**Lab Exercise 2 Inter-VLAN Routing on Layer 3 Switches**

Directory

[Objectives 1](#_Toc417241194)

[Requirements 1](#_Toc417241195)

[Inter-VLAN Routing 2](#_Toc417241196)

[What is Inter-LAN Routing? 2](#_Toc417241197)

[VLAN Routing Solutions 2](#_Toc417241198)

[Configure VLAN Interfaces On Layer 3 Switch S3610 6](#_Toc417241199)

# **Objectives**

* Consolidate what we have learned about VLAN configuration.
* Understand the basics of inter-VLAN routing and Layer 3 switches.
* Giving you an in-depth view on how VLAN routing of L3 switch can be setup to implement inter-VLAN communication.

# **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 with built-in routing capabilities.

**Turn in**

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

# **Inter-VLAN Routing**

## **What is Inter-LAN Routing?**

We have seen that using VLANs to segment a switched network provides improved performance, manageability, and security. Trunks are used to carry information from multiple VLANs between devices. A host can communicate with only those hosts that are members of the same VLAN, the computers on separate VLANs are unable to communicate without the intervention of a routing device. Any device that supports Layer 3 routing, such as a router or a multilayer switch, can be used to perform the necessary routing functionality. Regardless of the device used, the process of forwarding network traffic from one VLAN to another VLAN using routing is known as inter-VLAN routing.

Implementing inter-VLAN routing introduces several benefits, which include the following:

* Reduces broadcast domains, increasing network performance and efficiency.
* Multilayer topologies based upon inter-VLAN routing are much more scalable and implement more efficient mechanisms for accommodating redundant paths in the network than equivalent flat Layer 2 topologies that rely on spanning tree alone.
* Allows for centralized security access control between each VLAN.
* Increases manageability by creating smaller "troubleshooting domains," where the effect of a faulty network interface card (NIC) is isolated to a specific VLAN rather than the entire network.

## **VLAN Routing Solutions**

Virtual LANs (VLANs) divide one physical network into multiple broadcast domains. But VLAN-enabled switches cannot, by themselves, forward traffic across VLAN boundaries. So you need to have routing between these VLANs. To allow hosts in different VLANs communicate with each other, we need a Layer 3 device (like a router) for routing. This Layer 3 routing process can either be implemented using a router or a Layer 3 switch interface. The use of a Layer 3 device provides a method for controlling the flow of traffic between network segments, including network segments created by VLANs.

Within a LAN topology, inter-VLAN routing is used to route packets between different VLANs. Three common inter-VLAN routing architectures are used in modern LAN networks today:

* Router-on-a-stick
* Router-on-a-stick using trunks
* Layer 3 switching

**Router-on-a-stick**

In this legacy approach, inter-VLAN routing is performed by connecting different physical router interfaces to different physical switch ports. As you can see in [Figure 3-1](javascript:popUp('/content/images/bok_1587200600/elementLinks/05fig01.gif')), the switch ports connected to the router are placed in access mode and each physical interface is assigned to a different VLAN. Each router interface can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces.

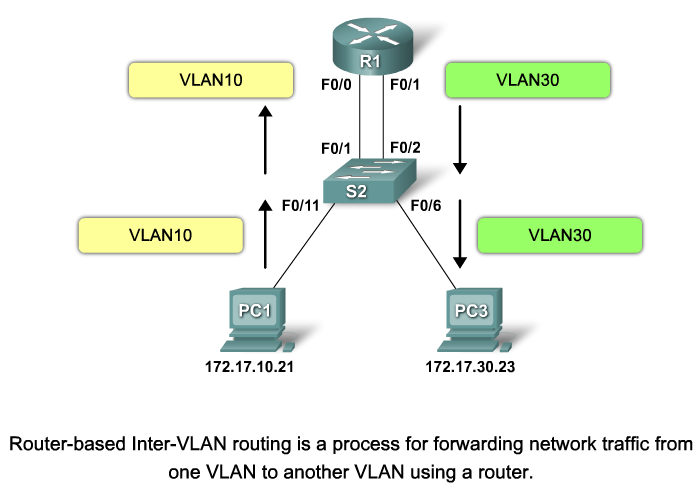


Figure 3-1 Router-on-a-Stick

The major issue with this architecture is performance. Because routers are software-based, they cannot route packets as fast as switches (hardware-based) can switch frames. Even if you are using high-performance routers, the physical interface connecting each VLAN to the router is a bottleneck. This restriction means that the router becomes a performance bottleneck when routing between high-speed VLANs.

