untagged, add PVID. Otherwise, receive it.
- Trunk port send frame
  - If VLAN ID equals to PVID, strip TAG. Otherwise, send it.

receive direction

PVID:1 🟧

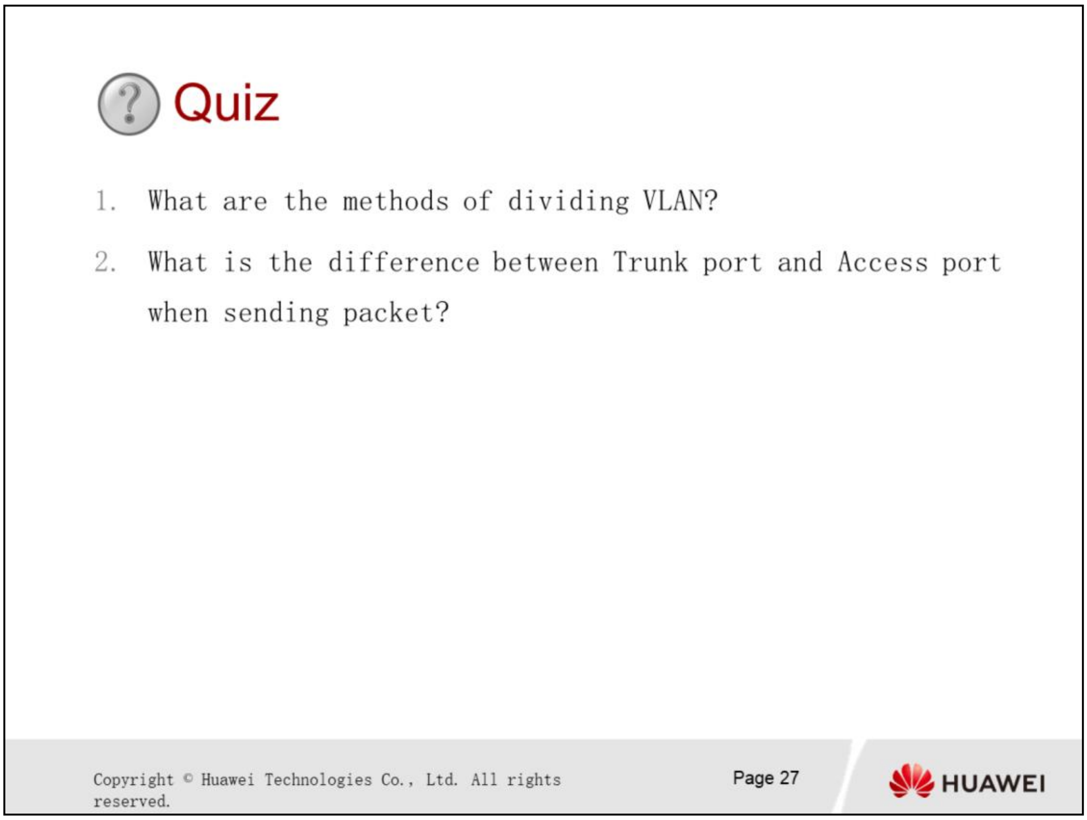
VLAN:2 🟪

Trunk

send direction

Trunk

- Trunk port receive frame
  - If the frame is untagged, add PVID. Otherwise, receive it.
- Trunk port send frame
  - If VLAN ID equals to PVID, strip TAG. Otherwise, send it.

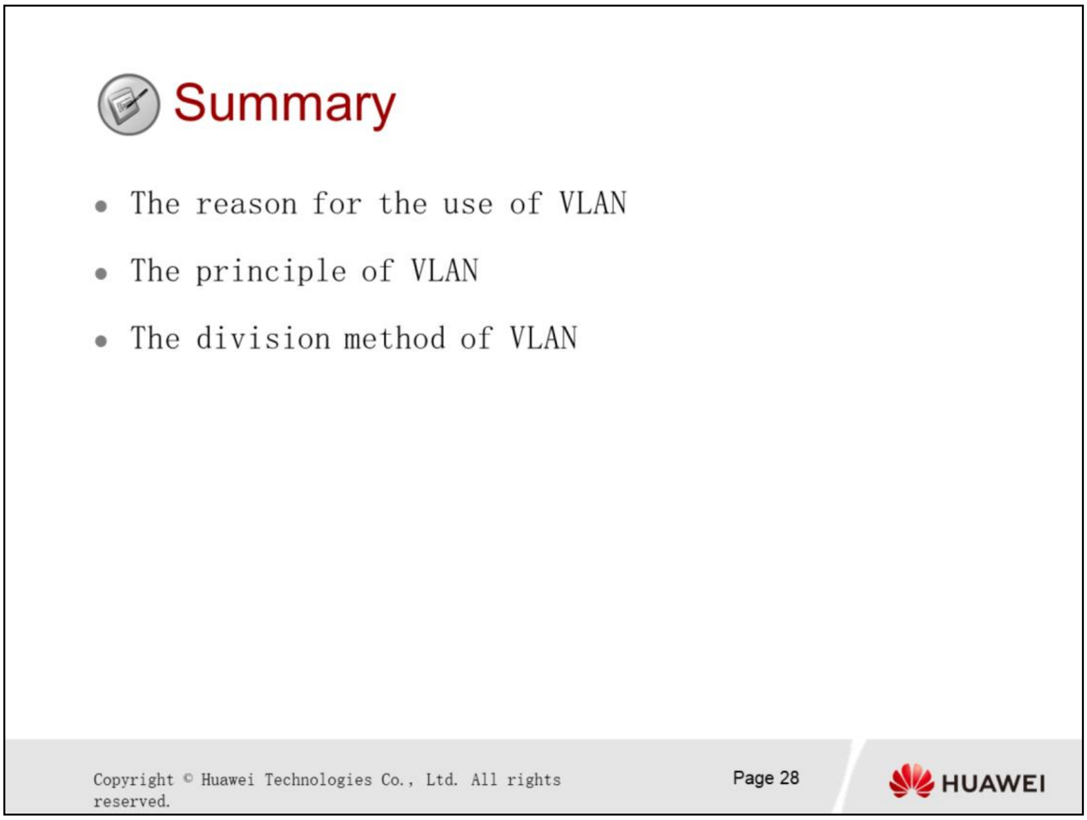


Quiz

1. What are the methods of dividing VLAN?
2. What is the difference between Trunk port and Access port when sending packet?

- Reference answer:

  1. Based on port, based on MAC, based on protocol, based on subnet.
  2. Trunk port sends packets with TAG, and Access ports send packet without TAG.



Summary

- The reason for the use of VLAN
- The principle of VLAN
- The division method of VLAN

Thank You

www.huawei.com