**网络技术实践**

**实验报告**

**学号：1120141831**

**姓名：朴泉宇**

**班级：07111403**

**北京理工大学**

**计算机学院**

**2017年11月**

**第二部分**

**网络配置(工程)**

**小组成员:宋傲、刘洪毅、林理露、朴泉宇、谷飒、许晟华、颜航**

**Lab Exercise2 VLAN Design and Configuration**

Directory

[**Objectives** 1](#_Toc430786015)

[**Requirements** 1](#_Toc430786016)

[**Step 1: Configure VLANs on one switch** 3](#_Toc430786017)

[**Step 2: MAC Address Table Management** 6](#_Toc430786018)

[**Step 3: Configure VLANs across switches** 9](#_Toc430786019)

[**Step 4: Configure Port Mirroring** 12](#_Toc430786020)

[**Step 5: Link Aggregation Configuration** 14](#_Toc430786021)

# **Objectives**

* Deepen understanding of LAN: IEEE 802 LAN standards, switched Ethernet, and VLAN.
* Mastering the basic methods of VLAN configuration.
* Mastering the basic operation, maintenance and troubleshooting of Ethernet switches.

# **Requirements**

**Wireshark:** This lab uses the Wireshark software tool to capture and examine a packet trace.

**ping:** This lab uses “ping” to send and receive messages. The ping command is used to verify that a device can communicate with another on a network.

**S3100:** A H3C Layer 2 switch.

**S3610:** A H3C Layer 3 switch.

**Turn in**

Hand in the exercise report including your answers to the questions, screens you capture and trace file you saved.

**Understanding VLAN**

**What is a LAN?**

Connecting the computers in your organization via a LAN can save you a lot of time and money. A LAN is a high-speed, fault-tolerant data network that covers a relatively small geographic area. Ittypically connects workstations, personal computers, printers, and other devices. LANs offercomputer users many advantages, including shared access to devices and applications, ﬁle exchangebetween connected users, and communication between users via electronic mail and otherapplications.

**What is a VLAN?**

VLANs, or virtual LANs, allow a network manager to logically segment a LAN into different broadcast domains. Since this is a logical segmentation and not a physical one, workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.

Switches on any network are by default set on broadcast mode. For example with 80 switches, if one broadcasts all the 79 others receive it. They in turn might generate their own broadcasts in response to it and the process cascades hereon. This results in the cause of what is called a **broadcast storm**. Not only does it eat up the bandwidth, but it also is a huge waste of switch resources. This causes the switch to become practically useless for the network and reduces the overall speed of the network.

A VLAN is defined as a broadcast domain within a switched network. Broadcast domains describe the extent that a network propagates a broadcast frame generated by a station. Some switches may be configured to support a single or multiple VLANs. Whenever a switch supports multiple VLANs, broadcasts within one VLAN never appear in another VLAN. Switch ports configured as a member of one VLAN belong to a different broadcast domain, as compared to switch ports configured as members of a different VLAN.

Creating VLANs enables administrators to build broadcast domains with fewer users in each broadcast domain. This increases the bandwidth available to users because fewer users will contend for the bandwidth.

# **Step 1: Configure VLANs on one switch**

**Device used**

H3CS3100orS3610.

H3CS3100 and S3610may be configured to support a single or multiple VLANs.

**Network Diagram**



**Tasks**

Create twoVLANs on a switch.

**Configuration procedure**

1. Choose one switch and one PC. The PC is used to configure the switch.
2. Connect console cable
3. Connect the DB-9 female connector of the console cable to the serial port of the PC.
4. Select the correspondent port on the right the patch panel and connect it to console port of a switchwith a patch cord.
5. Setting Terminal Parameters
6. [**Start/Program/Accessories/Communications/HyperTerminal**] to enter the HyperTerminal window
7. Click the http://www.h3c.com/portal/res/200906/01/20090601_773677_image078_636110_1285_0.png icon to establish a new connection.
8. Type in the name of the new connection in the connection description interface and click <**OK**>. Thenselect the **COM1** to be used from [**Connect using**].
9. Click <**OK**>.Set terminal parameters as follows:
   * + Baud rate to**9600**
     + data bits to **8**
     + parity check to **none**
     + stop bits to **1**
     + flow control to **none**
10. Click <**OK**> and the system will displaythe window of HyperTerminal. Select the window and press <**Enter**>, you will see the prompt like <H3C>.
11. Configure the switch A