Another issue with this architecture is the number of routers and physical interfaces required to support multiple VLANs. A dedicated Ethernet interface is required per VLAN. Routers are low-density devices, meaning that there is a high cost per port and multiple routing devices might be required to support multiple VLANs, increasing the complexity of the network.

Finally, all inter-VLAN traffic must travel via the router. All inter-VLAN traffic between the PCs must be sent through the router, which is inefficient.

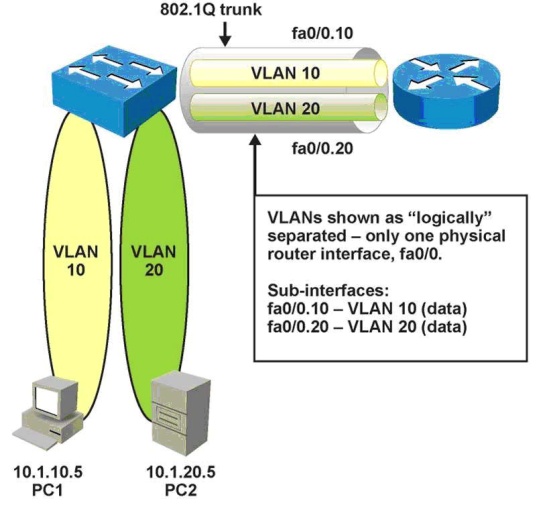
**Router-on-a-stick using trunks (One-armed router)**

Router-on-a-stick using trunks or one-armed router is a router that routes traffic between virtual local area networks (VLANs).

The router-on-a-stick architecture has physical limitations based upon a dedicated physical interface being required for each VLAN. This limitation can be removed by using trunk interfaces, where multiple VLANs are supported on a single physical interface by using tagging technologies such as 802.1Q. Rather than using physical interfaces to attach the router to each VLAN, virtual or logical interfaces are used to attach the router to each VLAN. [Figure 3-2](javascript:popUp('/content/images/bok_1587200600/elementLinks/05fig02.gif')) shows this architecture.

Virtual interfaces (rather than physical interfaces) are used to connect the router to each VLAN. A single physical trunk interface transports tagged VLAN traffic to the router, with the tag determining to which virtual interface a frame should be forwarded for routing. The router performs inter-VLAN routing by accepting VLAN-tagged traffic on the trunk interface coming from the adjacent switch, and then internally routing between the VLANs using virtual interfaces (or sub-interfaces). The router then forwards the routed traffic, VLAN-tagged for the destination VLAN, out the same physical interface as it used to receive the traffic.

Apart from the differences between using physical interfaces per VLAN as opposed to virtual interfaces per VLAN, this architecture is essentially identical to the traditional router-on-a-stick architecture and suffers the same performance limitations, because the routing engine is still software-based and the trunk interface is limited to 10 Mbps, 100 Mbps, or 1 Gbps.



[Figure 3-2](javascript:popUp('/content/images/bok_1587200600/elementLinks/05fig02.gif')) Router-on-a-Stick Using Trunks

**Layer 3 switching**

Layer 3 switching is a new form of inter-VLAN routing on the LAN. With a Layer 3 switch, the traditionally separated Layer 2 and Layer 3 functions are combined into a single device, eliminating the bottleneck associated with the cable between a router and switch by replacing the cable with a high-speed backplane connection. Layer 3 switches also typically perform routing in specially designed hardware circuitry rather than software, using specialized hardware that can perform routing functions at high speed. This means that the performance of Layer 3 switches is much higher than traditional router-on-a-stick architectures. In [Figure 3-3](javascript:popUp('/content/images/bok_1587200600/elementLinks/06fig01.gif')), a L3 switch provides switched LAN connections for each device in the network.



