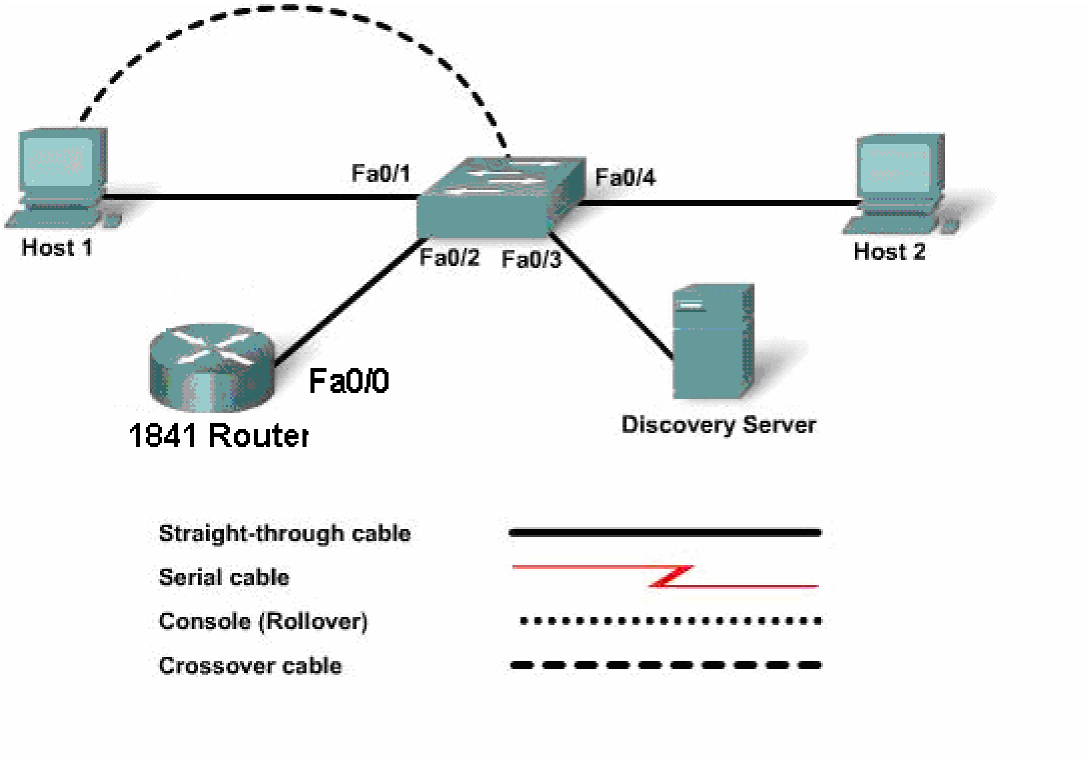
Lab 1.4.3 Monitoring VLAN Traffic



Device Designation	Device Name	Address	Subnet mask
S1	FC-ASW-1	—	—
PC1	Host1	172.17.1.10	255.255.0.0
PC2	Host2	172.17.1.11	255.255.0.0
1841 Router	Router	172.17.0.1	255.255.0.0
Discovery Server	Server	172.17.1.1	255.255.0.0

Objectives

- Observe broadcast traffic on a switch.
- Create and apply VLANs to separate local traffic.
- Observe broadcast traffic containment with VLANs.

640-802 CCNA Exam Objectives

This lab contains skills that relate to the following CCNA exam objectives:

- Perform and verify initial switch configuration tasks, including remote access management.
- Verify network status and switch operation using basic utilities (including: ping, traceroute, Telnet, SSH, arp, ipconfig), and **show** and **debug** commands.
- Describe how VLANs create logically separate networks and the need for routing between them.
- Configure, verify, and troubleshoot VLANs.

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

____

____

____

How is an understanding of VLANs useful in network administration?

____

____

____

How will a network administrator know if the VLAN is working correctly?

____

____

____

Background / Preparation

This lab demonstrates the flow of network traffic from host PCs attached to a switch. Currently, the switch is not configured to segment network traffic into VLANs. In this lab, you will observe the flow of traffic and then configure VLANs on the switch to contain local traffic in each respective VLAN. The effects of the VLANs on the network traffic will then be observed and discussed.

The packet capture program Wireshark (formerly known as Ethereal), is required to be installed on each PC used in this lab. Wireshark is a free, open source program that can be downloaded from http://www.wireshark.org/. See your instructor if this program is not available in the lab.

