Computer Network Course Practice

Lab-2 VLAN Configuration and Verification

CONTENTS

OBJECTIVES

1. Cable a network according to the topology diagram.
2. Understand the benefits of VLAN and how it works.
3. Create VLAN in different ways.
4. Understand the functions and differences of types of ports or links such as Access, Trunk and Hybrid.
5. Enable trunking on inter-switch connections.
6. Verify VLAN configuration.
7. Capture and analyze VLAN traffic, understand untagged and 802.1D tagged frame format.

REQUIRED RESOURCES

1. Huawei eNSP.
2. ping.
3. Wireshark.

BACKGROUND

VLAN

Virtual LAN (VLAN) based on switching technology is an important technology in Switched Ethernet. Modern switches use VLANs to improve network performance, expansibility, security, and manageability by separating large Layer 2 broadcast domains into smaller ones.

A VLAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2 network). It is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution, allowing a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. Hosts within a VLAN can communicate with each other but cannot communicate directly with hosts in other VLANs. Consequently, broadcast frames are confined to within a single VLAN. VLANs simplifies the task to divide and make groups in a network, based on their functional, security and management requirements without having to plug/unplug physical LAN cables or modify the existing network infrastructure.

Link and Port Types

There are two types of VLAN links: Access link and Trunk link. These links allow us to connect multiple switches together or just simple network devices e.g. PC, that will access the VLAN network.

- **Access link.** Access links are the most common type of links on any VLAN switch. An access link is a link that is part of only one VLAN, and normally is for end devices. Any device attached to an access link is unaware of a VLAN membership. An access link connection can understand only untagged or standard Ethernet frames. Switches remove any VLAN information from the frame before it is sent to an access link device.
- **Trunk link.** VLANs can span multiple switches, and you can have more than one VLAN on each switch. For multiple VLANs on multiple switches to be able to communicate via a single link between the switches, trunking must be used. A trunk link can transmit data frames from multiple VLANs and normally is used to connect switches to other switches or to routers. A trunk link is not assigned to a specific VLAN. Many VLAN traffic can be transported between switches using a single physical trunk link. Frames on a trunk link must be tagged so that other network devices can correctly identify VLAN information in the frames. A trunk link must operate at 100 Mbps or greater speeds.

Each port on a switch can be configured as an access, a trunk or a hybrid port, depending on the connected devices and the way they process frames. For a brief description of the port type, see Table 2-1.

Table 2-1 Description of the port type

Port Type	Allowed Frames	Common Use Cases	Comments
Access	untagged frames.	Connect end devices: PC, Server, Printer, etc.	A access port belongs to a single VLAN. All devices connected to this port will be in same broadcast domain. If no VLAN is configured for the access port, the port belongs to the default VLAN 1 (VLAN 1 cannot be modified or deleted).
Trunk	untagged frames in configured native VLAN (The default native VLAN is VLAN 1) and tagged frames from multiple VLANs	Connect switches, routers, APs, VoIP terminals, Servers with trunk capable NICs.	A trunk port belongs to and carry the traffic of more than one VLAN. A trunk port allows you to send frames from multiple VLANs across a single trunk link.

Hybrid	untagged or tagged frames according to the configuration.	Connect end devices or switches, routers, Servers with trunk capable NICs.	A hybrid port does not belong to any VLAN. By default, all switch ports are hybrid port.

VLAN Frame Tagging

To distinguish the traffic flows, all frames through trunk link are marked with special tags as they pass between the switches. It called VLAN tagging. When a frame contains a VLAN tag, it is a tagged frame. If it does not contain a VLAN tag, it is an untagged frame.

A VLAN tagging standard supported by most networking devices for supporting VLANs on Ethernet networks is the IEEE 802.1Q standard. IEEE 802.1Q adds a 4-byte VLAN tag between the Source address and Length/Type fields of an Ethernet frame.

The VLAN Frame tag is placed on the Ethernet frame when the frame reaches a switch from an access port, which is a member of a VLAN. If the switch has a trunk port, the frame can be forwarded out the trunk link port. This enables each switch to see what VLAN the frame belongs to and can forward the frame to corresponding VLAN access ports or to another VLAN trunk port. Before forwarding the frame to a VLAN access port, the switch removes the tag and the VLAN membership information is hence transparent to the end devices.