[Figure 3-3](javascript:popUp('/content/images/bok_1587200600/elementLinks/05fig02.gif')) Layer-3 switching

With a multilayer switch, traffic is routed internal to the switch device, which means packets are not filtered down a single trunk line to obtain new VLAN-tagging information. A multilayer switch does not, however, completely replace the functionality of a router. Routers support a significant number of additional features, such as the ability to implement greater security controls. Rather, a multilayer switch can be thought of as a Layer 2 device that is upgraded to have some routing capabilities.

To enable a multilayer switch to perform routing functions, the multilayer switch must have IP routing enabled.

Lab exercise 3 focuses on this method for the implementation of inter-VLAN routing. Lab exercise 4 focuses on the method of router-on-a-stick using trunks for the implementation of inter-VLAN routing.

**H3C VLAN Interface**

Hosts of different VLANs cannot communicate directly. That is, routers or Layer 3 switches are needed for packets to travel across different VLANs. On H3C S3610 switch, VLAN interfaces are used to forward VLAN packets on Layer 3.

VLAN interfaces are Layer 3 virtual interfaces (which do not exist physically on devices) used for Layer 3 interoperability between different VLANs. Each VLAN can have one VLAN interface. Packets of a VLAN can be forwarded on network layer through the corresponding VLAN interface. As each VLAN forms a broadcast domain, a VLAN can be an IP network segment and the VLAN interface can be the gateway to enable IP address-based Layer 3 forwarding.

The following are some of the reasons to configure VLAN interface:

* To provide a gateway for a VLAN so that traffic can be routed into or out of that VLAN
* To provide Layer 3 IP connectivity to the switch
* To support routing protocol and bridging configurations

# **Configure VLAN Interfaces On Layer 3 Switch S3610**

**Device used**

Two H3C S3100 and one S3610 switches.

**Network Topology**



Figure 3-4 Network Topology of Step 1

In this figure, a small sample network with the S3610 provides inter-VLAN routing between the various VLANs.

**Settings for Network Topology**

|  |  |  |
| --- | --- | --- |
| Table 3-1 Settings for Network Topology | | |
| **Property** | **Settings** |  |
| VLAN ID | VLAN 10, VLAN 20 |  |
| Subnet VLAN 10 | Subnet: 192.168.10.0/24  Default Gateway: **192.168.10.1/24** | Host address:  192.168.10.11 - 192.168.10.254 |
| Subnet VLAN 20 | Subnet: 192.168.20.0/24  Default Gateway: **192.168.20.1/24** | Host address:  192.168.20.11 - 192.168.20.254 |
| L3SA-VLAN Interface to VLAN 10 | IP address: **192.168.10.1/24** |  |
| L3SA-VLAN Interface to VLAN 20 | IP address: **192.168.20.1/24** |  |

**Tasks**

Create two VLANs across switches and allow hosts in different VLANs communicate with each other by configuring VLAN interfaces to forward VLAN packets on Layer 3 switch S3610.

**Configuration procedure**

1. Establishing configuration environment as you did in Step 1 of Lab Exercise 2 (see Step 1 of Lab Exercise 2).
2. Connect the hosts to the specified port and assign IP address and other configuration parameters manually to PC1 and PC2 of VLAN 10 and PC3 and PC4 of VLAN 20 as specified in Figure 3-4.
3. Find the address of the main network interface of PC1 to PC4 with the ipconfig command. Record the address information in Table 3-3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Table 3-2 | | | | |
| **Interface** | **VLAN belonged** | **Port No.** | **IP Address** | **MAC Address** |
| PC1 |  |  | IP address:  Mask:  Gateway:  DNS: |  |
| PC2 |  |  | IP address:  Mask:  Gateway:  DNS: |  |
| PC3 |  |  | IP address:  Mask:  Gateway:  DNS: |  |
| PC4 |  |  | IP address:  Mask:  Gateway:  DNS: |  |