**#Enter system view to enable configuration.**

<H3C> system-view

**# Assign a new name SA to the switch.**

[H3C]sysname SA

**#Create VLAN 10 and assign port Ethernet 1/0/5, 1/0/7 and 1/0/9 to VLAN 10.**

[SA] vlan 10

[SA-vlan10] port e1/0/5 e1/0/7 e1/0/9

[SA-vlan10] quit

**#Display VLAN information**

[SA] display vlan 10

**#Display interface information**

[SA] display interface Ethernet 1/0/5

**#Create VLAN 20 and assign port Ethernet 1/0/6, 1/0/8 and 1/0/10 to VLAN 20.**

[SA] vlan 20

[SA-vlan20] port e1/0/6 e1/0/8 e1/0/10

[SA-vlan20] quit

**#Display VLAN information**

[SA] display vlan 20

**#Display interface information**

[SA] display interface Ethernet 1/0/6

**Troubleshooting Ethernet Port Configuration**

* **Symptom:** Fail to configure the default VLAN ID of an Ethernet port.
* **Solution:** Use the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port.

After you finish the configuration, the hosts of the two VLAN should be isolated at the data link layer.

1. Install the USB Ethernet Card on your computers

Plug the USB card into the USB port of a PC, insert the CD into the CD drive, and let window XP to find and install card driver from the CD.

1. Connect PCs to the VLANs respectively
2. Choose a PC and connect the network cable to its NIC port.
3. Select the correspondent port on the left of the patch panel and connect it to a VLAN port of the switch with a patch cord.
4. Configure TCP/IP Properties

The network Address of VLAN 10 is assumed to be **192.168.10.0**, the mask is **255.255.255.0**, and default gateway is **192.168.10.1**, DNS Server is **192.168.10.200**.

The network Address of VLAN 20 is assumed to be **192.168.20.0**,the mask is **255.255.255.0**, and default gateway is **192.168.20.1**, DNS Server is **192.168.20.200**.

Because we will **ping** a host by its IP address, the DNS Server address can be any.

Assign IP address and other configuration parametersmanually to the host of VLAN 10 and VLAN 20 by the given information above.

Pick a host in the same VLAN as your PC and a host in a different VLAN from your PC and use ping to verify if a host can communicate with another on a network. For example, “ping 192.168.10.10” or “ping 192.168.20.10”.

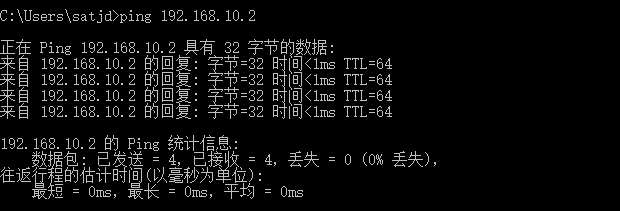
**Answer the following questions:**

1. What is the broadcast domain? What is the collision domain?

一个VLAN是一个广播域；交换机的每一个不同端口都是一个冲突域。

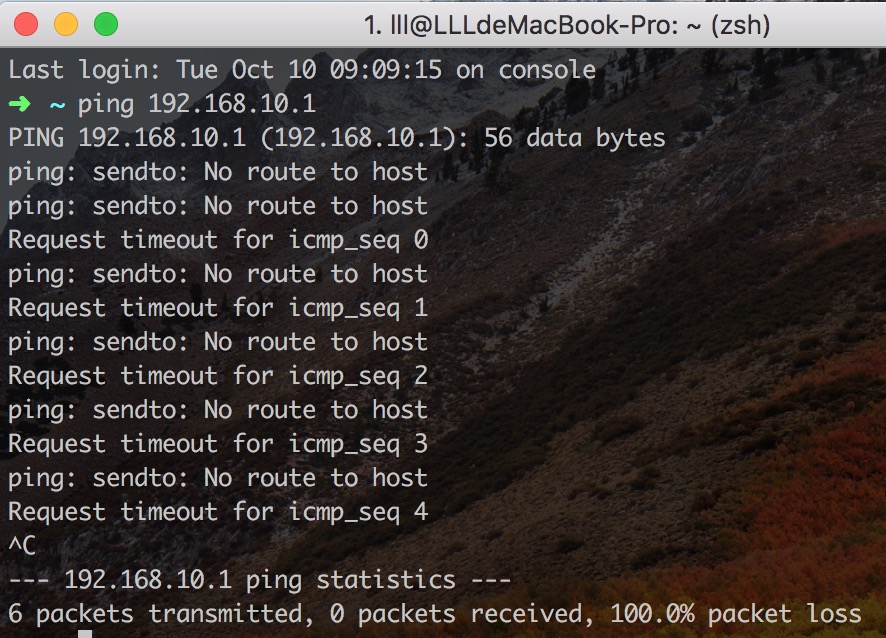
1. Can the hosts in the same VLAN communicate? (Show the ping message screen you captured.)