Ways to Configure VLAN

VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. The purpose of VLAN implementations is to associate interfaces with particular VLANs. VLANs can be implemented based on ports, MAC addresses, IP subnets, protocols, and policies. Table 2-2 compares different VLAN configuration methods.

Table 2-2 Comparisons among VLAN configuration methods

Method	Description	Usage Scenario
Port-based	VLANs are implemented based on interfaces.	Simple, commonly used, but does not allow users to move. Applies to networks of any scale and with devices at fixed locations.
MAC Address-based	VLANs are implemented based on source MAC addresses of frames. The network administrator preconfigures mappings between MAC addresses and VLAN IDs. When receiving an untagged frame, the switch adds the VLAN tag mapping the MAC address of the frame to the frame. Then the frame is transmitted in the specified VLAN.	When physical locations of users change, the network administrator does not need to reconfigure VLANs for the users. This improves security and access flexibility on a network. But the network administrator must predefine VLANs for all members on a network. Applies to small-scale networks where user terminals often change physical locations but their NICs seldom change, for example, mobile computers.
IP subnet-based	VLANs are implemented based on protocol types, source IP addresses and subnet masks. The network administrator preconfigures mappings between IP addresses and VLAN IDs. When receiving an untagged frame, the switch adds the VLAN tag mapping the IP address of the frame to the frame. Then the frame is transmitted in the specified VLAN.	When physical locations of users change, the network administrator does not need to reconfigure VLANs for the users. This method reduces communication traffic and allows a broadcast domain to span multiple switches. Applies to scenarios where there are high requirements for mobility and simplified management and low requirements for security.
Protocol-based	VLANs are implemented based on protocol types and encapsulation formats of frames, facilitating management and maintenance. The network administrator preconfigures mappings between protocol types and VLAN IDs. When receiving an untagged frame, the switch adds the VLAN tag mapping the protocol type of the frame to the frame. The frame is then transmitted in the specified VLAN.	The switch needs to analyze protocol type and convert the formats, which consumes excessive resources. Therefore, this mode slows down switch response time. Applies to networks using multiple protocols.
Policy-based	VLANs are implemented based on policies such as combinations of interfaces, MAC addresses, and IP addresses. The network administrator preconfigures policies. When receiving an untagged frame that matches a configured policy, the switch adds a specified VLAN tag to the frame. The frame is then transmitted in the specified VLAN.	This method provides high security. MAC addresses or IP addresses of users that have been bound to VLANs cannot be changed. The network administrator can flexibly select which policies to use according to the management mode and requirements. Applies to complex networks.

LAB-2-1: PORT-BASED VLAN CONFIGURATION

Requirements

A network topology is shown in Figure 2-1. Computers of departments A and B in a university are connected to a S5700 switch LSW1. To protect data, it is necessary to allow communication within the department, but isolate the communication between different departments. Please configure two port-based VLANs and assign the Gigabit ports GE /0/0/9 to GE 0/0/12 on the switch to VLAN 10 and ports GE 0/0/13 to GE 0/0/16 to VLAN 30. The computers of Department A are in VLAN 10, and the computers of Department B in VLAN 30.

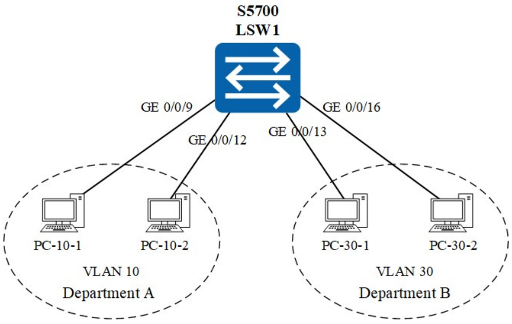

Figure 2-1 A switched Ethernet with two port-based VLANs

The IPv4 address allocation in different VLANs are shown in Table 2-3.