1. Connect three switches with two patch cords as showed in Figure 3-4. These ports are used as trunk ports.
2. Create VLAN 10 and VLAN 20 on switch L2SA (S3100) and switch L2SB (S3100) respectively. Configure the trunk port of the switch L2SA (S3100), switch L2SB (S3100) and switch L3SA (S3610). You have learned how to perform these configurations in Step 5 of Lab Exercise 2 (see Step 5 of Lab Exercise 2).
3. Verify the configuration. If your configurations are correct, the PC1 and PC3 within VLAN 10 can communicate each other, and the PC2 and PC4 within VLAN 20 can communicate each other. But the hosts within VLAN 10 cannot communicate with the hosts within VLAN 20 or vice versa.

If the PCs within VLAN 10 or the PCs within VLAN 20 cannot communicate each other, check the configurations of VLAN and trunk ports until the configurations are correct.

1. Configure Inter-VLAN routing on L3SA (S3610)

**Note:** Before creating a VLAN interface, make sure the corresponding VLAN has been created; otherwise, the VLAN interface cannot be created.

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

<L3SA> system-view

**# Display VLAN information**

[L3SA] display vlan 10

[L3SA] display vlan 20

**# Configure virtual interface to VLAN 10 and assign IP address to this virtual interface.**

[L3SA] interface vlan-interface 10

[L3SA-vlan-Interface10] ip address 192.168.10.1 255.255.255.0

[L3SA-vlan-Interface10] quit

**# Configure virtual interface to VLAN 20 and assign IP address to this virtual interface.**

[L3SA] interface vlan-interface 20

[L3SA-vlan-Interface20] ip address 192.168.20.1 255.255.255.0

[L3SA-vlan-Interface20] quit

**# Display VLAN interface information**

[L3SA] display interface vlan-interface 10

[L3SA] display interface vlan-interface 20

[L3SA] display interface vlan-interface

**# Display the brief configuration information of the interfaces in the current system.**

[L3SA] display ip interface brief

[L3SA] display ip interface brief vlan-interface 10

[L3SA] display ip interface brief vlan-interface 20

**# Display information about interface VLAN-interface 10 and 20.**

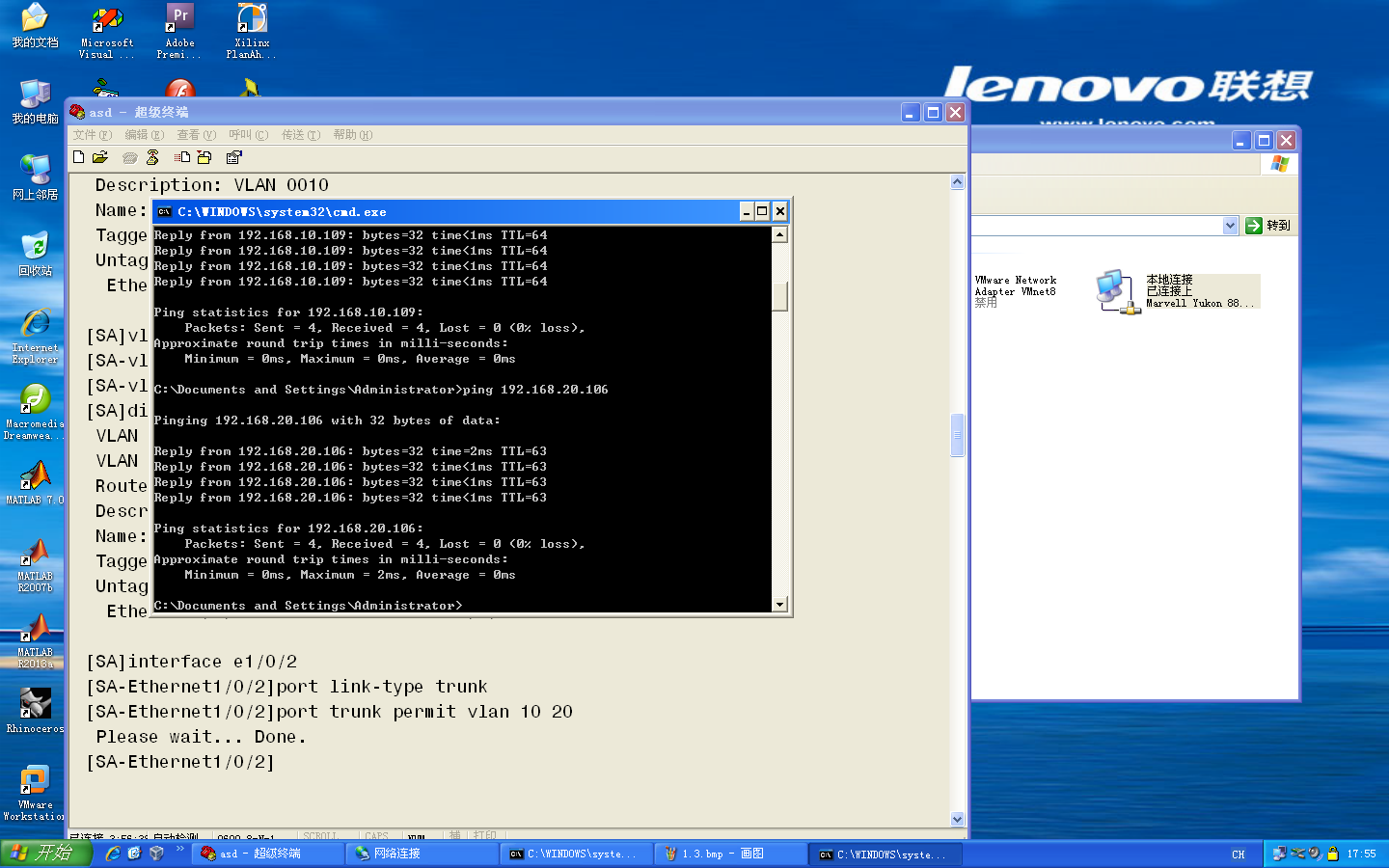
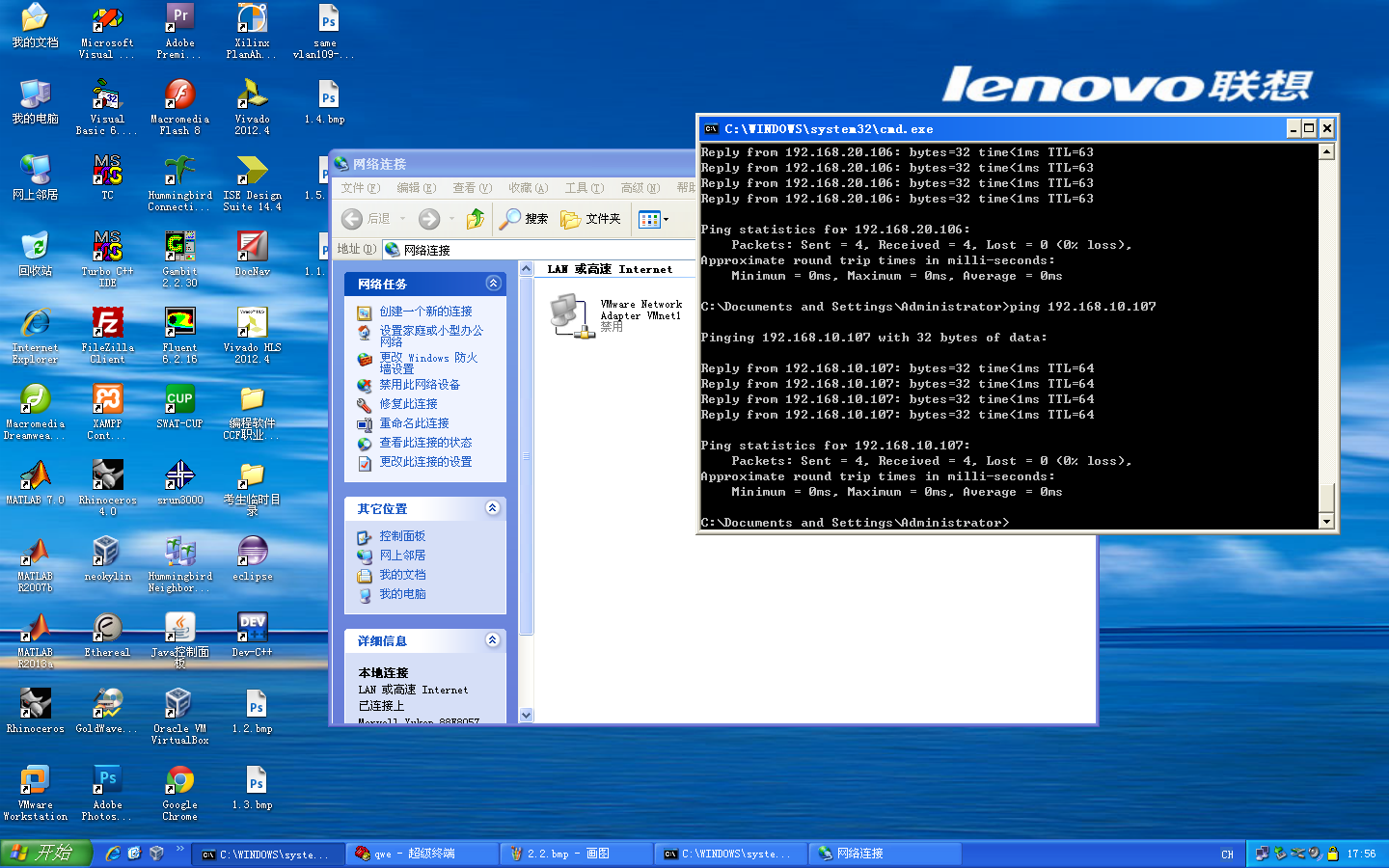
[L3SA] display ip interface

