Introduction to Routers

1 Introduction

Routers are the workhorses in IP internet networking. This lab will introduce the router and examine the interface between the Router and the Switch. You will need to setup the switch into the VLAN and 802.1Q trunking port from Lab6 and Lab8 prior to completing this experiment.

2 Setup

2.1 Switch Setup

Erase the Switch's configuration and restore your Switch setup from your USB drive that you created in Lab8.

2.2 Router Setup

Erase the Router's configuration, and setup the router into a default configuration as detailed below.

```
Router1% ena
 Password: "123"
Router1# write erase
Router1# reload
[after restarting, you should be prompted for setup as in Lab 8]
```

You won't have to configure IP or put an IP Address on any interfaces during the setup, you'll need to create and configure sub-interfaces in Section 3 below.

Figure 1 identifies the Ethernet0/0 and FastEthernet0/0 ports on the Router Model in the lab.
(There may be other ports on the router, but only the FastEthernet0/0 port will be used in this lab)
Please use Router1, which is the designate directly under the Switch.

When you configure the sub-interfaces in section 3 below, you use the same IOS commands/features on the router, as you've learned on the switch.

```
Router1# conf term
Router1 (config)#
```

Interface specific configuration can be entered after using the "interface" command in config mode, you should notice that the prompt changes, depending on what stage/level of the configuration you're dealing with.

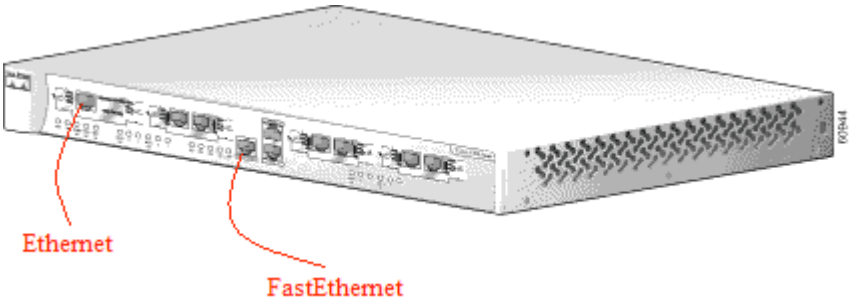

Figure 1 Cisco 1760 Router

3 VLAN Routing

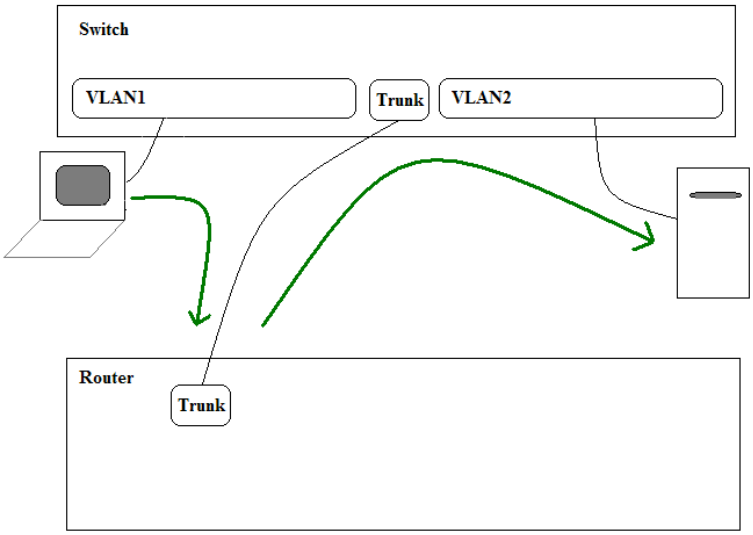

Figure 2 VLAN Logical Layout (Physical Links in Black, Logical Path in Green)

Wire the Switch port that you assigned as the Trunk in the configuration to the FastEthernet0/0 port on the Router. You'll need to set up Sub-Interfaces on the Router for each VLAN-ID that you've setup and are trunking to the Router. Sub-Interfaces are virtual ports that allow the Router to separate VLAN traffic, while allowing Layer3 protocols to think there are separate ports on each VLAN. *(Optional) For advanced information, Chapter 4 of the Cisco 1700 Series Router Software Configuration Guide located in the User Manuals folder on the desktop of the Linux Host for instructions on configuring routing among VLANs (ignore IPX Routing and NetWare Routing).*

Configuring Routing Among VLANs with IEEE 802.1Q Encapsulation

This describes the required and optional tasks for configuring routing between virtual LANs (VLANs) with IEEE 802.1Q encapsulation. The IEEE 802.1Q protocol is used to interconnect multiple switches and routers and to define VLAN topologies. IEEE 802.1Q support is available for Fast Ethernet interfaces.

IEEE 802.1Q Encapsulation Configuration Task List

You can configure routing among any number of VLANs in your network. This section provides procedures for configuring IEEE 802.1Q encapsulation. The process involves the following:

• Enabling the protocol on the router

• Enabling the protocol on the interface

• Defining the encapsulation format as IEEE 802.1Q

• Customizing the protocol to meet the requirements for your environment

Configuring IP Routing over IEEE 802.1Q

IP routing over IEEE 802.1Q extends IP routing capabilities to include support for routing IP frame types in VLAN configurations, using the IEEE 802.1Q encapsulation.

To route IP over IEEE 802.1Q between VLANs, you need to customize the subinterface to create the environment in which it will be used. Perform these tasks in the order in which they appear:

Enabling IP Routing

IP routing is automatically enabled in the Cisco IOS software for routers. To reenable IP routing if it has been disabled, use the following command in global configuration mode:

```
Router1(config)# ip routing
```

Once you have IP routing enabled on the router, you can customize the characteristics to suit your environment.

Defining the VLAN Encapsulation Format

To define the encapsulation format as IEEE 802.1Q, use the following commands in interface configuration mode.

	Command	Task
Step 1	**Interface fastethernet** *(mod)/(port).(subinterface-number)*	Specify the subinterface on which IEEE 802.1Q will be used. The Sub-interface numbers don't have to match the vlanid, but they are sometimes kept the same for convenience.

Step 2	**encapsulation dot1q** vlanid	Define the encapsulation format as IEEE 802.1Q (dot1q) and specifies the VLAN identifier. The VLAN IDs must match between the devices connected over the Trunk.

Assigning an IP Address to a Network Interface

An interface can have one primary IP address. To assign a primary IP address and a network mask to a network interface, use the following command in interface configuration mode. A mask identifies the bits that denote the network number in an IP address. When you use a mask to subnet a network, that mask is referred to as a subnet mask.

Command	Task
ip address *ip-address mask*	Set a primary IP address for an interface, while in interface-config mode.

Examples of IEEE 802.1Q Encapsulation Configuration

Configuring IP Routing over IEEE 802.1Q

(NOTE! These examples will need changes made, using the IP Addresses specific to your Work Area)

This configuration example shows IP being routed on VLAN 2 on a sub-interface 0.10: (Note the the physical interface fastethernet0/0, has no ip address assigned to it)

```
ip routing
interface fastethernet0/0
  no ip address
interface fastethernet0/0.10
```

```
encapsulation dot1q 1
ip address 10.101.0.31 255.255.255.0
interface fastethernet0/0.20
encapsulation dot1q 2
ip address 10.101.3.31 255.255.255.0
```

VLAN Commands

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs, use the encapsulation dot1q command in subinterface configuration mode.

The command is as follows:

```
encapsulation dot1q vlan-id
```

The following example encapsulates VLAN traffic, using the IEEE 802.1Q protocol for VLAN 3:

```
interface fastethernet0/0.11
encapsulation dot1q 3
```

To view VLAN subinterfaces, use the show vlans privileged EXEC command:

```
show vlans
```

The following is sample output from the show vlans command:

```
Router# show vlans
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)
     vLAN Trunk Interface: FastEthernet0
This is configured as native Vlan for the following interface(s):
     FastEthernet0
Virtual LAN ID: 2 (IEEE 802.1Q Encapsulation)
     vLAN Trunk Interface: FastEthernet0/0.10
     Protocols Configured: Address: Received: Transmitted:
        IP       10.101.0.31             10          10
Virtual LAN ID: 3 (IEEE 802.1Q Encapsulation)
```

```
vLAN Trunk Interface: FastEthernet0/0.11

Protocols Configured: Address: Received: Transmitted:

   IP       10.101.2.31             16          16
```

4 Experiment

Run the following commands to change the Linux Host's IP address to 10.10X.2.2, and set the default gateway to 10.10X.2.1. (please use your specific addresses for your work area)

```
misy@localhost ~ $ sudo /sbin/ifconfig eth0 10.10X.2.2 netmask
255.255.255.0
misy@localhost ~ $ sudo /sbin/route add default gw 10.10X.2.1
```

On the Windows Vista Host system, issue the following command in a CMD window, **or** add the Default Gateway through the TCP/IP IPv4 properties page of the Ethernet Network Connection Wizard. (It will install a static route to network 10.10X.2.0/24, to the router 10.10X.0.1. Again it must be customized for your workarea):

```
C:\> route add 10.10X.2.0 mask 255.255.255.0 10.10X.0.31 metric 1
```

Once you've successfully configured the VLAN router for the 802.1q interface of the router, startup Wireshark and try to ping between the Linux Host on VLAN2 of the router, and the Vista Host on VLAN1 of the router. Use the `tracert` (traceroute on Linux) command between hosts as a test as well.

If you don't succeed right away, you can use programs like PING to troubleshoot smaller sections of your network, trying to isolate the problem. For example:

- PING from Vista to Router's vlan1 IP_address on VLAN1
- PING from Linux to Router's vlan2 IP_address on VLAN2
- See if Wireshark on Vista can see PING's from Linux-to-Vista
- See if Wireshare on Linux can see PING's from Vista-to-Linux

5 Extension

Include the routing tables from the Vista Host (netstat -r), the Linux Host (netstat -r), and the Router (show ip route), in your report. Comment on how the tables are used to direct the packets from the Vista Host to the Linux Host and back again. Compare and contrast the features of the Switch, with the features of the Router. Could you use a router in place of a switch? A switch in place of a router? Explain. Why are you not asked to include the routing table from the Switch? Comment on the four troubleshooting tests above, in regard to what each one is testing.