Table 2-3 IPv4Address Allocation

	IPv4 Address	**Mask**
VLAN 10	**192.168.10.0**	**255.255.255.0**
PC-10-1	192.168.10.11	255.255.255.0
PC-10-2	192.168.10.12	255.255.255.0
VLAN 30	**192.168.30.0**	**255.255.255.0**
PC-30-1	192.168.30.11	255.255.255.0
PC-30-2	192.168.30.12	255.255.255.0

Steps

Step 1: Create the topology, cable a network.

1. Start eNSP and click the "New Topology" icon in the toolbar.
2. Add one S5700 switch and two PCs to the blank work area.
3. Cable as necessary.
4. Name the switch and PCs.

Step 2: Assign the IPv4 address and subnet mask for PCs.

1. Double-click each PC, select the "Basic Config" tab in the pop-up window, and configure the IPv4 address and subnet mask for it.
2. After configuration, click the "Save" icon in the toolbar to save the topology to the specified directory, and name the topology file **lab-2-1 VLAN.PORT.topo**.

Step 3: Start devices.

Click the " Start Device" icon ▶ in the toolbar to start all devices.

Step 4: Configure VLANs on the switch.

Double-click the icon of switch LSW1 in the work area to open the switch configuration window, then enter the following commands:

```
# enter the system view
<huawei> system-view
# set the device name
[huawei] sysname LSW1
# display default VLAN information
[LSW1] display vlan
[LSW1] display vlan summary
```

```
# display ports in VLANs
[LSW1] display port vlan

# create VLAN 10
[LSW1] vlan 10
[LSW1-vlan10] quit

# assign switch ports to VLAN 10
[LSW1] interface gigabitethernet 0/0/9
[LSW1-GigabitEthernet0/0/9] port link-type access
[LSW1-GigabitEthernet0/0/9] port default vlan 10
[LSW1-GigabitEthernet0/0/9] quit
# display interface GE 0/0/9 information
[LSW1] display interface gigabitethernet 0/0/9
# display interface GE 0/0/9 information of vlan
[LSW1] display port vlan gigabitethernet 0/0/9

[LSW1] interface gigabitethernet 0/0/10
[LSW1-GigabitEthernet0/0/10] port link-type access
[LSW1-GigabitEthernet0/0/10] port default vlan 10
[LSW1-GigabitEthernet0/0/10] quit
[LSW1] display interface gigabitethernet 0/0/10
[LSW1] display port vlan gigabitethernet 0/0/10

[LSW1] interface gigabitethernet 0/0/11
[LSW1-GigabitEthernet0/0/11] port link-type access
[LSW1-GigabitEthernet0/0/11] port default vlan 10
[LSW1-GigabitEthernet0/0/11] quit
[LSW1] display interface gigabitethernet 0/0/11
[LSW1] display port vlan gigabitethernet 0/0/11

[LSW1] interface gigabitethernet 0/0/12
[LSW1-GigabitEthernet0/0/12] port link-type access
[LSW1-GigabitEthernet0/0/12] port default vlan 10
[LSW1-GigabitEthernet0/0/12] quit
[LSW1] display interface gigabitethernet 0/0/12
[LSW1] display port vlan gigabitethernet 0/0/12

# examine that the VLAN 10 have been created
[LSW1] display vlan 10

# create VLAN 30。
[LSW1] vlan 30
[LSW1-vlan30] quit
# assign ports GE 0/0/13、0/0/14、0/0/15 和 0/0/16 to vlan 30 in batch
# create a port group, named pgvlan30
[LSW1] port-group pgvlan30
# add ports to the group
[LSW1-port-group-pgvlan30] group-member gigabitethernet 0/0/13 to gigabitethernet 0/0/16
# set port link type
[LSW1-port-group-pgvlan30] port link-type access
# assign ports in the group to vlan 30
[LSW1-port-group-pgvlan30] port default vlan 30
[LSW1-port-group-pgvlan30] quit
# display port group information
[LSW1] display port-group
[LSW1] display port-group pgvlan30
[LSW1] display vlan 30

# display ports in VLANs
[LSW1] display port vlan
```

Tips：

1. you can create VLANs in batch

```
# enter the system view
<huawei> system-view
# create VLAN 10 to 100 in batch
[huawei] vlan batch 10 to 100
```

2. Restore or set port to the default configurations

By default, all ports on Huawei switches belong to VLAN 1 and all ports are hybrid port. If you changed the link type of a port or assign the port to a VLAN other than the default VLAN of VLAN 1, you can restore the port to its default configuration. Different types of ports have different commands for restoring the default configuration, see Table 2-4.