[L3SA] display ip interface vlan-interface 10 [L3SA] display ip interface vlan-interface 20 **# Display statistics on IP traffics.**

[L3SA] display ip statistics

**# Rreset ip statistics**

[L3SA] reset ip statistics

1. Verify the inter-VLAN routing configuration.
   1. ping the address of interface VLAN 10 on L3SA (S3610) switch terminal****.
   2. Ping the address of interface VLAN 20 on L3SA (S3610) switch terminal. ****

If all the ping packets are transmitted and are received by the destination address, the VLAN interfaces are up and working. Or check the configurations until they are correct.

1. Configure your PCs to use the respective L3SA (S3610) VLAN interface as their default gateway. For example, PCs in VLAN 10 should use the interface VLAN 10 IP address as its default gateway.
2. Verify the connectivity. Ping from PC1 or PC2 in VLAN 10 to PC3 and PC4 in VLAN 20 or vice versa.

**Troubleshooting**

* **Symptom:** Cannot ping from PCs in VLAN 10 to PCs in VLAN 20 or vice versa.
* **Solution:** Check if the default gateway address assigned to PCs is correct. The default gateway address assigned to PCs in VLAN 10 should be 192.168.10.1, and that to PCs in VLAN 20 should be 192.168.20.1.

**Answer the following questions:**

1. What is the VLAN Interface or Virtual Interface?

vlan接口是二层（交换）通向三层（路由）的接口，可以在vlan接口上配ip地址，这个地址可作为vlan内各主机的网关地址，这样不同vlan间的主机报文就可以通过vlan接口在三层路由上互相转发，实现了vlan间互通

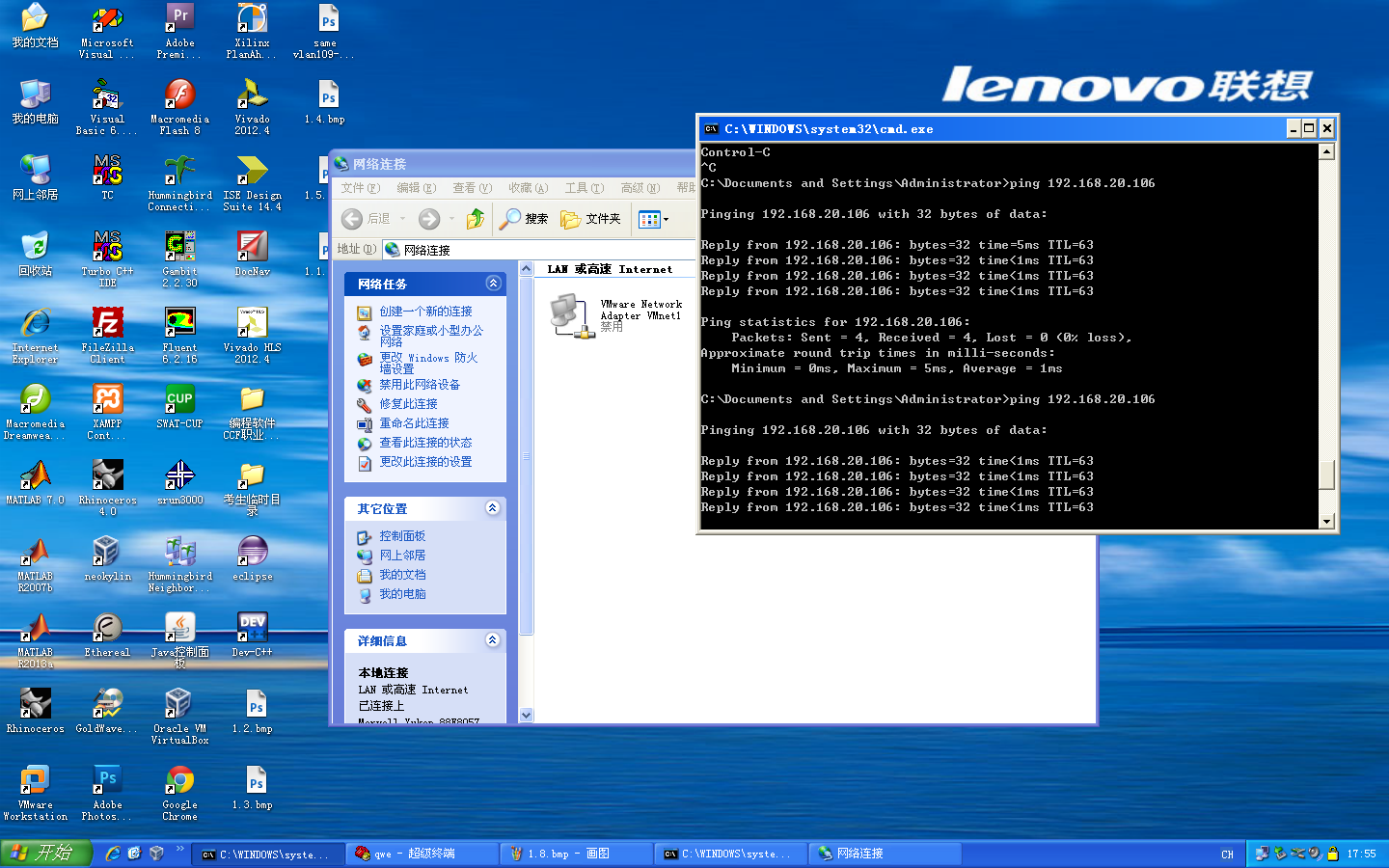
1. Explain how the VLAN Interfaces are used to route between VLANs.

通过路由器的不同物理接口与交换机上的每个VLAN分别连接

通过路由器的逻辑子接口与交换机的各个VLAN连接

用三层以上交换机代替路由器实现VLAN间的通信

1. Ping from one PC to other PCs; Paste the screen of the statistics on IP traffics you captured.

****