The Cisco IOS commands used in this lab are applicable to the Cisco 2960 switch. See your instructor about comparable commands if you are using other switch models in this lab.

Task 1: Demonstrate Broadcasts across a Single LAN

Step 1: Prepare the switch for configuration

NOTE: If the PCs used in this lab are also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so these can be restored at the conclusion of the lab.

a. Referring to the topology diagram, connect the console (or rollover) cable to the console port on the switch and the other cable end to the host computer with a DB-9 or DB-25 adapter to the COM 1 port. Ensure that power has been applied to both the host computer and switch.

b. Establish a HyperTerminal, or other terminal emulation program, connection from PC1 to the switch.

c. Ensure that the switch is ready for lab configuration by verifying that all existing VLAN and general configurations are removed.

1) Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

2) Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Step 2: Configure the PCs

a. Connect the two PCs to the switch as shown in the topology diagram.

b. Configure the two PCs to have the IP addresses and subnet mask shown in the topology table.

c. Clear the ARP cache on each PC by issuing the **`arp -d`** command at the PC command prompt.

d. Confirm that the ARP cache is clear by issuing the **`arp -a`** command.

Step 3: Generate and examine ARP broadcasts

a. Launch Wireshark on each PC and start the packet capture for the traffic seen by the NIC in each PC.

b. From the command line of each PC, ping all connected devices.

c. Monitor the operation of Wireshark. Note the ARP traffic registering on each PC.

d. Stop the Wireshark capture on each PC.

e. Examine the entries in the Wireshark Packet List (upper) Pane.

How many ARP captures occurred for each device?

____

List the source IP addresses of the ARP request and replies:

____

____

____

Did each device receive an ARP request from every PC connected to the switch?

____

f. Exit Wireshark. (You have the option to save the capture file for later examination.)

Task 2: Demonstrate Broadcasts within Multiple VLANs

Step 1: Configure the VLANs on the switch

a. Using the established console session from PC1 to the switch, set the hostname by issuing the following command from the global configuration mode:

```
Switch(config)# hostname FC-ASW-1
```

b. Set interfaces Fa0/1 and Fa0/2 to VLAN 10 by issuing the following commands from the global configuration and interface configuration modes:

```
FC_ASW-1(config)#interface FastEthernet0/1

FC_ASW-1(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10

FC_ASW-1(config-if)#interface FastEthernet0/2

FC_ASW-1(config-if)#switchport access vlan 10
```

c. Set interfaces Fa0/3 and Fa0/4 to VLAN 20 by issuing the following commands from the interface configuration mode:

```
FC_ASW-1(config-if)#interface FastEthernet0/3

FC_ASW-1(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20

FC_ASW-1(config-if)#interface FastEthernet0/4

FC_ASW-1(config-if)#switchport access vlan 20

FC_ASW-1(config-if)#end
```

d. Confirm that the interfaces are assigned to the current VLANs by issuing the **`show vlan`** command from the Privileged EXEC mode. If the VLANs are not assigned correctly, troubleshoot the command entries shown in Steps 1b and 1c and reconfigure the switch.

Step 2: Prepare the PCs

a. Clear ARP cache on each PC by issuing the **`arp -d`** command at the PC command prompt.

b. Confirm the ARP cache is clear by issuing the **`arp -a`** command.

Step 3: Generate ARP broadcasts

a. Launch Wireshark on each PC and start the packet capture for the traffic seen by the NIC in each PC.

b. From the command line of each PC, ping each of the other three devices connected to the switch.

c. Monitor the operation of Wireshark. Note the ARP traffic registering on the two PCs.

d. Stop the Wireshark capture on each PC.

e. Examine the entries in the Wireshark Packet List (upper) Pane.

How many ARP captures occurred for each PC?

____

List the source IP addresses:

____

____

____

What is the difference between the captured ARP packets for each PC this time and those captured in Task 1?

____

How many Ethernet broadcast domains are present now? __________

f. Exit Wireshark. (You have the option to save the capture file for later examination.)

Step 4: Clean up

Erase the configuration and reload the switch. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Task 3: Reflection

a. Discuss the use of VLANS in keeping data traffic separated. What are the advantages of doing this?

____

____

____

____

b. When designing a network list different criteria that could be used to divide a network into VLANs.

____

____

____