Table 2-4 Commands used to restore or set the port to the default configurations

Current Port Type	Commands
Access	undo port default vlan
Trunk	undo port trunk pvid vlan undo port trunk allow-pass vlan all port trunk allow-pass vlan 1
Hybrid	undo port hybrid pvid vlan undo port hybrid vlan all port hybrid untagged vlan 1

3. Remove or cancel operations

Just put “undo” in front of the previously issued command to cancel the operation of that command. For example,

```
# delete vlan 20。
undo vlan 20
# delete vlan 10 to 100 in batch
undo vlan batch vlan 10 to vlan 100
# Restore port 9 to the default vlan 1
[LSW1-GigabitEthernet0/0/9] undo port default vlan
```

Answer the following questions:

Q2-1.1. Paste the screenshot of the created topology.

Q2-1.2. Draw IEEE 802.1D tagged frame format.

Q2-1.3. Paste the screenshot of VLAN 10 information.

Q2-1.4. Paste the screenshot of VLAN 30 information

Q2-1.5. Suppose you are going to create a new VLAN 40, and add ports 17-20 to this VLAN in batches. Please list the configuration command.

Step 5: Verify the configurations.

Double-click each PCs, select the "Command" tab in the pop-up window, enter the following commands.

```
ping 192.168.10.11
ping 192.168.10.12
ping 192.168.30.11
ping 192.168.30.12
```

Answer the following questions:

Q2-1.6. Can PCs in the same VLAN ping each other? Please paste the screenshot of the ping result.

Q2-1.7. Can PCs in different VLANs ping each other? Please paste the screenshot of the ping result. If the ping fails, please explain the reasons.

LAB-2-2: MAC ADDRESS-BASED VLAN CONFIGURATION

Requirements

A network has been implemented in Lab-2-1. The computers of Department A are in VLAN 10, and the computers of Department B in VLAN 30. Now the staff of these two departments often have a meeting together. Each department has a laptop, and each department has a conference room. It is required that no matter which department's conference room is used, the laptops of each department can access the department's computers. The network topology is shown in Figure 2-2. Please configure MAC Address-based VLANs.

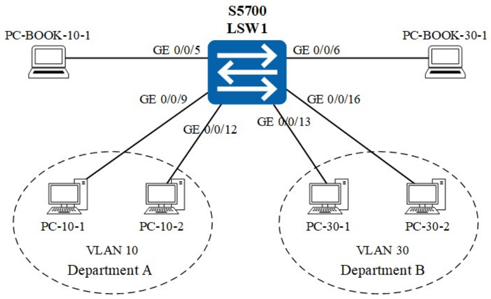

Figure 2-2 A switched Ethernet with two VLANs

The IPv4 address allocation in different VLANs are shown in Table 2-5.

Table 2-5 IPv4 Address Allocation

	IPv4 Address	**Mask**
VLAN 10	**192.168.10.0**	**255.255.255.0**
PC-10-1	192.168.10.11	255.255.255.0
PC-10-2	192.168.10.12	255.255.255.0
PC-BOOK-10-1	192.168.10.18	255.255.255.0
VLAN 30	**192.168.30.0**	**255.255.255.0**
PC-30-1	192.168.30.11	255.255.255.0
PC-30-2	192.168.30.12	255.255.255.0
PC-BOOK-30-1	192.168.30.18	255.255.255.0

Steps

Step 1: Load and modify the topology.