可以。



1. Can the hosts in the different VLAN communicate? (Show the ping message screen you captured.)

不可以。



# **Step 2:** **MAC Address Table Management**

**Introduction to MAC Address Table**

An Ethernet switch is mainly used to forward packets at the data link layer, that is, transmit the packets to the corresponding ports according to the destination MAC address of the packets. To forward packets quickly, a switch maintains a MAC address table, which is a Layer 2 address table recording the MAC address-to-forwarding port association. Each entry in a MAC address table contains the following fields:

* Destination MAC address
* ID of the VLAN which a port belongs to
* Forwarding egress port number on the local switch

Generally, the majority of MAC address entries are created and maintained through MAC address learning–Backward Learning Algorithm.

When forwarding a packet, an Ethernet switch adopts one of the two forwarding methods based upon the MAC address table entries.

* **Unicast forwarding:** If the destination MAC address carried in the packet is included in a MAC address table entry, the switch forwards the packet through the forwarding egress port in the entry.
* **Broadcast forwarding:** If the destination MAC address carried in the packet is not included in the MAC address table, tthe switch broadcasts the packet to all ports except the one that originally received the packet.

**Managing MAC Address Table**

|  |  |
| --- | --- |
| Task | Note |
| Entries in a MAC address table | You can add, modify, or remove a MAC address entry, remove all MAC address entries concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries).   * **Static MAC address entry:** Also known as permanent MAC address entry. This type of MAC address entries are added/removed manually by the network operator and cannot age out by themselves. * **Dynamic MAC address entry:**This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually. * **Blackhole MAC address entry:** This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries. |
| Aging of MAC address table | To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch starts an aging timer for an entry when dynamically creating the entry.  The switch removes the MAC address entry if no more packets with the MAC address recorded in the entry are received within the aging time. |

**Tasks**

In Step1, you have configured 2 VLANs on the switch. In this step, you are required to finish the following MAC address table management tasks:

* Set the aging timer to 500 seconds for dynamic MAC address entries.
* Add a static entry 000f-e234-dc71 for port Ethernet 1/0/9 in VLAN 10.
* Discards the packets destined for or originated from the MAC addresses????-????-????on specified port Ethernet 1/0/9.
* Only allow port Ethernet 1/0/9 to send packets destined for the address 000f-e234-dcdc.

**Configuration procedure**

Connect a host to the port Ethernet 1/0/9. Find and record the MAC address of this host.

**#Enter system view to enable configuration.**

<H3C> system-view

**# Assign a new name SA to the switch.**

[H3C]sysname SA

**# Display information about the current MAC table of SA.**

[SA]display mac-address

**# Display the MAC address entry for port Ethernet 1/0/9.**

[SA]display mac-address interface Ethernet 1/0/9

**# Add a static MAC address, with the VLAN, ports, and states specified.**

[SA] mac-address static 000f-e234-dc71 interface Ethernet 1/0/9vlan10

**# Display the MAC address entry for port Ethernet 1/0/9.**

[SA]display mac-addressinterface Ethernet 1/0/9

Now disconnect the host from the port Ethernet 1/0/9 and connect it to the port Ethernet 1/0/9 again.