1. Start eNSP and click the "Open" icon in the toolbar, and load the topology file **lab-2-1 VLAN.PORT.topo** saved in lab-2-1.
2. Add two more PCs for simulating laptop computers in the work area. Name the PCs and connect them to the ports GE 0/0/5 and GE 0/0/6.
3. Check and make sure the settings of the IP address and subnet mask of each PC match the address allocation.
4. Click the "Save As" icon in the toolbar to save the topology as **lab-2-2 VLAN.MAC.topo.**

Step 2: Start devices.

Click the " Start Device" icon ▶ in the toolbar to start all devices.

Step 3: Check VLAN Configurations.

Double-click the icon of switch LSW1 in the work area to open the switch configuration window. Enter the following commands to check if VLAN 10 and VLAN 30 have been created and the ports GE /0/0/9 to GE 0/0/12 on the switch have been assigned to VLAN 10 and ports GE 0/0/13 to GE 0/0/16 are assigned to VLAN 30. If not, follow the steps in lab-2-1 to create port-based VLANs.

```
<huawei> display vlan
<huawei> display vlan summary
<huawei> display port vlan
```

Step 4: Assign MAC Addresses to VLANs.

1. Record the MAC addresses of the two laptops in Table 2-6.

Table 2-6 MAC addresses of the two laptops

Laptop	MAC Address
PC-BOOK-10-1	
PC-BOOK-30-1	

2. Configure MAC Address-based VLANs

```
<LSW1> system-view
# enter VLAN mode
[LSW1] vlan 10
# assign MAC address to VLAN. The MAC address format is like xxxx-xxxx-xxxx, such as 5489-9841-80E3。
[LSW1-vlan10] mac-vlan mac-address PC-BOOK10-1's MAC address priority 0
[LSW1] vlan 30
[LSW1-vlan30] mac-vlan mac-address PC-BOOK10-1's MAC address priority 0

# configure the interface as a hybrid type and add it to the VLANs associated with MAC addresses in untagged mode.
[LSW1] interface gigabitethernet 0/0/5
[LSW1-GigabitEthernet0/0/5] port link-type hybrid
[LSW1-GigabitEthernet0/0/5] port hybrid untagged vlan 10 30
# enable MAC address-based VLAN assignment
[LSW1-GigabitEthernet0/0/5] mac-vlan enable
[LSW1-GigabitEthernet0/0/5] quit

[LSW1] interface gigabitethernet 0/0/6
[LSW1-GigabitEthernet0/0/6] port link-type hybrid
[LSW1-GigabitEthernet0/0/6] port hybrid untagged vlan 10 30
[LSW1-GigabitEthernet0/0/6] mac-vlan enable
[LSW1-GigabitEthernet0/0/6] quit

# check configurations of all MAC address-based VLANs
[LSW1] display mac-vlan mac-address all
# check configurations of MAC address-based VLAN 10 and 30
[LSW1] display mac-vlan vlan 10
[LSW1] display mac-vlan vlan 30
[LSW1] display vlan
[LSW1] display vlan summary
[LSW1] display port vlan
```

Answer the following questions:

Q2-2.1. Paste the screenshot of the created topology.

Q2-2.2. Paste the table of MAC addresses of the two laptops you recorded.

Q2-2.3. Paste the screenshot of the configuration information of all MAC address-based VLANs.

Q2-2.4. When adding members to VLAN 10 and VLAN 30 based on the MAC address, what is the difference between VLAN 10 and VLAN 30 information before and after adding members? Please paste the screenshot of VLAN 10 information before and after adding members.

Step 5: Verify the configurations.

Double-click PC-10-1 and PC-BOOK10-1, select the "Command" tab in the pop-up window, enter the following commands.

```
ping 192.168.10.11
ping 192.168.10.18
```

Double-click PC-30-1 and PC-BOOK30-1, select the "Command" tab in the pop-up window, enter the following commands.

```
ping 192.168.30.11
ping 192.168.30.18
```

Answer the following questions:

Q2-2.5. Can PC-10-1 ping PC-BOOK10-1 each other? Please paste the screenshot of the ping result.

Q2-2.6. Can PC-30-1 ping PC-BOOK30-1 each other? Please paste the screenshot of the ping result.

Delete the original connection of PC-BOOK10-1 and PC-BOOK30-1 to the switch, reconnect them to the switch, but exchange the switch ports they are connected to, and use the ping command to test whether the computers in the same VLAN can communicate.

Answer the following questions:

Q2-2.7. Paste the screenshot of the new topology.

Q2-2.8. Can PC-10-1 ping PC-BOOK10-1 each other? Please paste the screenshot of the ping result.

Q2-2.9. Can PC-30-1 ping PC-BOOK30-1 each other? Please paste the screenshot of the ping result.

LAB-2-3: IP SUBNET-BASED VLAN CONFIGURATION

Requirements

A network has been implemented in Lab-2-2. VLAN 10 and 30 are configured based on port and MAC address. The computers of Department A are in VLAN 10, and the computers of Department B in VLAN 30. Now, each department is equipped with a new computer, and each computer is required to access the VLAN of different departments as needed. The network topology is shown in Figure 2-3. Please configure IP subnet-based VLANs.

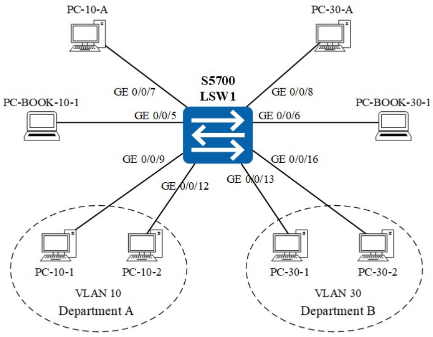

Figure 2-3 A switched Ethernet with two VLANs

The IPv4 address allocation in different VLANs are shown in Table 2-7.

Table 2-7 IPv4 Address Allocation

	IPv4 Address	**Mask**
VLAN 10	**192.168.10.0**	**255.255.255.0**
PC-10-1	192.168.10.11	255.255.255.0
PC-10-2	192.168.10.12	255.255.255.0
PC-BOOK-10-1	192.168.10.18	255.255.255.0
PC-10-A	192.168.10.20	255.255.255.0
VLAN 30	**192.168.30.0**	**255.255.255.0**
PC-30-1	192.168.30.11	255.255.255.0
PC-30-2	192.168.30.12	255.255.255.0
PC-BOOK-30-1	192.168.30.18	255.255.255.0
PC-30-A	192.168.30.20	255.255.255.0

Steps

Step 1: Load and modify the topology.

1. Start eNSP and click the "Open" icon in the toolbar, and load the topology file **lab-2-2 VLAN.MAC.topo** saved in lab-2-2.
2. Add two more PCs for simulating laptop computers in the work area. Name the PCs and connect them to the ports GE 0/0/7 and GE 0/0/8.
3. Check and make sure the settings of the IP address and subnet mask of each PC match the address allocation.
4. Click the "Save As" icon in the toolbar to save the topology as **lab-2-3 VLAN.IPsubnet.topo**.

Step 2: Start devices.

Click the " Start Device" icon in the toolbar to start all devices.

Step 3: Check VLAN Configurations.

Double-click the icon of switch LSW1 in the work area to open the switch configuration window. Enter the following commands to check whether VLAN 10 and VLAN 30 have been created and the ports have been assigned to the specified VLANs. If not, follow the steps in lab-2-2 to create VLANs, assign ports and MAC addresses to the VLANs.

```
<huawei> display vlan
<huawei> display vlan summary
<huawei> display port vlan
```