**Answer the following questions:**

1. Has the port Ethernet 1/0/9 learned the host’s MAC address?If not, Why?

Ethernet 1/0/9没有学习主机的MAC地址。

在上述的操作中，已经将1/0/9的静态地址设置为：000f-e234-dc71。

**# Undo the previous static MAC address setting and restore.**

[SA] undo mac-address static 000f-e234-dc71 interface Ethernet 1/0/9 vlan10

Disconnect the host from the port Ethernet 1/0/9 and connect it to the port Ethernet 1/0/9 again.

**# Display the MAC address entry for port Ethernet 1/0/9.**

[SA]display mac-addressinterface Ethernet 1/0/9

You’ll find the port Ethernet 1/0/9 has learned the MAC address of the host and you can ping other hosts from this machine.

**# Add a black hole MAC address of the host, with the VLAN and ports specified.Replace ????-????-???? with the MAC address of the host you recorded.**

[SA] mac-address blackhole????-????-????interface Ethernet 1/0/9vlan10

**# Display the MAC address entry for port Ethernet 1/0/9.**

[SA]display mac-addressinterface Ethernet 1/0/9

pingother hosts of VLAN 10 from the host and ping this host from the hosts.

**Answer the following questions:**

1. Can the host ping other hosts of VLAN 10 or vice versa?If not, Why?

可以。

黑洞仅设置在了1/0/9，其他端口不受影响。

**# Display the age time of MAC address entry.**

[SA] display mac-address aging-time

**# Set the aging timer for dynamic MAC address entries to 500 seconds.**

[SA] mac-address timer aging 500

**# Display the age time of MAC address entry.**

[SA] display mac-address aging-time

**# Display the MAC address entry for port Ethernet 1/0/9.**

[SA]display mac-addressinterface Ethernet 1/0/9

**# Disable Ethernet 1/0/9 from learning MAC addresses dynamically, and add a static MAC address entry000f-e234-dcdc. So that port Ethernet 1/0/9 can only send packets destined for the host, and other hosts cannot communicate through this port.**

[SA] interface Ethernet 1/0/9

[SA-Ethernet1/0/10] mac-address max-mac-count 0

[SA-Ethernet1/0/10] mac-address static 0014-234-dcdcvlan 10

**# Display the MAC address entry for port Ethernet 1/0/9.**

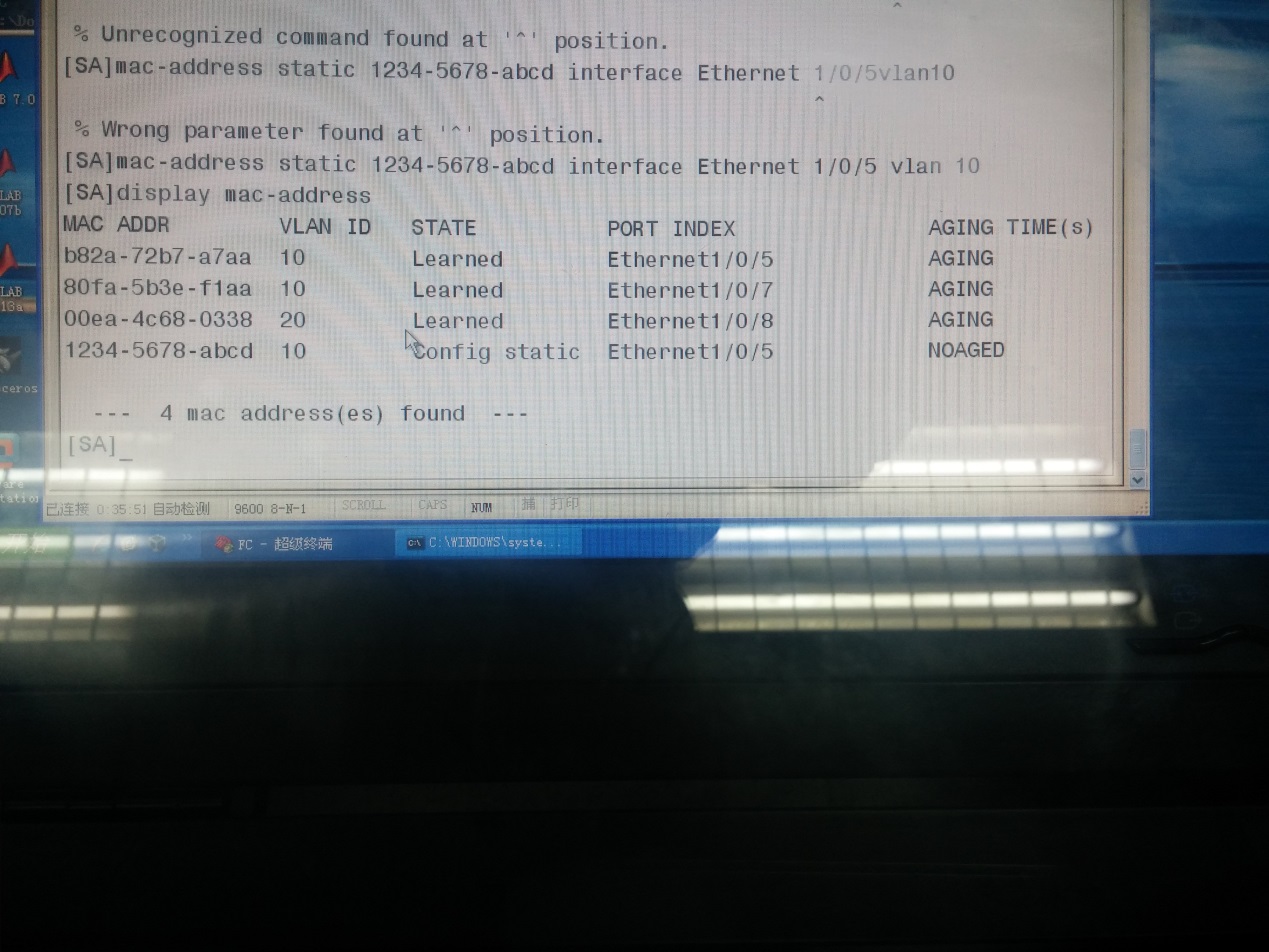
[SA]display mac-addressinterface Ethernet 1/0/9

**Answer the following questions:**

1. What is the original age time of MAC address entry?

300秒。

1. Show the captured screen of the MAC address entry for port Ethernet 1/0/9.



# **Step 3: Configure VLANsacrossswitches**

**Device used**

A S3100and a S3610.

**Network Diagram**



**Tasks**

Create 2 VLANs across 2 switches and allow the hosts in the same VLAN can communicate.

**Configuration procedure**

1. Choose one S3100and one S3610 switch and 2 PCs. These2 PCsare used for the configuration of oneswitch respectively.
2. Connect two switches with a patch cord. Plug each end of the cable into the port e/1/0/2 of each switch. The port e/1/0/2 now is used as a trunk port.
3. Configure the switch S3100

**# Create VLAN 10and VLAN 20 on Switch S3100.**

**#Enter system view to enable configuration.**

<H3C> system-view

**# Assign a new name SA to the switch.**

[H3C]sysname SA

**#Create VLAN 10 and assign portEthernet 1/0/5, 1/0/7 and 1/0/9 to VLAN 10.**

[SA] vlan 10

[SA-vlan10] port e1/0/5 e1/0/7

[SA-vlan10] quit

**#Display VLAN information**

[SA] display vlan 10

**#Create VLAN 20 and assign portEthernet 1/0/6, 1/0/8 and 1/0/10 to VLAN 20.**

[SA] vlan 20

[SA-vlan20] port e1/0/6 e1/0/8

[SA-vlan20] quit

**#Display VLAN information**

[SA] display vlan20

**# Configure port Ethernet 1/0/2 as a trunk port permitting the frames of VLAN 10 and VLAN 20 to pass through with VLAN tags.**

[SA]interface e1/0/2

[SA-Ethernet1/0/2] port link-type trunk

[SA-Ethernet1/0/2] port trunk permit vlan10 20

1. Configure the switch S3610

**# Create VLAN 20and VLAN 30 on Switch S3610 as you have done on Switch S3100.**

**#Enter system view to enable configuration.**

<H3C> system-view

**# Assign a new name SB to the switch.**

[H3C]sysname SB

**#Create VLAN 10 and assign port Ethernet 1/0/5 and 1/0/7 to VLAN 10.**

[SB] vlan 10

[SB-vlan10] port e1/0/5 e1/0/7

[SB-vlan10] quit

**#Display VLAN information**

[SB] display vlan 10

**#Create VLAN 20 and assign port Ethernet 1/0/6 and 1/0/8 to VLAN 20.**

[SB] vlan20

[SB-vlan20] port e1/0/6 e1/0/8

[SB-vlan20] quit

[SB] display vlan20 #Display VLAN information

**# Configure port Ethernet 1/0/2 as a trunk port permitting the frames of VLAN 10 and VLAN 20 to pass through with VLAN tags.**

[SB] interface e1/0/2

[SB-Ethernet1/0/2] port link-type trunk

[SB-Ethernet1/0/2] port trunk permit vlan10 20

**Troubleshooting Ethernet Port Configuration**

* **Symptom:** Fail to configure the default VLAN ID of an Ethernet port.
* **Solution:** Use the **display interface**or **display port** command to check if the port is a trunk port or a hybrid port.

After you finish the configuration, the hosts of the two VLAN should be isolated at the data link layer.

1. Choose 2 PCs and connect them to the VLAN 10. One PC is connected to the port of VLAN 10 of SA, the other to the port of VLAN 10 of SB. The network Address of VLAN 10 is assumed to be 192.168.10.0, the mask is 255.255.255.0, and default gateway is 192.168.10.1, DNS Server is 192.168.10.200. Set the host’s TCP/IP parameters.
2. Choose 2 PCs and connect them to the VLAN 20. One PC is connected to the port of VLAN 20 of SA, the other to the port of VLAN 20 of SB. The network Address of VLAN 20 is assumed to be 192.168.20.0, the mask is 255.255.255.0, and default gateway is 192.168.20.1, DNS Server is 192.168.20.200. Set the host’s TCP/IP parameters.

Pick a host in the VLAN 10 or VLAN 20, use ping to verify if thehost can communicate with other PCs of VLAN 10 or VLAN 20.

**Answer the following questions:**

1. What is trunk port? What type of Ethernet frames can be forwarded through the trunk link? Draw a figure to show the format of VLAN-tagged Ethernet frame.

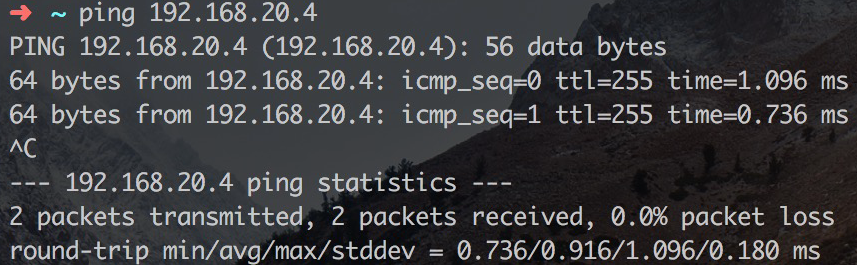
Trunk端口指将多个物理端口通过配置形成一条逻辑端口。

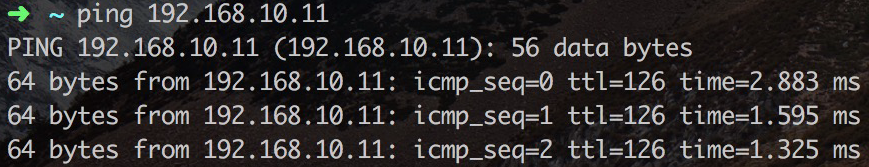
IEEE802.3SNAP帧。



1. Can the hosts of VLAN 10 or VLAN 20 communicate each other? (Show the ping message screen you captured.)

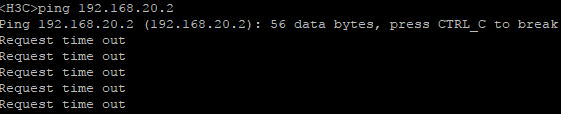
可以。





1. Can the hosts of VLAN 10 communicate with the hosts of VLAN 20? (Show the ping message screen you captured.)

不可以。



# **Step 4: Configure Port Mirroring**

**Mirroring Overview**

Mirroring refers to the process of copying packets of one or more ports (source ports) to a destination port which is connected to a data detection device. Users can then use the data detection device to analyze the mirrored packets on the destination port for monitoring and troubleshooting the network.

H3C S3100 and S3610 series Ethernet switches support two kinds of port mirroring: local port mirroring and remote port mirroring.

* **Local port mirroring** copies packets passing through one or more ports (known as source ports) of a device to the monitor port (also destination port) for analysis and monitoring purpose. In this case, the source ports and the destination port are located on the same device.
* **Remote port mirroring** does not require the source and destination ports to be on the same device. The source and destination ports can be located on multiple devices across the network. Therefore, administrators can monitor the traffic on remote devices conveniently.Currently, remote port mirroring can only be implemented on Layer 2.

**Device used**

S3610.

**Network Diagram**



**Tasks**

The administrator wants to monitor the packets received on and sent from the VLAN10 and VLAN 20 configured in Step 3 through the data detection device, for example, **Wireshark**.

Use the local port mirroring function to meet the requirement.

* Configure Ethernet 1/0/2, 1/0/5, and 1/0/6 of SB (S3610) as mirroring source ports.
* Configure Ethernet 1/0/20of SB (S3610) as the mirroring destination port.

**Configuration procedure**

**# Configure the switch SB(S3610).**

**#Enter system view to enable configuration.**

<SB> system-view

**# Create a local port mirroring group.**

[SB] mirroring-group 1 local

**# Add port Ethernet 1/0/2, 1/0/5, and 1/0/6 to the port mirroring group as source ports. Add port Ethernet 1/0/20 to the port mirroring group as the destination port.**

[SB] mirroring-group 1 mirroring-port Ethernet 1/0/2 Ethernet 1/0/5 Ethernet 1/0/6 both **#can be** both |inbound | outbound

[SB] mirroring-group 1 monitor-port Ethernet 1/0/20

**# Display the configuration of all the port mirroring groups.**

[SB] display mirroring-group all

After the configurations, you can monitor all packets received on and sent from the VLAN 10 and VLAN 20, and all packets transmitted on the trunk link on aPC connected to Ethernet 1/0/20 of SB(S3610).

**Capture a Trace**

1. Choose a PC and connect it to the Ethernet 1/0/20 of SB(S3610).
2. Launch Wireshark and start a capture of Ethernet frames.
3. Pick a host of the VLAN 10 and ping the other hosts of the VLAN 10.
4. Pick a host of the VLAN 20 and ping the other hosts of VLAN 20
5. After the ping command is complete, return to Wireshark, stop and save the trace.
6. Examine the packets that you captured.

**Answer the following questions:**

1. Explain what the port mirroring is used for?

端口镜像用于监视一些端口的流量，便于调试。

1. What is the tag value of VLAN 10 and VLAN 20?

IGMP Snooping.

1. Inspecting the trace, can you distinguish which packets from which port?

查看包的标记即可。

# **Step 5: Link Aggregation Configuration**

**Link Aggregation****Overview**

**Link aggregation**

Link aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link. In addition, it provides reliable connectivity because these member ports can dynamically back up each other.

**LACP**

Link aggregation control protocol (LACP) is designed to implement dynamic link aggregation and deaggregation. This protocol is based on IEEE802.3ad and uses link aggregation control protocol data units (LACPDUs) to interact with its peer.

**Approaches to Link Aggregation**

Two ways are available for implementing link aggregation.

* Manual link aggregations are created manually. Member ports in a manual aggregation are LACP-disabled.
* Static LACP link aggregations are created manually. After you add a port to a static aggregation, LACP is enabled on it automatically.

**Device used**

A S3100and a S3610.

**Network Diagram**



**Tasks**

* Connects Switch A to Switch B with three ports Ethernet1/0/2 to Ethernet1/0/4. It is required that incoming/outgoing load between the two switches can be shared among these three ports.
* Configure manual link aggregation and allow VLAN 10 and VLAN 20 to communicate respectively.

**Configuration procedure**

1. Connect two switches with patch-cords.
2. Configure manual link aggregation and allowthe host of VLAN 10 and VLAN 20 to communicate respectively.
3. Configure the switch SA(S3100).

**#Enter system view to enable configuration.**

<SA> system-view

**# Configure port Ethernet 1/0/2, 1/0/3, and 1/0/4 as trunk ports permitting the frames of VLAN 10 and VLAN 20 to pass through with VLAN tags.**

[SA]interface e1/0/2

[SA-Ethernet1/0/2] port link-type trunk

[SA-Ethernet1/0/2] port trunk permit vlan10 20

[SA]interface e1/0/3

[SA-Ethernet1/0/3] port link-type trunk

[SA-Ethernet1/0/3] port trunk permit vlan10 20

[SA]interface e1/0/4

[SA-Ethernet1/0/4] port link-type trunk

[SA-Ethernet1/0/4] port trunk permit vlan10 20

**# Create manual aggregation group 1.**

[SA] link-aggregation group 1 mode manual

**# Add Ethernet1/0/2 through Ethernet1/0/4 to aggregation group 1.**

[SA] interface Ethernet1/0/2

[SA-Ethernet1/0/2] port link-aggregation group 1

[SA-Ethernet1/0/2] quit

[SA] interface Ethernet1/0/3

[SA-Ethernet1/0/3] port link-aggregation group 1

[SA-Ethernet1/0/3] quit

[SA] interface Ethernet1/0/4

[SA-Ethernet1/0/4] port link-aggregation group 1

1. Configure the switch SB (S3610).

**#Enter system view to enable configuration.**

<SA> system-view

**# Configure port Ethernet 1/0/2, 1/0/3, and 1/0/4 as trunk ports permitting the frames of VLAN 10 and VLAN 20 to pass through with VLAN tags.**

[SB]interface e1/0/2

[SB-Ethernet1/0/2] port link-type trunk

[SB-Ethernet1/0/2] port trunk permit vlan10 20

[SB]interface e1/0/3

[SB-Ethernet1/0/3] port link-type trunk

[SB-Ethernet1/0/3] port trunk permit vlan10 20

[SB]interface e1/0/4

[SB-Ethernet1/0/4] port link-type trunk

[SB-Ethernet1/0/4] port trunk permit vlan10 20

**# Create manual aggregation group 1.**

[SB] link-aggregation group 1 mode manual

**# Add Ethernet1/0/2 through Ethernet1/0/4 to aggregation group 1.**

[SB] interface Ethernet1/0/2

[SB-Ethernet1/0/2] port link-aggregation group 1

[SB-Ethernet1/0/2] quit

[SB] interface Ethernet1/0/3

[SB-Ethernet1/0/3] port link-aggregation group 1

[SB-Ethernet1/0/3] quit

[SB] interface Ethernet1/0/4

[SB-Ethernet1/0/4] port link-aggregation group 1

1. Display information of link aggregations

**# Display summary information of all aggregation groups of SA and SB**

[SA] display link-aggregation summary

[SB] display link-aggregation summary

**#Display detailed information of a specific aggregation group of SA and SB**

[SA] display link-aggregation verbose 1

[SA] display link-aggregation verbose 1

**# Displaylink-aggregation information of a specific interface of SA and SB**

[SA] display link-aggregation interface ethernet1/0/2

[SB] display link-aggregation interface ethernet1/0/2

1. Testing the configuration

Pick a host of VLAN 10 or VLAN 20, pingthe other hosts of VLAN 10 or VLAN 20. Observe the port LED of Ethernet 1/0/2, 1/0/3, 1/0/4 on the switch panel. Flashing LED indicates that the ping traffic is transmitting through on the port. Disconnect the part cable, issue a ping commandand check if thehost can communicate with other hosts and if there are losses of ICMP message.

**Answer the following questions:**

1. What is link-aggregation? What is LACP used for?

链路聚合，用于将多个低带宽的物理接口绑在一起，当作一个高带宽的接口来用，在逻辑上就是一个接口。

链路聚合控制协议，是实现链路动态汇聚的协议。

1. When you ping another host from a host of VLAN 10, which trunk port is used for the communication?When you disconnect the cable of this port, which trunk port is selected to use for the communication?
2. Show the link-aggregation information of interface Ethernet 1/0/3.