Step 4: Configure IP subnet-based VLANs.

```
<LSW1> system-view
# enter VLAN mode
[LSW1] vlan 10
# associate IP subnets to VLAN 10 and 30.
# configure the switch to forward packets with the IP address of 192.168.10.0/24 and priority of 1 in VLAN 10.
[LSW1-vlan10] ip-subnet-vlan 1 ip 192.168.10.0 24 priority 1
[LSW1-vlan10] quit
[LSW1] vlan 30
[LSW1-vlan30] ip-subnet-vlan 1 ip 192.168.30.0 24 priority 1
[LSW1-vlan30] quit

# configure interfaces and enable IP subnet-based VLAN assignment.
[LSW1] interface gigabitethernet 0/0/7
[LSW1-GigabitEthernet0/0/7] port link-type hybrid
[LSW1-GigabitEthernet0/0/7] port hybrid untagged vlan 10 30
[LSW1-GigabitEthernet0/0/7] ip-subnet-vlan enable
[LSW1-GigabitEthernet0/0/7] quit

[LSW1] interface gigabitethernet 0/0/8
[LSW1-GigabitEthernet0/0/8] port link-type hybrid
[LSW1-GigabitEthernet0/0/8] port hybrid untagged vlan 10 30
[LSW1-GigabitEthernet0/0/8] ip-subnet-vlan enable
[LSW1-GigabitEthernet0/0/8] quit

# check configurations of all IP subnet-based VLANs
[LSW1] display ip-subnet-vlan vlan all
# check configurations of IP subnet-based VLAN 10 and 30
[LSW1] display ip-subnet-vlan vlan 10
[LSW1] display ip-subnet-vlan vlan 30
[LSW1] display vlan
[LSW1] display vlan summary
# Display information about interfaces in VLANs
[LSW1] display port vlan
```

Answer the following questions:

Q2-3.1. Paste the screenshot of the created topology.

Q2-3.2. Paste the screenshot of the configuration information of all IP subnet-based VLANs.

Step 5: Verify the configurations.

Double-click PC-10-1, PC-BOOK10-1 and PC-10-A, select the "Command" tab in the pop-up window, enter the following commands.

```
ping 192.168.10.11
ping 192.168.10.18
ping 192.168.10.20
```

Double-click PC-30-1 PC-BOOK30-1 and PC-30-A, select the "Command" tab in the pop-up window, enter the following commands.

```
ping 192.168.30.11
ping 192.168.30.18
ping 192.168.30.20
```

Answer the following questions:

Q2-3.3. Can PC-10-1, PC-BOOK10-1 and PC-10-A ping each other? Please paste the screenshot of the ping result.

Q2-3.4. Can PC-30-1, PC-BOOK30-1 and PC-30-A ping each other? Please paste the screenshot of the ping result.

Keep the connections, but assign new IP addresses to PC-10-A and PC-30-A. Set the IP address of PC-10-A to 192.168.30.20 in VLAN 30 and PC-10-B to 192.168.10.20 in VLAN 10. Use the ping command to test whether the computers in the same VLAN can communicate.

Answer the following questions:

Q2-3.5. Can PC-10-1, PC-BOOK10-1 and PC-30-A ping each other? Please paste the screenshot of the ping result.

Q2-3.6. Can PC-30-1, PC-BOOK30-1 and PC-10-A ping each other? Please paste the screenshot of the ping result.

Q2-3.7. Paste information about ports or interfaces that belong to each VLAN.

LAB-2-4: 802.1Q TRUNK CONFIGURATION

Requirements

A network has been implemented in Lab-2-1. The computers of Department A are in VLAN 10, and the computers of Department B in VLAN 30. Recently, the staff and computers in these two departments have increased, and there are also more offices. The original switch can no longer connect to more computers, and the system needs to be expanded. The solution is to add a switch and configure a trunk between the switches to achieve VLAN cross-switch span. The network topology is shown in Figure 2-4. Please configure trunk between switches to span VLANs across switches.

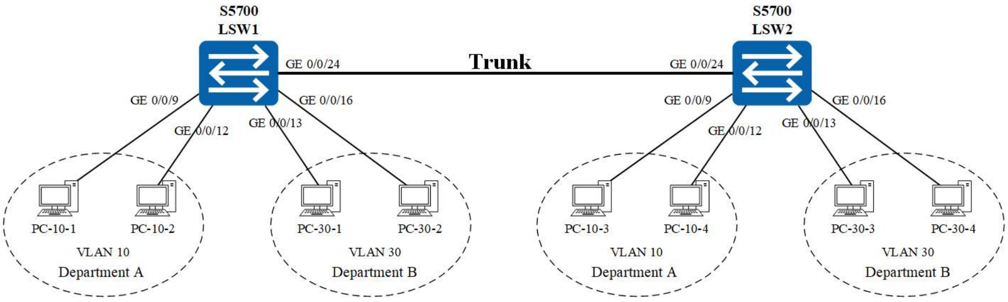

Figure 2-4 VLAN span across switches

The IPv4 address allocation in different VLANs are shown in Table 2-8.

Table 2-8 IPv4 Address Allocation

	IPv4 Address	**Mask**
VLAN 10	**192.168.10.0**	**255.255.255.0**
PC-10-1	192.168.10.11	255.255.255.0
PC-10-2	192.168.10.12	255.255.255.0
PC-10-3	192.168.10.13	255.255.255.0
PC-10-4	192.168.10.14	255.255.255.0
VLAN 30	**192.168.30.0**	**255.255.255.0**
PC-30-1	192.168.30.11	255.255.255.0
PC-30-2	192.168.30.12	255.255.255.0
PC-30-3	192.168.30.13	255.255.255.0
PC-30-4	192.168.30.14	255.255.255.0

Steps

Step 1: Load and modify the topology.

1. Start eNSP and click the "Open" icon in the toolbar, and load the topology file **lab-2-1 VLAN.PORT.topo** saved in lab-2-1.
2. Add another one S5700 switch and four more PCs to the work area. Name the switch and PCs and cable as necessary.
3. Check and make sure the settings of the IP address and subnet mask of each PC match the address allocation.
4. Click the "Save As" icon in the toolbar to save the topology as **lab-2-4 VLAN.TRUNK.topo**.

Step 2: Start devices.

Click the " Start Device" icon in the toolbar to start all devices.

Step 3: Check and Config VLAN on switches.

Double-click the icon of switch LSW1 and LSW2 in the work area to open the switch configuration window. Enter the following commands to check whether VLAN 10 and VLAN 30 have been created and the ports have been assigned to the specified VLANs on the switch LSW1 and LSW2. If not, follow the steps in lab-2-1 to create VLANs and assign ports to the VLANs on LSW1 and LSW2.

```
<huawei> display vlan
<huawei> display vlan summary
<huawei> display port vlan
```

Step 4: Configure a trunk between switches.

1. Configure LSW1.

```
<LSW1> system-view
# set the link type of interface GE 0/0/24 to trunk. By default, the link type of an interface is hybrid.
[LSW1] interface gigabitethernet 0/0/24
[LSW1-GigabitEthernet0/0/24] port link-type trunk
# add the trunk interface to the VLAN 10 and 30, allowing their traffic be transported.
# command "port trunk allow-pass vlan all" add the trunk interface to all VLAN.
[LSW1-GigabitEthernet0/0/24] port trunk allow-pass vlan 10 30
```

2. Configure LSW2.

Configure the interface GE 0/0/24 on the switch LSW2 as a trunk port in the same way as configuring interface GE 0/0/24 on switch LSW1.

Step 5: Verify the configurations and analyze the traffic on the trunk link.

Start data capture on interfaces GE 0/0/9 and GE 0/0/24 on switch LSW1.
Ping PC-10-3 from PC-10-1 command window and visa versa.
Ping PC-30-3 from PC-30-1 command window and visa versa.

Answer the following questions:

Q2-4.1. Paste the screenshot of the created topology.
Q2-4.2. Can PC-10-1 and PC-10-3 ping each other? Please paste the screenshot of the ping result.
Q2-4.3. Can PC-30-1 and PC-30-3 ping each other? Please paste the screenshot of the ping result.
Q2-4.4. Can PC-10-1 and PC-30-3 ping each other? Please paste the screenshot of the ping result.
Q2-4.5. Are the Ethernet frames captured on interface GE 0/0/24 on switch LSW1 tagged or untagged frames? If they are tagged frames, what are the VLAN IDs? Please paste the screenshot of all field information of two captured Ethernet frames with different VLAN IDs.
Q2-4.6. Are the Ethernet frames captured on interface GE 0/0/9 on switch LSW1 tagged or untagged frames? If they are tagged frames, what are the VLAN IDs? Please paste the screenshot of all field information of a captured Ethernet frame.

COMMENTS

Your comments and/or suggestions on this lab: