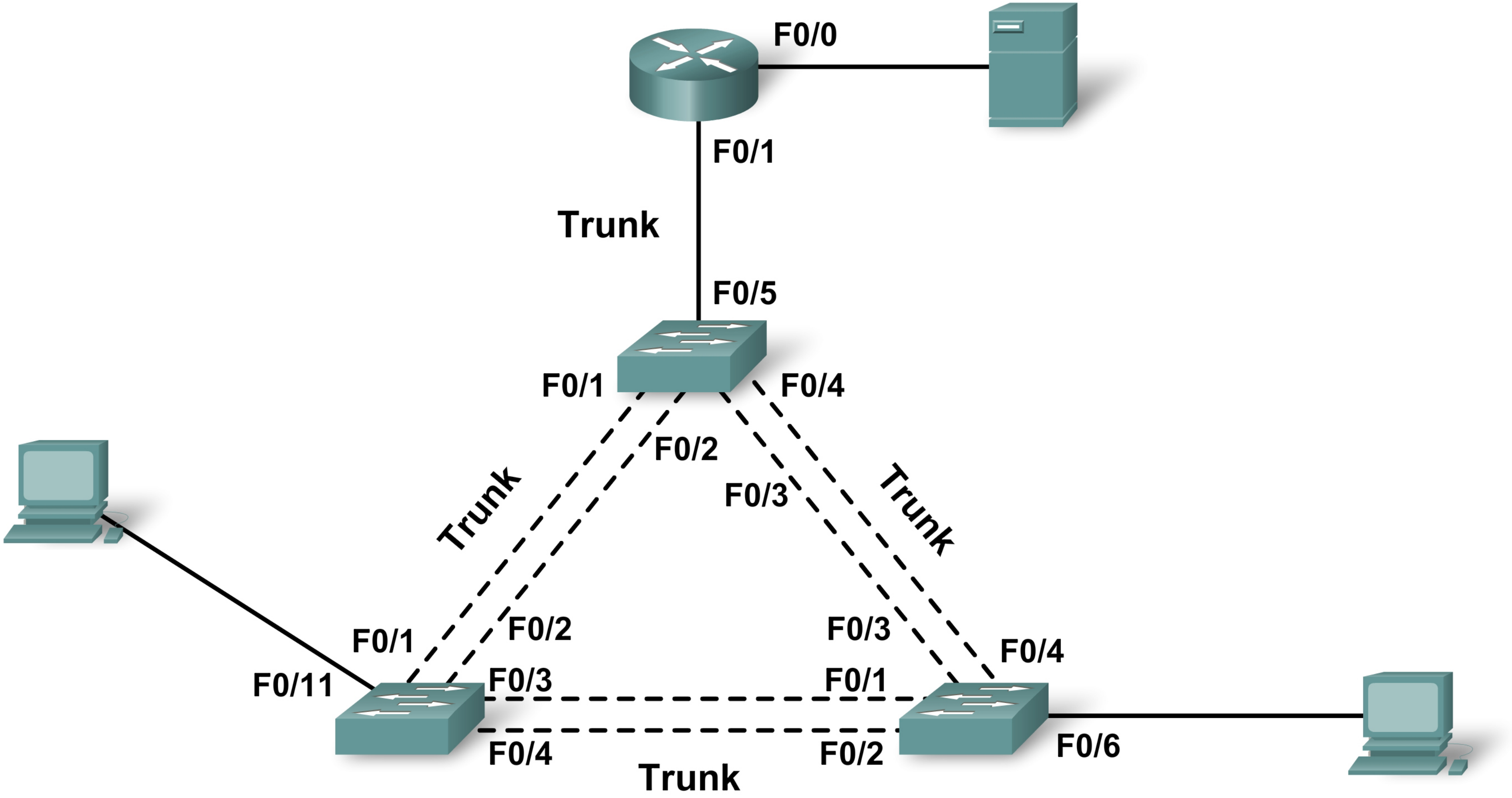
Cisco | Networking Academy®
Mind Wide Open™

CCNA Discovery 3:

Introducing Routing and Switching in the Enterprise v4.0
Student Lab Manual

Proposed NDG NetLab Configuration



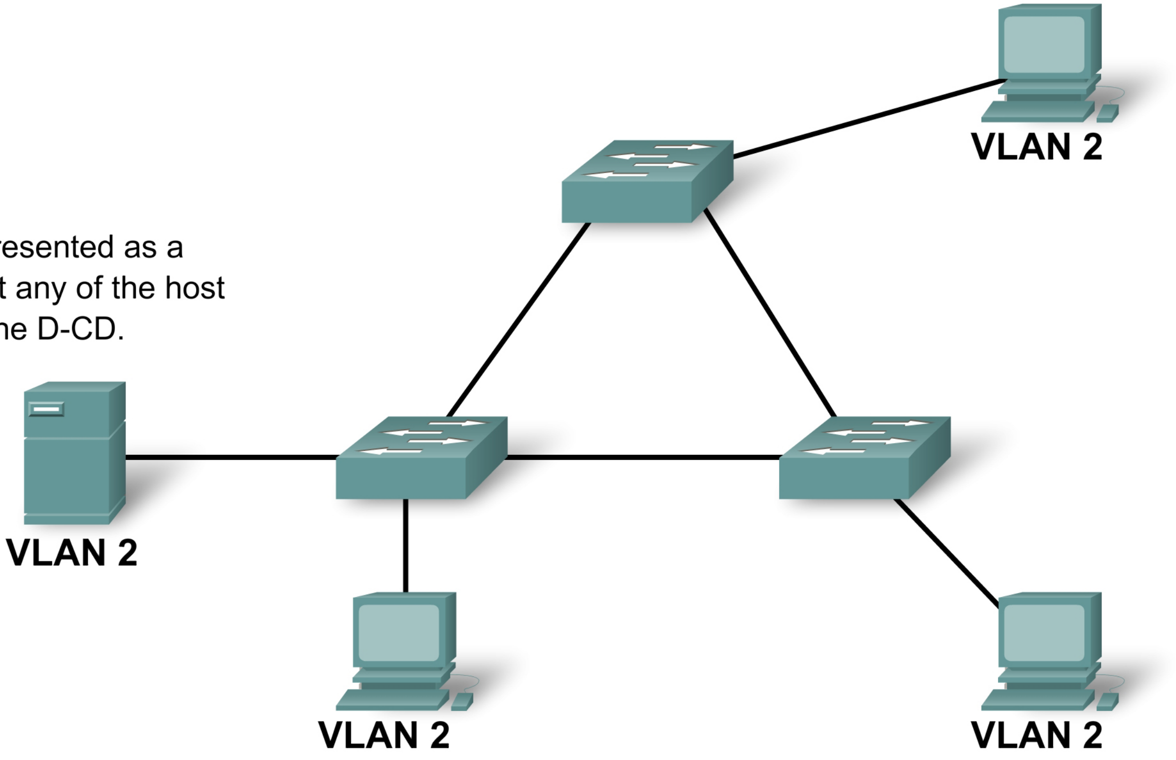
Part 1:

Examine port security – concept of VLAN

All devices in the same VLAN
(not VLAN 1)

Chapter 3

Server – Currently represented as a stand-alone device, but any of the host devices can maintain the D-CD.



VLAN 2 – IP address 192.168.2.x

This topology could be used for: STP, concept of basic VLAN

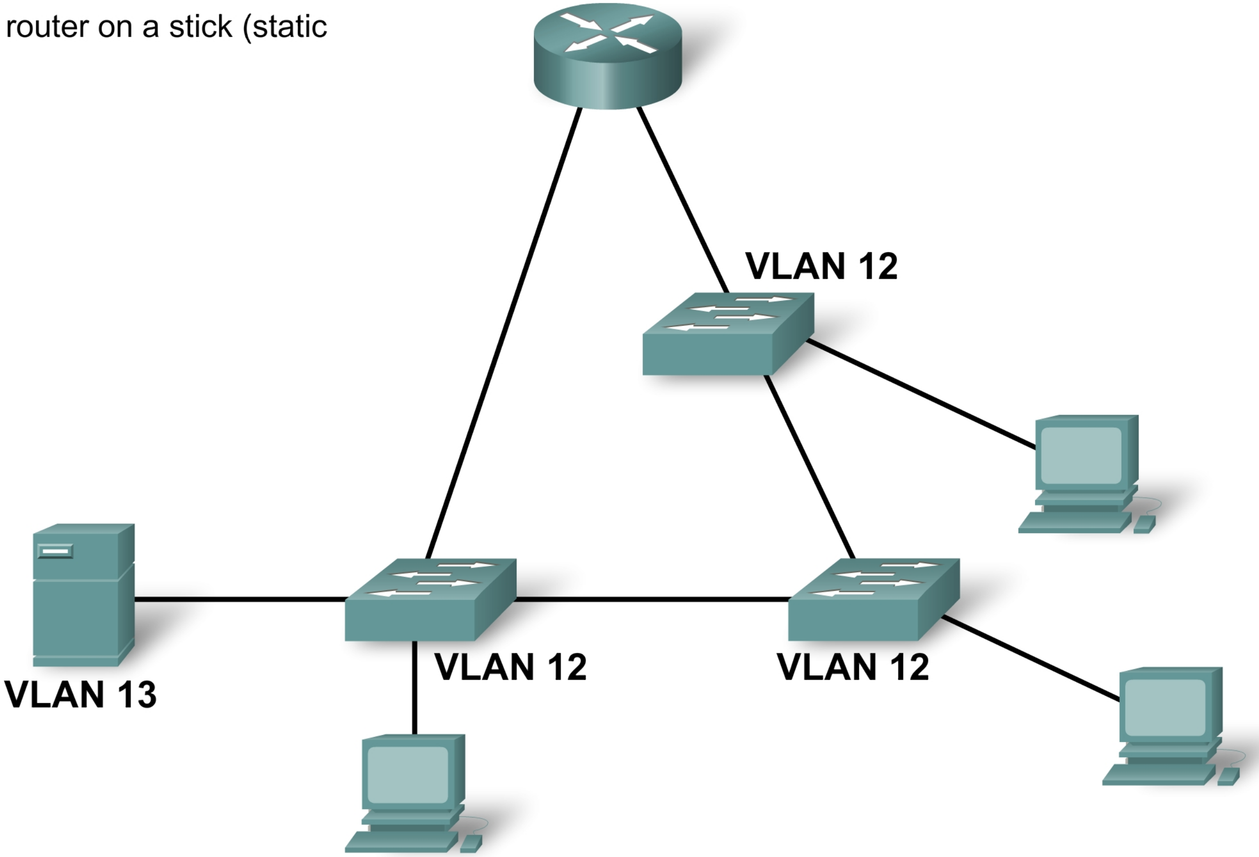
Netlab users, please reference proposed NDG topology

Part 2

Further explain concept of VLAN for server farm

All users in VLAN 2 --- all servers in VLAN 3

Need for router – no router on a stick (static routing)



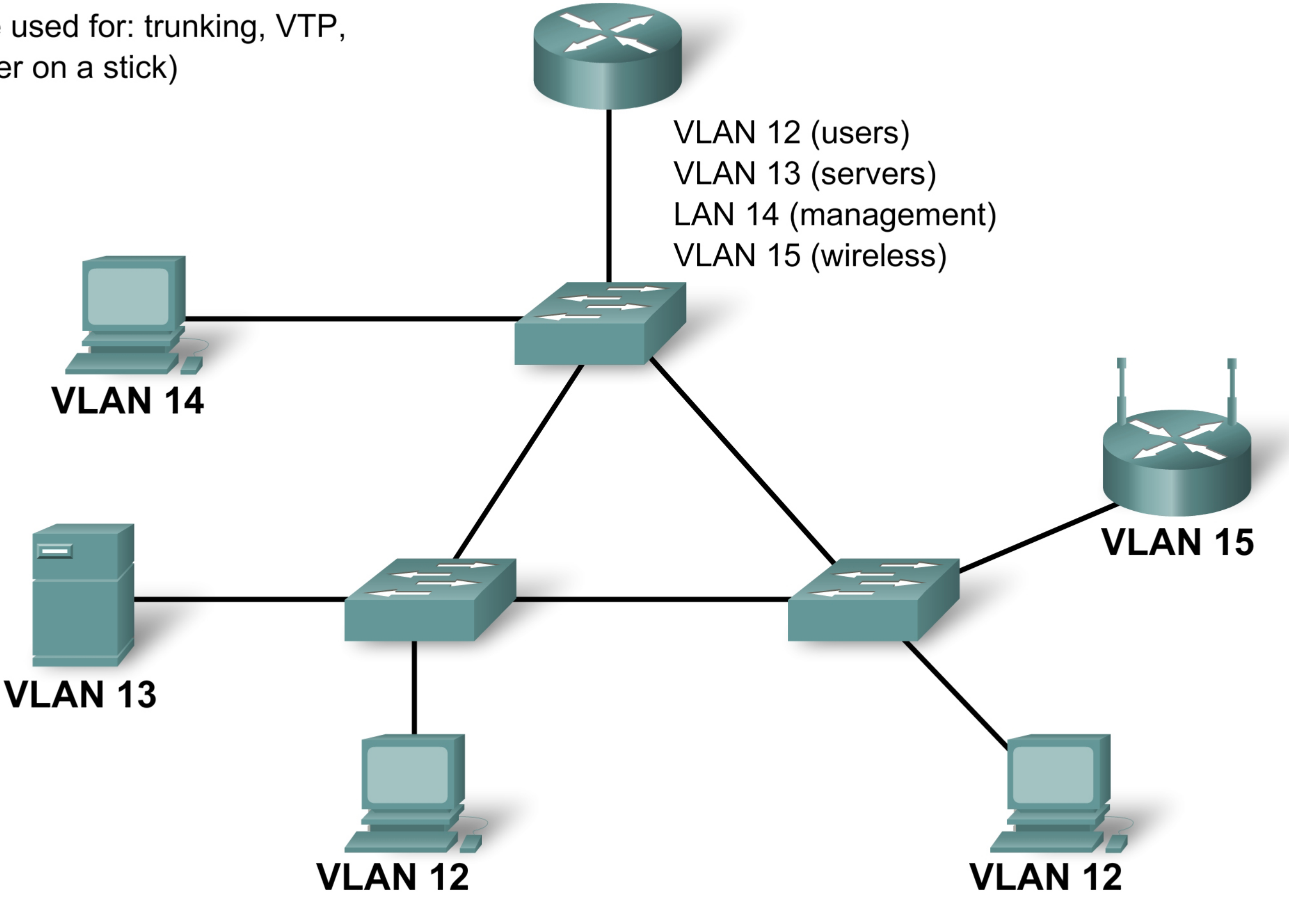
VLAN 12 – IP address 192.168.12.x
VLAN 13 – IP address 192.168.13.x

This topology could be used for: inter-vlan routing (not using trunking); STP

Part 3:

Further explain concept of VLAN for server farm
All users in VLAN 2 --- all servers in VLAN 3
Need for router, router on a stick (static routes)

This topology could be used for: trunking, VTP,
inter-vlan routing (router on a stick)



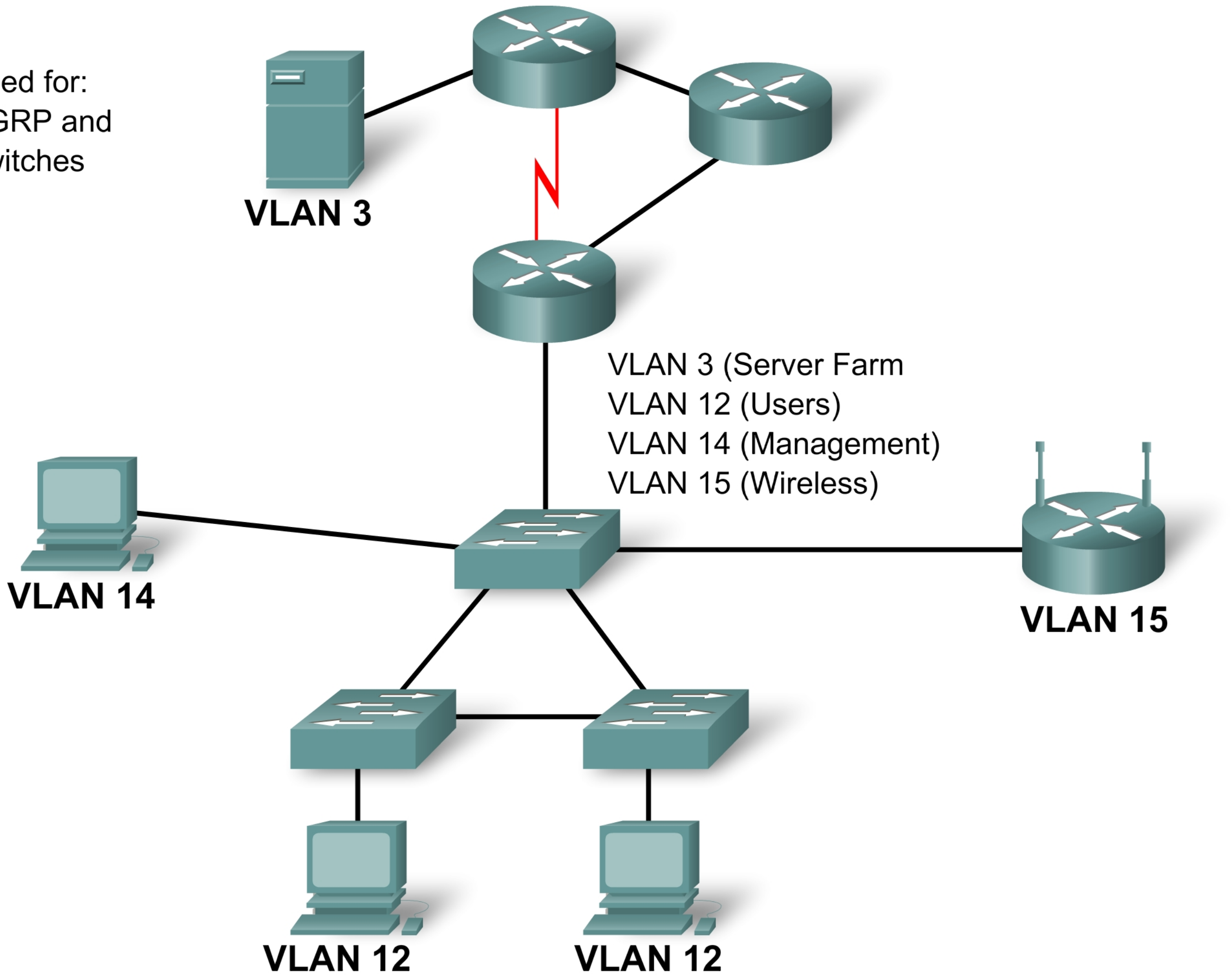
VLAN 12 – IP address 192.168.12.x
VLAN 13 – IP address 192.168.13.x
VLAN 14 – IP address 192.168.14.x
VLAN 15 – IP address 192.168.15.x

Netlab users, please reference proposed NDG topology

Part 4:

Connecting multiple buildings in an Enterprise..
Using Ethernet

This topology could be used for:
routing protocols RIP, EIGRP and
OSPF– with or without switches

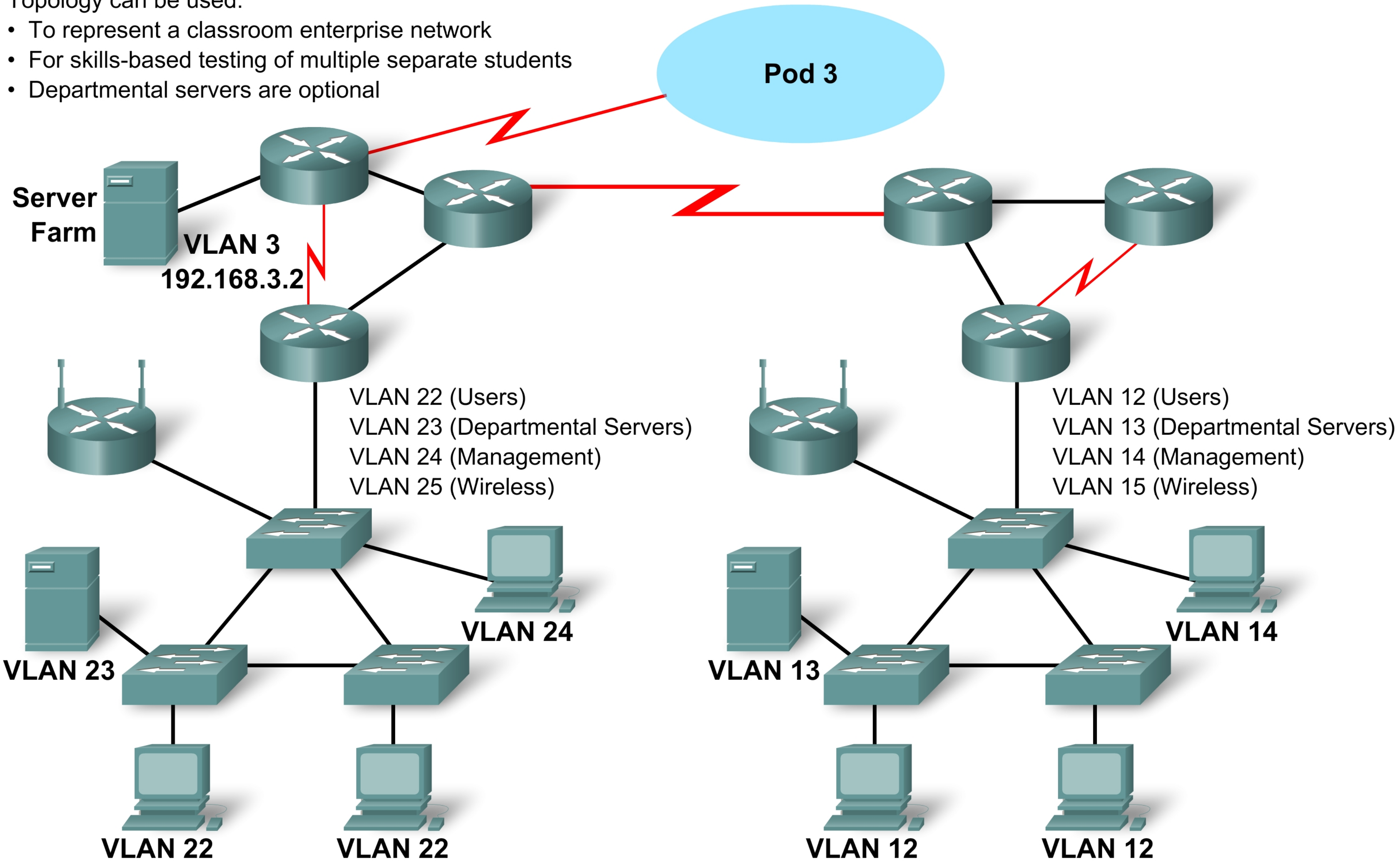


VLAN 3 (Server Farm
VLAN 12 (Users)
VLAN 14 (Management)
VLAN 15 (Wireless)

VLAN 3 – IP address 192.168.3.x
VLAN 12 – IP address 192.168.12.x
VLAN 14 – IP address 192.168.14.x
VLAN 15 – IP address 192.168.15.x

Topology can be used:

- To represent a classroom enterprise network
- For skills-based testing of multiple separate students
- Departmental servers are optional



VLAN 22 (Users)
VLAN 23 (Departmental Servers)
VLAN 24 (Management)
VLAN 25 (Wireless)

VLAN 12 (Users)
VLAN 13 (Departmental Servers)
VLAN 14 (Management)
VLAN 15 (Wireless)

VLAN 22 – IP address 192.168.22.x
VLAN 23 – IP address 192.168.23.x
VLAN 24 – IP address 192.168.24.x
VLAN 25 – IP address 192.168.25.x

VLAN 12 – IP address 192.168.12.x
VLAN 13 – IP address 192.168.13.x
VLAN 14 – IP address 192.168.14.x
VLAN 15 – IP address 192.168.15.x

CCNA Discovery Server Live CD v2.0

Installation Instructions

Overview

The Discovery Server Live CD provides all of the network services necessary to support the CCNA Discovery curriculum and hands-on labs. The Live CD is built using the ADIOS development platform and is based on Fedora Core 6. It requires no installation and will run on minimal hardware. The Live CD runs adequately on a PII machine with 256 MB of RAM, an Ethernet interface card, and a CDROM drive. Because the entire server runs from RAM, there is no need for the machine to have a hard disk drive or operating system. The Discovery Server Live CD will run on less powerful hardware but will run noticeably slower. More powerful hardware provides better performance. Increasing the amount of RAM has the most impact on speed and performance.

NOTE: Although the Discovery Server Live CD will run on a broad range of computers, it will not run on every system. The machine used to run the Discovery Server Live CD must be able to support Fedora Core 6. The current version of the Live CD is known to have problems with USB keyboards and certain BIOSs and chipsets. If the server fails to run on your hardware, try a different machine. The Discovery Server Live CD runs with fewer problems on older hardware.

The CD is built entirely from open source solutions and can be freely duplicated and distributed. The CD must be distributed in its entirety; no copyright notices should be removed or altered.

The server is designed to provide preconfigured services such as DHCP, DNS, FTP, TFTP, HTTP, SSH, Telnet, SMTP, POP3, IMAP, and streaming video. Many other services and tools are available on the CD to allow the creation of more challenging lab exercises. The following applications are among the more useful:

- WireShark, a packet sniffer
- nmap, a port scanner
- Diag, a network diagramming tool
- Complete office suite, including word processing, presentation, and spreadsheet applications

Starting the Server

Obtain a Discovery Server Live CD from your instructor and use it to boot the computer that will be used for the Discovery Server.

NOTE: You may first have to modify the boot order in your computer BIOS setup program. The CD/DVD drive must be listed before the system hard disk drive. Some systems have a designated key that you can press to display a menu of boot choices during the boot process; other systems require the change to be made in the BIOS. Often a message appears on the bottom of the screen during boot that lists which key should be pressed to enter the BIOS setup or to boot from the CD. If no message is displayed, consult your system documentation for details.

1. Before starting the server, be sure to connect the computer NIC to a switch or router port using an appropriate cable.
2. To start the Discovery Server Live CD, insert the CD into the CDROM drive and reboot the machine.
3. During startup, you will be presented with a list of boot options. At the first options menu, select ’a’. All other options are provided in the event that ’a‘ does not run properly on your machine. During the booting process you may notice that the eth0 address and the DHCP daemon (dhcpd) fail. This is normal on some machines and these functions will be started manually. Allow the server to boot fully into the KDE graphical environment.

When booted, a screen similar to that shown in Figure 1 displays.

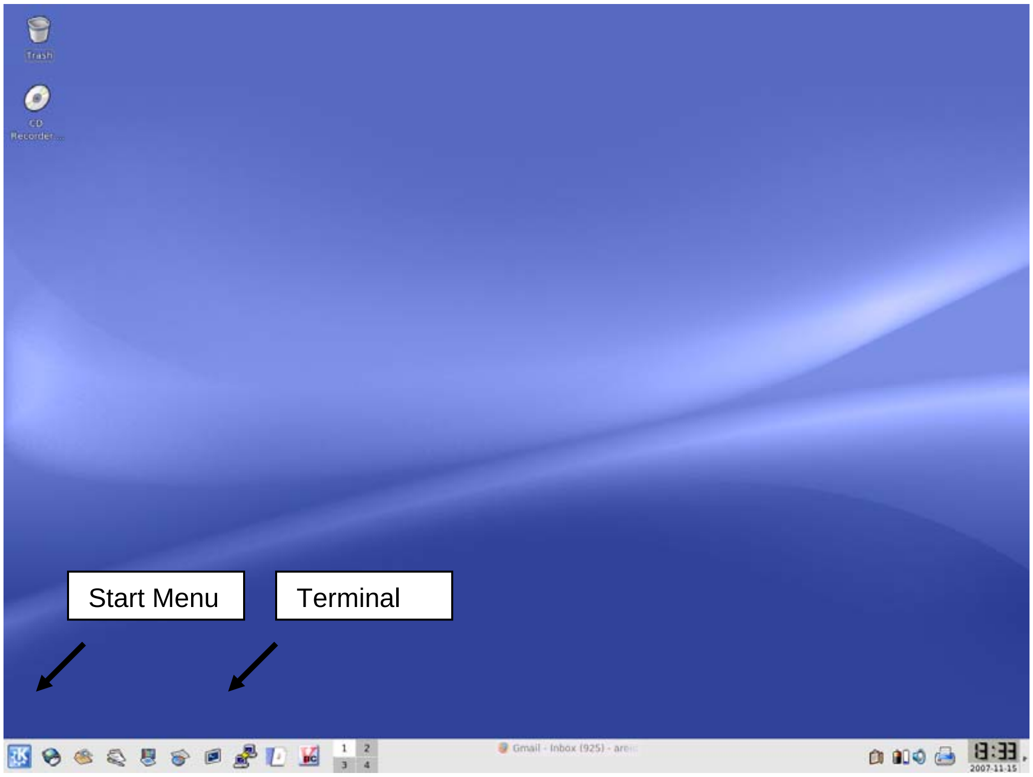


Figure 1: The KDE Display

Quick Info

Root Password:	discoverit
User Accounts:	20 ordinary user accounts set up as userX with a password of cheetahX where X is any number between 1 and 20 inclusive
Server Name:	server.discovery.ccna
IP Address:	172.17.1.1
Subnet Mask:	255.255.0.0
Default Gateway:	172.17.0.1

DHCP

Pool Address Range:	172.17.1.50 to 172.17.1.254
Lease:	4 hours
Default Gateway:	172.17.1.1
Domain Name:	discovery.ccna

DNS

Resolves names for the discovery.ccna domain

server.discovery.ccna	resolves to 172.17.1.1
server-1.discovery.ccna	resolves to 172.17.1.1 (for the troubleshooting labs in CCNA Discovery 1)
server-2.discovery.ccna	resolves to 172.17.1.2 (for the troubleshooting labs in CCNA Discovery 1)

Configuring the Server

The following instructions address the most common setup processes and issues:

NOTE: On some hardware, eth0 may be the wireless NIC. In that case, these instructions will apply to **eth1**, which should be the first Ethernet card in the system. You may also notice **eth0** and **eth0.bak** on some hardware. This is normal and will not interfere with the setup.

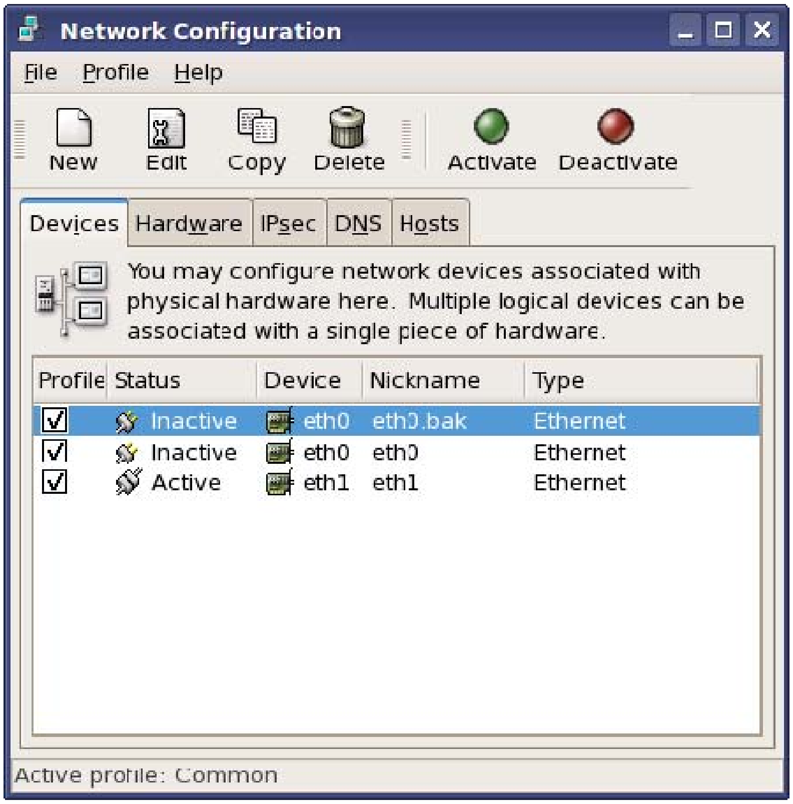
After the server has started, it may be necessary to manually configure the IP address information, start the DHCP daemon (dhcpd), and restart the DNS (named). To determine if these steps are necessary, use the following procedure to check the IP address assigned to the computer's NIC:

1. Choose **Terminal** to open a terminal window.
2. Enter **su -** and click **Enter** (note that the '**-**' is very important).
3. When prompted, enter the root password **discoverit**.
4. When the terminal window is open, enter the **`ifconfig`** command to see information about the interfaces found in the machine.

If the IP address information is not correct, complete Steps A and B below.

A. Setting the Network Address

1. From the K start button in the lower left corner of the screen, click **Administration** and then click **Network**.
2. When prompted, enter the root password **discoverit** and click **OK**. The Network Configuration window, similar to that shown in Figure 2, should open. The interfaces displayed will depend on the computer system.



You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

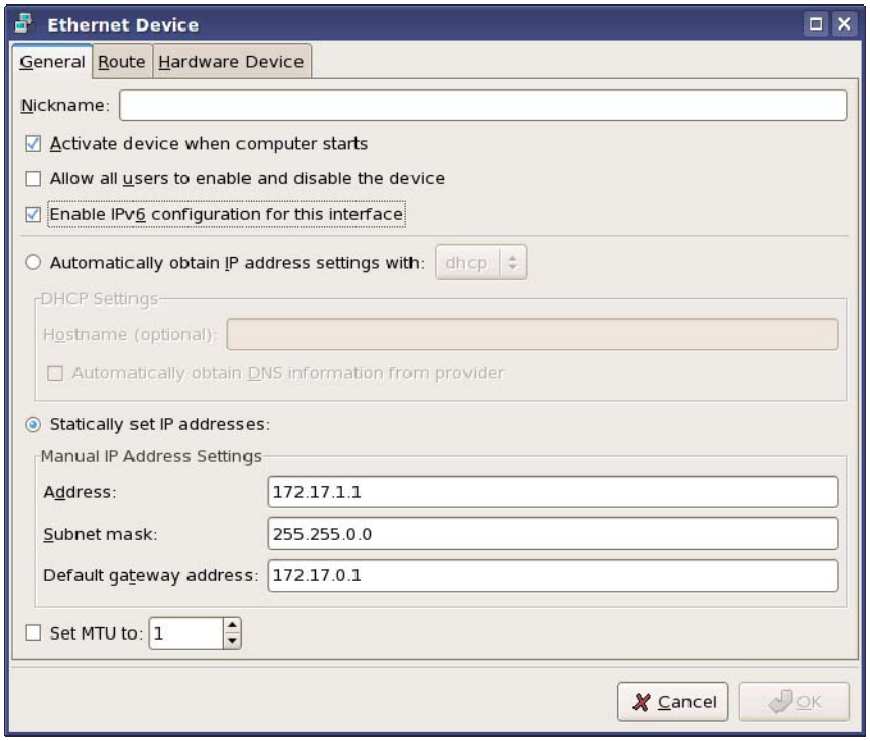
Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0.bak	Ethernet
☑	Inactive	eth0	eth0	Ethernet
☑	Active	eth1	eth1	Ethernet

Active profile: Common

Figure 2: The Network Configuration Window

3. On the Network Configuration window, click the **Devices** tab.

4. Select **eth0** or the interface that corresponds to your first Ethernet card and then click **Edit**. This should display the Ethernet Device configuration pane shown in Figure 3.



Nickname:

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

☑ Enable IPv6 configuration for this interface

○ Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

□ Automatically obtain DNS information from provider

● Statically set IP addresses:

Manual IP Address Settings

Address: 172.17.1.1

Subnet mask: 255.255.0.0

Default gateway address: 172.17.0.1

□ Set MTU to: 1

Figure 3: The Ethernet Device Configuration Pane

5. To set the IP addressing information, click the **Statically set IP addresses** radio button and enter the following information:

   Address: **172.17.1.1**

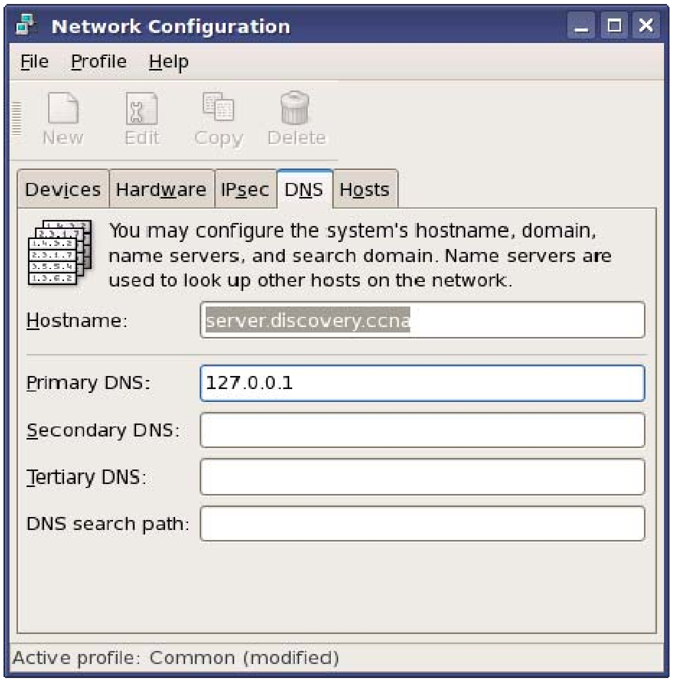
   Subnet mask: **255.255.0.0**

   Default gateway address: **172.17.0.1**

6. Click **OK**.
7. Return to the Network Configuration window and click the **DNS** tab.
8. Enter the following information, as shown in Figure 4:

   Set hostname: **server.discovery.ccna**

   Set Primary DNS: **127.0.0.1**



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname: server.discovery.ccna

Primary DNS: 127.0.0.1

Secondary DNS:

Tertiary DNS:

DNS search path:

Active profile: Common (modified)

Figure 4: Discovery Server DNS Configuration

9. Next, click the **Devices** tab.
10. Choose **eth0**.
11. Click **Activate**.
12. Answer **Yes / OK** to any questions.
13. Close the Network Configuration window. When prompted, click **Yes** to save changes.

B. Starting DNS and DHCP

The DNS service must be restarted to reflect the new IP address on the Ethernet interface. In addition, because the Ethernet interface failed to initialize during startup, the DHCP service must also be manually started.

1. Click **Terminal** to open a terminal window.
2. Enter **su -** and click **Enter** (note that the '**-**' is very important).
3. When prompted, enter the root password **discoverit**.
4. Enter **service named restart** and press **Enter**.
5. Enter **dhcpd** and press **Enter**.

You should now have a fully operational server. It may take a few minutes for DNS to become fully operational.

Streaming Video Server

Some of the labs in CCNA Discovery 4 require that a video stream be established. This service is off by default and must be turned on.

To stream a video, use the following procedure from the server console:

1. Choose **Terminal** to open a terminal window.
2. Enter **su -** and click **Enter** (note that the '**-**' is very important).
3. When prompted, enter the root password **discoverit**.

After you are logged in as root and have a terminal session open, complete the following steps:

1. Enter **cd /** to go to the root directory.
2. Enter **cd /usr/StreamingServer** to go to the directory with the streaming server files.
3. Enter **DarwinStreamingServer** to start the server.
4. Enter **perl streamingadminserver.pl** to start the administration server.

When the administration server is running, all further configuration is accomplished using a web browser.

1. Use a web browser to bring up the configuration server by connecting to the server on port 1220 (http://172.17.1.1:1220). All usernames and passwords are **stream**.
2. Delete any old playlists that may be **present**.
3. Create a new playlist by dragging the movie file to the right box. Select ***Sequential Looped*** for the play mode, name the stream, and click the **Save Changes** button at the bottom of the screen.
4. Click the button next to the stream name to start the streaming video.
5. To connect to the stream, use the Quicktime Player (free download from Apple Inc. at www.apple.com).
6. Launch Quicktime Player.
7. Under **File**, click **Open URL**.
8. Enter the URL **rtsp://<server ip>/stream**; for example, **rtsp://172.17.1.1/MWO.sdp**, assuming that the server has the default IP address of 172.17.1.1 and the stream was named MWO.sdp for "Mind Wide Open."

NOTE: The Discovery Server Live CD is provided without warranty of any kind. It is intended to be used only to support the CCNA Discovery labs. For information on the Cisco Networking Academy Program, visit http://cisco.netacad.net.

Quick Start Instructions

1. Obtain a Discovery Server Live CD from your instructor.
2. In the BIOS of the computer to be used as a server, change the boot order to boot from the CD-ROM first.
3. Connect the NIC of the computer being used for the Discovery Server to a switch or router per the lab setup using an appropriate cable.
4. Disable all extra network cards in the machine.
5. Insert the CD and restart the computer to boot to the CD.
6. At the first options menu, select ’a’.
7. If the second menu displays, select ‘1’. **NOTE:** This menu will not be seen on all machines.
8. Follow the instructions above to set IP address, streaming, etc.

Common Issues and Answers

Problem: Machine boots to the first menu and then freezes.

Solution: This occurs on many machines that use a USB keyboard. Discovery Server does not currently support USB keyboards. If the machine is capable of using a PS/2 style keyboard, replace the USB keyboard with one using a PS/2 interface and restart the server. If the machine is not capable of accepting a PS/2 style keyboard, try a different machine.

Problem: Machine boots to a command prompt and not to the graphical screen.

Solution: On some machines, the graphical interface is started but hidden from view. If presented with a login prompt, switch to the graphical interface by pressing **Alt-F7**.

Problem: Multiple network cards are visible in setup.

Solution: The Discovery Server is currently designed to use only a single NIC. If multiple NICs are enabled in the machine, these will be detected and shown as eth0, eth1, eth2, etc. On some machines an eth0.bak interface also appears. The first network card is eth0, and this is the one that should normally be terminated and configured.

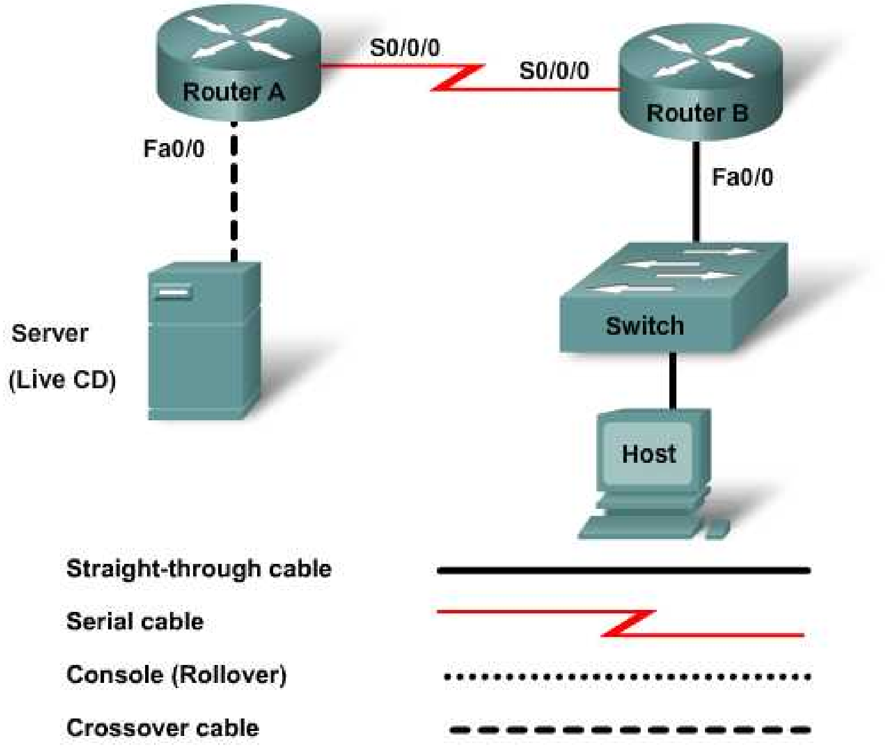
Problem: Eth0 interface is not working but eth1 is present.

Solution: This occurs on many laptop computers that have an internal wireless NIC. The wireless NIC appears as eth0 and the standard Ethernet NIC is eth1. In this case, configure eth1 with the appropriate IP address.

Problem: Machine will not work with Discovery Server.

Solution: The Discovery Server does not work on all machines. If it does not work on your machine, try another computer. If another computer is not available, run the server in a virtual environment using software such as Microsoft Virtual PC, VMWare, or Innotek VirtualBox software.

Lab 1.2.2 Capturing and Analyzing Network Traffic



Host Name	IP Address Fa0/0	Subnet Mask	IP Address S0/0/0	Subnet Mask	Default Gateway
RouterA	172.17.0.1	255.255.0.0	192.168.1.1 (**DCE**)	255.255.255.0	N/A
RouterB	192.168.3.1	255.255.255.0	192.168.1.2	255.255.255.0	N/A
Server	172.17.1.1	255.255.0.0			172.17.0.1
Switch					
Host	192.168.3.2	255.255.255.0			192.168.3.1

Objectives

- Use Wireshark to capture protocol data packets as they cross the networks.
- Use Wireshark to analyze protocol data packets from the captured results.

Background / Preparation

This lab focuses on the basic configuration of the Cisco 1841 or comparable routers using Cisco IOS commands. The information in this lab applies to other routers; however, command syntax may vary. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or comparable routers with minimum one serial and one fast Ethernet interface
- Two Windows-based PCs, one with a terminal emulation program. Use one PC as the host, and use the other as the server.
- RJ-45-to-DB-9 connector console cable to configure the routers
- Two straight-through Ethernet cables
- One crossover Ethernet cable
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that all routers and the switch have been erased and have no startup configurations. If you need instructions, refer to the end of this lab. Instructions are provided for both the switch and router.

Step 1: Connect the routers and configure

a. Connect the two routers with a serial cable. RouterA will provide the clocking signal between the two routers. Use S0/0/0 on both routers to connect them.

b. Use RIP as the protocol when configuring both routers. Advertise the appropriate networks on each router.

c. Connect the Fa0/0 on RouterA with a crossover cable to the server running the Discovery Server Live CD.

d. RouterB will use a straight-through cable from its Fa0/0 to connect to the switch through the Fa0/1. Configure the routers as shown in the topology diagram above.

Step 2: Connect the host to the switch and configure

Step 3: Verify connectivity using ping

a. To verify that the network is set up successfully, ping from the host to the server.

b. If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the host, server, and router configurations.

c. Was the ping successful? ____

Step 4: Launch Wireshark

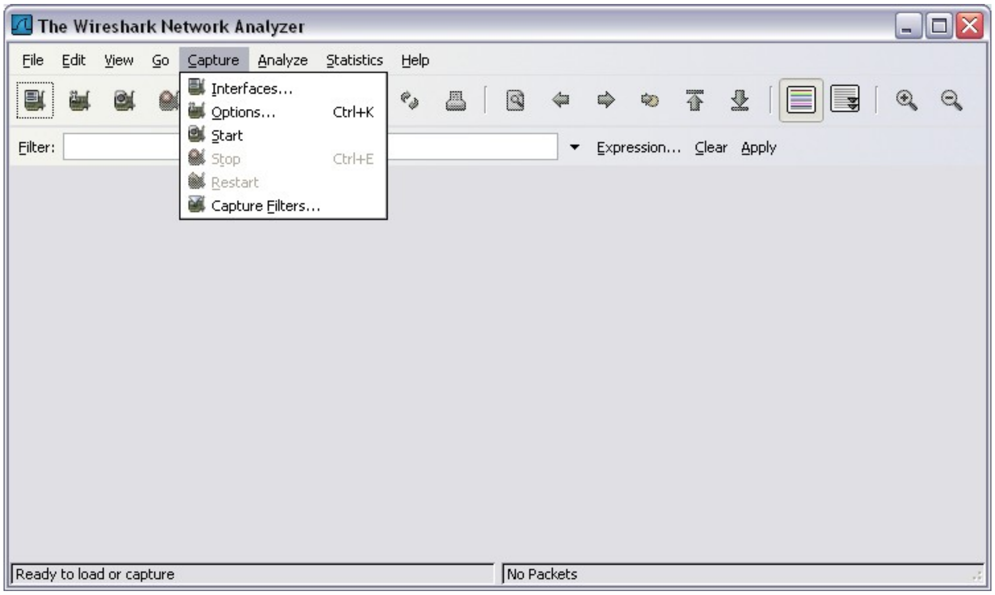
NOTE: Wireshark may be downloaded from the Internet at www.wireshark.org and installed on each local host. If this is not possible, Wireshark may be run from the Discovery Live CD. Check with your instructor to determine which procedure to follow.

a. If running Wireshark from the local host, double-click on the icon to begin the application and proceed to step d. If running Wireshark from the Discovery server, proceed to step b.

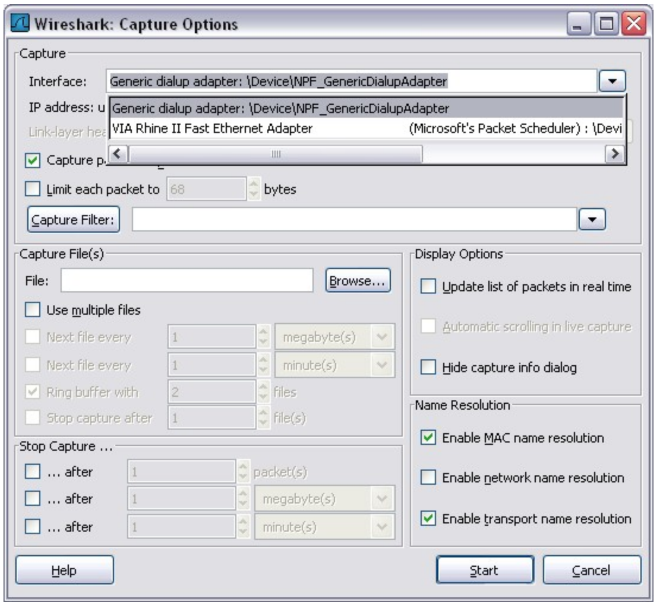
b. From the **K Start** menu on the server desktop, choose **Internet> Wireshark Network Analyzer**.

c. Launch Wireshark if it is not already open. If prompted for a password, enter **discoverit**.

d. To start data capture, go to the **Capture** menu click **Options**. The **Options** dialog provides a range of settings and filters that determine how much data traffic is captured.



e. Ensure that Wireshark is set to monitor the correct interface. From the **Interface** drop-down list, select the network adapter in use. For most computers, this will be the connected Ethernet Adapter.

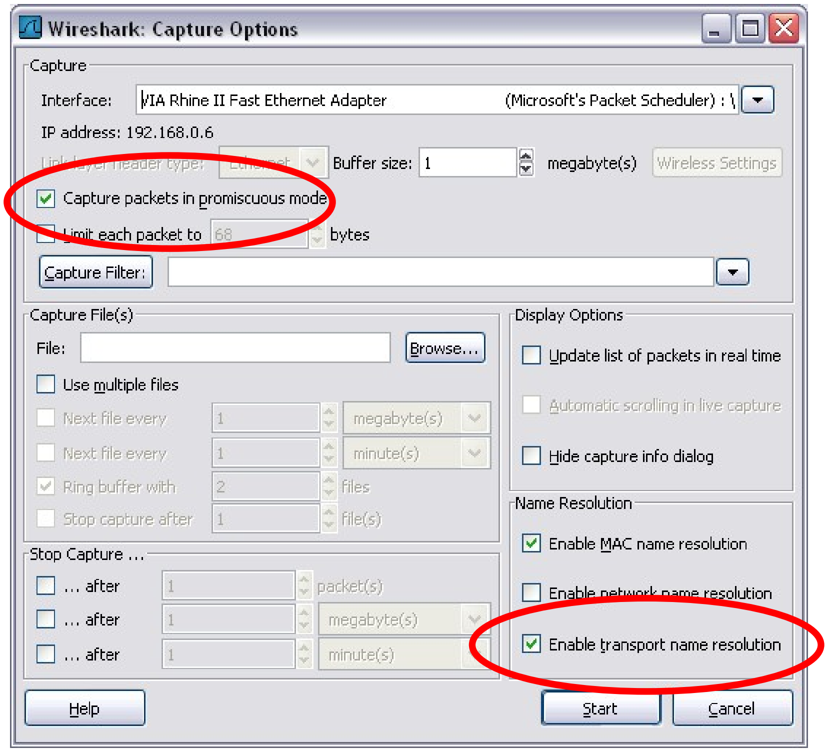


Interface: Generic dialup adapter: \Device\NPF_GenericDialupAdapter

Generic dialup adapter: \Device\NPF_GenericDialupAdapter
VIA Rhine II Fast Ethernet Adapter (Microsoft's Packet Scheduler) : \Devi

☑ Capture p
☐ Limit each packet to 68 bytes
☐ Use multiple files
☐ Next file every 1 megabyte(s)
☐ Next file every 1 minute(s)
☑ Ring buffer with 2 files
☐ Stop capture after 1 file(s)
☐ ... after 1 packet(s)
☐ ... after 1 megabyte(s)
☐ ... after 1 minute(s)
☐ Update list of packets in real time
☐ Automatic scrolling in live capture
☐ Hide capture info dialog
☑ Enable MAC name resolution
☐ Enable network name resolution
☑ Enable transport name resolution

f. Next, other options can be set. The two options highlighted below are worth examination: Capture packets in promiscuous mode and Enable transport name resolution.



Wireshark: Capture Options

Capture

Interface: VIA Rhine II Fast Ethernet Adapter (Microsoft's Packet Scheduler) : \

IP address: 192.168.0.6

Link-layer header type: Ethernet Buffer size: 1 megabyte(s) Wireless Settings

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File: Browse...

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 2 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

□ Update list of packets in real time

□ Automatic scrolling in live capture

□ Hide capture info dialog

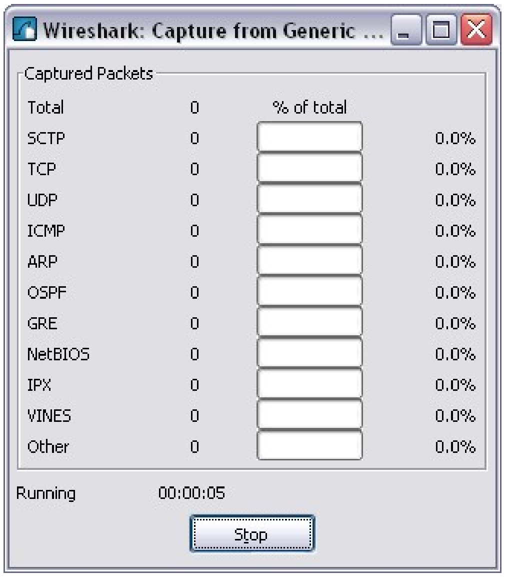
Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

☑ Enable transport name resolution

- **Setting Wireshark to capture packets in promiscuous mode**
- **Setting Wireshark for network name resolution**
- Clicking the **Start** button starts the data capture process. A message box displays the progress of this process.
- Create some traffic to be captured. Issue a **`ping`** and **`tracert`** from the host and watch for routing updates.

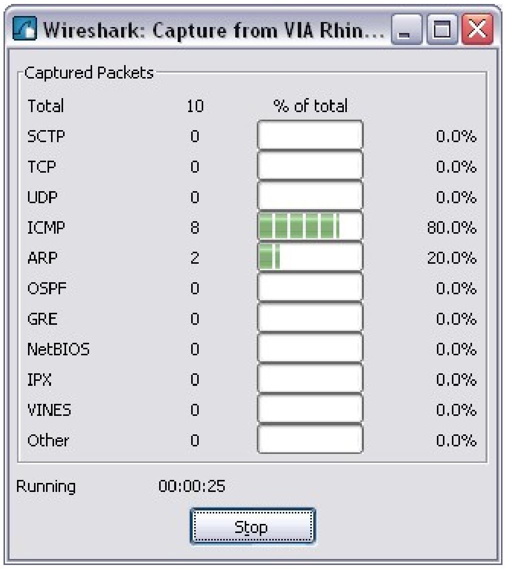


Wireshark: Capture from Generic ...

Captured Packets

Total	0	% of total	
SCTP	0		0.0%
TCP	0		0.0%
UDP	0		0.0%
ICMP	0		0.0%
ARP	0		0.0%
OSPF	0		0.0%
GRE	0		0.0%
NetBIOS	0		0.0%
IPX	0		0.0%
VINES	0		0.0%
Other	0		0.0%

Running 00:00:05

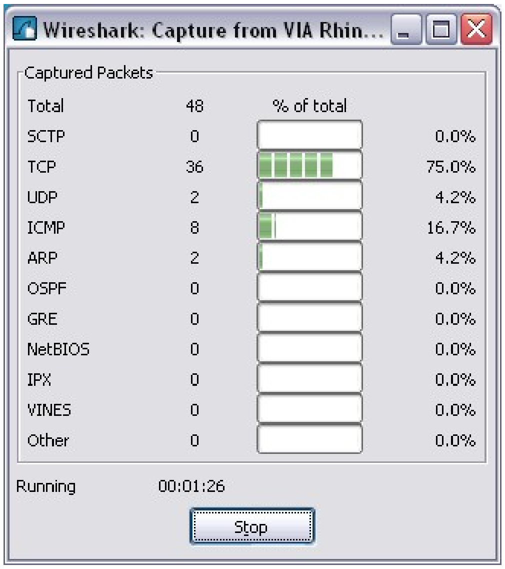


Wireshark: Capture from VIA Rhin...

Captured Packets

Total	10	% of total
SCTP	0	0.0%
TCP	0	0.0%
UDP	0	0.0%
ICMP	8	80.0%
ARP	2	20.0%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	0	0.0%

Running 00:00:25



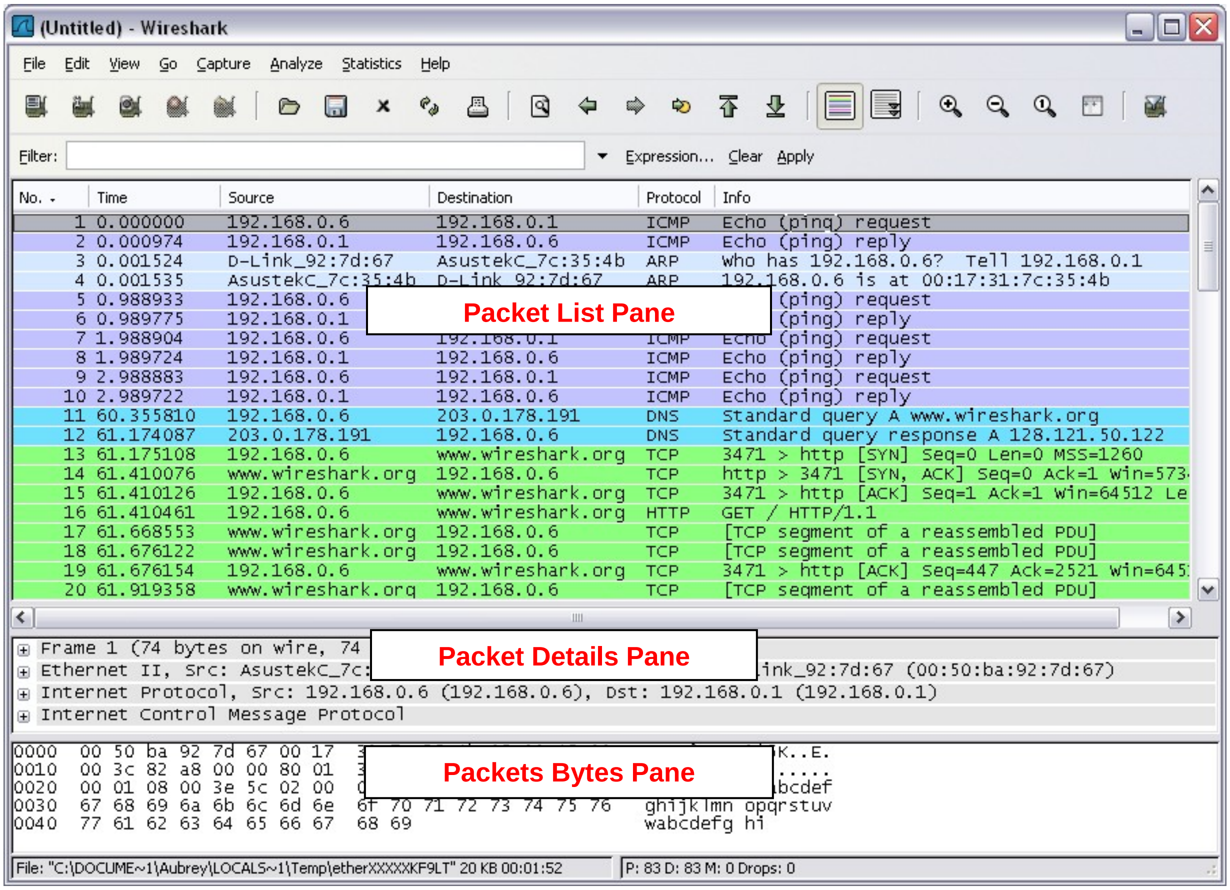
Wireshark: Capture from VIA Rhin...

Captured Packets

Total	48	% of total
SCTP	0	0.0%
TCP	36	75.0%
UDP	2	4.2%
ICMP	8	16.7%
ARP	2	4.2%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	0	0.0%

Running 00:01:26

- Clicking the **Stop** button terminates the capture process. The main screen is displayed.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.6	192.168.0.1	ICMP	Echo (ping) request
2	0.000974	192.168.0.1	192.168.0.6	ICMP	Echo (ping) reply
3	0.001524	D-Link_92:7d:67	AsustekC_7c:35:4b	ARP	Who has 192.168.0.6? Tell 192.168.0.1
4	0.001535	AsustekC_7c:35:4b	D-Link_92:7d:67	ARP	192.168.0.6 is at 00:17:31:7c:35:4b
5	0.988933	192.168.0.6			(ping) request
6	0.989775	192.168.0.1			(ping) reply
7	1.988904	192.168.0.6	192.168.0.1	ICMP	Echo (ping) request
8	1.989724	192.168.0.1	192.168.0.6	ICMP	Echo (ping) reply
9	2.988883	192.168.0.6	192.168.0.1	ICMP	Echo (ping) request
10	2.989722	192.168.0.1	192.168.0.6	ICMP	Echo (ping) reply
11	60.355810	192.168.0.6	203.0.178.191	DNS	Standard query A www.wireshark.org
12	61.174087	203.0.178.191	192.168.0.6	DNS	Standard query response A 128.121.50.122
13	61.175108	192.168.0.6	www.wireshark.org	TCP	3471 > http [SYN] Seq=0 Len=0 MSS=1260
14	61.410076	www.wireshark.org	192.168.0.6	TCP	http > 3471 [SYN, ACK] Seq=0 Ack=1 Win=573
15	61.410126	192.168.0.6	www.wireshark.org	TCP	3471 > http [ACK] Seq=1 Ack=1 Win=64512 Le
16	61.410461	192.168.0.6	www.wireshark.org	HTTP	GET / HTTP/1.1
17	61.668553	www.wireshark.org	192.168.0.6	TCP	[TCP segment of a reassembled PDU]
18	61.676122	www.wireshark.org	192.168.0.6	TCP	[TCP segment of a reassembled PDU]
19	61.676154	192.168.0.6	www.wireshark.org	TCP	3471 > http [ACK] Seq=447 Ack=2521 Win=645
20	61.919358	www.wireshark.org	192.168.0.6	TCP	[TCP segment of a reassembled PDU]

```
⊞ Frame 1 (74 bytes on wire, 74
⊞ Ethernet II, Src: AsustekC_7c:                         ink_92:7d:67 (00:50:ba:92:7d:67)
⊞ Internet Protocol, Src: 192.168.0.6 (192.168.0.6), Dst: 192.168.0.1 (192.168.0.1)
⊞ Internet Control Message Protocol
```

```
0000  00 50 ba 92 7d 67 00 17  3                          K..E.
0010  00 3c 82 a8 00 00 80 01  3                          .....
0020  00 01 08 00 3e 5c 02 00  0                          bcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "C:\DOCUME~1\Aubrey\LOCALS~1\Temp\etherXXXXXKF9LT" 20 KB 00:01:52 | P: 83 D: 83 M: 0 Drops: 0

- The PDU (or Packet) List pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes.
- The PDU (or Packet) Details pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail.
- The PDU (or Packet) Bytes pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List pane, and highlights the field selected in the Packet Details pane.

Packet List Pane

Each line in the Packet List pane corresponds to one PDU or packet of the captured data. If you select a line in this pane, additional details are displayed in the Packet Details and Packet Bytes panes. The example above shows the PDUs captured when the ping utility was used and http://www.Wireshark.org was accessed. Packet number 1 is selected in this pane.

Packet Details Pane

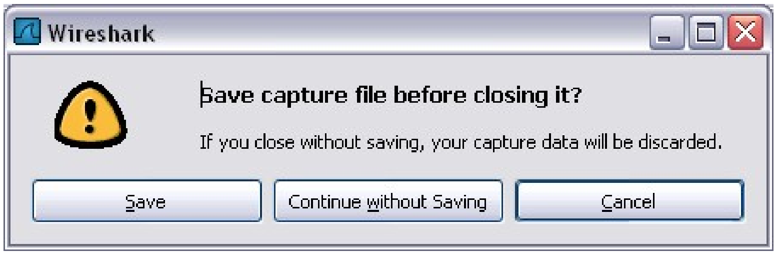
The Packet Details pane shows the current packet (selected in the Packet List pane) in a more detailed form. This pane shows the protocols and protocol fields of the selected packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed.

Packet Bytes Pane

The Packet Bytes pane shows the data of the current packet (selected in the Packet List pane) in what is known as "hexdump" style. In this lab, this pane will not be examined in detail. However, when a more in-depth analysis is required, this displayed information is useful for examining the binary values and content of PDUs.

The information captured for the data PDUs can be saved in a file. This file can then be opened in Wireshark for future analysis without the need to recapture the same data traffic again. The information displayed when a capture file is opened is the same as the original capture.

When closing a data capture screen or exiting Wireshark, you are prompted to save the captured PDUs.



Save capture file before closing it?

If you close without saving, your capture data will be discarded.

Step 5: Ping PDU Capture

a. Launch Wireshark.

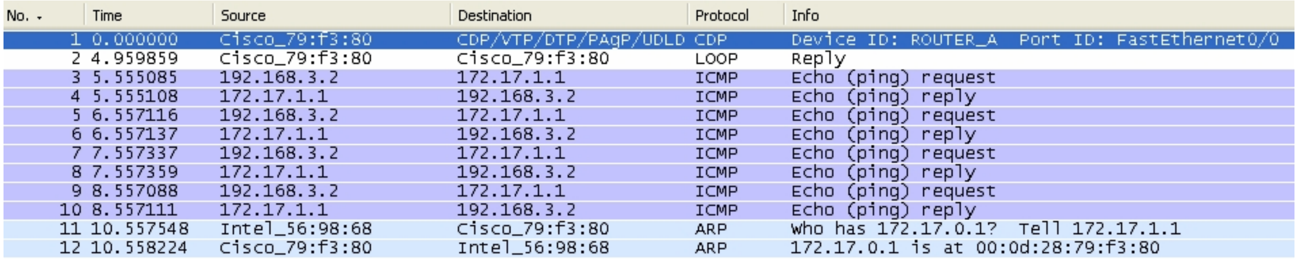
b. Set the Capture Options as described in Step 4 and start the capture process.

c. From the command line of the host, ping the IP address of the server on the other end of the lab topology. In this case, ping the Discovery Server Live CD using the command **`ping 172.17.1.1`**.

d. After receiving the successful replies to the ping in the command-line window, stop the packet capture.

Step 6: Examine the Packet List pane

a. The Packet List pane on Wireshark should now look similar to this:



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_79:f3:80	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: ROUTER_A Port ID: FastEthernet0/0
2	4.959859	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
3	5.555085	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
4	5.555108	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
5	6.557116	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
6	6.557137	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
7	7.557337	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
8	7.557359	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
9	8.557088	192.168.3.2	172.17.1.1	ICMP	Echo (ping) request
10	8.557111	172.17.1.1	192.168.3.2	ICMP	Echo (ping) reply
11	10.557548	Intel_56:98:68	Cisco_79:f3:80	ARP	Who has 172.17.0.1? Tell 172.17.1.1
12	10.558224	Cisco_79:f3:80	Intel_56:98:68	ARP	172.17.0.1 is at 00:0d:28:79:f3:80

b. Look at the packets listed; we are interested in the packets numbered 3 through 10.

c. Locate the equivalent packets on the packet list on your computer. The numbers may be different.

d. From the Wireshark Packet List, answer the following questions:

1) What protocol is used by ping? ____________________________________

2) What is the full protocol name? ____________________________________

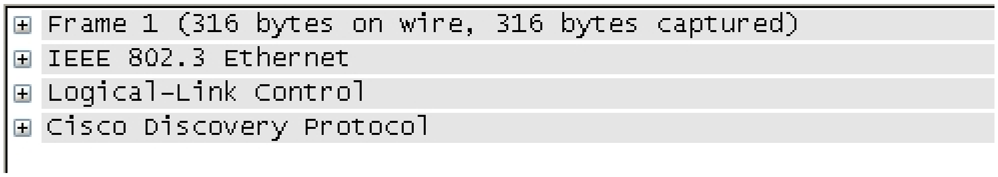
3) What are the names of the two ping messages? ____________________________________ and

4) Are the listed source and destination IP addresses what you expected? _____________

5) Why?

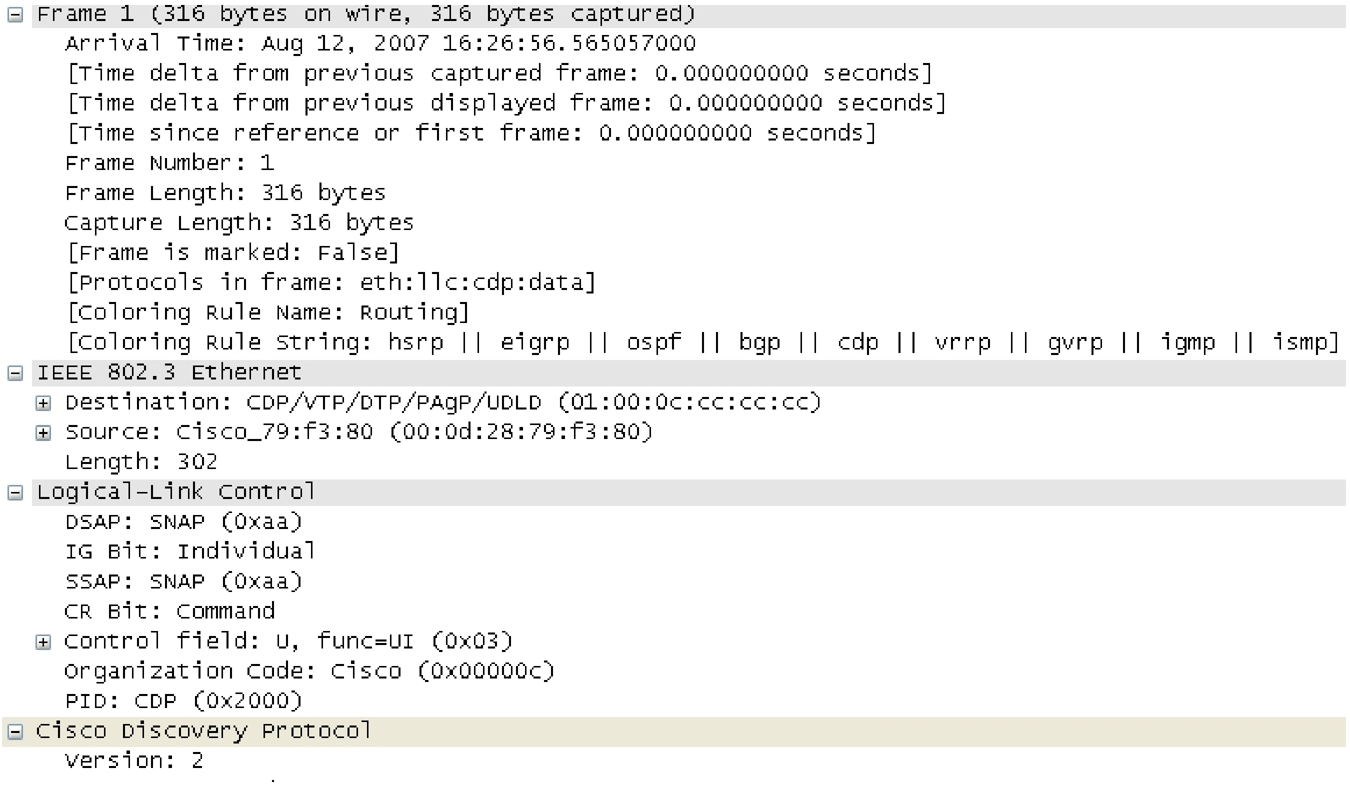
Step 7: Examine the Packet Details pane

a. Select (highlight) the first echo request packet on the list with the mouse. The Packet Detail pane will now display something similar to this:



```
⊞ Frame 1 (316 bytes on wire, 316 bytes captured)
⊞ IEEE 802.3 Ethernet
⊞ Logical-Link Control
⊞ Cisco Discovery Protocol
```

b. Click each of the four **+** to expand the information. The packet Detail Pane will now be similar to:

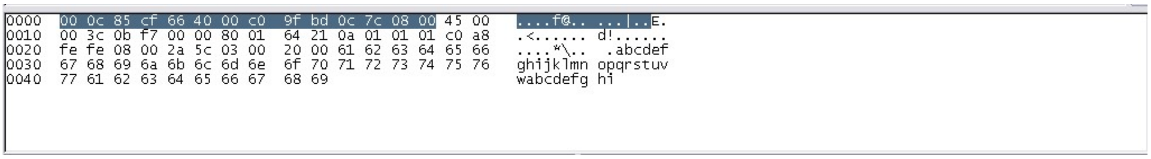


```
⊟ Frame 1 (316 bytes on wire, 316 bytes captured)
    Arrival Time: Aug 12, 2007 16:26:56.565057000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 316 bytes
    Capture Length: 316 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:llc:cdp:data]
    [Coloring Rule Name: Routing]
    [Coloring Rule String: hsrp || eigrp || ospf || bgp || cdp || vrrp || gvrp || igmp || ismp]
⊟ IEEE 802.3 Ethernet
  ⊞ Destination: CDP/VTP/DTP/PAgP/UDLD (01:00:0c:cc:cc:cc)
  ⊞ Source: Cisco_79:f3:80 (00:0d:28:79:f3:80)
    Length: 302
⊟ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ⊞ Control field: U, func=UI (0x03)
    Organization Code: Cisco (0x00000c)
    PID: CDP (0x2000)
⊟ Cisco Discovery Protocol
    Version: 2
```

c. Spend some time scrolling through this information. At this stage of the course, you may not fully understand the information displayed. Make a note of the information you do recognize.

d. Locate the two different types of Source and Destination.

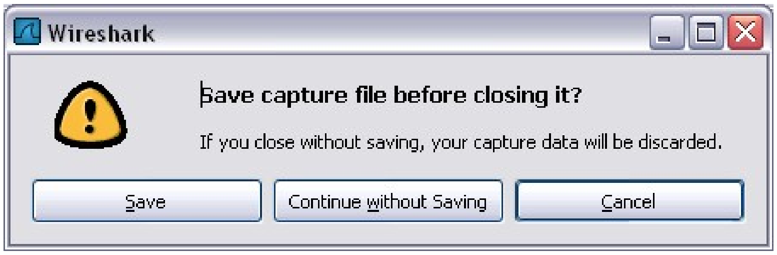
e. Select a line in the Packets Detail pane (middle pane). Notice that all or part of the information in the Packet Bytes pane also becomes highlighted.



```
0000  00 0c 85 cf 66 40 00 c0  9f bd 0c 7c 08 00 45 00   ....f@.. ...|..E.
0010  00 3c 0b f7 00 00 80 01  64 21 0a 01 01 01 c0 a8   .<...... d!......
0020  fe fe 08 00 2a 5c 03 00  20 00 61 62 63 64 65 66   ....*\..  .abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

f. Go to the **File** menu and click **Close**.

g. Click **Continue without Saving** when this message box appears.



Save capture file before closing it?

If you close without saving, your capture data will be discarded.

Step 8: Perform an FTP PDU Capture

a. Assuming that Wireshark is still running from the previous steps, start packet capture by clicking the **Start** option on the Wireshark **Capture** menu.

b. At the command line on your host, enter **ftp 172.17.1.1**. When the connection is established, enter **anonymous** as the user.

c. When successfully logged in, enter **get /pub/Discovery_1/document_1** and press the **Enter** key. Note that there is a space after **get**. This command will start downloading the file from the ftp server. The output will look similar to:

```
C:\> ftp 172.17.1.1
Connected to 172.17.1.1
220 Welcome to The CCNA-Discovery FTP service.
ftp> get /pub/Discovery_1/document_1
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pub/Discovery_1/document_1
<73 bytes>.
226 File send OK.
ftp: 73 bytes received in 0.03Seconds 2.35Kbytes/sec.
```

d. When the file download is complete, enter **`quit`**.

```
ftp> quit
221 Goodbye.

C:\>
```

e. Stop the PDU capture in Wireshark.

Step9: Examine the Packet List pane

a. Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.

b. Locate and note those PDUs associated with the file download. These will be the PDUs from the Layer 4 protocol TCP and the Layer 7 protocol FTP.

c. Identify the three groups of PDUs associated with the file transfer. The first group is associated with the connection phase and logging into the server. List examples of messages exchanged in this phase.

d. Locate and list examples of messages exchanged in the second phase that is the actual download request and the data transfer.

e. The third group of PDUs relate to logging out and breaking the connection. List examples of messages exchanged during this process.

f. Locate recurring TCP exchanges throughout the FTP process. What feature of TCP does this indicate?

Step 10: Examine Packet Details and Packet Byte panes

a. Select (highlight) a packet on the list associated with the first phase of the FTP process. View the packet details in the Packet Details pane.

b. What are the protocols encapsulated in the frame?

c. Highlight the packets containing the username and password. Examine the highlighted portion in the Packet Byte pane. What does this say about the security of this FTP login process?

NOTE: SDM Enabled Routers – If the startup-config file is erased on an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Contact your instructor if necessary.

Connect the Host to attach to Fast Ethernet switch port Fa0/2. Configure the host as shown in the topology diagram above.

If this feature is *not* checked, only PDUs destined for this computer will be captured.

If this feature is checked, all PDUs destined for this computer *and* all those detected by the computer NIC on the same network segment (i.e., those that "pass by" the NIC but are not destined for the computer) are captured.

NOTE: As you use different intermediary devices (hubs, switches, routers) to connect end devices on a network, you will experience different Wireshark results.

This option allows you to control whether or not Wireshark translates network addresses found in PDUs into names. Although this is a useful feature, the name resolution process may add extra PDUs to your captured data, perhaps distorting the analysis.

There are also a number of other capture filtering and process settings available on this screen.

As data PDUs are captured, the types and number are indicated in the message box. The examples show the capture of a ping process and then accessing a web page.

This main display window of Wireshark has three panes.

Clicking **Continue without Saving** closes the file or exits Wireshark without saving the displayed captured data.

____

____

As you can see, the details for each section and protocol can be expanded further.

Why are there two types?

____

What protocols are in the Ethernet frame?

____

For example, if the second line (+ Ethernet II) is highlighted in the Details pane, the Bytes pane now highlights the corresponding values.

This example shows the particular binary values that represent that information in the PDU. At this point in the course, it is not necessary to understand this information in detail.

____

____

____

____

____

____

____

____

____

____

____

____

____

NOTE: Capture Options do not have to be set if continuing from previous steps of this lab.

____

____

____

____

____

If there was no VLAN file, this message is displayed:

The responding line prompt is:

Press **Enter** to confirm.

The response should be:

Verify that the VLAN configuration was deleted in Step b using the **`show vlan`** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present, you must power cycle the switch (hardware restart) instead of issuing the **`reload`** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it, and then plug it back in. If the VLAN information was successfully deleted in Step b, go to Step e and restart the switch using the **`reload`** command.

NOTE: This step is not necessary if the switch was restarted using the power cycle method.

The responding line prompt is:

The responding line prompt is:

The first line of the response is:

After the switch has reloaded, the line prompt is:

The responding line prompt is:

The responding line prompt is:

The response is:

The responding line prompt is:

The responding line prompt is:

In the first line of the response is:

After the router has reloaded the line prompt is:

The responding line prompt is:

The router is ready for the assigned lab to be performed.

This is the interface that a PC will connect to using a browser to bring up SDM. The PC IP address should be set to 10.10.10.2 255.255.255.248.

NOTE: An SDM router other than the 1841 may require connection to a different port to access SDM.

Replace <`username`> and <`password`> with the username and password that you want to configure.

d. Highlight a packet associated with the second phase. From any pane, locate the packet containing the filename. What is the filename that was downloaded?

e. When finished, close the Wireshark file and continue without saving.

Step 11: Perform an HTTP PDU Capture

a. Start packet capture. Assuming that Wireshark is still running from the previous steps, start packet capture by clicking the **Start** option on the Wireshark **Capture** menu.

b. Launch a web browser on the computer that is running Wireshark.

c. Enter the IP address of the Discovery Server 172.17.1.1 in the address box. When the webpage has fully downloaded, stop the Wireshark packet capture.

Step 12: Examine the Packet List pane

a. Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.

b. Locate and identify the TCP and HTTP packets associated with the webpage download.

c. Note the similarity between this message exchange and the FTP exchange.

Step 13: Examine the Packet Details and Bytes panes

a. In the Packet List pane, highlight an HTTP packet that has the notation **(text/html)** in the **Info** column.

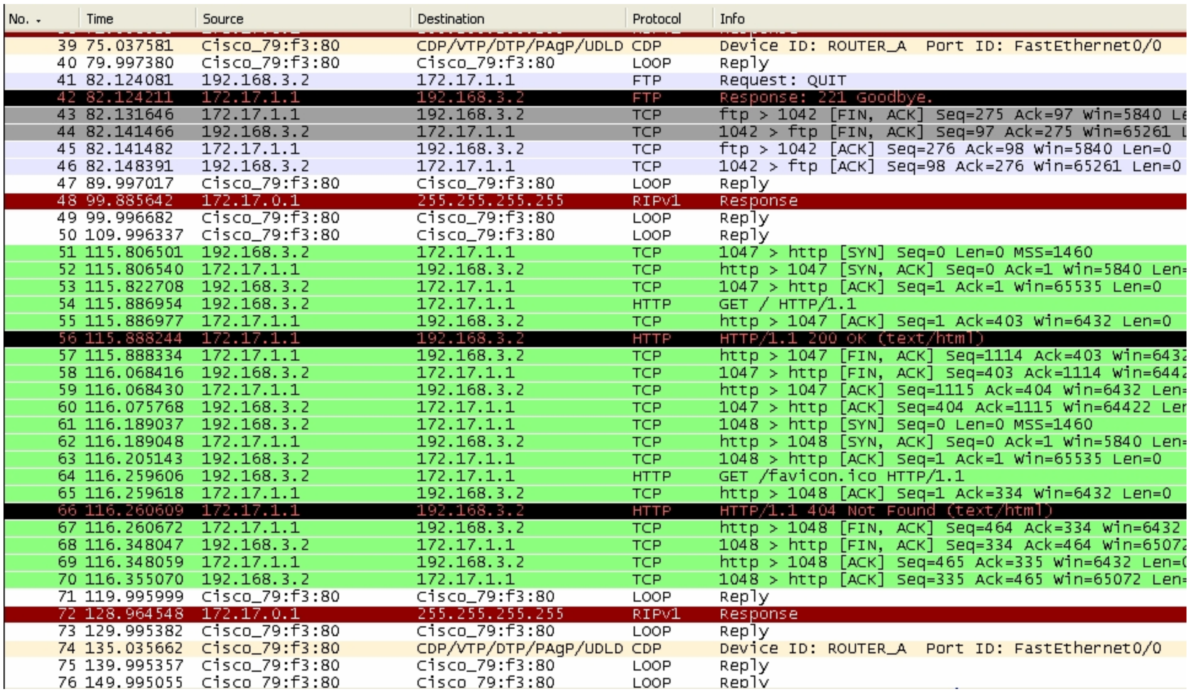
b. In the Packet Details pane, click the **+** next to **Line-based text data: html**. When this information expands, what is displayed?

c. Examine the highlighted portion of the Byte pane. This portion shows the HTML data carried by the packet.

d. When finished, close the Wireshark file and continue without saving.

Step 14: Analyze the capture

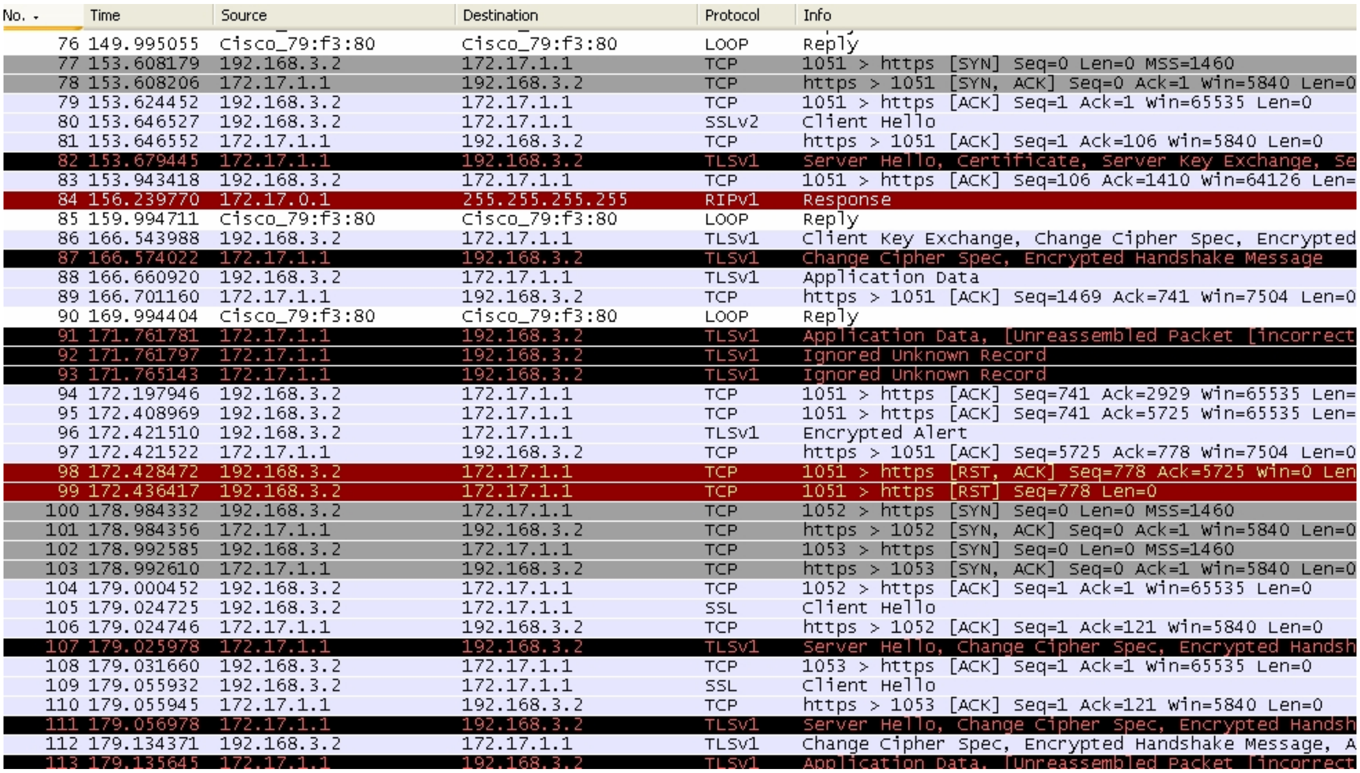
a. Look at the capture below and examine the various protocols being used in this network.



```
No.  Time          Source            Destination             Protocol  Info
  39 75.037581     Cisco_79:f3:80    CDP/VTP/DTP/PAgP/UDLD   CDP       Device ID: ROUTER_A  Port ID: FastEthernet0/0
  40 79.997380     Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
  41 82.124081     192.168.3.2       172.17.1.1              FTP       Request: QUIT
  42 82.124211     172.17.1.1        192.168.3.2             FTP       Response: 221 Goodbye.
  43 82.131646     172.17.1.1        192.168.3.2             TCP       ftp > 1042 [FIN, ACK] Seq=275 Ack=97 Win=5840 Le
  44 82.141466     192.168.3.2       172.17.1.1              TCP       1042 > ftp [FIN, ACK] Seq=97 Ack=275 Win=65261 L
  45 82.141482     172.17.1.1        192.168.3.2             TCP       ftp > 1042 [ACK] Seq=276 Ack=98 Win=5840 Len=0
  46 82.148391     192.168.3.2       172.17.1.1              TCP       1042 > ftp [ACK] Seq=98 Ack=276 Win=65261 Len=0
  47 89.997017     Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
  48 99.885642     172.17.0.1        255.255.255.255         RIPv1     Response
  49 99.996682     Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
  50 109.996337    Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
  51 115.806501    192.168.3.2       172.17.1.1              TCP       1047 > http [SYN] Seq=0 Len=0 MSS=1460
  52 115.806540    172.17.1.1        192.168.3.2             TCP       http > 1047 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
  53 115.822708    192.168.3.2       172.17.1.1              TCP       1047 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  54 115.886954    192.168.3.2       172.17.1.1              HTTP      GET / HTTP/1.1
  55 115.886977    172.17.1.1        192.168.3.2             TCP       http > 1047 [ACK] Seq=1 Ack=403 Win=6432 Len=0
  56 115.888244    172.17.1.1        192.168.3.2             HTTP      HTTP/1.1 200 OK (text/html)
  57 115.888334    172.17.1.1        192.168.3.2             TCP       http > 1047 [FIN, ACK] Seq=1114 Ack=403 Win=6432
  58 116.068416    192.168.3.2       172.17.1.1              TCP       1047 > http [FIN, ACK] Seq=403 Ack=1114 Win=6442
  59 116.068430    172.17.1.1        192.168.3.2             TCP       http > 1047 [ACK] Seq=1115 Ack=404 Win=6432 Len=
  60 116.075768    192.168.3.2       172.17.1.1              TCP       1047 > http [ACK] Seq=404 Ack=1115 Win=64422 Len
  61 116.189037    192.168.3.2       172.17.1.1              TCP       1048 > http [SYN] Seq=0 Len=0 MSS=1460
  62 116.189048    172.17.1.1        192.168.3.2             TCP       http > 1048 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
  63 116.205143    192.168.3.2       172.17.1.1              TCP       1048 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
  64 116.259606    192.168.3.2       172.17.1.1              HTTP      GET /favicon.ico HTTP/1.1
  65 116.259618    172.17.1.1        192.168.3.2             TCP       http > 1048 [ACK] Seq=1 Ack=334 Win=6432 Len=0
  66 116.260609    172.17.1.1        192.168.3.2             HTTP      HTTP/1.1 404 Not Found (text/html)
  67 116.260672    172.17.1.1        192.168.3.2             TCP       http > 1048 [FIN, ACK] Seq=464 Ack=334 Win=6432
  68 116.348047    192.168.3.2       172.17.1.1              TCP       1048 > http [FIN, ACK] Seq=334 Ack=464 Win=65072
  69 116.348059    172.17.1.1        192.168.3.2             TCP       http > 1048 [ACK] Seq=465 Ack=335 Win=6432 Len=0
  70 116.355070    192.168.3.2       172.17.1.1              TCP       1048 > http [ACK] Seq=335 Ack=465 Win=65072 Len=
  71 119.995999    Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
  72 128.964548    172.17.0.1        255.255.255.255         RIPv1     Response
  73 129.995382    Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
  74 135.035662    Cisco_79:f3:80    CDP/VTP/DTP/PAgP/UDLD   CDP       Device ID: ROUTER_A  Port ID: FastEthernet0/0
  75 139.995357    Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
  76 149.995055    Cisco_79:f3:80    Cisco_79:f3:80          LOOP      Reply
```

b. List the protocols used on the network shown above.

c. Examine the capture below.



No.	Time	Source	Destination	Protocol	Info
76	149.995055	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
77	153.608179	192.168.3.2	172.17.1.1	TCP	1051 > https [SYN] Seq=0 Len=0 MSS=1460
78	153.608206	172.17.1.1	192.168.3.2	TCP	https > 1051 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
79	153.624452	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
80	153.646527	192.168.3.2	172.17.1.1	SSLv2	Client Hello
81	153.646552	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1 Ack=106 Win=5840 Len=0
82	153.679445	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Certificate, Server Key Exchange, Se
83	153.943418	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=106 Ack=1410 Win=64126 Len=
84	156.239770	172.17.0.1	255.255.255.255	RIPv1	Response
85	159.994711	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
86	166.543988	192.168.3.2	172.17.1.1	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted
87	166.574022	172.17.1.1	192.168.3.2	TLSv1	Change Cipher Spec, Encrypted Handshake Message
88	166.660920	192.168.3.2	172.17.1.1	TLSv1	Application Data
89	166.701160	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=1469 Ack=741 Win=7504 Len=0
90	169.994404	Cisco_79:f3:80	Cisco_79:f3:80	LOOP	Reply
91	171.761781	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet [incorrect
92	171.761797	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
93	171.765143	172.17.1.1	192.168.3.2	TLSv1	Ignored Unknown Record
94	172.197946	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=2929 Win=65535 Len=
95	172.408969	192.168.3.2	172.17.1.1	TCP	1051 > https [ACK] Seq=741 Ack=5725 Win=65535 Len=
96	172.421510	192.168.3.2	172.17.1.1	TLSv1	Encrypted Alert
97	172.421522	172.17.1.1	192.168.3.2	TCP	https > 1051 [ACK] Seq=5725 Ack=778 Win=7504 Len=0
98	172.428472	192.168.3.2	172.17.1.1	TCP	1051 > https [RST, ACK] Seq=778 Ack=5725 Win=0 Len
99	172.436417	192.168.3.2	172.17.1.1	TCP	1051 > https [RST] Seq=778 Len=0
100	178.984332	192.168.3.2	172.17.1.1	TCP	1052 > https [SYN] Seq=0 Len=0 MSS=1460
101	178.984356	172.17.1.1	192.168.3.2	TCP	https > 1052 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
102	178.992585	192.168.3.2	172.17.1.1	TCP	1053 > https [SYN] Seq=0 Len=0 MSS=1460
103	178.992610	172.17.1.1	192.168.3.2	TCP	https > 1053 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
104	179.000452	192.168.3.2	172.17.1.1	TCP	1052 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
105	179.024725	192.168.3.2	172.17.1.1	SSL	Client Hello
106	179.024746	172.17.1.1	192.168.3.2	TCP	https > 1052 [ACK] Seq=1 Ack=121 Win=5840 Len=0
107	179.025978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
108	179.031660	192.168.3.2	172.17.1.1	TCP	1053 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
109	179.055932	192.168.3.2	172.17.1.1	SSL	Client Hello
110	179.055945	172.17.1.1	192.168.3.2	TCP	https > 1053 [ACK] Seq=1 Ack=121 Win=5840 Len=0
111	179.056978	172.17.1.1	192.168.3.2	TLSv1	Server Hello, Change Cipher Spec, Encrypted Handsh
112	179.134371	192.168.3.2	172.17.1.1	TLSv1	Change Cipher Spec, Encrypted Handshake Message, A
113	179.135645	172.17.1.1	192.168.3.2	TLSv1	Application Data, [Unreassembled Packet [incorrect

d. What two protocols are listed in this capture that was not listed in the previous capture?

e. Compare the first capture in Step 14 with the second capture. What is one noticeable difference between the HTTP and HTTPS protocols?

Step 15: Reflection

How are the OSI and TCP/IP Layer models reflected in the captured network data provided by Wireshark?

____

____

____

Erasing and Reloading the Switch

For the majority of the labs in CCNA Discovery, it is necessary to start with an unconfigured switch. Using a switch with an existing configuration may produce unpredictable results. The following instructions prepare the switch prior to performing the lab so that previous configuration options do not interfere. Instructions are provided for the 2900 and 2950 series switches.

a. Enter into privileged EXEC mode by typing **enable**. If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

b. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
%Error deleting flash:vlan.dat (No such file or directory)
```

c. Remove the switch startup configuration file from NVRAM.

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

d. Check that VLAN information was deleted.

e. Restart the software using the **`reload`** command.

1) At the privileged EXEC mode, enter the **`reload`** command:

```
Switch# reload
System configuration has been modified. Save? [yes/no]:
```

2) Type **n,** and then press **Enter**.

```
Proceed with reload? [confirm] [Enter]
Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
```

3) Type **n,** and then press **Enter**.

```
Press RETURN to get started! [Enter]
```

Erasing and Reloading the Router

a. Enter the privileged EXEC mode by typing **enable**.

```
Router>enable
```

c. In privileged EXEC mode, enter the **`erase startup-config`** command.

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

d. Press **Enter** to confirm.

```
Erase of nvram: complete
```

e. In privileged EXEC mode, enter the **`reload`** command.

```
Router# reload
System configuration has been modified. Save? [yes/no]:
```

f. Type **n** and then press **Enter**.

```
Proceed with reload? [confirm]
```

g. Press **Enter** to confirm.

```
Reload requested by console.
Would you like to enter the initial configuration dialog? [yes/no]:
```

h. Type **n** and then press **Enter**.

```
Press RETURN to get started!
```

i. Press **Enter**.

SDM Router Basic IOS Configuration to Bring Up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

a. Set the router Fa0/0 IP address.

```
Router(config)#interface Fa0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.248
Router(config-if)#no shutdown
```

f. Enable the router's HTTP/HTTPS server, using the following Cisco IOS commands:

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

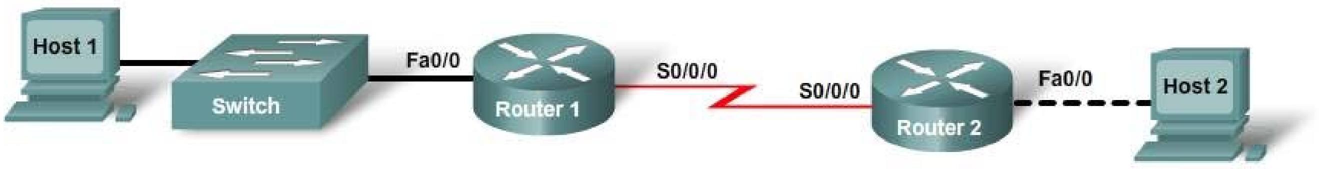
g. Create a user account with privilege level 15 (enable privileges).

```
Router(config)#username <username> privilege 15 password 0 <password>
```

h. Configure SSH and Telnet for local login and privilege level 15.

```
Router(config)#line vty 0 4
Router(config-line)#privilege level 15
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#transport input telnet ssh
Router(config-line)#exit
```

Lab 2.3.5 Configuring Basic Routing and Switching



Device Designation	Host Name / Interface	IP Address Fa0/0	VLAN 1 IP Address	Subnet Mask	IP Address S0/0/0	Subnet Mask	Default Gateway
Router1	R1	192.168.1.1		255.255.255.0	192.168.2.1	255.255.255.0	
Router2	R2	192.168.3.1		255.255.255.0	192.168.2.2	255.255.255.0	
Switch	Switch1		192.168.1.5	255.255.255.0			192.168.1.1
Host1	Host1	192.168.1.10		255.255.255.0			192.168.1.1
Host2	Host2	192.168.3.10		255.255.255.0			192.168.3.1

Objectives

- Configure static routes.
- Configure a routing protocol (RIP v2).
- Configure a switch management VLAN IP address.
- Test and verify configurations.

Background / Preparation

This lab reviews the primary IOS commands used to manage, configure, and monitor devices in a multirouter network. In this lab, you will configure two routers using static routes and then using a routing protocol; configure a switch, including access to management functions; and configure two hosts. You will make and verify configuration changes on the switch. You will also verify network configurations and connectivity.

The following resources are required:

- Cisco 2960 switch or other comparable switch
- Two 1841 or other compatible Cisco routers with Fast Ethernet interfaces to connect to switch and host
- Two Windows-based PCs, at least one with a terminal emulation program
- At least one RJ45-to-DB-9 connector console cable
- Two straight-through Ethernet cables
- One crossover Ethernet cable
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Go to the “Erasing and Reloading the Switch” instructions at the end of this lab. Perform those steps on the switch in this lab assignment before continuing.

NOTE: Go to the “Erasing and Reloading the Router” instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1: Connect PC1 to the switch

a. Connect PC1 to Fast Ethernet switch port Fa0/1. Configure PC1 to use the IP address, mask, and gateway as shown in the topology diagram.

b. Establish a terminal emulation session to the switch from PC1.

Step 2: Perform an initial configuration on the switch

a. Configure the hostname of the switch as Switch1.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname Switch1
```

b. Set the privileged EXEC mode password to **cisco**.

```
Switch1(config)#enable password cisco
```

c. Set the privileged EXEC mode secret password to **class**.

```
Switch1(config)#enable secret class
```

d. Configure the console and virtual terminal lines to use a password and require it at login.

```
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#end
```

e. Exit from the console session and log in again.

Which password was required?

____

Why?

____

____

Step 3: Configure the switch management interface on VLAN 1

a. Enter the interface configuration mode for VLAN 1.

```
Switch1(config)#interface vlan 1
```

b. Set the IP address, subnet mask, and default gateway for the management interface.

```
Switch1(config-if)#ip address 192.168.1.5 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
Switch1(config)#ip default-gateway 192.168.1.1
```

c. Why does interface VLAN1 require an IP address in this LAN?

d. What is the purpose of the default gateway?

Step 4: Verify configuration of the switch

a. Verify that the IP address of the management interface on the switch VLAN 1 and the IP address of PC1 are on the same local network. Use the **`show running-config`** command to check the IP address configuration of the switch.

b. Save the configuration.

Step 5: Perform basic configuration of router R1

a. Connect switch port Fa0/3 to interface Fa0/0 of router R1.

b. Establish a terminal emulation session to router R1 from PC1.

c. Enter privileged EXEC mode, and then global configuration mode.

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#
```

d. Configure the router name as R1.

```
Router(config)#hostname R1
```

e. Disable DNS lookup.

```
R1(config)#no ip domain-lookup
```

Why would DNS lookup be disabled in a lab environment?

f. Configure the EXEC mode password.

```
R1(config)#enable secret class
```

Why is it not necessary to use the **`enable password`** *`password`* command?

g. Configure a message-of-the-day banner using the **`banner motd`** command.

Where does this banner display?

h. Configure the console and virtual terminal lines to use a password and require it at login.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#end
```

Step 6: Configure interfaces and static routing on router R1

a. Configure the FastEthernet 0/0 interface with the IP address 192.168.1.1/24.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

b. Configure the Serial 0/0/0 interface with the IP address 192.168.2.1/24. Set the clock rate to 64000.

```
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
```

c. Return to global configuration mode.

d. Create a static route to enable R1 to reach the network attached to the R2 Fa0/0 interface. Use the next hop interface on R2 as the path to this network.

```
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

Why is this static route the only one required?

____

e. Return to privileged EXEC mode.

f. Save the configuration.

g. Shut down R1.

Step 7: Connect PC2 to router R2

a. Connect PC2 to the Fast Ethernet interface 0/0 of router R2.

What kind of cable is required to connect a host directly to a router Ethernet port?

____

b. Establish a terminal emulation session with router R2 from PC2.

Step 8: Perform basic configuration of router R2

c. Repeat Step 5, a through h, making the hostname R2.

d. Configure the Serial 0/0/0 interface with the IP address 192.168.2.2/24.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 192.168.2.2 255.255.255.0
R2(config-if)#no shutdown
```

e. Configure the FastEthernet 0/0 interface with the IP address 192.168.3.1/24.

```
R2(config-if)#interface fastethernet 0/0
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#no shutdown
```

f. Create a static route to enable R2 to reach the network attached to the R1 Fa0/0 interface. Use the next hop interface on R1 as the path to this network.

```
R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

g. Return to privileged EXEC mode.

h. Save the configuration.

i. Shut down R2.

Step 9: Connect the internetwork

a. Connect R1 and R2 using a serial cable between their configured serial interfaces.

b. Verify that the serial DCE cable is connected to R1 and that the serial DTE cable is connected to R2.

c. Start up both routers, and log in.

Step 10: Verify and test the configurations

a. To verify that PC1 and Switch1 are correctly configured, ping the switch IP address from PC1.

b. To verify that Switch1 and R1 are correctly configured, ping the router Fa0/0 interface (default gateway) IP address from the Switch1 CLI.

c. To verify that PC2 and R2 are correctly configured, ping the router Fa0/0 interface from PC2.

Were the pings successful? __________

If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the host, switch, and router configurations.

d. Verify that the routing tables have routes to all configured networks by using the **`show ip route`** command.

What does the “S” indicate?

____

e. Verify the router interface configurations using the **`show ip interface brief`** command.

What should the output indicate for correctly configured, active interfaces?

____

What should the output indicate for any interface that has not been configured?

____

f. View devices from R1’s terminal session using the **`show cdp neighbors`** command.

If an additional switch is added between PC2 and R2, would that switch appear in this command output? ______ No. Why or why not? ____

CDP only displays directly-connected Cisco devices.

Step 11: Remove Static Route and configure a routing protocol on router R1

a. Remove the static route to 192.168.3.0.

```
R1(config)#no ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

b. Enable RIP v2 routing and advertise the participating networks.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
```

c. Return to privileged EXEC mode.

d. Save the configuration.

Step 12: Remove Static Route and configure a routing protocol on router R2

a. Remove the static route to 192.168.1.0.

```
R2(config)#no ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

b. Enable RIP v2 routing and advertise the participating networks.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
```

c. Return to privileged EXEC mode.

d. Save the configuration.

Step 13: Verify and test the configurations

a. To verify that PC1 and Switch1 are correctly configured, ping the switch IP address from PC1.

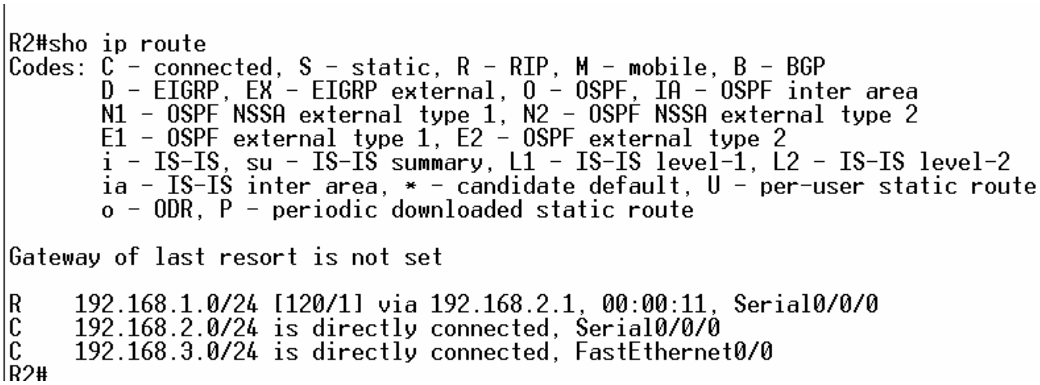
b. To verify that Switch1 and R1 are correctly configured, ping the router Fa0/0 interface (default gateway) IP address from the Switch1 CLI.

c. To verify that PC2 and R2 are correctly configured, ping the router Fa0/0 interface from PC2.

Were the pings successful? _________

If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the host, switch, and router configurations.

d. Verify that the routing tables have routes to all configured networks by using the **`show ip route`** command. R2's routing table should display:



```
R2#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:11, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R2#
```

What does the "R" indicate?

____

On R1, which route would be displayed with an "R"? ______________________

e. Verify the router interface configurations using the **`show ip interface brief`** command.

f. View devices from R1's terminal session using the **`show cdp neighbors`** command.

Step 14: Use the switch management interface

a. Open a command prompt on PC1, and enter the **`telnet`** command followed by the IP address assigned to management interface VLAN 1.

b. Enter the vty password configured in Step 2 to gain access to the switch.

c. At the switch prompt, issue the **`show version`** command.

```
Switch1>show version
```

d. What is the Cisco IOS version of this switch? ___________________

e. Determine which MAC addresses the switch has learned by using the **`show mac-address-table`** command at the privileged EXEC mode prompt.

```
Switch1#show mac-address-table
```

How can you determine the MAC address belonging to PC1?

____

Does PC1's MAC address match one in the switch table? ______

f. To allow the switch port FastEthernet 0/1 to accept only one device, configure port security as follows:

```
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security mac-address sticky
Switch1(config-if)#end
```

g. Check the port security settings.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1            1          1                0         Shutdown
---------------------------------------------------------------------------
```

If a host other than PC1 attempts to connect to Fa0/1, what will happen?

____

It is sometimes necessary to set the speed and duplex of a port to ensure that it operates in a particular mode. You can set the speed and duplex with the **duplex** and **speed** commands while in interface configuration mode. To force FastEthernet port 5 to operate at half duplex and 10 Mbps, issue the following commands:

```
Switch>enable
Switch#configure terminal
Switch(config-if)#interface fastethernet 0/5
Switch(config-if)#speed 10
Switch(config-if)#duplex half
Switch(config-if)#end
Switch#
```

h. Issue the **show interfaces** command. What is the duplex and speed setting for Fa0/5 now?

____

i. Enter **quit** at the switch command prompt to terminate the Telnet session.

Step 15: Reflection

a. Describe a situation in which you would use virtual terminal access to manage a switch, as you did in Step 11.

____

____

b. Which symbol is used to show a successful ping in the Cisco IOS software?___________

c. Which commands used in this lab would provide the best documentation for this network?

____

____

d. This lab gave you an opportunity to review and display your knowledge of configuration commands. If you were asked to state three rules for “best practices” in device configuration, what would they be?

____

____

____

e. Erase and reload all devices.

Erasing and Reloading the Switch

For the majority of the labs in CCNA Discovery, it is necessary to start with an unconfigured switch. Using a switch with an existing configuration may produce unpredictable results. The following instructions prepare the switch prior to performing the lab so that previous configuration options do not interfere. Instructions are provided for the 2900 and 2950 series switches.

b. Enter into privileged EXEC mode by typing **enable**. If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

c. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

d. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

e. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step b using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present, you must power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it, and then plug it back in. If the VLAN information was successfully deleted in Step b, go to Step e and restart the switch using the **reload** command.

f. Restart the software using the **reload** command.

NOTE: This step is not necessary if the switch was restarted using the power cycle method.

1) At the privileged EXEC mode, enter the **reload** command:

```
Switch(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

2) Type **n,** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response is:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt is:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

3) Type **n,** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started! [Enter]
```

Erasing and Reloading the Router

g. Enter the privileged EXEC mode by typing **enable**.

```
Router>enable
```

h. In privileged EXEC mode, enter the **`erase startup-config`** command.

```
Router#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

i. Press **Enter** to confirm.

The response is:

```
Erase of nvram: complete
```

j. In privileged EXEC mode, enter the **`reload`** command.

```
Router(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

k. Type **n** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm]
```

l. Press **Enter** to confirm.

In the first line of the response is:

```
Reload requested by console.
```

After the router has reloaded the line prompt is:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

m. Type **n** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started!
```

n. Press **Enter**.

The router is ready for the assigned lab to be performed.

SDM Router Basic IOS Configuration to Bring Up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

o. Set the router Fa0/0 IP address.

This is the interface that a PC will connect to using a browser to bring up SDM. The PC IP address should be set to 10.10.10.2 255.255.255.248.

NOTE: An SDM router other than the 1841 may require connection to a different port to access SDM.

```
Router(config)#interface Fa0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.248
Router(config-if)#no shutdown
```

p. Enable the router's HTTP/HTTPS server, using the following Cisco IOS commands:

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

q. Create a user account with privilege level 15 (enable privileges).

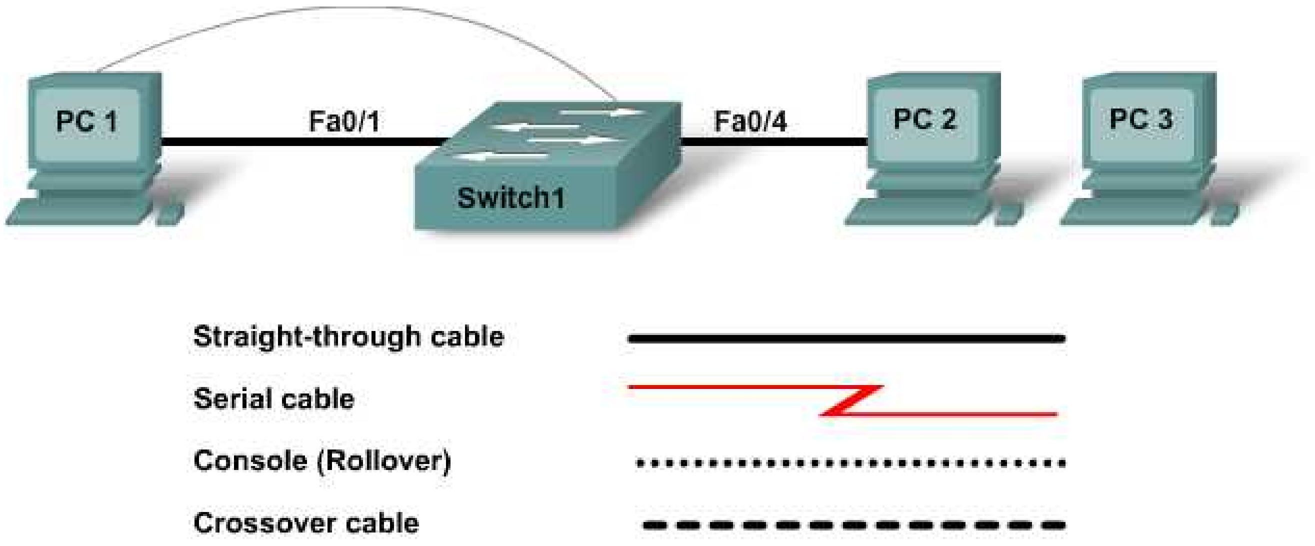
```
Router(config)#username <username> privilege 15 password 0 <password>
```

Replace <`username`> and <`password`> with the username and password that you want to configure.

r. Configure SSH and Telnet for local login and privilege level 15.

```
Router(config)#line vty 0 4
Router(config-line)#privilege level 15
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#transport input telnet ssh
Router(config-line)#exit
```

Lab 3.1.4 Applying Basic Switch Security



Device Designation	IP Address	Subnet Mask	Default Gateway	Enable Secret Password	vty and Console Password
PC 1	192.168.1.3	255.255.255.0	192.168.1.1		
PC 2	192.168.1.4	255.255.255.0	192.168.1.1		
PC 3	192.168.1.5	255.255.255.0	192.168.1.1		
Switch1	192.168.1.2	255.255.255.0	192.168.1.1	class	cisco

Objectives

- Configure passwords to ensure that access to the CLI is secured.
- Configure a switch to remove http server status for security.
- Configure port security.
- Disable unused ports.
- Test security configuration by connecting unspecified hosts to secure ports.

Background / Preparation

Set up a network similar to the one in the topology diagram.

The following resources are required:

- One Cisco 2960 or comparable switch
- Two Windows-based PCs, at least one with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable

- Two straight-through Ethernet cables (PC1 and PC2 to switch)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that the switch has been erased and has no startup configurations. Instructions for erasing both switches and routers are provided in the Lab Manual, located on Academy Connection in the Tools section.

Step 1: Connect PC1 to the switch

a. Connect PC1 to Fast Ethernet switch port Fa0/1. Configure PC1 to use the IP address, mask, and gateway shown in the table.

b. Establish a terminal emulation session to the switch from PC1.

Step 2: Connect PC2 to the switch

a. Connect PC2 to Fast Ethernet switch port Fa0/4.

b. Configure PC2 to use the IP address, mask, and gateway shown in the table.

Step 3: Configure PC3 but do not connect

A third host is needed for this lab.

a. Configure PC3 using IP address 192.168.1.5. The subnet mask is 255.255.255.0, and the default gateway is 192.168.1.1.

b. Do not connect this PC to the switch yet. It will be used for testing security.

Step 4: Perform an initial configuration on the switch

a. Configure the hostname of the switch as **Switch1**.

```
Switch>enable
Switch#config terminal
Switch(config)#hostname Switch1
```

b. Set the privileged EXEC mode password to **cisco**.

```
Switch1(config)#enable password cisco
```

c. Set the privileged EXEC mode secret password to **class**.

```
Switch1(config)#enable secret class
```

d. Configure the console and virtual terminal lines to use a password and require it at login.

```
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#end
```

e. Exit from the console session and log in again.

Which password was required to enter privileged EXEC mode? ______________________________

Why? ____

Step 5: Configure the switch management interface on VLAN 1

a. Enter the interface configuration mode for VLAN 1.

```
Switch1(config)#interface vlan 1
```

b. Set the IP address, subnet mask, and default gateway for the management interface.

```
Switch1(config-if)#ip address 192.168.1.2 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
Switch1(config)#ip default-gateway 192.168.1.1
Switch1(config)#end
```

Why does interface VLAN 1 require an IP address in this LAN?

____

What is the purpose of the default gateway?

____

Step 6: Verify the management LANs settings

a. Verify that the IP address of the management interface on the switch VLAN 1 and the IP address of PC1 and PC2 are on the same local network. Use the **show running-config** command to check the IP address configuration of the switch.

b. Verify the interface settings on VLAN 1.

```
Switch1#show interface vlan 1
```

What is the bandwidth on this interface? ____

What are the VLAN states?

VLAN 1 is __________ and line protocol is __________.

Step 7: Disable the switch from being an http server

Turn off the feature of the switch being used as an http server.

```
Switch1(config)#no ip http server
```

Step 8: Verify connectivity

a. To verify that hosts and switch are correctly configured, ping the switch IP address from the hosts.

Were the pings successful? ___________________________

If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the host and switch configurations.

b. Save the configuration.

Step 9: Record the host MAC addresses

Determine and record the Layer 2 addresses of the PC network interface cards. From the command prompt of each PC, enter **ipconfig /all**.

PC1 ____

PC2 ____

PC3 ____

Step 10: Determine what MAC addresses the switch has learned

Determine what MAC addresses the switch has learned by using the **show mac-address-table** command at the privileged EXEC mode prompt.

```
Switch1#show mac-address-table
```

How many dynamic addresses are there? _____________

How many total MAC addresses are there? ____________

Do the MAC addresses match the host MAC addresses? ____________

Step 11: View the show mac-address-table options

View the options that the **show mac-address-table** command has available.

```
Switch1(config)#show mac-address-table ?
```

What options are available? ____

____

Step 12: Set up a static MAC address

Set up a static MAC address on FastEthernet interface 0/4. Use the address that was recorded for PC2 in Step 9. The MAC address 00e0.2917.1884 is used in this example statement only.

```
Switch1(config)#mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Step 13: Verify the results

a. Verify the MAC address table entries.

```
Switch1#show mac-address-table
```

How many dynamic MAC addresses are there now? __________

How many static MAC addresses are there now? _____________

b. Remove the static entry from the MAC Address Table.

```
Switch1(config)#no mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Step 14: List port security options

a. Determine the options for setting port security on interface FastEthernet 0/4.

```
Switch1(config)#interface fastethernet 0/4
Switch1(config-if)#switchport port-security ?
```

What are some available options? ____

b. To allow the switch port FastEthernet 0/4 to accept only one device, configure port security.

```
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security mac-address sticky
```

c. Exit configuration mode and check the port security settings.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/4        1            0                0           Shutdown
---------------------------------------------------------------------------
```

If a host other than PC2 attempts to connect to Fa0/4, what will happen?

____

Step 15: Limit the number of hosts per port

a. On interface FastEthernet 0/4, set the port security maximum MAC count to 1.

```
Switch1(config-if)#switchport port-security maximum 1.
```

b. Disconnect the PC attached to FastEthernet 0/4. Connect PC3 to FastEthernet 0/4. PC3 has been given the IP address of 192.168.1.5 and has not yet been attached to the switch. It may be necessary to ping the switch address 192.168.1.2 to generate some traffic.

Record any observations. ____

____

Step 16: Configure the port to shut down if there is a security violation

a. In the event of a security violation, the interface should be shut down. To make the port security shut down, enter the following command:

```
Switch1(config-if)#switchport port-security violation shutdown
```

What other action options are available with port security? _____________________________

____

b. If necessary, ping the switch address 192.168.1.2 from the PC3 192.168.1.5. This PC is now connected to interface FastEthernet 0/4. This ensures that there is traffic from the PC to the switch.

c. Record any observations.

____

____

d. Check the port security settings.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/4        1             1                0           Shutdown
---------------------------------------------------------------------------
```

Step 17: Show port 0/4 configuration information

To see the configuration information for FastEthernet port 0/4 only, enter **show interface fastethernet 0/4** at the privileged EXEC mode prompt.

```
Switch1#show interface fastethernet 0/4
```

What is the state of this interface?

FastEthernet0/4 is __________ and line protocol is __________.

Step 18: Reactivate the port

a. If a security violation occurs and the port is shut down, use the **shutdown** / **no shutdown** commands to reactivate the port.

b. Try reactivating this port a few times by switching between the original port 0/4 host and the new one. Plug in the original host, enter the **no shutdown** command on the interface, and ping using the command prompt.

The ping will have to be repeated multiple times; alternately, use the **ping 192.168.1.2 –n 200** command. This command sets the number of ping packets to 200 instead of 4. Then switch hosts and try again.

Step 19: Disable unused ports

Disable any ports not being used on the switch.

```
Switch1(config)#interface range Fa0/5 - 24
Switch1(config-if-range)#shutdown

Switch1(config)#interface range gigabitethernet0/1 - 2
Switch1(config-if-range)#shutdown
```

Step 20: Reflection

a. Why would port security be enabled on a switch? ____

____

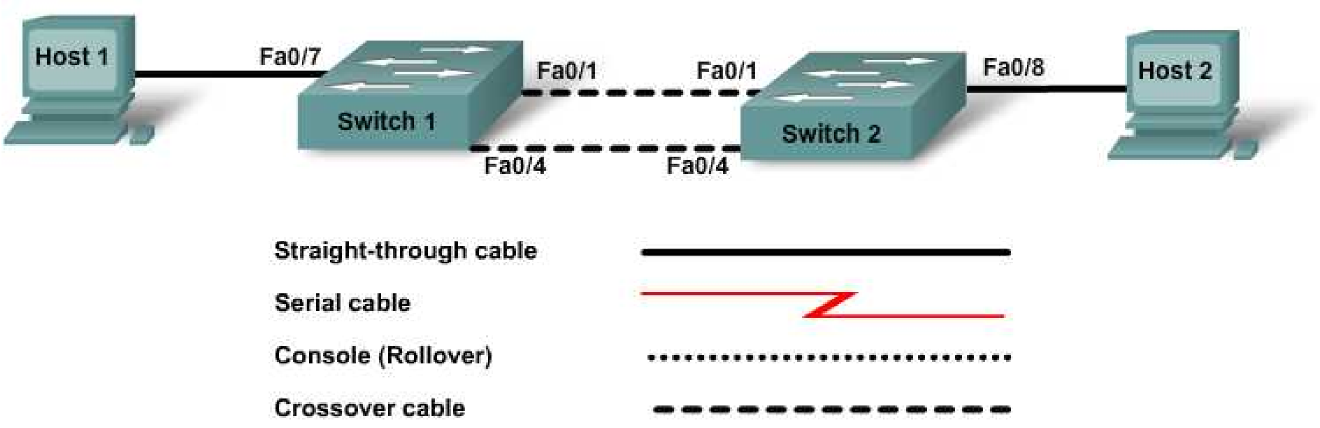
b. Why should unused ports on a switch be disabled? ______________________________________

____

CCNA Discovery

Introducing Routing and Switching in the Enterprise

Lab 3.2.3 Building a Switched Network with Redundant Links



Switch Designation	Switch Name	Enable Secret Password	Enable, Console, and vty Passwords	VLAN 1 IP Address	Subnet Mask	Default Gateway
Switch 1	SwitchA	class	cisco	192.168.1.2	255.255.255.0	N/A
Switch 2	SwitchB	class	cisco	192.168.1.3	255.255.255.0	N/A

Objectives

- Create a switched network with redundant links.
- Determine which switch is selected to be the root bridge with the factory default settings.
- Configure the BID on a switch to control the selection of the root bridge.

Background / Preparation

This lab examines the effect that selection of a root bridge has on traffic patterns in a switched network with redundant links. You will configure the network with default factory settings and then reassign the root bridge by changing the bridge priority value. You will observe the spanning tree as the network adjusts to the changes.

The following resources are required:

- Two Cisco 2960 switches or other comparable switches
- Two Windows-based PCs, one with a terminal emulation program; one as the host, one as the server
- At least one RJ-45-to-DB-9 connector console cable to configure the switches
- Two straight-through Ethernet cables
- Two crossover Ethernet cables
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers - If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Cable the network

a. Connect Host 1 to Switch 1 Fast Ethernet port Fa0/7, using a straight-through Ethernet cable.

b. Connect Host 2 to Switch 2 Fast Ethernet port Fa0/8, using a straight-through Ethernet cable.

c. Connect Switch 1 Fast Ethernet port Fa0/1 to Switch 2 Fast Ethernet port Fa0/1, using a crossover Ethernet cable.

d. Create a redundant link between the switches by connecting Switch 1 Fast Ethernet port Fa0/4 to Switch 2 Fast Ethernet port Fa0/4, using a crossover Ethernet cable.

What typically undesirable traffic pattern have you created by using the two crossover cables between the two switches? ____

Predict: What do you think the switches will do to keep this from becoming a problem?

____

____

Step 2: Configure the switches

a. Establish a terminal emulation session to Switch 1 from Host 1.

b. Configure the switch hostname, passwords, interface VLAN 1 IP address, and subnet mask on Switch 1.

c. Save the configuration.

d. Establish a terminal emulation session to Switch 2 from either Host 1 or Host 2.

e. Configure the switch hostname, passwords, interface VLAN 1 IP address, and subnet mask on Switch 2.

f. Save the configuration.

Step 3: Configure the hosts

a. Configure each host to use an IP address in the same network as the switches.

b. Configure each host to use the same subnet mask as the switches.

Why is no default gateway specified for this network?

____

Step 4: Verify connectivity

a. To verify that the network is set up successfully, ping from Host 1 to Host 2.

Was the ping successful? _____________

b. If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated.

If the ping is not successful, what utility could you use to determine where the connection is failing?

____

Step 5: Examine interface VLAN 1 information

a. From the terminal emulation session on either switch, enter the command **`show interface vlan1 ?`** at the privileged EXEC mode prompt.

```
SwitchA#show interface vlan1 ?
```

List some of the options that are available.

____

b. On SwitchA, enter the command **`show interface vlan1`** at the privileged EXEC mode prompt.

```
SwitchA#show interface vlan1
```

What is the MAC address of the switch? _______________________________________

What other term for MAC address is used? _________

c. On SwitchB, enter the command **`show interface vlan1`** at the privileged EXEC mode prompt.

What is the MAC address of the switch? _______________________________________

Which switch should be the root of the spanning tree for this network? ______________

Step 6: Examine the spanning-tree tables on each switch

a. On SwitchA, enter the command **`show spanning-tree`** at the privileged EXEC mode prompt.

b. On SwitchB, enter the command **`show spanning-tree`** at the privileged EXEC mode prompt.

c. Examine the outputs and answer the following questions:

Which switch is the root bridge? ______________

What is the priority of the root bridge? _____________

What is the bridge ID of the root bridge? _____________________

Which ports are forwarding on the root bridge? ___________________________

Which ports are blocking on the root bridge? _____________________________

What is the priority of the non-root bridge? ______________________________

What is the bridge ID of the non-root bridge? ___________________________

Which ports are forwarding on the non-root bridge? ___________________________________

Which ports are blocking on the non-root bridge? _____________________________________

d. Examine the link lights on both switches.

Can you tell which port is in blocking state? ____

Why is there no change in the link lights? ____

Step 7: Reassign the root bridge

What would you do if you wanted a different switch to be the root bridge for this network?

____

Why might you want to do this?

____

For the purposes of this lab, assume that the switch that is currently the root bridge is undesirable.

The example assumes that SwitchB is preferred as the root switch. To “force” SwitchB to become the new root bridge, you need to configure a new priority for it.

a. Go to the console and enter configuration mode on SwitchB.

b. Determine the options that can be configured for the Spanning Tree Protocol by issuing this command:

```
SwitchB(config)#spanning-tree ?
```

c. List the options that are available: ____

____

d. Set the priority of the switch to 4096.

```
SwitchB(config)#spanning-tree vlan 1 priority 4096
SwitchB(config)#exit
```

Step 8: Look at the spanning-tree table

a. On SwitchA, enter **`show spanning-tree`** at the privileged EXEC mode prompt.

b. On SwitchB, enter **`show spanning-tree`** at the privileged EXEC mode prompt.

c. Examine the outputs and answer the following questions:

Which switch is the root bridge? ____

What is the priority of the root bridge? __________________________________

What is the bridge ID of the root bridge? ____

Which ports are forwarding on the root bridge? ____________________________________

Which ports are blocking on the root bridge? _________________________________

What is the priority of the non-root bridge? ____

What is the bridge ID of the non-root bridge? _______________________________________

Which ports are forwarding on the non-root bridge? _________________________________

Which ports are blocking on the non-root bridge? __________________________________

Step 9: Verify the running configuration file on the root bridge

a. On the switch that was changed to be the root bridge, enter the **`show running-config`** command at the privileged EXEC mode prompt.

b. Locate the spanning-tree priority information for this switch.

c. How can you tell from the information given that this switch is the root bridge?

____

Step 10: Reflection

Suppose that you are adding new switches to a company’s network. Why should you plan the physical design carefully? Why should you be prepared to make adjustments to factory default settings?

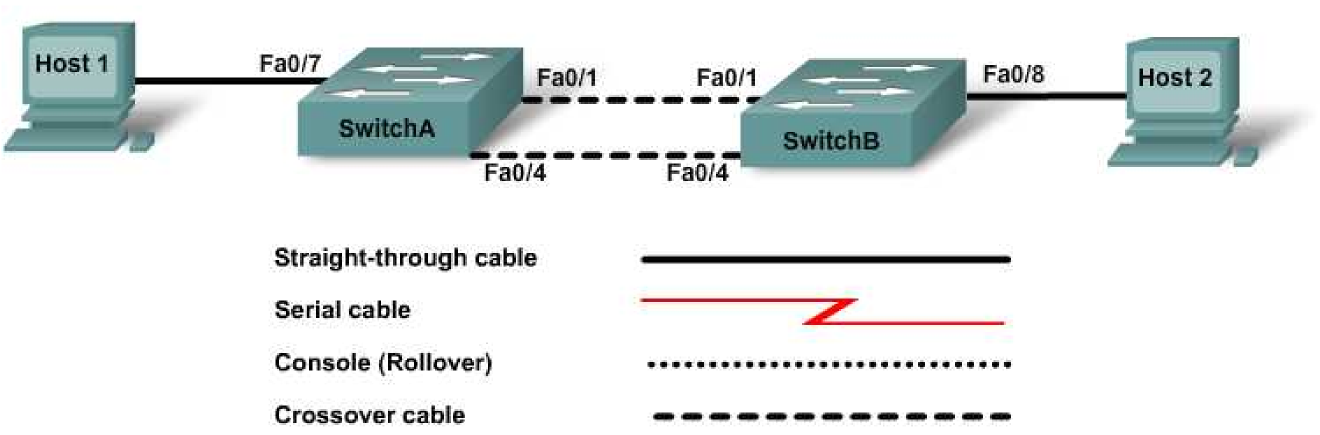
____

____

____

____

Lab 3.2.4 Verifying STP with Show Commands



Switch Designation	Switch Name	Enable Secret Password	Enable, Console, and vty Passwords	VLAN 1 IP Address	Subnet Mask	Default Gateway
Switch 1	SwitchA	class	cisco	192.168.1.2	255.255.255.0	N/A
Switch 2	SwitchB	class	cisco	192.168.1.3	255.255.255.0	N/A

Objectives

- Create a switched network with redundant links.
- Observe how the Spanning Tree Protocol adjusts to changes in the switched network topology.
- Verify the status of a spanning tree.

Background / Preparation

This lab demonstrates advantages and disadvantages of the Spanning Tree Protocol in dealing with changes to a switched network with redundant links. You will configure the network with default factory settings and then examine the spanning-tree tables for the switches before and after a link is removed. You will use various **show** commands to verify the operation of the spanning-tree algorithm.

The following resources are required:

- Two Cisco 2960 switches or other comparable switches
- Two Windows-based PCs, one with a terminal emulation program, one as the host, one as the server
- At least one RJ-45-to-DB-9 connector console cable to configure the switches
- Two straight-through Ethernet cables

- Two crossover Ethernet cables
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers - If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Cable the network

a. Connect Host 1 to Switch 1 Fast Ethernet port Fa0/7, using a straight-through Ethernet cable.

b. Connect Host 2 to Switch 2 Fast Ethernet port Fa0/8, using a straight-through Ethernet cable.

c. Connect Switch 1 Fast Ethernet port Fa0/1 to Switch 2 FastEthernet port Fa0/1, using a crossover Ethernet cable.

d. Create a redundant link between the switches by connecting Switch 1 Fast Ethernet port Fa0/4 to Switch 2 Fast Ethernet port Fa0/4, using a crossover Ethernet cable.

What is the advantage of providing redundant links in a network like this one?

____

____

Step 2: Configure the switches

a. Establish a terminal emulation session to Switch 1 from Host 1.

b. Configure the switch hostname, passwords, interface VLAN 1 IP address, and subnet mask on Switch 1.

c. Save the configuration.

d. Establish a terminal emulation session to Switch 2 from either Host 1 or Host 2.

e. Configure the switch hostname, passwords, interface VLAN 1 IP address, and subnet mask on Switch 2.

f. Save the configuration.

Step 3: Configure the hosts

a. Configure each host to use an IP address in the same network as the switches.

b. Configure each host to use the same subnet mask as the switches.

Step 4: Verify connectivity

a. To verify that the network is set up successfully, ping from Host 1 to Host 2.

Was the ping successful? _____________

b. If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated.

Step 5: Examine interface VLAN 1 information

a. On SwitchA, enter the command **`show interface vlan1`** at the privileged EXEC mode prompt.

What is the MAC address of SwitchA? ____

b. On SwitchB, enter the command **`show interface vlan1`** at the privileged EXEC mode prompt.

What is the MAC address of SwitchB? ____

Which switch should be the root of the spanning tree for this network?

____

Step 6: Determine the roles of ports participating in the spanning tree on each switch

a. On SwitchA, enter the command **`show spanning-tree`** at the privileged EXEC mode prompt.

b. On SwitchB, enter the command **`show spanning-tree`** at the privileged EXEC mode prompt.

Which switch is the root bridge? ____

c. The spanning tree is using three ports on each switch. Complete this chart indicating the port state and role for each port.

SwitchA		
Interface	**Role**	**State**
SwitchB		
Interface	**Role**	**State**

Step 7: Create a change in the network topology

a. Remove the crossover cable from the forwarding port on the non-root bridge.

b. Wait a few seconds, and then enter the **`show spanning-tree`** command again on the non-root bridge.

What changes do you see in the spanning tree?

____

c. Check the spanning tree on the root bridge.

What changes have occurred there?

____

d. Continue to check the spanning tree on both switches until a new tree has been calculated and all ports are either forwarding or blocking.

How long does it take for this to happen?

____

e. Replace the cable that was removed in Step 7a.

f. Wait again until both switches have recalculated their tables.

How much time has passed since you first removed the crossover cable?

____

What effect did these topology changes have on network uptime?

____

Step 8: Examine the spanning tree on each switch

a. On each switch, enter the command **`show spanning-tree detail`**.

b. Examine the information for port Fa0/1. The output shows the interface, role, and state for each switch. It also provides details about port activity and characteristics.

   How might the following information help you to verify the status of the network and troubleshoot network problems?

   1) Number of transitions to forwarding state:

   ____

   ____

   2) Number of BPDUs that have been sent and received:

   ____

   ____

c. On each switch, enter the following commands. Determine the type of information that each command provides:

   `show spanning-tree bridge`

   ____

   ____

   `show spanning-tree summary`

   ____

   ____

Step 9: Reflection

Your networking team is deciding whether to disable Spanning Tree Protocol on the switches in your corporate network. Explain how you would feel about this decision. What are the advantages and disadvantages? How would this decision affect your network design?

____

____

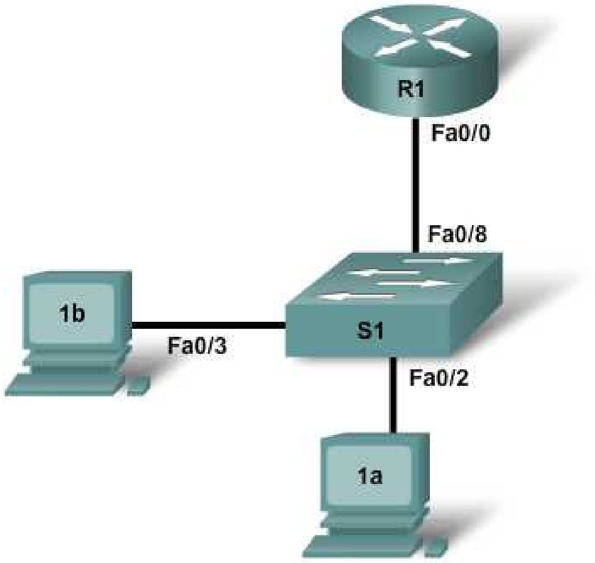
____

____

____

____

Lab 3.3.2 Configuring, Verifying, and Troubleshooting VLANs



Device	Host Name / Interface	Fa0/0 or NIC Address	VLAN 1 address
Router 1	R1	172.16.1.1/24	n/a
Switch 1	S1	n/a	172.16.1.2/24
Host 1a	n/a	172.16.1.10/24	n/a
Host 1b	n/a	172.16.1.11/24	n/a

Objectives

- Observe default switch VLAN configuration and operation.
- Configure static VLANs on a switch.
- Verify VLAN configuration and operation.
- Modify an existing VLAN configuration.

Background / Preparation

This lab focuses on the basic VLAN configuration of the Cisco 2960 switch (or similar) using Cisco IOS commands. The information in this lab applies to other switches; however, command syntax may vary. Depending upon the switch model, the interface designations may differ. For example, modular switches have multiple slots; therefore, the Fast Ethernet ports may be FastEthernet 0/1 or FastEthernet 1/1, depending on the slot and port. The router used can be any router.

The following resources are required:

- One Cisco 2960 switch or equivalent switch
- One Cisco 1841 router or equivalent
- Two Windows-based PCs with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the switch and the router
- Three straight-through Ethernet cables to connect from the PCs to Switch 1

NOTE: Make sure that the router and all the switches have been erased and have no startup configurations. For detailed instructions, refer to the Lab Manual that is located on Academy Connection in the Tools section.

NOTE: SDM Routers – If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the router Fa0/0 interface with a straight-through cable to Switch 1 Fa0/8 interface.

b. Connect the Host 1a Ethernet interface with a straight-through cable to Switch 1 Fa0/2 interface.

c. Connect the Host 1b Ethernet interface with a straight-through cable to Switch 1 Fa0/3 interface.

d. Connect a PC with a console cable to perform configurations on the router and switches.

e. Configure IP addresses on the hosts as shown in the chart.

Step 2: Perform basic configuration on the router

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. Configure Router 1 with a hostname and console, Telnet, and privileged passwords according to the table diagram.

Step 3: Configure Switch 1

a. Configure S1 hostname and passwords.

b. Configure Switch 1 with a hostname and console, Telnet, and privileged passwords according to the addressing table.

c. Configure S1 with an IP address and default gateway.

```
S1(config)#interface vlan1
S1(config-if)#ip address 172.16.1.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 172.16.1.1
S1(config)#end
```

Step 4: Verify connectivity and default VLAN configuration

a. Verify LAN connectivity by pinging from the router to the switch and the hosts. Also verify that you can ping from host to host.

b. Verify default VLAN configuration with the **`show vlan`** command on S1.

```
S1#show vlan
```

Are all switch ports assigned to VLAN 1? __________

Step 5: Configure VLANs on S1

a. Create and name two additional VLANs on S1.

```
S1(config)#vlan 20
S1(config-vlan)#name fred
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name wilma
S1(config-vlan)#exit
```

b. Verify the creation of the new VLANs with the **`show vlan`** command.

```
S1#show vlan
```

Do the new VLANs appear in the output? ___________

What interfaces belong to the new VLANs? __________

c. Assign interfaces to VLANs. Assign S1 port Fa0/2 to VLAN 20 and ports Fa0/3 – Fa0/8 to VLAN 30.

```
S1(config)#int Fa0/2
S1(config-if)#switchport access vlan 20
S1(config-if)#exit
S1(config-)#interface range Fa0/3 - 8
S1(config-if-range)#switchport access vlan 30
S1(config-if-range)#end
S1#show running-config
```

Observe that the **`switchport access`** command was applied to ports Fa0/2 – Fa0/8.

d. Verify the port assignments of the new VLANs with the **`show vlan`** command.

```
S1#show vlan
```

Which interfaces now belong to VLAN 1? ____________________

Which interfaces belong to VLAN 20? _______________________

Which interfaces belong to VLAN 30? _______________________

e. Other commands can be used to show different amounts of information or specific pieces of information. Enter the following commands on S1 and observe the output:

```
S1#show vlan brief
```

Is all of the basic VLAN membership information shown? __________

```
S1#show vlan id 30
```

What information is shown? ____________________

```
S1#show vlan name fred
```

What information is shown? ____________________

Step 6: Verify VLAN segmentation

In the previous step, the ports connected to R1 and Host 1b were placed in one VLAN and Host 1a was placed in another. Even though these hosts are connected to one switch, it appears as if there are two separate switches. Connectivity tests will prove this.

a. Ping from Host 1b to R1.

Were the pings successful? __________

b. Ping from Host 1b to Host 1a.

Were the pings successful? __________

c. Ping from Host 1b to R1.

Were the pings successful? __________

Why were some pings successful and others not?

____

How could Host 1b communicate with Host 1a in different VLAN?

____

Step 7: Change and delete VLAN configurations

a. Reassign S1 port Fa0/3 to VLAN 20.

```
S1(config)#interface Fa0/3
S1(config-if)#switchport access vlan 20
S1(config)#end
S1#show vlan
```

Does the output reflect the VLAN membership change? __________

b. Remove VLAN 30.

Which two commands would be used to delete all VLAN configuration and return to the default configuration?

____

Step 8: Reflection

a. Why would VLANs be configured in a network?

____

____

____

____

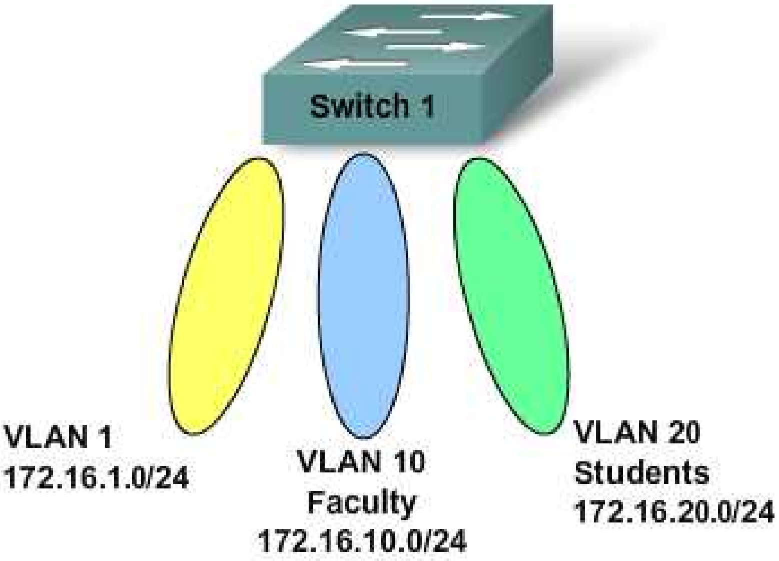
b. What must be set up to communicate between VLANS?

____

c. With no configuration, what VLAN are all ports a member of?

____

Lab 3.4.1 Creating VLANs and Assigning Ports



Device	Host Name	VLAN 10	VLAN 20	VLAN 1	VLAN 1 IP Address
Switch 1	Switch 1	Fa0/5 – Fa0/6	Fa0/7 – Fa0/8	All Remaining Ports	172.16.1.2/24

Objectives

- Configure three VLANs on a switch.
- Verify connectivity.

Background / Preparation

This lab focuses on the basic VLAN configuration of the Cisco 2960 switch (or similar) using Cisco IOS commands. The information in this lab applies to other switches; however, command syntax may vary. Depending upon the switch model, the interface designations may differ. For example, modular switches have multiple slots; therefore, the Fast Ethernet ports may be Fast Ethernet 0/1 or Fast Ethernet 1/1, depending on the slot and port.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Three Windows-based PCs with a terminal emulation program
- One RJ-45-to-DB-9 connector console cable to configure the switch
- Three straight-through Ethernet cables to connect from the PCs to Switch 1

NOTE: Make sure that the switch has been erased and has no startup configurations. Instructions for erasing the switch are provided in the Lab Manual, located on Academy Connection in the Tools section.

Step 1: Connect the equipment

a. Connect PC1 to the switch with a console cable.

b. Connect PC1 to switch port Fast Ethernet 0/4 with a straight-through Ethernet cable.

c. Connect PC2 to switch port Fast Ethernet 0/5 with a straight-through Ethernet cable.

d. Connect PC3 to switch port Fast Ethernet 0/7 with a straight-through Ethernet cable.

Step 2: Perform basic PC configuration

Use this table to configure addressing on the PCs.

Computer	IP Address	Subnet Mask	Default Gateway
PC 1	172.16.1.3	255.255.255.0	172.16.1.1
PC 2	172.16.10.3	255.255.255.0	172.16.10.1
PC 3	172.16.20.3	255.255.255.0	172.16.20.1

Step 3: Configure Switch 1

a. Configure Switch 1 with a hostname and console, Telnet, and privileged passwords.

b. Configure Switch 1 with the VLAN 1 IP address of 172.16.1.2/24.

```
Switch1(config)#interface vlan1
Switch1(config-if)#ip address 172.16.1.2 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
```

c. Create VLAN 10, named **Faculty**, and VLAN 20, named **Students**.

```
Switch1(config)#vlan 10
Switch1(config-vlan)#name Faculty
Switch1(config-vlan)#exit
Switch1(config)#vlan 20
Switch1(config-vlan)#name Students
Switch1(config-vlan)#exit
```

d. Configure Switch 1 with the default gateway address of 172.16.1.1.

```
Switch1(config)#ip default-gateway 172.16.1.1
```

e. Configure Switch 1 to place interfaces Fa0/5 and Fa0/6 in VLAN 10.

```
Switch1(config)#interface Fa0/5
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#interface Fa0/6
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#exit
```

f. Configure Switch 1 to place interfaces Fa0/7 and Fa0/8 in VLAN 20.

```
Switch1(config)#interface Fa0/7
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#interface Fa0/8
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#end
Switch1#
```

g. Save the configuration.

```
Switch1#copy running-config startup-config
```

h. By default, there is only a single VLAN for all ports. You cannot rename or delete VLAN 1. Therefore, no further configuration is necessary to assign the rest of the ports to VLAN 1. To prove this, issue the command **`show vlan brief`**.

Are all other switch ports in VLAN 1? _______

Which switch ports are in VLAN 10? ___________________

Which switch ports are in VLAN 20? ___________________

i. Issue the command **`show vlan`**.

What difference is noticed between the two commands **`show vlan brief`** and **`show vlan`**?
____

____

Step 4: Verify connectivity

a. Ping from each PC to Switch1 address of 172.16.1.2.

Are PC1 pings successful? __________

Are PC2 pings successful? __________

Are PC3 pings successful? __________

b. Ping from PC1 to PC2 and PC3.

Can PC1 ping PC2? _________

Can PC1 ping PC3? _________

Step 5: Reflection

a. Why can PC1 ping Switch1 when PC2 and PC3 cannot?

____

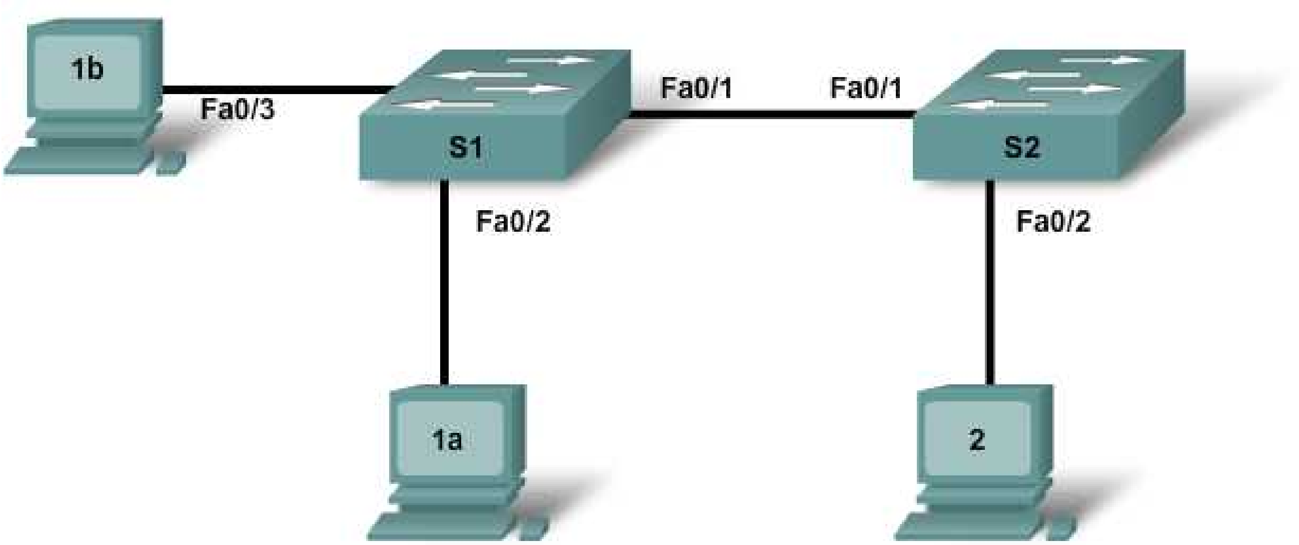
____

b. The PCs cannot ping each other. Why?

____

____

Lab 3.4.2 Configuring a Trunk Port to Connect Switches



Device	Host Name / Interface	Fa0/0 or NIC Address	VLAN1 address
Switch 1	S1	n/a	172.16.1.1/24
Switch 2	S2	n/a	172.16.1.2/24
Host 1a	n/a	172.16.1.10/24	n/a
Host 1b	n/a	172.16.1.11/24	n/a
Host 2	n/a	172.16.1.12/24	n/a

Objectives

- Observe default switch VLAN configuration and operation.
- Configure static VLANs on a switch.
- Verify VLAN configuration and operation.
- Configure trunking between switches.

Background / Preparation

This lab focuses on the basic VLAN configuration of the Cisco 2960 switch (or similar) using Cisco IOS commands. The information in this lab applies to other switches; however, command syntax may vary. Depending upon the switch model, the interface designations may differ. For example, modular switches have multiple slots; therefore, the Fast Ethernet ports may be Fast Ethernet 0/1 or Fast Ethernet 1/1, depending on the slot and port.

The following resources are required:

- Two Cisco 2960 switches or equivalent switches
- Two Windows-based PCs with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the switch and the router
- Three straight-through Ethernet cables to connect from the PCs to the switches
- One crossover Ethernet cable to connect S1 to S2

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

Step 1: Connect the equipment

a. Connect Switch 1 Fa0/1 interface to Switch 2 Fa0/1 interface with a crossover cable.

b. Connect Host 1a Ethernet interface with a straight-through cable to Switch 1 Fa0/2 interface.

c. Connect Host 1b Ethernet interface with a straight-through cable to Switch 1 Fa0/3 interface.

d. Connect Host 2 Ethernet interface with a straight-through cable to Switch 2 Fa0/2 interface.

e. Connect a PC with a console cable to perform configurations on the router and switches.

f. Configure IP addresses on the hosts as shown in the chart.

Step 2: Perform basic configuration of Switch 1 and Switch 2

a. Connect a PC to the console port of the switches to perform configurations using a terminal emulation program.

b. Configure Switch 1 with a hostname and console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

c. Configure Switch 2 with a hostname and console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 3: Configure host PCs

Configure the host PCs according to the information in the table and diagram.

Step 4: Verify default VLAN configuration and connectivity

a. When directly connecting some switches, as in this lab, the switch ports automatically configure themselves for trunking. To prevent this, manually configure the switch ports for normal operation on S1 and S2.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode access
S2(config)#interface fa0/1
S2(config-if)#switchport mode access
```

b. Verify default VLAN configurations on both switches with the **show vlan** command.

```
S1#show vlan
S2#show vlan
```

Is every switch port assigned to a VLAN? ____________

Which VLAN do the ports appear in? ____________

Should any host or switch be able to ping any other host or switch at this time? ____________

c. Verify this by pinging from Host 1a to all the other hosts and switches.

Are all the pings successful? ____________

Step 5: Create and verify VLAN configuration

a. Create and name VLANs 2 and 3 on both switches.

```
S1(config)#vlan 2
S1(config-vlan)#name fred
S1(config-vlan)#exit
S1(config)#vlan 3
S1(config-vlan)#name wilma
S1(config-vlan)#exit


S2(config)#vlan 2
S2(config-vlan)#name fred
S2(config-vlan)#exit
S2(config)#vlan 3
S2(config-vlan)#name wilma
S2(config-vlan)#exit
```

b. Assign switch ports to VLANs. The ports connecting Hosts 1a and 2 will be assigned to VLAN 2 and the port connecting Host 1b will be assigned to VLAN 3. Save the configurations.

```
S1(config)#int fa0/2
S1(config-if)#switchport access vlan 2
S1(config-if)#exit
S1(config)#interface fa0/3
S1(config-if)#switchport access vlan 3
S1(config-if)#end
S1#copy running-config startup-config

S2(config)#int fa0/2
S2(config-if)#switchport access vlan 2
S2(config-if)#end
S2#copy running-config startup-config
```

c. Test connectivity between devices.

1) Ping from S1 to S2.

Are the pings successful? ____________

To what VLAN do the management interfaces of S1 and S2 belong? ____________

2) Ping from Host 1a to Host 2.

Are the pings successful? ____________

To what VLAN do Hosts 1a and 2 belong?

____

To what VLAN do the Fa0/1 interfaces of the switches belong? ____________

If Hosts 1a and 2 belong to the same VLAN, why can't they ping each other?

____

3) Ping from host 1a to S1.

Are the pings successful? ____________

Why can't Host 1a ping S1?

____

Step 6: Configure and verify trunking

To allow connectivity within multiple VLANs across multiple switches, trunking can be configured. Without trunking, each VLAN requires a separate physical connection between switches.

a. Configure trunking on S1 and S2. Port Fa0/1 on S1 is already connected to port Fa0/1 on S2.

```
S1(config)#int Fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#end

S2(config)#int Fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#end
```

b. Verify the creation of the trunk with the **show interfaces trunk** command.

```
S1#show interfaces trunk

S2#show interfaces trunk
```

Do the trunk interfaces appear in the output? _______________

What VLAN is set as the native VLAN? _______________

What VLANs are allowed to communicate over the trunk? _______________

c. View the VLAN configuration on both switches with the **show vlan** command.

```
S1#show vlan

S2#show vlan
```

Do the S1 and S2 Fa0/1 interfaces appear in a VLAN? Why or why not?

____

d. Retest the connectivity between devices.

   1) Ping from S1 to S2.

      Are the pings successful? ____________

   2) Ping from Host 1a to Host 2.

      Are the pings successful? ____________

   3) Ping from Host 1b to Host 2.

      Are the pings successful? ____________

   4) Ping from Host 1a to S1.

      Are the pings successful? ____________

e. The ping test should show that devices that belong to the same VLAN can now communicate with each other across switches, but devices in different VLANs cannot communicate with each other.

   What would have to be configured to allow devices in different VLANs to communicate with each other?

   ____

Step 7: Observe the default trunking behavior of switches

a. Previously in this lab, the Fa0/1 interfaces on the switches were manually configured for trunking. Remove that configuration with the **no switchport mode trunk** command.

```
S1(config)#int Fa0/1
S1(config-if)#no switchport mode trunk
S1(config-if)#end

S2(config)#int Fa0/1
S2(config-if)#no switchport mode trunk
S2(config-if)#end
```

b. View the trunking status of the switch ports.

```
S1#show interfaces trunk

S2#show interface trunk
```

   Are Fa0/1 on S1 and S2 in trunking mode?

   ____

   What trunking mode did they default to?

   ____

   What trunking encapsulation did they default to?

   ____

Step 8: Reflection

a. Why would trunking be configured in a network?

____

____

____

____

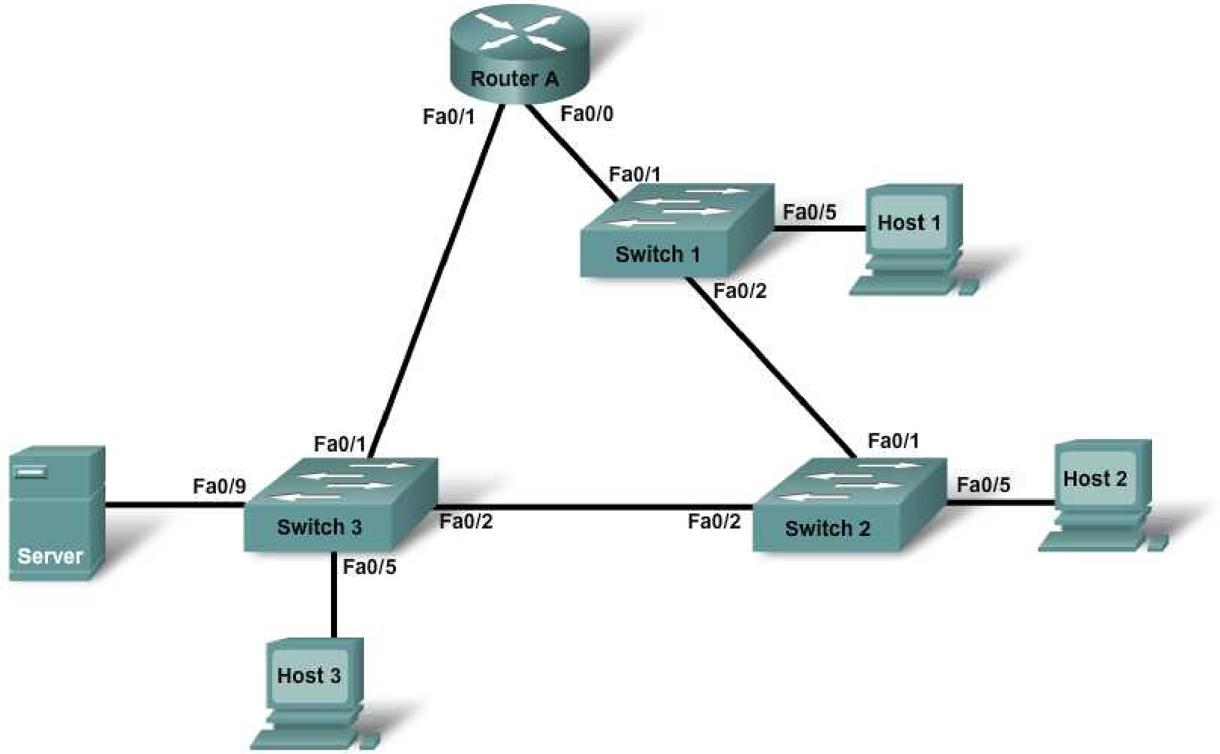
b. Does trunking allow for communication between VLANS?

____

c. With no configuration, from which VLAN are frames forwarded across the trunk without VLAN tagging added?

____

Lab 3.4.3 Part A: Configuring Inter-VLAN Routing



Device	FastEthernet 0/0	FastEthernet 0/1	IP Address	Default Gateway	Enable Secret Password	Enable, vty, and Console Passwords
Router A	192.168.12.1	192.168.13.1			cisco	class
Switch 1			192.168.12.2	192.168.12.1	cisco	class
Switch 2			192.168.12.3	192.168.12.1	cisco	class
Switch 3			192.168.13.2	192.168.13.1	cisco	class
Host 1			192.168.12.4	192.168.12.1		
Host 2			192.168.12.5	192.168.12.1		
Host 3			192.168.12.6	192.168.12.1		
Server			192.168.13.3	192.168.13.1		

Objectives

- Configure a router for inter-VLAN communication.
- Verify connectivity between VLANs.

Background / Preparation

This is a two part lab: Part A configures inter-VLAN routing using separate router interfaces for each VLAN. Part B configures inter-VLAN routing using subinterfaces. It is important to complete both Part A and Part B of the lab.

This lab focuses on the basic configuration of the Cisco 1841 router or a comparable router using Cisco IOS commands. Part A of this lab shows how two different VLANs communicate through a router using separate Fast Ethernet interfaces for each VLAN. This is not a recommended practice, because this topology does not scale well. Trunking requires fewer router and switch ports, which will be shown in Part B of this lab. The information in this lab applies to other routers; however, command syntax may vary.

The following resources are required:

- Three Cisco 2960 switches or other comparable switch
- One router with 2 Ethernet interfaces to connect to switches
- Four Windows-based PCs, one with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the router and switches
- Two straight-through Ethernet cables to connect from the router to Switch 1 and Switch 3
- Four straight-through Ethernet cables to connect the hosts and server to the switches
- Two crossover Ethernet cables to connect Switch 1 to Switch 2 and Switch 2 to Switch 3

NOTE: Make sure the router and all the switches have been erased and have no startup configurations. For instructions, refer to the end of this lab. Instructions are provided for both the switch and router.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Router A Fa0/0 interface with a straight-through cable to the Fa0/1 interface on Switch 1.

b. Connect the Switch 1 Fa0/2 port to the Switch 2 Fa0/1 switch port using a crossover cable.

c. Connect the Fa0/2 port of Switch 2 to the Fa0/2 port of Switch 3 using a crossover cable.

d. Use a straight-through cable to connect the Fa0/1 port of Switch 3 to the Fa0/1 interface of Router A Fa0/1 port.

e. Connect a PC with a console cable to perform configurations on the router and switches.

f. Connect the remaining PCs as shown in the diagram. Use switchport Fa0/5 on Switches 1, 2, and 3 to connect each PC to each switch. Use Fa0/9 to connect the server to Switch 3.

Step 2: Perform basic configurations on the router

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. Configure Router A with a hostname and console, Telnet, and privileged passwords according to the table and diagram.

Step 3: Configure Fast Ethernet connections for each VLAN on the router

a. Configure Router A Fa0/0 interface to be on the same network as VLAN 12.

```
RouterA(config)#interface fa0/0
RouterA(config-if)#ip address 192.168.12.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
```

b. Configure Router A Fa0/1 interface to be on the same network as VLAN 13.

```
RouterA(config)#interface fa0/1
RouterA(config-if)#ip address 192.168.13.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
```

Step 4: Configure Switch 1

a. Configure Switch 1 with a hostname and console, Telnet and privileged passwords according to the table and diagram.

b. Configure Switch 1 with the VLAN 1 IP address of 192.168.12.2/24 and a default gateway of 192.168.12.1. Assigning an IP address to the switch allows for remote configuration.

Step 5: Configure Switch 2

a. Configure Switch 2 with a hostname and console, Telnet, and privileged passwords according to the table and diagram.

b. Configure Switch 2 with the VLAN 1 IP address of 192.168.12.3/24 and a default gateway of 192.168.12.1.

Step 6: Configure Switch 3

a. Configure Switch 3 with a hostname and console, Telnet, and privileged passwords according to the table and diagram.

b. Configure Switch 3 with the VLAN 1 IP address of 192.168.13.2/24 and a default gateway of 192.168.13.1.

Step 7: Configure Host 1

Configure Host 1 with an IP address of 192.168.12.4, subnet mask of 255.255.255.0, and a default gateway of 192.168.12.1.

Step 8: Configure Host 2

Configure Host 2 with an IP address of 192.168.12.5, subnet mask of 255.255.255.0, and a default gateway of 192.168.12.1.

Step 9: Configure Host 3

Configure Host 3 with an IP address of 192.168.12.6, subnet mask of 255.255.255.0, and a default gateway of 192.168.12.1.

Step 10: Configure the server

Configure the server with an IP address of 192.168.13.3, subnet mask of 255.255.255.0, and a default gateway of 192.168.13.1.

Step 11: Verify connectivity

The router should be able to ping the interfaces of the other devices.

a. From the router, issue a ping to Host 1.

Is the ping successful? ________

b. From the router, issue a ping to Host 2.

Is the ping successful? ________

c. From the router, issue a ping to Host 3.

Is the ping successful? ________

d. From the router, issue a ping to the server.

Is the ping successful? ________

Host 1 should be able to ping all other devices.

a. From Host 1, ping Host 2.

Is the ping successful? _______________

b. From Host 1, ping the server.

Is the ping successful? ____________

Why can Host 1 ping the server? ____

c. From the server, ping Host 1.

Is the ping successful? __________

If the pings are not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the router and switch configurations.

d. From Switch 3, issue the command **`show spanning-tree.`**

Which ports are being used on Switch 3? _______________________________________

What is the role of each of these ports? ____

Which switch is acting as the root? ____

What is the protocol that allows VLANs to communicate without switching loops?

____

Step 12: Reflection

a. Why does this topology not scale well?

____

____

____

____

b. Why would a VLAN benefit from trunking?

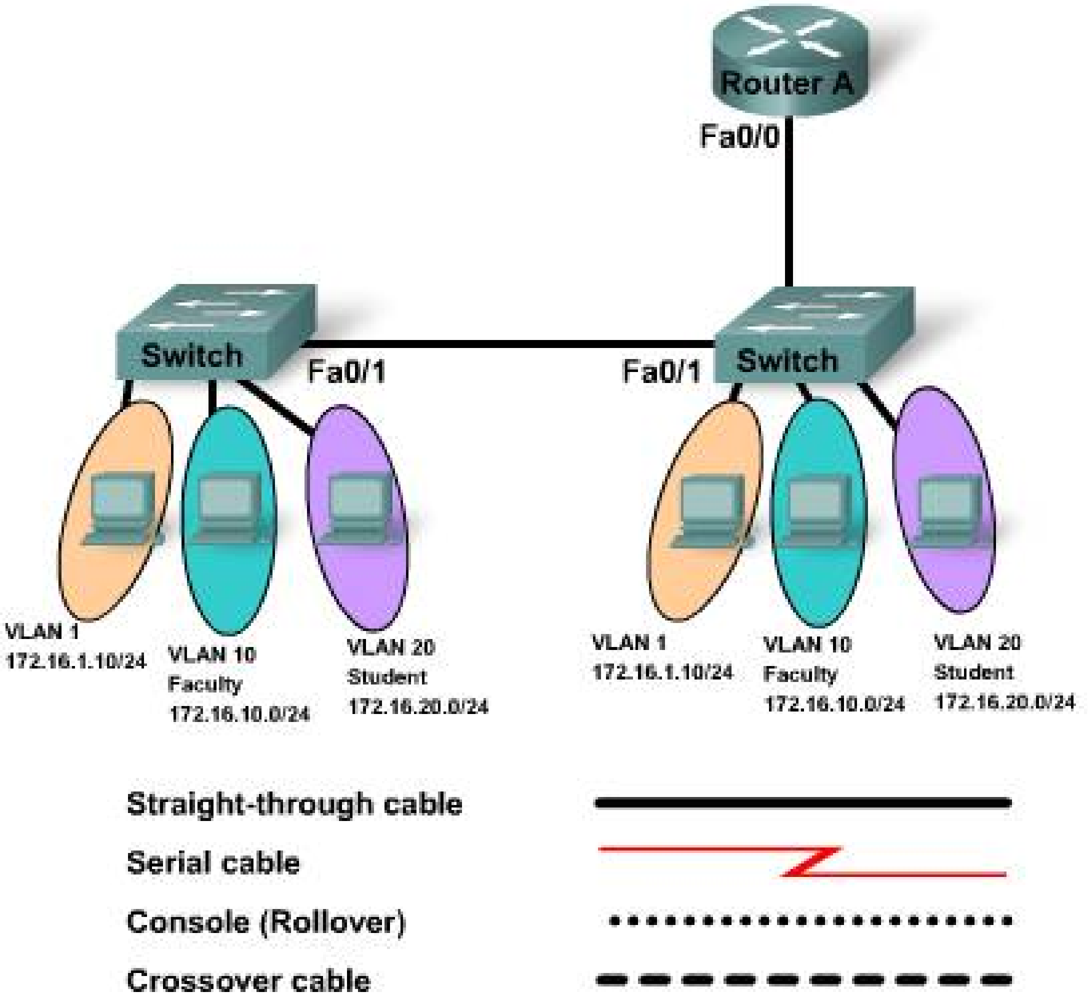
____

____

c. Which device provides connectivity between different VLANs?

____

Lab 3.4.3 Part B: Configuring Inter-VLAN Routing



Device	Host Name / Interface	VLAN 10	VLAN 20	VLAN 1	IP Address	Trunk
Router A	RouterA					Fa0/0
Switch 1	Switch1	Fa0/5 – Fa0/6	Fa0/7 – Fa0/8	All Remaining Ports	172.16.1.2/24	Fa0/1, Fa0/2
Switch 2	Switch2	Fa0/5 – Fa0/6	Fa0/7 – Fa0/8	All Remaining Ports	172.16.1.3/24	Fa0/1
All device passwords: enable=cisco secret=class						

Objectives

- Configure two switches, one as a VTP server and the other as a VTP client.
- Configure three VLANs on the VTP server switch and propagate this information to the VTP client.
- Configure VLAN configuration on Router A.
- Configure inter-VLAN routing using a router-on-a-stick configuration.
- Verify connectivity between the VLANs.

Background / Preparation

This lab focuses on the basic configuration of the Cisco 1841 or comparable router using Cisco IOS commands. The information in this lab applies to other routers; however, command syntax may vary. Depending upon the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or S0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Two Cisco 2960 switches or other comparable switches
- One router with Fast Ethernet interface to connect to switch
- One Windows-based PC with a terminal emulation program
- One RJ-45-to-DB-9 connector console cable to configure the router and switches
- One straight-through Ethernet cable to connect from the router to Switch 1
- One crossover Ethernet cable to connect Switch 1 to Switch 2

NOTE: Make sure the router and all the switches have been erased and have no startup configurations. For instructions, refer to the end of this lab. Instructions are provided for both the switch and router.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the router Fa0/0 interface with a straight-through cable to Switch 1 Fa0/2 interface.

b. Connect Switch 1 Fa0/1 port to the Fa0/1 port on Switch 2 using a crossover cable.

c. Connect a PC with a console cable to perform configurations on the router and switches.

Step 2: Perform basic configurations on the router

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. Configure Router A with a hostname and console, Telnet, and privileged passwords according to the table diagram.

Step 3: Configure VLAN trunking on the router

Configure Router A Fa0/0 interface to trunk for VLAN 1, VLAN 10, and VLAN 20 with 802.1Q encapsulation.

```
RouterA(config)#interface fa0/0
RouterA(config-if)#no shutdown
RouterA(config-if)#interface fa0/0.1
RouterA(config-subif)#encapsulation dot1Q 1
RouterA(config-subif)#ip address 172.16.1.1 255.255.255.0
RouterA(config-subif)#exit
RouterA(config)#interface fa0/0.10
RouterA(config-subif)#encapsulation dot1Q 10
RouterA(config-subif)#ip address 172.16.10.1 255.255.255.0
RouterA(config-subif)#exit
RouterA(config)#interface fa0/0.20
RouterA(config-subif)#encapsulation dot1Q 20
RouterA(config-subif)#ip address 172.16.20.1 255.255.255.0
RouterA(config-subif)#end
```

Step 4: .Configure Switch 1

a. Configure Switch 1 with a hostname and console, Telnet, and privileged passwords according to the table diagram.

b. Configure Switch 1 with the VLAN 1 IP address of 172.16.1.2/24.

c. On Switch 1, create VLAN 10, named **Faculty**, and VLAN 20, named **Students**.

```
Switch1(config)#vlan 10
Switch1(config-vlan)#name Faculty
Switch1(config-vlan)#exit
Switch1(config)#vlan 20
Switch1(config-vlan)#name Students
Switch1(config-vlan)#exit
Switch1(config)#
```

d. Configure Switch 1 with the default gateway address of 172.16.1.1.

e. Configure Switch 1 with the interfaces Fa0/5 and Fa0/6 on VLAN 10.

```
Switch1(config)#interface fa0/5
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#exit
Switch1(config)#interface fa 0/6
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#exit
```

f. Configure Switch 1 with the interfaces Fa0/7 and Fa0/8 on VLAN 20.

```
Switch1(config)#interface fa0/7
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#exit
Switch1(config)#interface fa0/8
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#end
```

g. Configure all other interfaces on Switch 1 in VLAN 1. By default, there is only a single VLAN for all ports. You cannot rename or delete VLAN 1. Therefore, no further configuration is necessary. To prove this, issue the command **`show vlan brief`**.

   Are all other switch ports in VLAN 1? _______

   Which switch ports are in VLAN 10? ___________________

   Which switch ports are in VLAN 20? ___________________

h. Issue the command **`show vlan`**.

   What difference is noticed between the two commands **`show vlan brief`** and **`show vlan`**?

   ____

   ____

Step 5: Configure VLAN trunking on Switch 1

a. Configure trunking between Switch 1 and Switch 2 with 802.1 encapsulation using port Fa0/1 on both switches.

```
Switch1(config)#int fa0/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#exit
```

b. Configure trunking between Switch 1 and Router A with 802.1 encapsulation using port Fa0/2 on Switch 1.

```
Switch1(config)#int fa0/2
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#end
Switch1#
```

c. From Switch 1, issue the command **`show interfaces trunk`**.

   Which interfaces on Switch 1 are in trunk mode? __________________________________

   Which VLANs are allowed and active in the management domain? ____________________

Step 6: Configure VTP on Switch 1

a. Configure Switch 1 as part of VTP domain Group 1.

```
Switch1(config)#vtp domain Group1
Changing VTP domain name from NULL to Group1
```

b. Configure Switch 1 as the VTP server and Switch 2 as the VTP client.

```
Switch1(config)#vtp mode server
Device mode already VTP SERVER.
Switch1(config)#end
```

Step 7: Configure Switch 2

a. Configure Switch 2 with a hostname and console, Telnet, and privileged passwords according to the table diagram.

b. Configure Switch 2 with the VLAN 1 IP address of 172.16.1.3/24.

c. Configure Switch 2 with the default gateway address of 172.16.1.1.

d. Configure Switch 2 with the interfaces Fa0/5 and Fa0/6 on VLAN 10.

```
Switch2(config)#interface fa0/5
Switch2(config-if)#switchport mode access
```

```
Switch2(config-if)#switchport access vlan 10
Switch2(config-if)#exit
Switch2(config)#interface fa 0/6
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 10
Switch2(config-if)#exit
```

e. Configure Switch 2 with the interfaces Fa0/7 and Fa0/8 on VLAN 20.

```
Switch2(config)#interface fa0/7
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 20
Switch2(config-if)#exit
Switch2(config)#interface fa0/8
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 20
Switch2(config-if)#exit
```

Step 8: Configure VLAN trunking on Switch 2

```
Switch2(config)#int fa0/1
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#exit
```

Step 9: Configure VTP on Switch 2

```
Switch2(config)#vtp mode client
```

From Switch 2, verify that all VLANs have been propagated across the domain by issuing the command **show vtp status**.

What is the VTP version used on Switch 2? _____________________

What is the maximum VLANs supported locally? _________________

What VTP operating mode is used on Switch 2? __________________

What is the VTP domain name? ______________________________

How did Switch 2 learn the domain name and VLAN information? ____________________________

____

Step 10: Verify connectivity

The router and switches should be able to ping the interfaces of the other devices.

a. From each device, issue a ping to all interfaces.

Are the router pings successful? ________

b. From Switch 1, ping to all other devices.

Are Switch 1 pings successful? __________

c. From Switch 2, ping to all other devices.

Are Switch 2 pings successful? __________
If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the router and switch configurations.

Step 11: Reflection

a. Why would VLANs be configured in a network?

____

____

____

____

b. Why would a VLAN benefit from trunking?

____

____

c. Why should VTP be used?

____

____

d. Which device provides connectivity between different VLANs?

____

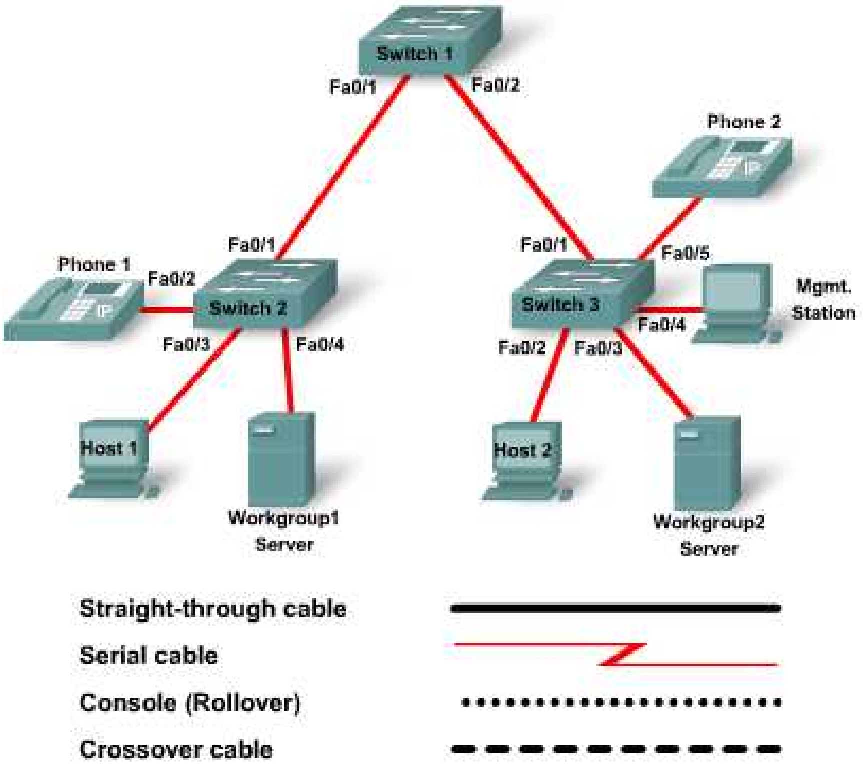
e. What are some benefits of VLANs?

____

____

____

Lab 3.5.4 Planning and Building a Switched Network



Objectives

- Develop a plan for building a switched network design utilizing best practices
- Design a switched network capable of handling diverse traffic types
- Plan and configure VLANs in the network
- Plan and configure network management of the switched network
- Design and configure the switched network

Background / Preparation

This activity focuses on utilizing best practices to plan, design and build a switched network utilizing VLANs. Industry best practices are implemented to help develop a stable, functioning network. As depicted in the drawing there are many elements to a corporate network. Network servers, end devices and various forms of communication and network management are implemented in today's converged networks. All of these things need to be accounted for in a good network design. This activity will provide a scenario to provide requirements for building a switched network.

The following resources are required:

- Three Cisco 2960 switches or equivalent
- One Windows-based PC with a terminal emulation program
- RJ-45-to-DB-9 connector console cable to configure the switch.
- Two crossover Ethernet cables to connect the switches.

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers - If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Plan and design the network.

The network design will include the following:

a. Separate VLANs for IP phones, two workgroups, network management and unused ports

b. VTP will be configured for ease of VLAN management.

c. Workgroup servers will be placed in the same VLAN as the workgroup hosts.

d. VLAN trunking will be utilized to reduce the number of switch interconnections.

e. All IP addresses will be assigned in the range from 172.16.1.x to 172.16.5.x, all with a /24 mask.

Given these requirements and the diagram provided, a switched network will be created that meets these needs and implements best practices for network design.

Step 2: Connect the equipment and perform basic configuration.

a. Connect the Switch1's Fa0/1 interface with a crossover cable to Switch2's Fa0/1 interface.

b. Connect the Switch1's Fa0/2 interface with a crossover cable to Switch3's Fa0/1 interface.

c. Connect a PC with a console cable to perform configurations on the switches.

d. Configure Switch1, Switch2 and Switch3 with a hostname and console, telnet and privileged passwords.

Step 3: Configure trunking on the switches.

a. To accommodate the communication for all of the VLANs between switches, trunking will be configured between Switch1 and Switches 2 and 3. Trunking mode will be forced between the switches with the **switchport mode trunk** command. All other switch ports will not be trunking and therefore will be configured as access ports with the **switchport mode access command**.

b. Configure the trunking ports on the switches.

```
Switch1(config)#interface fa0/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#interface fa0/2
Switch1(config-if)#switchport mode trunk
Switch2(config)#interface fa0/1
Switch2(config-if)#switchport mode trunk
Switch3(config)#interface fa0/1
Switch3(config-if)#switchport mode trunk
```

c. Configure all other ports on the switches as access ports. Also, best practices call for all unused switch ports to be disabled, so all of the ports will be shutdown and then brought up as utilized.

```
Switch1(config)#interface range fa0/3 - 24
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#shutdown


Switch2(config)#interface range fa0/2 - 24
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#shutdown

Switch3(config)#interface range fa0/2 - 24
Switch3(config-if-range)#switchport mode access
Switch3(config-if-range)#shutdown
```

Step 4: Create and verify VTP configuration.

a. VTP will be used to simplify the VLAN configuration. Switch 1 will be utilized as the VTP server, while Switches 2 and 3 will be VTP clients and receive their VLAN information from Switch 1. The VTP domain will be called Cisco and a VTP password of “myvlans” will be configured.

```
Switch1(config)#vtp mode server
Switch1(config)#vtp domain cisco
Switch1(config)#vtp password myvlans
Switch1(config)#end


Switch2(config)#vtp mode client
Switch2(config)#vtp domain cisco
Switch2(config)#vtp password myvlans
Switch2(config)#end

Switch3(config)#vtp mode client
Switch3(config)#vtp domain cisco
Switch3(config)#vtp password myvlans
Switch3(config)#end
```

b. Use the **show vtp status** command to verify the VTP configuration.

```
Switch1#show vtp status
Switch2#show vtp status
Switch3#show vtp status
```

Does the output from switch1 indicate that it is the VTP server?______________

Do the outputs from switches 2 and 3 indicate that they are VTP clients?_______

Record the configuration revision number from each of the switches.

Switch1______ Switch2_______ Switch3______

Step 5: Configure and verify VLANs.

Separate VLANs will be created for the different traffic groups. By default, all interfaces will belong to VLAN1. This VLAN will be utilized to contain all of the unused ports. When routing is implemented, this VLAN would not be routed so as to create a "dead zone" for all unused ports.
VLAN 10 will be created for the network management network.
VLAN 20 will be created for workgroup1.
VLAN 30 will be created for workgroup2.
VLAN 40 will be created for IPphones.

a. Create the VLANs on Switch1.

```
Switch1(config)#vlan 10
Switch1(config-vlan)#name management
Switch1(config-vlan)#vlan 20
Switch1(config-vlan)# name workgroup1
Switch1(config-vlan)#vlan 30
Switch1(config-vlan)#name workgroup2
Switch1(config-vlan)#vlan 40
Switch1(config-vlan)#name IPphones
```

b. Verify the creation of the VLANs on all of the switches with the **show vlan** command.

```
Switch1#show vlan

Switch2#show vlan

Switch3#show vlan
```

Do the newly created VLANs appear in the outputs?____

c. View the VTP status on all of the switches with the **show vtp status** command.

```
Switch1#show vtp status

Switch2#show vtp status

Switch3#show vtp status
```

Have the VTP revision numbers changed from the before?____________

Step 6: Configure switch management interfaces.

In the previous step, VLAN 10 was created as the management VLAN. By default, only the VLAN1 logical interface is visible on the switch configuration, but as soon as it is accessed the VLAN 10 interface will appear.

a. Configure the management interfaces on the switches.

```
Switch1(config)#int vlan 10
Switch1(config-if)#ip address 172.16.1.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#end
Switch1#

Switch2(config)#int vlan 10
Switch2(config-if)#ip address 172.16.1.2 255.255.255.0
Switch2(config-if)#no shutdown
Switch2(config-if)#end
Switch2#

Switch3(config)#int vlan 10
Switch3(config-if)#ip address 172.16.1.3 255.255.255.0
Switch3(config-if)#no shutdown
Switch3(config-if)#end
Switch3#
```

b. Verify connectivity by pinging from Switch1 to the other switches.

```
Switch1# ping 172.16.1.2

Switch1# ping 172.16.1.3
```

Is Switch1 able to ping the other switches?___________

Step 7: Configure VLAN assignments.

In preparation for connecting hosts as shown in the diagram on the first page of this lab, ports must be assigned to the proper VLANs to allow for communication between devices and to allow control of communication between VLANs with access control lists on routers.

a. Assign the ports to the proper VLANs on the switches.

```
Switch2(config)#int fa0/2
Switch2(config-if)#switchport access vlan 40
Switch2(config-if)#int fa0/3
Switch2(config-if)#switchport access vlan 20
Switch2(config-if)#int fa0/4
Switch2(config-if)#switchport access vlan 20

Switch2(config)#int fa0/2
Switch2(config-if)#switchport access vlan 30
Switch2(config-if)#int fa0/3
```

```
Switch2(config-if)#switchport access vlan 30
Switch2(config-if)#int fa0/4
Switch2(config-if)#switchport access vlan 10
Switch2(config-if)#int fa0/5
Switch2(config-if)#switchport access vlan 40
```

With the VLAN assignments made, the switch ports can be brought up as the devices are connected.

Step 8: Reflection

Why is trunking configured in a network?

____

____

____

____

Why is VTP configured in a network? ____

____

Why are unused ports shutdown and assigned to an unused VLAN?

____

____

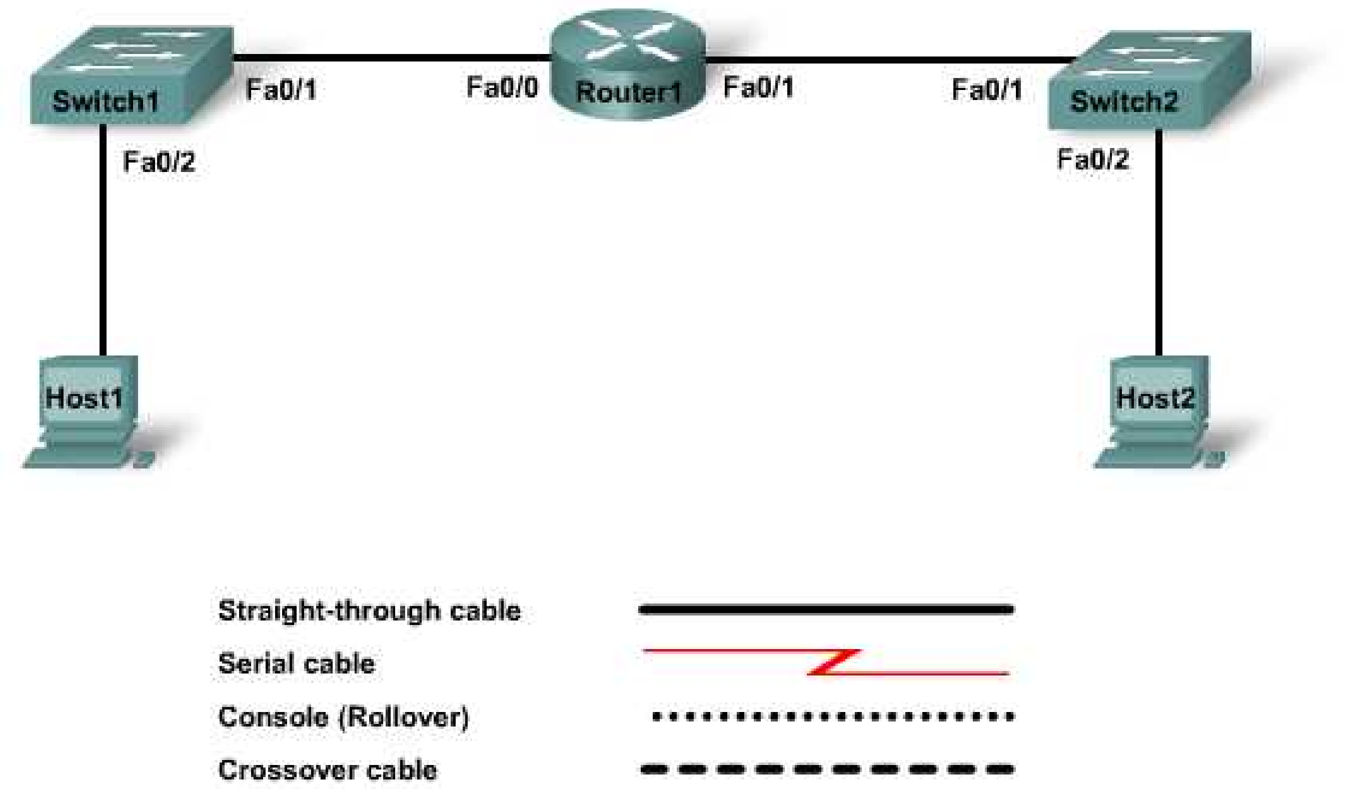
Why are VLANs used to separate network traffic?

____

____

____

Lab 4.2.3.2 Designing and Applying an IP Addressing Scheme



Device Name	Enable Secret Password	Enable, Console, and vty Passwords	IP Address	Subnet Mask	Default Gateway
Switch1	class	cisco	VLAN 1: 192.168.1.34	255.255.255.224 (/27)	192.168.1.33
Switch2	class	cisco	VLAN 1: 192.168.1.66	255.255.255.224 (/27)	192.168.1.65
Router1	class	cisco	FA0/0: 192.168.1.33 FA0/1: 192.168.1.65	255.255.255.224 (/27)	N/A
Host1	N/A	N/A	192.168.1.35	255.255.255.224 (/27)	192.168.1.33
Host2	N/A	N/A	192.168.1.67	255.255.255.224 (/27)	192.168.1.65

Objectives

- Create a network with two subnets of the same size.
- Verify the status of the network connections.

Background / Preparation

This lab is a review of basic subnetting configuration of a router with two switches attached.

The following resources are required:

- One Cisco 1841 router or similar router with two Ethernet interfaces
- Two Cisco 2960 switches or other comparable switches
- Two Windows-based PCs, each with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cables to configure the switches
- Four straight-through Ethernet cables
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers - If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Cable the network

a. Connect Host1 to Switch1 port Fa0/2, using a straight-through Ethernet cable.

b. Connect Host2 to Switch2 port Fa0/2, using a straight-through Ethernet cable.

c. Connect Switch1 port Fa0/1 to Router1 port Fa0/0, using a straight-through Ethernet cable.

d. Connect Switch2 port Fa0/1 to Router1 port Fa0/1, using a straight-through Ethernet cable.

Step 2: Configure the router

a. Establish a terminal emulation session from either host to Router1.

b. Configure the router hostname, passwords, interface IP addresses, and subnet mask. Also configure RIP as the routing protocol.

c. Save the configuration.

Step 3: Configure the switches

a. Establish a terminal emulation session to Switch1 from Host1.

b. Configure the switch hostname, passwords, interface VLAN 1 IP address, subnet mask, and default gateway on Switch1.

c. Save the configuration.

d. Establish a terminal emulation session to Switch2 from Host2.

e. Configure the switch hostname, passwords, interface VLAN 1 IP address, subnet mask, and default gateway on Switch2.

f. Save the configuration.

Step 4: Configure the hosts

a. Configure Host1 using the IP address, subnet mask, and default gateway from the table.

b. Configure Host2 using the IP address, subnet mask, and default gateway from the table.

Step 5: Verify connectivity

To verify that the network is set up successfully, ping from Host 1 to Host 2.

Was the ping successful? _____________

If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated.

Step 6: Reflection

Subnetting allows the addresses in a network range to be split into smaller groups. This lab split the total number of addresses, 256, into smaller groups of equal size.

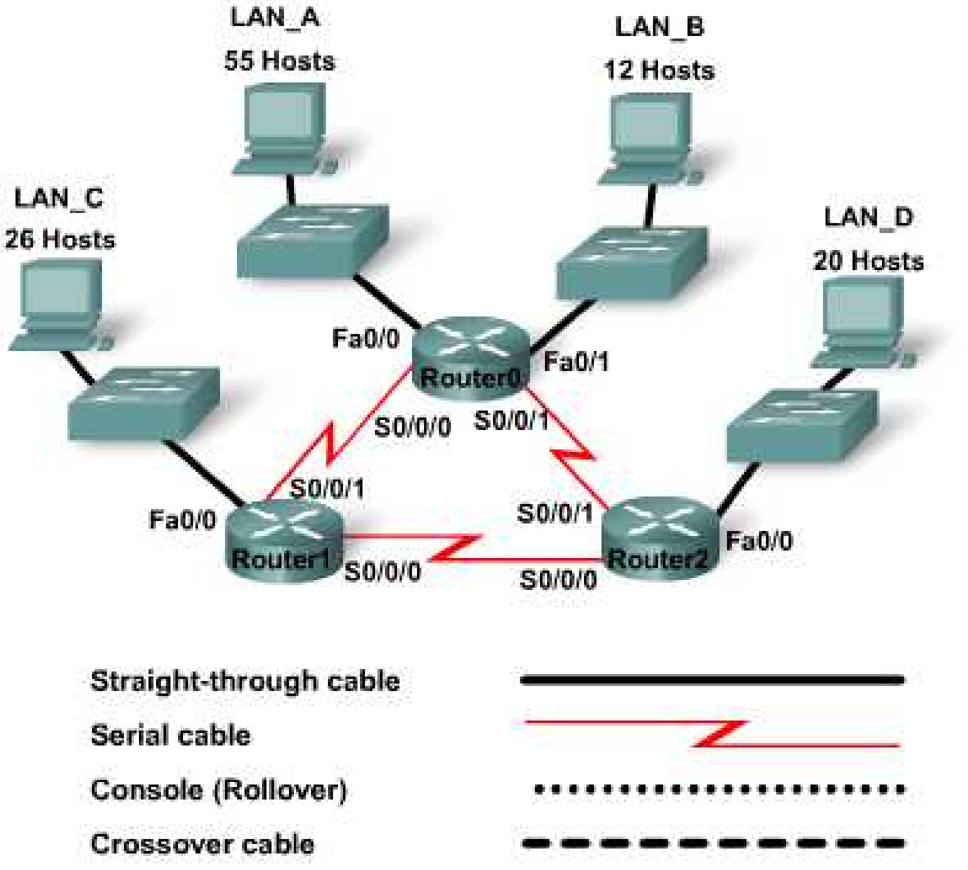
How many address are in each subnet? _______

How may total subnets were created? _______

The subnet mask is 255.255.255.224. How many host bits were “borrowed” for subnetting? _______

What is the total number of network and subnet bits in each address? _______

Lab 4.2.5.5 Calculating a VLSM Addressing Scheme



Objectives

- Determine the number of subnets needed.
- Determine the number of hosts needed for each subnet.
- Design an appropriate addressing scheme using VLSM.
- Assign IP configurations to device interfaces.
- Examine the use of the available network address space.

Background / Preparation

This lab explores the use of VLSM to meet the needs of a network topology. In this lab, you will assess the topology, determine the addressing scheme to meet its needs, and prepare documentation for the addressing. You have been assigned the 192.168.1.0/24 network to address this network.

Step 1: Examine the network requirements

Use the topology diagram to determine the answers to the questions below. Remember that IP addresses will be needed for each LAN and WAN interface.

a. How many subnets are needed? __________

b. What is the maximum number of IP addresses that are needed for a single subnet? __________

c. How many host IP addresses are needed for the largest LAN? __________

d. How many host IP addresses are needed for the next-largest LAN? __________

e. How many host IP addresses are needed for the smallest LAN? __________

f. How many host IP addresses are needed for each WAN link? __________

g. What is the total number of host IP addresses that are needed for this network? __________

h. What is the total number of host IP addresses that are available in the 192.168.1.0/24 network? __________

i. If the network is subnetted to provide 7 usable subnets, can the addressing requirements be met?

____

Step 2: Design an IP addressing scheme to fit the network requirements

a. Determine the subnet information for the largest subnet needed.

What is the smallest size subnet that can be used to meet this requirement? __________

Will a subnet of this size allow for future growth of 10 – 15%? __________

Fill in the chart below with the appropriate information. Assign the first available subnet on the 192.168.1.0 network to this LAN.

LAN_A Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address

b. Assign the next available subnet to the next-largest LAN.

c. Fill in the chart below with the appropriate information.

LAN_D Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address

d. Continue assigning subnets of appropriate sizes to the remaining LANs.

LAN_C Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address

LAN_B Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address

Step 3: Assign subnets to the WAN links between routers

Start with the next available subnet. Complete the chart below with the addressing information.

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
WAN link between Router0 and Router1					
WAN link between Router1 and Router 2					
WAN link between Router2 and Router0					

Step 4: Assign IP configurations to router interfaces

Complete the chart below with IP assignments for router interfaces. Use the first available host IP address for the router's LAN interface.

Device	Interface	IP Address	Subnet Mask
Router0	Fa0/0		
	Fa0/1		
	S0/0/0		
	S0/0/1		
Router1	Fa0/0		
	S0/0/0		
	S0/0/1		
Router2	Fa0/0		
	S0/0/0		
	S0/0/1		

Step 5: Assign IP configurations to workstations

One workstation has been provided to represent each LAN. Complete the chart below with IP configuration information for each representative workstation.

LAN	IP Address	Subnet Mask	Default Gateway
LAN_A			
LAN_B			
LAN_C			
LAN_D			

Step 6: Reflection

a. What is the last host IP address that will be used by this VLSM scheme?

____

b. Your largest LAN can accommodate 15% growth with your VLSM scheme. Which of the other LANs can also accomplish this goal?

____

c. If you decided to change the masks on those LANs that did not meet the 15% growth goal, would you have enough addresses to complete your scheme? __________.

d. What would the new network addresses be for the four LANs?

LAN_A: ____

LAN_D: ____

LAN_C: ____

LAN_B: ____

e. If you wanted to provide redundant backup WAN links between your routers, how many more subnets would you need? __________

f. Could you do it with this VLSM scheme? __________

g. Summarize the advantages of using VLSM for network addressing schemes:

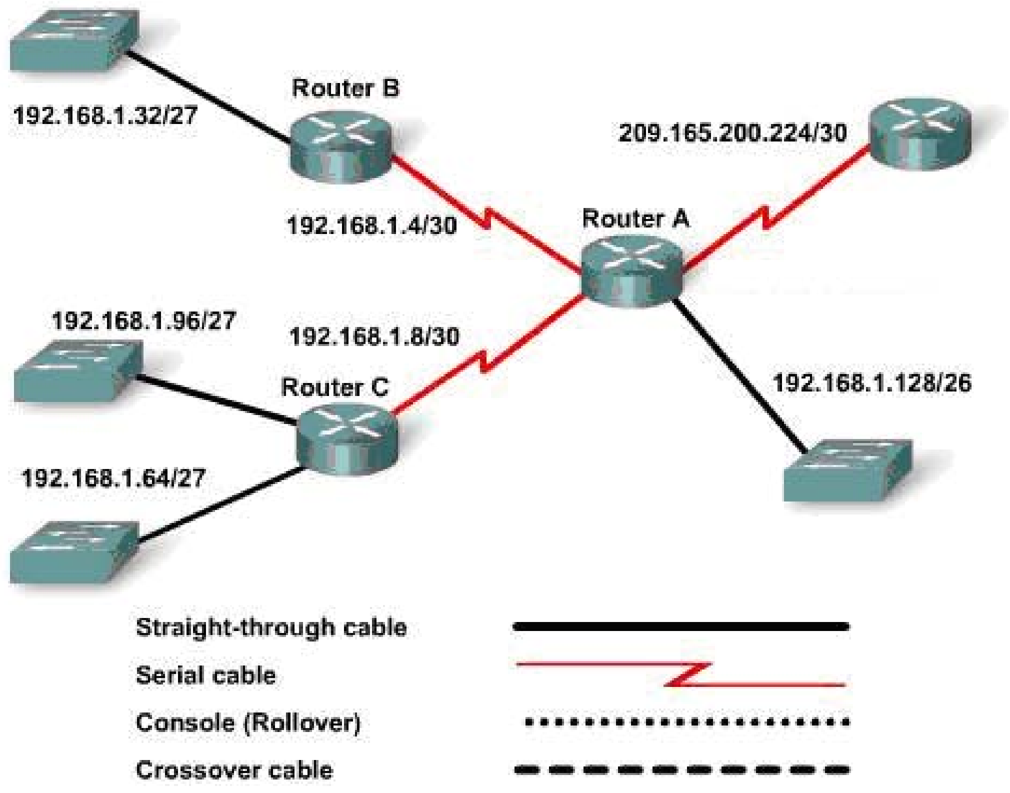
____

____

____

____

Lab 4.3.3.3 Calculating Route Summarization



Device	Fa0/0 Network and Subnet Mask	Fa0/1 Network and Subnet Mask	Serial 0/0/0 Network and Subnet Mask	Serial 0/0/1 Network and Subnet Mask	Serial 0/1/0 Network and Subnet Mask
RouterA	192.168.1.128/26	N/A	192.168.1.4/30	192.168.1.8/30	209.165.200.224/30
RouterB	192.168.1.32/27	N/A	192.168.1.4/30	N/A	N/A
RouterC	192.168.1.64/27	192.168.1.96/27	192.168.1.8/30	N/A	N/A

Objectives

- Calculate route summarization for each router.
- Calculate the total summarization so that RouterA can pass a smaller routing table to the ISP.

Background / Preparation

Use the information in the topology to calculate the route summarization for each router. Begin with RouterC, because it has two FastEthernet networks and RouterB has only one.

After completing the table for RouterB, calculate the summarization for RouterC (it only advertises one route).

Next, calculate the summarization for RouterA. It will summarize its own network on FastEthernet 0/0, the Serial networks, and the summary routes from RouterB and RouterC.

Step 1: Complete this summarization table for RouterC

RouterC	Network Number in Binary	Network Number in Decimal
Fa0/0		
Fa0/1		
Summary Route		

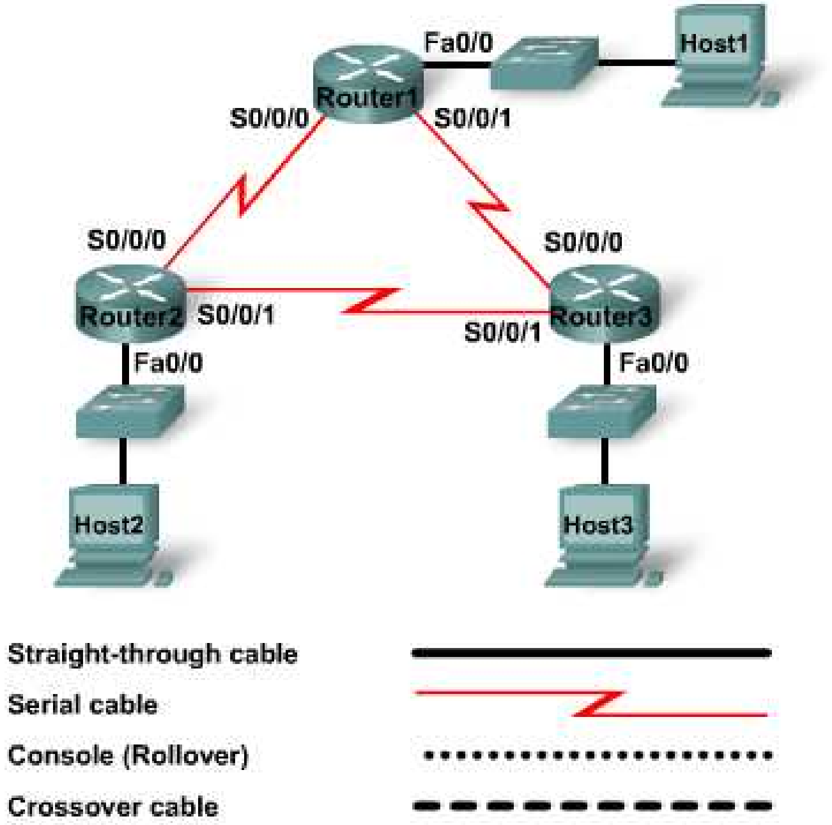
Step 2: Complete this summarization table for RouterB

RouterB	Network Number in Binary	Network Number in Decimal
Fa0/0		
Fa0/1	NA	NA
Summary Route		

Step 3: Complete this summarization table for RouterA

RouterA	Network Number in Binary	Network Number in Decimal
Fa0/0		
Fa0/1	NA	NA
Serial 0/0/0		
Serial 0/0/1		
Summary Route from RouterC		
Summary Route from RouterB		
Summary Route		

Lab 4.3.4.3 Configuring a LAN with Discontiguous Subnets



Device	Host Name	FastEthernet 0/0/ Subnet Mask	Serial 0/0/0 / Subnet Mask	Interface Type	Serial0/ 0/1 Subnet Mask	Interface Type	Enable Secret Password	Enable, vty, and Console Password
Router1	Main	172.30.0.1/24	10.0.0.1/30	DCE	10.0.0.5/30	DCE	class	cisco
Router2	Branch1	172.30.1.1/24	10.0.0.2/30	DTE	10.0.0.9/30	DCE	class	cisco
Router3	Branch2	172.30.2.1/24	10.0.0.6/30	DTE	10.0.0.10/30	DTE	class	cisco
			Default Gateway					
Host 1	Host1	172.30.0.2/24	172.30.0.1					
Host 2	Host2	172.30.1.2/24	172.30.1.1					
Host 3	Host3	172.30.2.2/24	172.30.2.1					

Objectives

- Configure routers and hosts to use discontiguous subnets.
- Observe the effects of discontiguous subnets on routing tables.
- Modify the existing configuration to improve results.

Background / Preparation

Good VLSM implementation requires assigning subnets contiguously. However, meeting network design requirements can result in subnets that are separated by a different network. In this lab, according to a VLSM scheme, subnets assigned to two LANs are separated from each other by a public network connecting the two routers. The results of this condition are seen in the routing tables. After the problem has been identified, you will take steps to improve the ability of the routers to report all the existing routes.

The following resources are required:

- Three routers with 2 serial connections and 1 Ethernet interface to connect to a switch
- Three Cisco 2960 switches or other comparable switches
- Three Windows-based PCs, one with a terminal emulation program, and both set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switches
- Six straight-through Ethernet cables to connect from the routers to the switches and from the hosts to the switches

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router1 Serial 0/0/0 interface to Router2 Serial 0/0/0 interface using a serial cable.

b. Connect Router2 Serial 0/0/1 interface to Router3 Serial 0/0/1 interface using a serial cable.

c. Connect Router1 to Router3 with a serial cable as shown in the diagram and table.

d. Connect the Fa0/0 interface of each router to the Fa0/1 interface on the corresponding switch.

e. Connect a PC with a console cable to perform configurations on the routers and switches.

f. Connect each host PC to the Fa0/2 interface on its switch using a straight-through cable.

Step 2: Perform basic configurations on Router1

Perform basic configuration on Router1 with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Use RIP as the routing protocol, and advertise the attached networks. Save the configuration.

Step 3: Configure the other routers

Perform similar basic configurations on Router2 and Router3 with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Use RIP as the routing protocol, and advertise the attached networks. Save the configurations.

Step 4: Configure the hosts with the proper IP address, subnet mask, and default gateway

Configure each host with the proper IP address, subnet mask, and default gateway.

From the configurations given, what would be the next available subnetwork IP address on the 172.30.0.0 network? _________________________

If you needed to accommodate an additional LAN with 60 hosts, what mask would you use for that subnetwork? ____________________________

Step 5: Verify that the network is functioning

a. From each host, ping its default gateway.

   Was the ping from Host1 successful? __________

   Was the ping from Host2 successful? __________

   Was the ping from Host3 successful? __________

   If the answer is **no** for any question, troubleshoot the router and host configurations to find the error. Ping again until they are successful.

b. For each router, view the status of the interface.

```
Main#show ip interfaces brief
Branch1#show ip interface brief
Branch2#show ip interface brief
```

   Is the status and protocol listed as **up** for all active interfaces? __________

   If the answer is **no**, troubleshoot the router configurations to find the error. Recheck until the status and protocol are **up**.

Step 6: Examine the routing tables

a. From the network topology, how many routes should each router report in its routing table to have a complete picture of the network? __________

b. On each router, view the routing table. The command and output for Main is shown below:

```
Main#show ip route
<<output omitted>>
Gateway of last resort is not set
     10.0.0.0/30 is subnetted, 3 subnets
C       10.0.0.0 is directly connected, Serial0/0/0
C       10.0.0.4 is directly connected, Serial0/0/1
R       10.0.0.8 [120/1] via 10.0.0.2, 00:00:21, Serial0/0/0
                 [120/1] via 10.0.0.6, 00:00:15, Serial0/0/1
     172.30.0.0/24 is subnetted, 1 subnets
C       172.30.0.0 is directly connected, FastEthernet0/0
```

   What problem do you see in the routing tables? ____

   ____

Step 7: Identify and attempt to correct the problem

a. From the router configurations, identify the reason for the problem you found in Step 6.

____

____

b. On each router, issue the commands to correct this problem. A sample command and output for Main is shown.

```
Main(config-router)#version 2
Main(config-router)#end
Main#show ip route
<<output omitted>>
Gateway of last resort is not set
     10.0.0.0/30 is subnetted, 3 subnets
C       10.0.0.0 is directly connected, Serial0/0/0
C       10.0.0.4 is directly connected, Serial0/0/1
R       10.0.0.8 [120/1] via 10.0.0.2, 00:00:08, Serial002/0
                 [120/1] via 10.0.0.6, 00:00:02, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
R       172.30.0.0/16 [120/1] via 10.0.0.2, 00:00:08, Serial0/0/0
                      [120/1] via 10.0.0.6, 00:00:02, Serial0/0/1
C       172.30.0.0/24 is directly connected, FastEthernet0/0
```

c. Re-examine the routing tables carefully.

Explain why, even though each router now has RIP routes, there is still a problem with the tables.

____

What should be done to correct the problem?

____

d. On all three routers, issue the command to correct this issue. A sample for Main is shown.

```
Main(config-router)#no auto-summary
```

Step 8: Verify that the problem has been corrected

View the routing table. Routes should be reported as shown for the Main router.

```
Main#show ip route
<<output omitted>>
  Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 3 subnets
C       10.0.0.0 is directly connected, Serial0/0/0
C       10.0.0.4 is directly connected, Serial0/0/1
R       10.0.0.8 [120/1] via 10.0.0.2, 00:00:02, Serial0/0/0
                 [120/1] via 10.0.0.6, 00:00:02, Serial0/0/1
     172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
R       172.30.0.0/16 [120/1] via 10.0.0.2, 00:00:32, Serial0/0/0
                      [120/1] via 10.0.0.6, 00:00:29, Serial0/0/1
C       172.30.0.0/24 is directly connected, FastEthernet0/0
R       172.30.1.0/24 [120/1] via 10.0.0.2, 00:00:02, Serial0/0/0
R       172.30.2.0/24 [120/1] via 10.0.0.6, 00:00:02, Serial0/0/1
```

Are all expected routes being reported now? __________

Why are there two routes reported to the 10.0.0.8 subnetwork?

____

Step 9: Reflection

a. When would it be important to view all possible routes in a routing table?

____

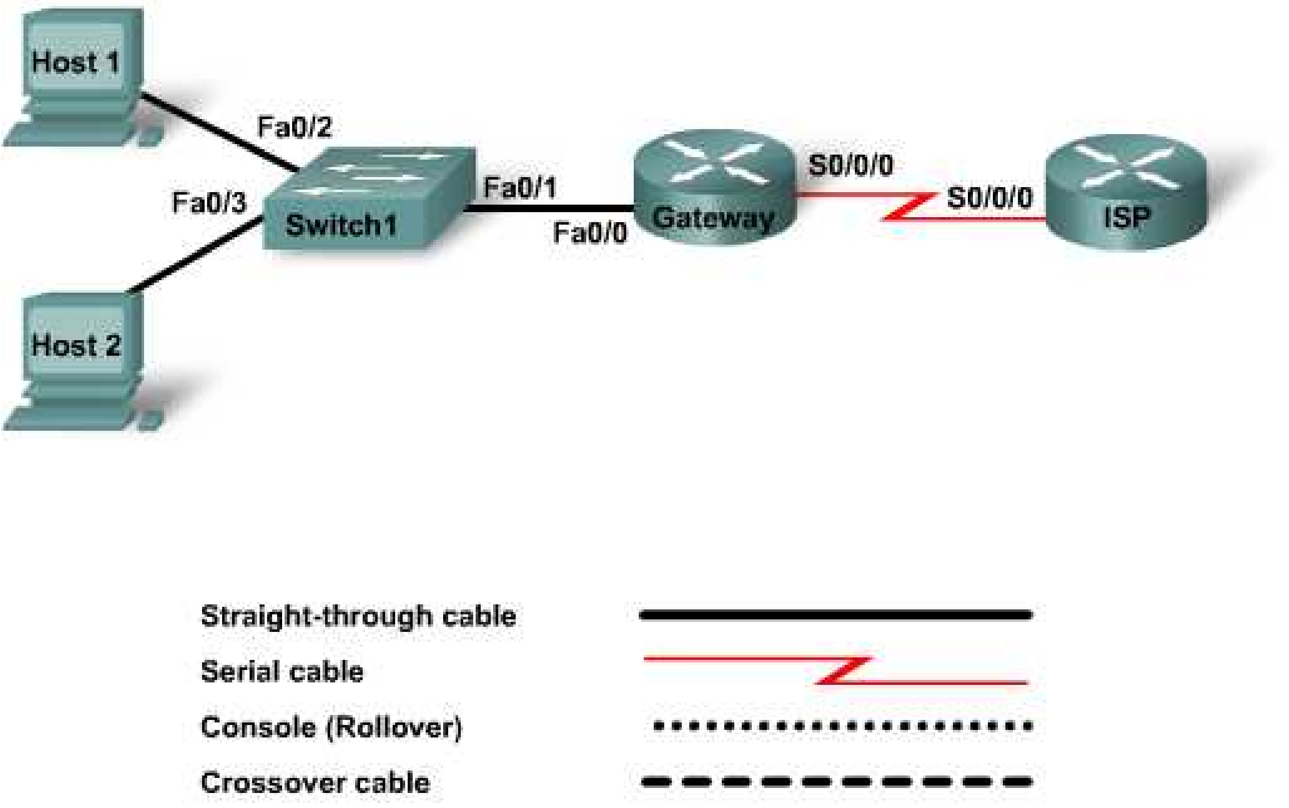
____

b. RIP version 2 supports VLSM, but changing to version 2 did not fully resolve the problem. Why?

____

____

Lab 4.4.3.3 Configure and Verify Static NAT



Device	Host Name	FastEthernet 0/0 / Subnet Mask	Interface Type	Serial 0/0/0/ IP Address	Loopback 0 Address	Enable Secret Password	Enable, vty, and Console Password
Router 1	Gateway	10.10.10.1/24	DTE	209.165.201.33/30		cisco	class
Router 2	ISP	N/A	DCE	209.165.201.34/30	172.16.1.1/32	cisco	class
Switch 1	Switch1					cisco	class

Objectives

- Configure a router to use network address translation (NAT) to convert internal IP addresses, typically private addresses, into outside public addresses.
- Verify connectivity.
- Verify NAT statistics.

Background / Preparation

An ISP has allocated to a company the public classless interdomain routing (CIDR) IP address 209.165.200.224/27. This provides them with 30 public IP addresses. Because the company has an internal requirement for more than 30 addresses, the IT manager decides to implement NAT. The addresses 209.165.200.225 to 209.165.200.241 are for static allocation and 209.165.200.242 to 209.165.200.254 are for dynamic allocation. Routing will be done between the ISP and the gateway router used by the company. A static route will be used between the ISP and the gateway router, and a default route will be used between the gateway and the ISP router. The ISP connection to the Internet will be represented by a loopback address on the ISP router.

This lab focuses on the basic configuration of the Cisco 1800 router, or comparable router, using Cisco IOS commands. The information in this lab applies to other routers; however, command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two routers, each with a serial connection and one Ethernet interface to connect to the switch
- Two Windows-based PCs for hosts, one with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the router and switches
- Three straight-through Ethernet cables to connect from the router to Switch 1 and to connect both hosts to the switch
- One serial cable to connect from Router 1 to Router 2

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router 1 Serial 0/0/0 interface to Router 2 Serial 0/0/0 interface using a serial cable.

b. Connect Router 1 Fa0/0 interface to Switch 1 Fa0/1 interface using a straight-through cable.

c. Connect a PC with a console cable to perform configurations on the routers and switch.

d. Connect both hosts to Fa0/2 and Fa0/3 on the switch using straight-through cables.

Step 2: Perform basic configurations on Router 2

a. Connect a PC to the console port of Router 2 to perform configurations using a terminal emulation program.

b. Configure Router 2 with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 3: Configure the gateway router

Perform basic configuration on Router 1 as the Gateway router with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 4: Configure Switch 1

Configure Switch 1 with a hostname, console, Telnet, and privileged passwords according to the table diagram.

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway. Host 1 should be assigned 10.10.10.2/24 and Host 2 should be assigned 10.10.10.3/24. The default gateway should be 10.10.10.1.

b. Each workstation should be able to ping the attached router. If the ping was not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Verify that the network is functioning

From the attached hosts, ping the FastEthernet interface of the default gateway router.

Was the ping from Host 1 successful? __________

Was the ping from Host 2 successful? __________

If the answer is no for either question, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

Step 7: Create a static route

Create a static route from the ISP to the Gateway router. Addresses 209.165.200.224/27 have been allocated for Internet access outside of the company. Use the **ip route** command to create the static route.

```
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.33
```

Is the static route in the routing table? __________

What command checks the routing table contents? ______________________________

If the route was not in the routing table, give one reason why this might be so?

____

Step 8: Create a default route

a. From the Gateway router to the ISP router, create a static route to network 0.0.0.0 0.0.0.0, using the **`ip route`** command. This will forward any unknown destination address traffic to the ISP by setting a Gateway of Last Resort on the Gateway router.

```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.34
```

Is the static route in the routing table? __________

b. Try to ping from one of the workstations to the ISP serial interface IP address.

   Was the ping successful? __________

   Why? ____

Step 9: Define the pool of usable public IP addresses

To define the pool of public addresses, use the **ip nat pool** command.

```
Gateway(config)#ip nat pool public_access 209.165.200.242
209.165.200.253 netmask 255.255.255.224
```

Step 10: Define an access list that will match the inside private IP addresses

To define the access list to match the inside private addresses, use the **access-list** command.

```
Gateway(config)#access-list 1 permit 10.10.10.0 0.0.0.255
```

Step 11: Define the NAT translation from inside list to outside pool

To define the NAT translation, use **the ip nat inside source** command.

```
Gateway(config)#ip nat inside source list 1 pool public_access
```

Step 12: Specify the interfaces

The active interfaces on the router need to be specified as either inside or outside interfaces with respect to NAT. To do this, use the **ip nat inside** or **ip nat outside** command.

```
Gateway(config)#interface fastethernet 0/0
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface serial 0/0/0
Gateway(config-if)#ip nat outside
```

Step 13: Configure Static Mapping

a. Host 1, 10.10.10.2/24, will be designated as the public WWW server. Therefore, it needs a permanent public IP address mapping. This mapping is defined using a static NAT mapping.

b. To configure a static IP NAT mapping, use the **ip nat inside source static** command at the privileged EXEC mode prompt.

```
Gateway(config)#ip nat inside source static 10.10.10.2 209.165.200.224
```

   This permanently maps 209.165.200.224 to the inside address 10.10.10.2.

c. Look at the translation table:

```
Gateway#show ip nat translations
```

   Does the mapping appear in the output of the **show** command? __________

Step 14: Test the configuration

a. From the 10.10.10.2 workstation, verify that it can ping 172.16.1.1.

Is the ping successful? __________

Why? ____

b. From the ISP router, ping the host with the static NAT translation by typing **`ping 10.10.10.2`**.

Is the ping successful? __________

Why? ____

c. From the ISP router, ping 209.165.200.224. If successful, look at the NAT translation on the Gateway router, using the command **`show ip nat translations`**.

What is the translation of the inside local host addresses?

____________________________________ = ____________________________________

Step 15: Verify NAT statistics

To view the NAT statistics, type the **`show ip nat statistics`** command at the privileged EXEC mode prompt.

How many active translations have taken place? __________

How many addresses are in the pool? __________

How many addresses have been allocated so far? __________

Step 16: Reflection

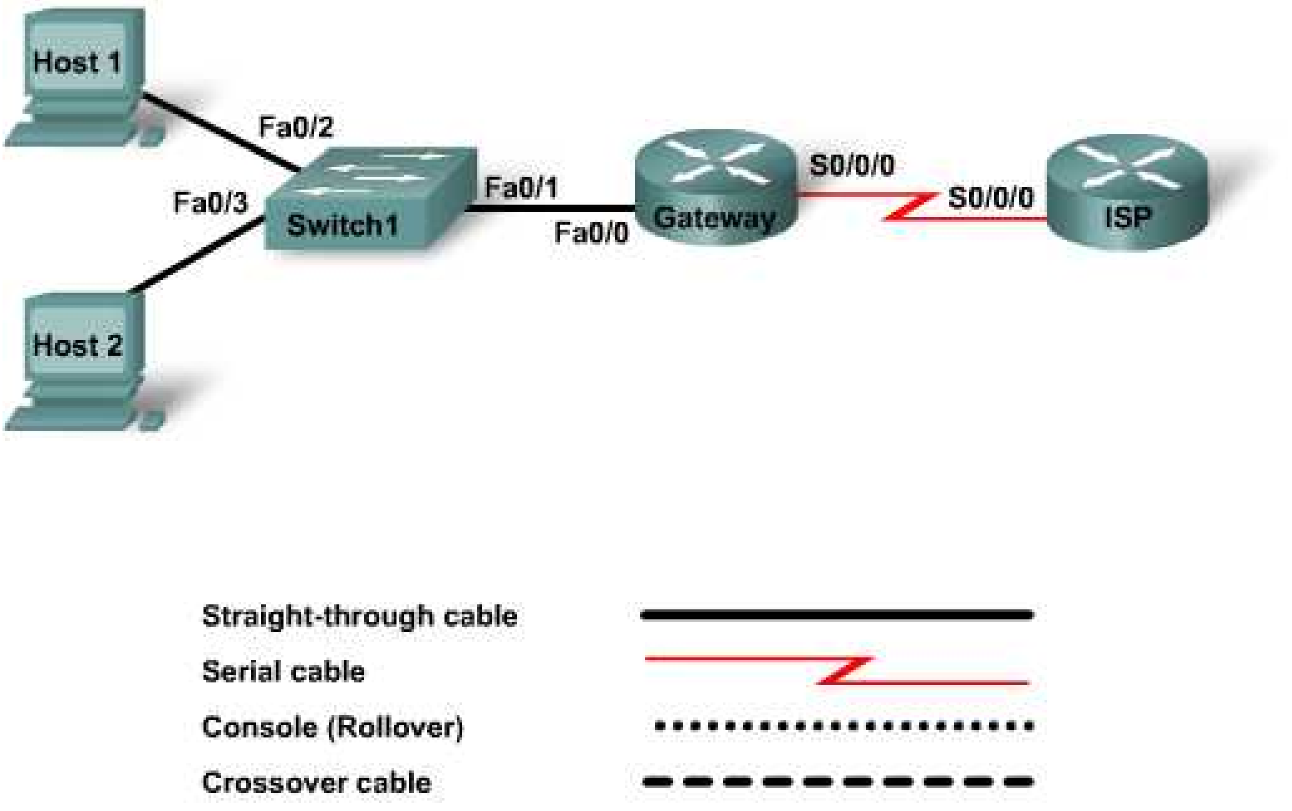
Why would NAT be used in a network? ____

____

____

____

Lab 4.4.3.4 Configure and Verify Dynamic NAT



Device	Host Name	Fast Ethernet 0/0/ IP Address	Interface Type	Serial 0/0/0 IP Address	Loopback 0 Address / mask	Enable Secret Password	Enable, vty, and Console Password
Router 1	Gateway	10.10.10.1/24	DTE	209.165.201.33/30		cisco	class
Router 2	ISP	N/A	DCE	209.165.201.34/30	172.16.1.1/32	cisco	class
Switch 1	Switch1					cisco	class

Objectives

- Configure a router to use network address translation (NAT) to convert internal IP addresses, typically private addresses, into outside public addresses.
- Verify connectivity.
- Verify NAT statistics.

Background / Preparation

An ISP has allocated a company the public classless interdomain routing (CIDR) IP address 209.165.200.224/27. This provides them with 30 public IP addresses. Because the company has an internal requirement for more than 30 addresses, the IT manager decides to implement NAT. The addresses 209.165.200.225 to 209.165.200.241 are for static allocation and 209.165.200.242 to 209.165.200.254 are for dynamic allocation. Routing will be done between the ISP and the gateway router used by the company. A static route will be used between the ISP and the gateway router, and a default route will be used between the gateway and the ISP router. The ISP connection to the Internet will be represented by a loopback address on the ISP router.

This lab focuses on the basic configuration of the Cisco 2800 router, or comparable router, using Cisco IOS commands. The information in this lab applies to other routers; however, command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switches or other comparable switch
- Two routers, each with a serial connection and one Ethernet interface to connect to the switch
- Two Windows-based PCs for hosts, one with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the router and switches
- Three straight-through Ethernet cables to connect from the router to Switch 1 and to connect both hosts to the switch
- One serial cable to connect from Router 1 to Router 2

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router 1 Serial 0/0/0 interface to Router 2 Serial 0/0/0 interface using a serial cable.

b. Connect Router 1 Fa0/0 interface to Switch 1 Fa0/1 interface using a straight-through cable.

c. Connect a PC with a console cable to perform configurations on the routers and switch.

d. Connect both hosts to Fa0/2 and Fa0/3 on the switch using straight-through cables.

Step 2: Perform basic configurations on Router 2

a. Connect a PC to the console port of Router 2 to perform configurations using a terminal emulation program.

b. Configure Router 2 with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 3: Configure the gateway router

Perform basic configuration on Router 1 as the Gateway router with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 4: Configure Switch 1

Configure Switch 1 with a hostname, console, Telnet, and privileged passwords according to the table diagram.

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway. Host 1 should be assigned 10.10.10.2 /24 and Host 2 should be assigned 10.10.10.3 /24. The default gateway should be 10.10.10.1.

b. Each workstation should be able to ping the attached router. If the ping was not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Verify that the network is functioning

From the attached hosts, ping the FastEthernet interface of the default gateway router.

Was the ping from Host 1 successful? __________

Was the ping from Host 2 successful? __________

If the answer is no for either question, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

Step 7: Create a static route

Create a static route from the ISP to the Gateway router. Addresses 209.165.200.224/27 have been allocated for Internet access outside of the company. Use the **ip route** command to create the static route.

```
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.33
```

Is the static route in the routing table? __________

What command checks the routing table contents? ______________________________

If the route was not in the routing table, give one reason why this might be so?

____

Step 8: Create a default route

a. From the Gateway router to the ISP router, create a static route to network 0.0.0.0 0.0.0.0, using the **ip route** command. This will forward any unknown destination address traffic to the ISP by setting a Gateway of Last Resort on the Gateway router.

```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.34
```

Is the static route in the routing table? _________________________

b. Try to ping from one of the workstations to the ISP serial interface IP address.

Was the ping successful? __________

Why? ____

Step 9: Define the pool of usable public IP addresses

To define the pool of public addresses, use the **ip nat pool** command.

```
Gateway(config)#ip nat pool public_access 209.165.200.242
209.165.200.254 netmask 255.255.255.224
```

Step 10: Define an access list that will match the inside private IP addresses

To define the access list to match the inside private addresses, use the **access-list** command.

```
Gateway(config)#access-list 1 permit 10.10.10.0 0.0.0.255
```

Step 11: Define the NAT translation from inside list to outside pool

To define the NAT translation, use **the ip nat inside source** command.

```
Gateway(config)#ip nat inside source list 1 pool public_access
```

Step 12: Specify the interfaces

The active interfaces on the router need to be specified as either inside or outside interfaces with respect to NAT. To do this, use the **ip nat inside** or **ip nat outside** command.

```
Gateway(config)#interface fastethernet 0/0
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface serial 0/0/0
Gateway(config-if)#ip nat outside
```

Step 13: Test the configuration

From Host 1 PC, ping 172.16.1.1. Open multiple command prompt windows on each workstation and telnet to the 172.16.1.1 address in each window. When successful, look at the NAT translation on the Gateway router, using the command **show ip nat translations**.

What is the translation of the inside local host addresses?

_________________________________ = _________________________________

The inside global address is assigned by? ___________________________________

The inside local address is assigned by? ____________________________________

Step 14: Verify NAT statistics

To view the NAT statistics type the **show ip nat statistics** command at the privileged EXEC mode prompt.

How many active translations have taken place? __________

How many addresses are in the pool? __________

How many addresses have been allocated so far? __________

Step 15: Reflection

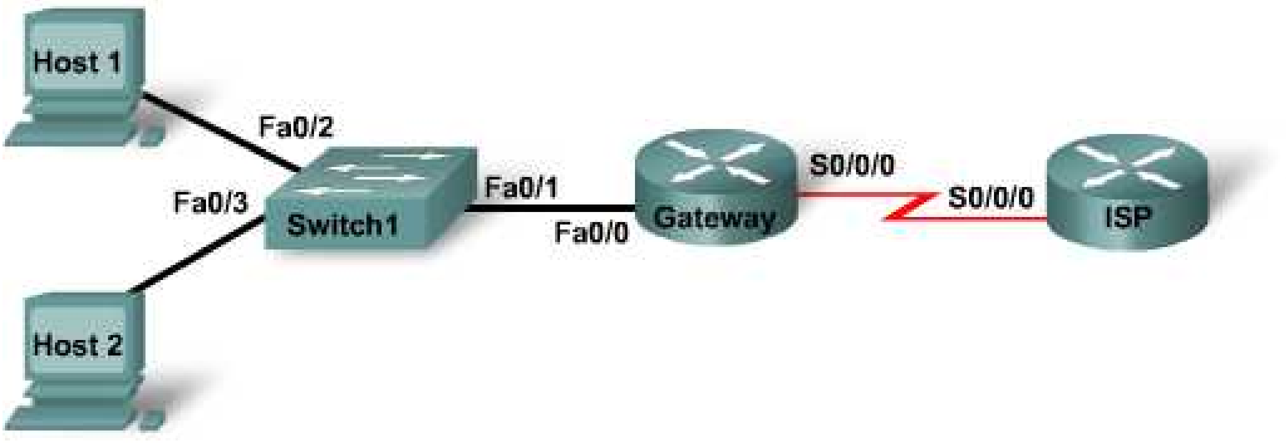
Why would NAT be used in a network? ____

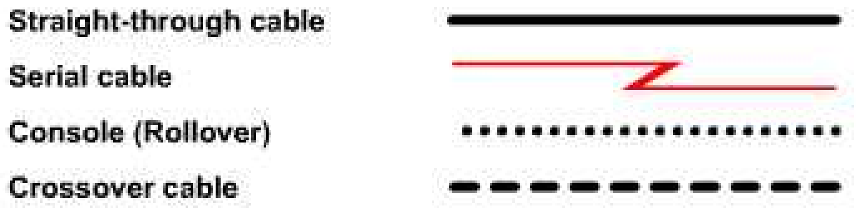
____

____

____

Lab 4.4.4.3 Configure and Verify PAT





Device	Host Name	Fast Ethernet 0/0 Subnet Mask	Interface Type	Serial 0/0/0 Subnet Mask	Loopback 0 Address / Subnet Mask	Enable Secret Password	Enable, vty, and Console Password
Router 1	Gateway	10.10.10.1/24	DTE	209.165.201.33/30		class	cisco
Router 2	ISP	N/A	DCE	209.165.201.34/30	172.16.1.1/32	class	cisco
Switch 1	Switch1					class	cisco

Objectives

- Configure a router to use port address translation (PAT) to convert internal IP addresses, typically private addresses, into outside public addresses.
- Verify connectivity.
- Verify PAT statistics.

Background / Preparation

An ISP has allocated to a company a single IP address, 209.165.201.33, to be used on the Internet connection from the company gateway router to the ISP. A static route will be used between the ISP and the gateway router, and a default route will be used between the gateway and the ISP router. The ISP connection to the Internet will be represented by a loopback address on the ISP router.

In this lab, you will configure the gateway router to use PAT to convert multiple internal addresses into the one usable public address. You will test, view, and verify that the translations are taking place, and you will interpret the NAT/PAT statistics to monitor the process.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two routers, each with a serial connection and one Ethernet interface to connect to the switch
- Two Windows-based PCs, one with a terminal emulation program, and both set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the router and switches
- Three straight-through Ethernet cables to connect from the router to Switch 1 and to connect both hosts to the switch
- One serial cable to connect from Router 1 to Router 2

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router 1 Serial 0/0/0 interface to Router 2 Serial 0/0/0 interface using a serial cable.

b. Connect Router 1 Fa0/0 interface to the Switch 1 Fa0/1 interface using a straight-through cable.

c. Connect a PC with a console cable to perform configurations on the routers and switch.

d. Connect both hosts to ports Fa0/2 and Fa0/3 on the switch using straight-through cables.

Step 2: Perform basic configurations on Router 2

a. Connect a PC to the console port of Router 2 to perform configurations using a terminal emulation program.

b. Configure Router 2 with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 3: Configure the gateway router

Perform basic configuration on Router 1 as the Gateway router with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 4: Configure Switch 1

Configure Switch 1 with a hostname, console, Telnet, and privileged passwords according to the table diagram.

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

Configure each host with the proper IP address, subnet mask, and default gateway. Both hosts should receive IP addresses in the 10.10.10.0/24 network. The default gateway should be the FastEthernet interface IP address of the Gateway router.

Step 6: Verify that the network is functioning

From the attached hosts, ping the FastEthernet interface of the default gateway router.

Was the ping from Host 1 successful? __________

Was the ping from Host 2 successful? __________

If the answer is no for either question, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

Predict: If you attempted to ping the loopback IP address on ISP, would the ping be successful? Explain your answer.

____

____

Step 7: Create a default route

a. From the Gateway router to the ISP router, create a static route to network 0.0.0.0 0.0.0.0, using the **`ip route`** command. This will forward any unknown destination address traffic to the ISP by setting a Gateway of Last Resort on the Gateway router.

```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.34
```

b. View the routing table on the Gateway router to verify the default route.

   Is the static route in the routing table? __________

c. Try to ping from one of the workstations to the ISP serial interface IP address.

   Was the ping successful? __________

   Why? ____

Step 8: Create a static route

a. Create a static route from the ISP to the private network attached to the Gateway router. Use the **`ip route`** command to create the static route.

```
ISP(config)#ip route 10.10.10.0 255.255.255.0 209.165.201.33
```

   Is the static route in the routing table? ____

b. Now that both static and default routes are in place, ping from Host 1 to the loopback address on ISP.

   Is the ping successful? ______

   If the ping is not successful, troubleshoot the router and host configurations and retest.

Step 9: Define the pool of usable public IP addresses

To define the pool of public addresses, use the **`ip nat pool`** command.

```
Gateway(config)#ip nat pool public_access 209.165.201.33 209.165.201.33
netmask 255.255.255.252
```

Step 10: Define an access list that will match the inside private IP addresses

To define the access list to match the inside private addresses, use the **`access-list`** command.

```
Gateway(config)#access-list 1 permit 10.10.10.0 0.0.0.255
```

Step 11: Define the NAT translation from inside list to outside pool

To define the NAT translation, use **`the ip nat inside source`** command.

```
Gateway(config)#ip nat inside source list 1 pool public_access overload
```

Step 12: Specify the interfaces

The active interfaces on the router need to be specified as either inside or outside interfaces with respect to NAT. To do this, use the **`ip nat inside`** or **`ip nat outside`** command.

```
Gateway(config)#interface fastethernet 0/0
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface serial 0/0/0
Gateway(config-if)#ip nat outside
```

Step 13: Generate traffic from Gateway to the ISP

From Host 1 PC, ping 172.16.1.1. Open multiple DOS windows on each workstation and Telnet to the 172.16.1.1 address.

Step 14: Verify that NAT/PAT is working

a. To view the NAT statistics type the **`show ip nat statistics`** command at the privileged EXEC mode prompt on the Gateway router.

How many active translations have taken place? __________

How many addresses are in the pool? __________

How many addresses have been allocated so far? __________

b. When successful, look at the NAT translation on the Gateway router, using the command **show ip nat translations**.

```
Gateway#show ip nat translations
Pro  Inside global      Inside local     Outside local     Outside global
icmp 209.165.201.33:2   10.10.10.10:2    172.16.1.1:2      172.16.1.1:2
icmp 209.165.201.33:3   10.10.10.10:3    172.16.1.1:3      172.16.1.1:3
icmp 209.165.201.33:4   10.10.10.10:4    172.16.1.1:4      172.16.1.1:4
icmp 209.165.201.33:5   10.10.10.10:5    172.16.1.1:5      172.16.1.1:5
icmp 209.165.201.33:6   10.10.10.10:6    172.16.1.1:6      172.16.1.1:6
```

How can you tell that PAT is using a single IP address for all translations? ________________

____

What feature of the translation chart illustrates how PAT is able to keep each data translation separate from the others? ____

____

Step 15: Adjust the Gateway configuration to use an alternate PAT approach

a. Clear the NAT translation table.

```
Gateway#clear ip nat translation *
```

b. Remove the command that created a NAT pool.

```
Gateway(config)#no ip nat pool public_access 209.165.201.33
209.165.201.33 netmask 255.255.255.252
```

c. Remove the command that associated the pool with your ACL.

```
Gateway(config)#no ip nat inside source list 1 pool public_access
overload
```

d. Enter a command that associates the source list with the outside interface.

```
Gateway(config)#ip nat inside source list 1 interface serial 0/0/0
overload
```

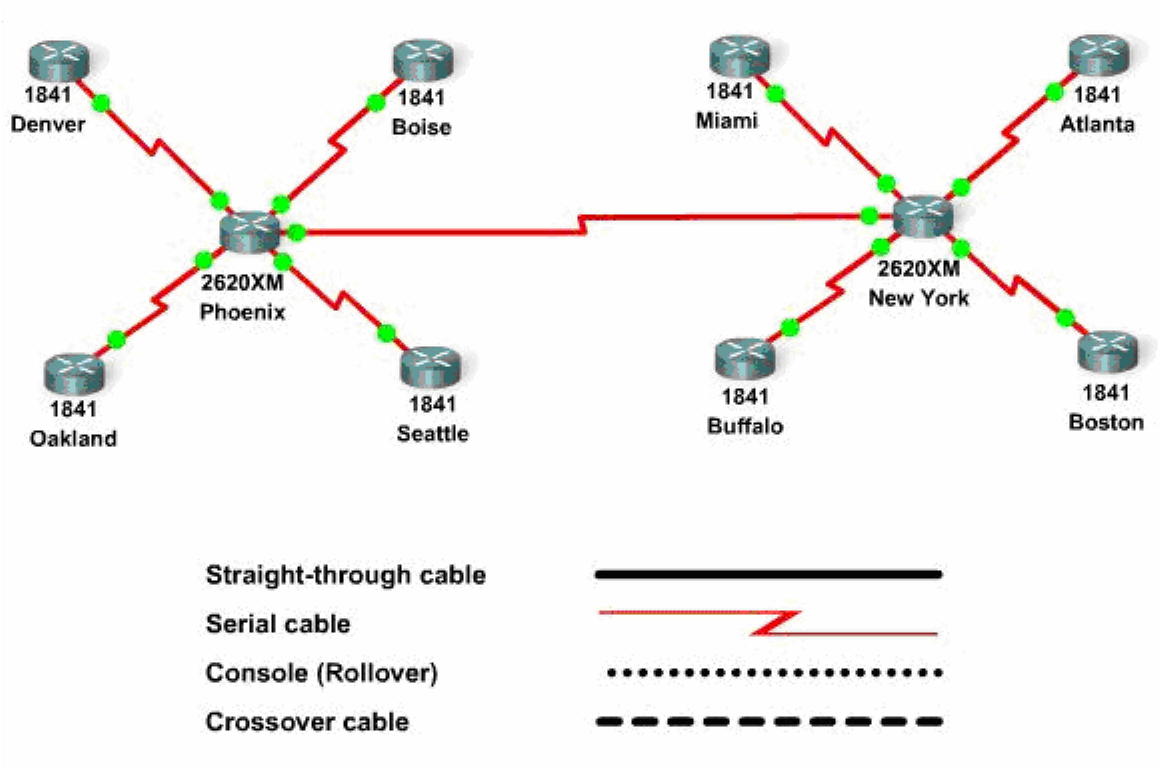
e. Verify that this alternate approach works by generating traffic from the hosts to the loopback, and then by using the **show ip nat statistics** and **show ip nat translations** commands. Results should be similar to those achieved using the NAT pool.

Step 16: Reflection

What advantages does PAT provide? ____

____

Lab 5.1.2.4 Designing and Creating a Redundant Network



Objective

- Create an efficient and reliable network design with redundancy

Background / Preparation

Recently the New York router failed and the entire east coast operations lost 16 hours of production. The estimated cost of the outage was $600,000. The network engineering office has been provided additional money to create a more redundant network in an attempt to minimize future outages.

The head of design office has tasked you as the lead designer. With a budget of $5400 for monthly fees, you must meet the following design requirements.

- A minimum of three T-1 links must connect the east and west coast operations.
- Each router must have at least one 64 Kbps redundant link.
- Each router must also have at least two paths between the east and west coast operations.
- The failure of one device should not affect the connectivity of another site.

The east coast consist of the New York, Miami, Atlanta, Boston, and Buffalo routers, while the west coast consist of the Phoenix, Denver, Boise, Seattle, and Oakland routers.

Cost for new circuits:
$400 month – 64 Kbps circuit
$1900 month - 1.544 Mbps (T-1) circuit

Step 1: Determine the minimum number of links to meet the requirements

a. Identify the two links to meet requirement 1.

b. Determine the cost of those two links.

c. Identify the required links to meet requirement 2, 3, and 4.

d. Determine if the design is within budget.

Step 2: Implement the design

a. Using Packet Tracer, create the network including the redundant links specified in Step 1.

Step 3: Verify the design

a. Do three paths between the east and west coast operations exist?

b. Does each site have at least two links?

c. Does each site on the east coast have two paths to the west coast?

d. Does each site on the west coast have two paths to the east coast?

e. Will one device failure affect multiple sites?

Reflection

a. What network topology was implemented before adding redundancy?

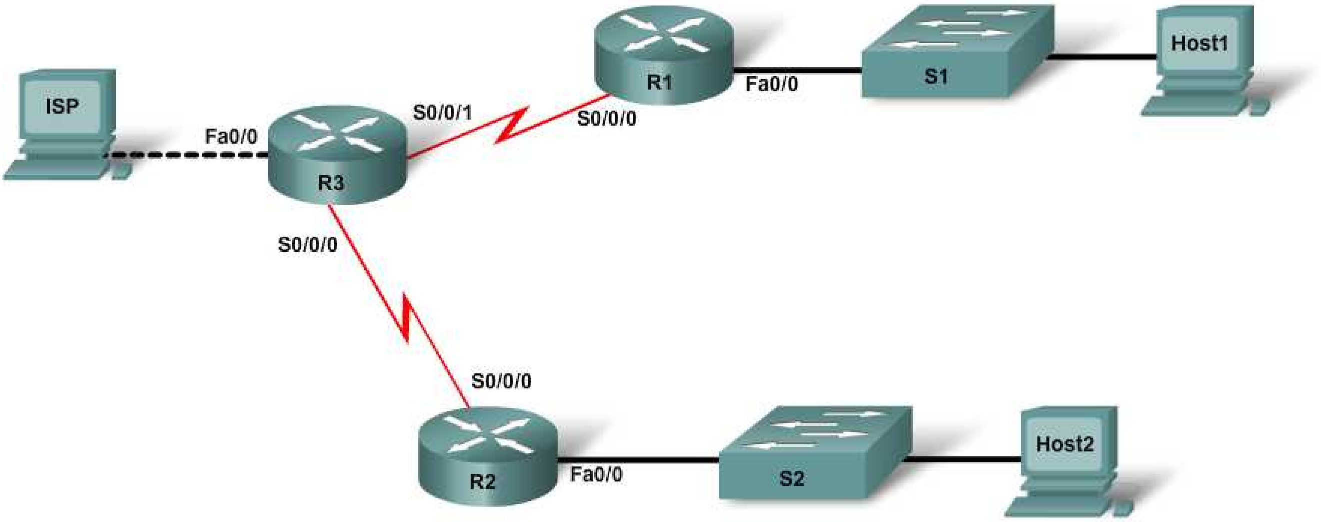
b. What network topology is now implemented after adding redundancy?

c. What is an advantage to using the topology implemented after adding redundancy?

d. What is a disadvantage to using the topology implemented after redundancy was added?

e. Why would a company, such as the one in this case, suddenly decide to implement the type of topology used in step b?

Lab 5.2.3 Configuring RIPv2 with VLSM, and Default Route Propagation



Device	Host Name	Interface Fa0/0 / Subnet Mask	Interface S0/0/0 / Subnet Mask	Interface S0/0/1 / Subnet Mask	Serial Interface Type	Default Gateway	Enable Secret Password	VTY, Console Password
Router1	R1	172.16.1.1/24	172.16.3.1/30	N/A	DTE		class	cisco
Router2	R2	172.16.2.1/24	172.16.3.5/30	N/A	DTE		class	cisco
Router3	R3	209.165.201.1 /24	172.16.3.6/30	172.16.3.2/30	DCE		class	cisco
Switch1	S1						class	cisco
Switch2	S2						class	cisco
PC 1	Host1	172.16.1.2/24				172.16.1.1/24		
PC 2	Host2	172.16.2.2/24				172.16.2.1/24		
PC 3	ISP	209.165.201.2 /24				209.165.201.1/ 24		

Objectives

- Configure a three-router topology using VLSM.
- Configure RIP version 2 as the routing protocol.
- Configure and propagate a default route through RIP.

Background / Preparation

Set up a network similar to the one in the topology diagram. This lab presents a three-router corporate network using variably-subnetted private IP addressing. From one router, a public network connection to a host PC simulates the corporate network's Internet connection. You will configure RIPv2 as the routing protocol for the corporate network, and a pathway for Internet traffic will be established through a default route.

The following resources are required:

- Three Cisco 1841 routers or comparable routers
- Two Cisco 2960 switches or other comparable switches
- Three Windows-based PCs, at least one with a terminal emulation program
- Minimum of one RJ-45-to-DB-9 connector console cable
- Two serial cables to connect R3 to both R1 and R2
- One crossover Ethernet cable (PC3 to R3)
- Four straight-through Ethernet cables (PC1 to S1, PC2 to S2, S1 to R1, and S2 to R2)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers - If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment.

a. Connect Router3 to Router1 and Router2 with serial cables.

b. Connect Router1's Fa0/0 interface with a straight-through cable to Switch1's Fa0/1 interface.

c. Connect Router2's Fa0/0 interface with a straight-through cable to Switch2's Fa0/1 interface

d. Connect PC1 to Switch1 and PC2 to Switch 2 with straight-through cables.

e. Connect PC3 to Router3's Fa0/0 interface with a crossover cable.

f. Connect a PC with a console cable to perform configurations on the routers and switches.

Step 2: Perform basic configurations on the routers.

a. Establish a console session with Router1 and configure hostname, passwords, and interfaces as described in the table. Save the configuration.

b. Establish a console session with Router2 and perform a similar configuration, using the addresses and other information from the table. Save the configuration.

c. Establish a console session with Router3. Configure hostname, passwords, and interfaces according to the table. Note that both serials are DCE on this router. Save the configuration.

Step 3: Perform basic configurations on the switches.

a. Establish a console session with Switch1 and configure hostname and passwords according to the table. Save the configuration.

b. Perform a similar configuration on Switch2, configuring the hostname and passwords as described for S1. Save the configuration.

Step 4: Configure the hosts with the proper IP address, subnet mask, and default gateway.

a. Configure each host with the proper IP address, subnet mask, and default gateway. Host1 should be assigned 172.16.1.2/24 and Host 2 should be assigned 172.16.2.2 /24. Host3, which is used to simulate Internet access, should be assigned 209.165.201.2/24. All three PCs use their attached router's Fa0/0 interface as the default gateway.

b. Each workstation should be able to ping the attached router. If the ping was not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 5: Configure RIP v2 routing

a. On R1, configure RIP version 2 as the routing protocol and advertise the appropriate networks:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 172.16.1.0
R1(config-router)#network 172.16.3.0
```

Predict: how will RIP report these subnets in the routing table?

____

b. From the network commands, which interfaces are participating in RIP routing? _____________

c. Perform a similar configuration on R2, setting the version, advertising the appropriate networks, and turning off auto-summarization

d. On R3, perform a similar configuration. Do not advertise the 209.165.201.0/24 network.

Step 6: Configure and redistribute a default route for Internet access.

a. From the R3 router to the host simulating the Internet, create a static route to network 0.0.0.0 0.0.0.0, using the **ip route** command. This will forward any unknown-destination address traffic to the PC simulating the Internet by setting a Gateway of Last Resort on the R3 router.

```
R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

b. R3 will advertise this route to the other routers if this command is added to its RIP configuration:

```
R3(config)#router rip
R3(config-router)#default-information originate
```

Step 7: Verify the routing configuration.

a. View the routing table on R3:

```
R3#show ip route
<<output omitted>>
Gateway of last resort is 209.165.201.2 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 4 subnets
R       172.16.1.0 [120/1] via 172.16.3.1, 00:00:17, Serial0/0/0
R       172.16.2.0 [120/1] via 172.16.3.5, 00:00:12, Serial0/0/1
C       172.16.3.0 is directly connected, Serial0/0/0
C       172.16.3.4 is directly connected, Serial0/0/1
C    209.165.201.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 209.165.201.2
```

How can you tell from the routing table that the subnetted network shared by R1, R2 and R3 has a pathway for Internet traffic?

b. View the routing tables on R2 and R1.

How is the pathway for Internet traffic provided in their routing tables?

Step 8: Verify connectivity.

a. Simulate sending traffic to the Internet by pinging from the host PCs to 209.165.201.2.

Were the pings successful? _____

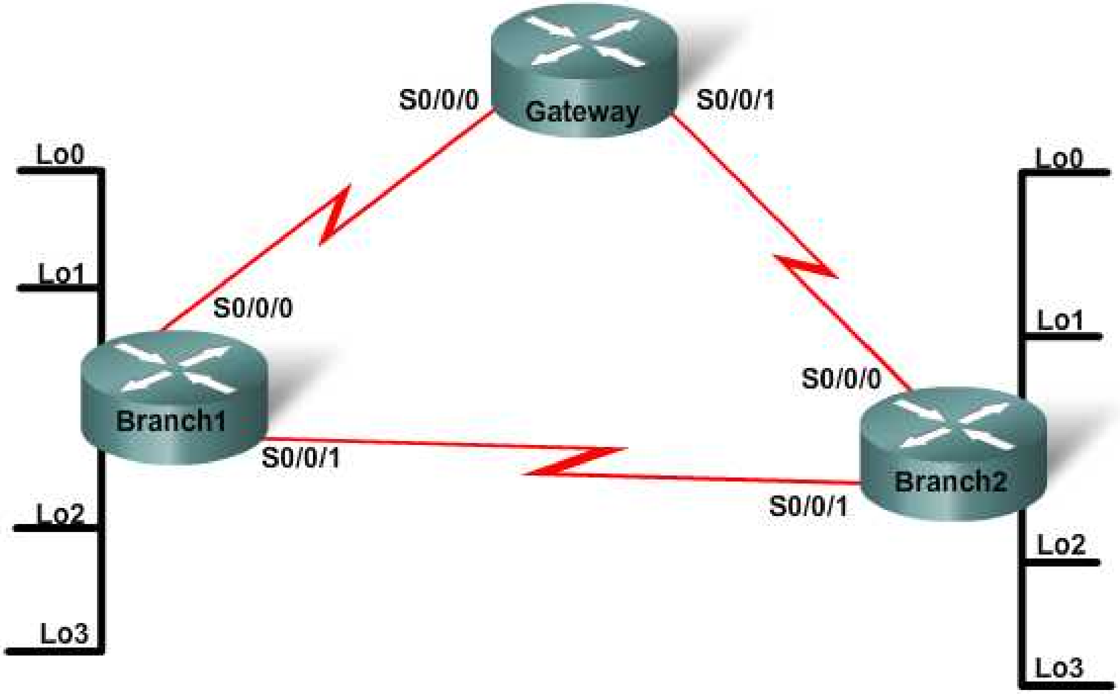
b. Verify that hosts within the subnetted network can reach each other by pinging between Host1 and Host2.

Were the pings successful? _____

Step 9: Reflection.

a. How did R1 and R2 learn the pathway to the Internet for this network?

Lab 5.4.1.4 Implementing EIGRP



Device	Host Name	Loopback Interfaces / Subnet Masks	Interface S0/0/0 / Subnet Mask	Serial Interface Type	Interface S0/0/1 / Subnet Mask	Serial Interface Type	Enable Secret Password	vty, Console Password
Router1	Gateway	N/A	10.0.0.1/30	DCE	10.0.0.5/30	DCE	class	cisco
Router2	Branch1	Lo0 172.16.0.1/24 Lo1 172.16.1.1/24 Lo2 172.16.2.1/24 Lo3 172.16.3.1/24	10.0.0.2/30	DTE	10.0.0.9/30	DCE	class	cisco
Router3	Branch2	Lo0 172.17.0.1/24 Lo1 172.17.1.1/24 Lo2 172.17.2.1/24 Lo3 172.17.3.1/24	10.0.0.6/30	DTE	10.0.0.10/30	DTE	class	cisco

Objectives

- Configure a three-router topology with EIGRP and MD5 authentication.
- Verify EIGRP configuration and route table population.

Background / Preparation

Set up a network similar to the one in the diagram. This lab presents a two-router corporate network using four Class C private networks. Each router has one LAN attached to a Fast Ethernet interface. There are two serial connections between the two routers.

The following resources are required:

- Two Cisco 1841 or comparable routers (must have at least 1 Ethernet and 2 serial ports)
- Two Cisco 2960 switches or other comparable switches
- Two Windows-based PCs, each with a terminal emulation program
- Two RJ-45-to-DB-9 connector console cables
- Two serial cables to connect Router1 to Router2
- Four straight-through Ethernet cables (PC1 to Switch1, PC2 to Switch2, Switch1 to R1, and Switch2 to Router2)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router1 to Router2 and Router3 using serial cables.

b. Connect Router2 to Router3 using serial cables.

c. Connect a PC with a console cable to perform configurations on the routers.

Step 2: Perform basic configurations on the routers

a. Establish a console session with Router1 and configure hostname, passwords, and interfaces as described in the table. Save the configuration.

b. Establish a console session with Router2 and perform a similar configuration, using the addresses and other information from the table. Save the configuration.

c. Establish a console session with Router3. Configure hostname, passwords, and interfaces according to the table. Save the configuration.

Step 3: Configure EIGRP routing with default commands

a. On Gateway, configure EIGRP as the routing protocol with an autonomous system number of 100, and advertise the appropriate networks.

```
Gateway(config)#router eigrp 100
Gateway(config-router)#network 10.0.0.0
Gateway(config-router)#network 10.0.0.4
```

Predict: How will EIGRP report these subnets in the routing table?

____

____

b. On Branch1, configure EIGRP as the routing protocol with an autonomous system number of 100, and advertise the appropriate networks:

```
Branch1(config)#router eigrp 100
Branch1(config-router)#network 10.0.0.0
Branch1(config-router)#network 10.0.0.8
Branch1(config-router)#network 172.16.0.0
Branch1(config-router)#network 172.16.1.0
Branch1(config-router)#network 172.16.2.0
Branch1(config-router)#network 172.16.3.0
```

c. Perform a similar configuration on Branch2, using EIGRP 100 and advertising the appropriate networks.

Step 4: Configure MD5 Authentication

a. Create a keychain named **discchain.**

b. Configure a key 1 that has a key string of **san-fran**.

c. Enable the workgroup router to utilize EIGRP MD5 authentication with each of your EIGRP neighbors and to use the keychain **icndchain**.

```
Branch1(config)#key chain discchain
Branch1(config-keychain)#key 1
Branch1(config-keychain-key)#key-string san-fran
Branch1(config-keychain-key)#end
Branch1#config terminal
Branch1(config)#interface serial0/1/1
Branch1(config-if)#ip authentication mode eigrp 100 md5
Branch1(config-if)#ip authentication key-chain eigrp 100 discchain
(repeat for all routers on all necessary interfaces)
```

d. Look at the contents of the Router1 routing table to ensure all routing updates are being accepted.

```
Gateway#show ip route
```

List the routes that are shown:

____

____

____

____

Step 5: Reflection

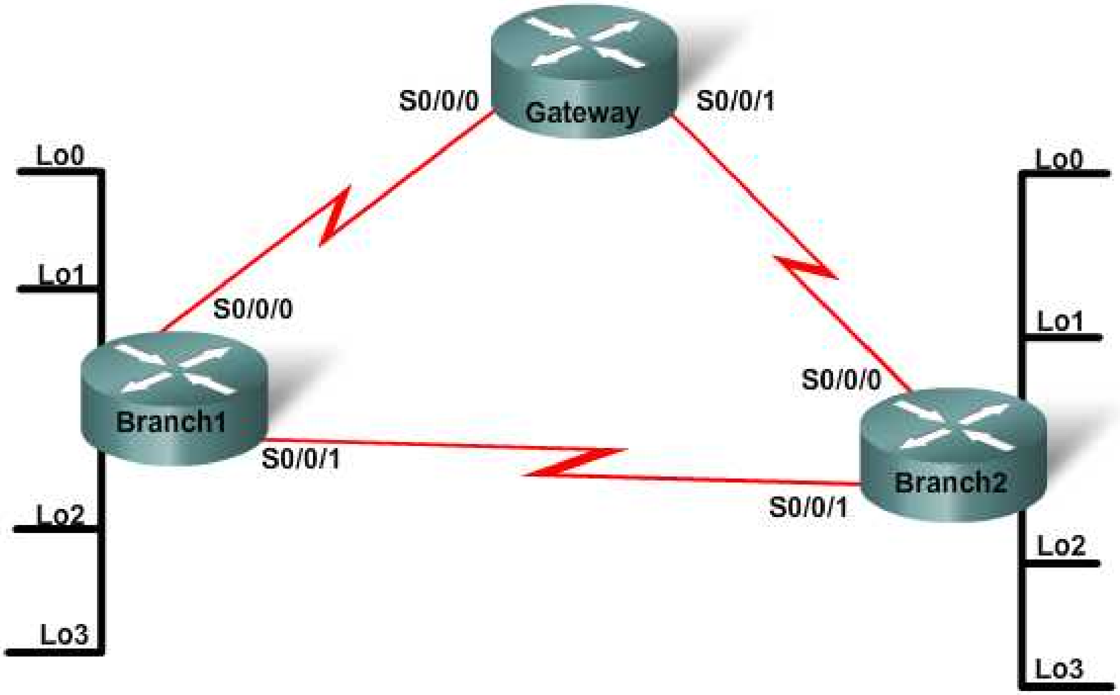
a. What is the importance of enabling authentication on the routing updates?

____

____

____

Lab 5.4.2.4 EIGRP Configuring Automatic and Manual Route Summarization and Discontiguous Subnets



Device	Host Name	Loopback Interfaces / Subnet Masks	Interface S0/0/0 / Subnet Mask	Serial Interface Type	Interface S0/0/1 / Subnet Mask	Serial Interface Type	Enable Secret Password	vty, Console Password
Router1	Gateway	N/A	10.0.0.1/30	DCE	10.0.0.5/30	DCE	class	cisco
Router2	Branch1	Lo0 172.16.0.1/24 Lo1 172.16.1.1/24 Lo2 172.16.2.1/24 Lo3 172.16.3.1/24	10.0.0.2/30	DTE	10.0.0.9/30	DCE	class	cisco
Router3	Branch2	Lo0 172.17.0.1/24 Lo1 172.17.1.1/24 Lo2 172.17.2.1/24 Lo3 172.17.3.1/24	10.0.0.6/30	DTE	10.0.0.10/30	DTE	class	cisco

Objectives

- Configure a three-router topology with discontiguous subnets using EIGRP with automatic summarization.
- Disable auto-summarization and configure a manual summarization.
- Observe and interpret the results in the routing table.

Background / Preparation

Set up a network similar to the one in the topology diagram. This lab presents a three-router corporate network using variably subnetted private IP addressing. On Branch1and Branch2, loopbacks simulate LANs attached to those routers. The design creates discontiguous subnets on the routers which will be “hidden” when EIGRP is configured with automatic summarization as the default. You will disable automatic summarization and configure manual summarization to verify that the routers share subnet information.

The following resources are required:

- Three Cisco 1841 routers or comparable routers
- At least one PC with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable
- Serial cables to connect R1 to both R2 and R3, and to connect R2 to R3

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router1 to Router2 and Router3 using serial cables.

b. Connect Router2 to Router3 using serial cables.

c. Connect a PC with a console cable to perform configurations on the routers.

Step 2: Perform basic configurations on the routers

a. Establish a console session with Router1 and configure hostname, passwords, and interfaces as described in the table. Save the configuration.

b. Establish a console session with Router2 and perform a similar configuration, using the addresses and other information from the table. Save the configuration.

c. Establish a console session with Router3. Configure hostname, passwords, and interfaces according to the table. Save the configuration.

Step 3: Configure EIGRP routing with default commands

a. On Gateway, configure EIGRP as the routing protocol with an autonomous system number of 100, and advertise the appropriate networks.

```
Gateway(config)#router eigrp 100
Gateway(config-router)#network 10.0.0.0
Gateway(config-router)#network 10.0.0.4
```

Predict: How will EIGRP report these subnets in the routing table?

b. On Branch1, configure EIGRP as the routing protocol with an autonomous system number of 100, and advertise the appropriate networks:

```
Branch1(config-router)#network 10.0.0.0 0.0.0.3
Branch1(config-router)#network 10.0.0.8 0.0.0.3
Branch1(config-router)#network 172.16.0.0 0.0.0.255
Branch1(config-router)#network 172.16.1.0 0.0.0.255
Branch1(config-router)#network 172.16.2.0 0.0.0.255
Branch1(config-router)#network 172.16.3.0 0.0.0.255
```

c. Perform a similar configuration on Branch2, using EIGRP 100 and advertising the appropriate networks.

Step 4: Verify the routing configuration

View the routing table on Gateway.

```
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:02:33, Null0
C       10.0.0.0/30 is directly connected, Serial0/0/0
C       10.0.0.4/30 is directly connected, Serial0/0/1
D       10.0.0.8/30 [90/2681856] via 10.0.0.6, 00:03:19, Serial0/0/1
                    [90/2681856] via 10.0.0.2, 00:02:34, Serial0/0/0
D    172.16.0.0/16 [90/2297856] via 10.0.0.2, 00:02:09, Serial0/0/0
D    172.17.0.0/16 [90/2297856] via 10.0.0.6, 00:03:15, Serial0/0/1
```

Which subnets are not reported in this output?

Why are there two paths reported for the 10.0.0.8/30 route?

Step 5: Remove Automatic summarization

On each of the three routers, remove automatic summarization to force EIGRP to report all subnets. A sample command is given for Gateway.

```
Gateway(config)#router eigrp 100
Gateway(config-router)# no auto-summary
```

Step 6: Verify the routing configuration

View the routing table again on Gateway.

```
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:01:02, Null0
C       10.0.0.0/30 is directly connected, Serial0/0/0
C       10.0.0.4/30 is directly connected, Serial0/0/1
D       10.0.0.8/30 [90/2681856] via 10.0.0.6, 00:00:09, Serial0/0/1
                    [90/2681856] via 10.0.0.2, 00:00:09, Serial0/0/0
```

```
          172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
     D       172.16.0.0/16 is a summary, 00:01:02, Null0
     D       172.16.0.0/24 [90/2297856] via 10.0.0.2, 00:00:09, Serial0/0/0
     D       172.16.1.0/24 [90/2297856] via 10.0.0.2, 00:00:09, Serial0/0/0
     D       172.16.2.0/24 [90/2297856] via 10.0.0.2, 00:00:09, Serial0/0/0
     D       172.16.3.0/24 [90/2297856] via 10.0.0.2, 00:00:09, Serial0/0/0
          172.17.0.0/16 is variably subnetted, 5 subnets, 2 masks
     D       172.17.0.0/16 is a summary, 00:01:02, Null0
     D       172.17.0.0/24 [90/2297856] via 10.0.0.6, 00:00:09, Serial0/0/1
     D       172.17.1.0/24 [90/2297856] via 10.0.0.6, 00:00:09, Serial0/0/1
     D       172.17.2.0/24 [90/2297856] via 10.0.0.6, 00:00:09, Serial0/0/1
     D       172.17.3.0/24 [90/2297856] via 10.0.0.6, 00:00:09, Serial0/0/1
```

Are all subnets represented in the table? __________

What kind of interface is “Null0”? ____

Step 7: Configure manual summarization

On Branch2, configure manual summarization to force EIGRP to summarize only the 172.17.0.0 subnets.

```
Branch2(config)#interface s0/0/0
Branch2(config-if)#ip summary-address eigrp 100 172.17.0.0
255.255.252.0
Branch2(config)#interface s0/0/1
Branch2(config-if)#ip summary-address eigrp 100 172.17.0.0
255.255.252.0
```

View the routing tables of Branch1 and Gateway again. Describe the effect that these summary commands have on the routing tables.

____

____

Step 7: Reflection

a. Although removing automatic summarization solved the issue of missing subnets, what possible problem could it cause?

____

____

b. How could removing automatic summarization help in troubleshooting an EIGRP network?

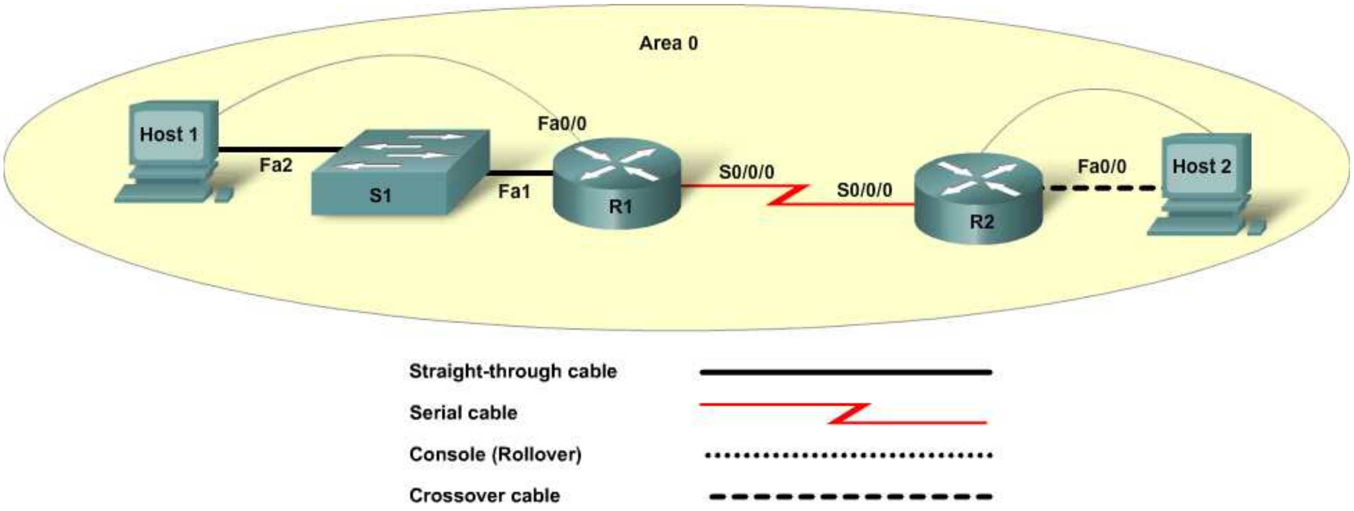
____

____

c. How did the use of loopback interfaces make this lab easier to complete?

____

Lab 6.2.1 Configuring and Verifying Single Area OSPF



Device	Host Name	Fast Ethernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Network Statements	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.129/26	192.168.15.1/30	DCE	192.168.1.128 192.168.15.0	class	cisco
Router 2	R2	192.168.0.1/24	192.168.15.2/30	DTE	192.168.15.0 192.168.0.0	class	cisco
Switch 1	S1					class	cisco

Objectives

- Set up an IP addressing scheme for OSPF Area 0.
- Configure and verify OSPF routing.
- View the routing table.
- Verify connectivity.

Background / Preparation

In this lab, you will cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed in the addressing table may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to 1841 routers. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two routers, each with a serial connection and an Ethernet interface
- Two Windows-based PCs, each with a terminal emulation program, and each set up as a host
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Two straight-through Ethernet cables
- One crossover Ethernet cable
- One 2-part (DTE/DCE) serial cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router 1 Serial 0/0/0 interface to Router 2 Serial 0/0/0 interface using a serial cable.

b. Connect Router 1 Fa0/0 interface to Switch 1 Fa0/1 port using a straight-through cable.

c. Connect each PC with a console cable to perform configurations on the router and switches.

d. Connect Host 1 to the Switch 1 Fa0/2 port using a straight-through cable.

e. Connect a crossover cable between Host 2 and the Fa0/0 interface of Router 2.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. Configure Router 1 with a hostname, interfaces, console, Telnet, IP addresses, and privileged passwords according to the table and topology diagram. Save the configuration.

Step 3: Perform basic configuration on Router 2

Perform basic configuration on Router 1 as the gateway router with a hostname, interfaces, console, Telnet, and privileged passwords according to the table and topology diagram. Save the configuration.

Step 4: Perform basic configuration on Switch 1

Configure Switch 1 with a hostname, console, Telnet, and privileged passwords according to the table and topology diagram.

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway.

1) Host 1 should be assigned 192.168.1.130/26 and the default gateway of 192.168.1.129.

2) Host 2 should be assigned 192.168.0.2/24 and the default gateway of 192.168.0.1.

b. Each workstation should be able to ping the attached router. If the ping was not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Verify that the network is functioning

a. From the attached hosts, ping the FastEthernet interface of the default gateway router.

Was the ping from the first host successful? ____________________

Was the ping from the second host successful? _________________

If the answer is no for either question, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

b. Use the command **`show ip interface brief`** and check the status of each interface.

What is the state of the interfaces on each router?

R1:

FastEthernet 0/0: __________________

Serial 0/0/0: ________________________

Serial 0/0/1: ________________________

R2:

FastEthernet 0/0: __________________

Serial 0/0/0: ________________________

Serial 0/0/1: ________________________

c. Ping from one of the router connected serial interfaces to the other connected serial interface.

Was the ping successful? __________

If the answer is no, troubleshoot the router configurations to find the error. Ping again until successful.

Step 7: Configure OSPF routing on R1

a. Configure an OSPF routing process on router R1. Use OSPF process number 1 and ensure that all networks are in Area 0.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.128 0.0.0.63 area 0
R1(config-router)#network 192.168.15.0 0.0.0.3 area 0
R1(config-router)#end
```

b. Examine the router running configuration.

Did the IOS automatically add any lines under the **`router ospf 1`** command? __________

If so, what did it add? ____

c. If there were no changes to the running configuration, enter the following commands:

```
R1(config)#router ospf 1
R1(config-router)#log-adjacency-changes
R1(config-router)#end
```

d. Show the routing table for R1.

```
R1#show ip route
```

Are there any OSPF entries in the routing table now? __________

Why? ____

Step 8: Configure OSPF routing on R2

a. Configure an OSPF routing process on router R2. Use OSPF process number 1 and ensure that all networks are in Area 0.

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.0.0 0.0.0.255 area 0
R2(config-router)#network 192.168.15.0 0.0.0.3 area 0
R2(config-router)#end
```

b. Examine the R2 running configuration.

Did the IOS automatically add any lines under the **`router ospf 1`** command? __________

If so, what did it add? ____

c. If there were no changes to the running configuration, enter the following commands:

```
R2(config)#router ospf 1
R2(config-router)#log-adjacency-changes
R2(config-router)#end
```

d. Show the routing table for R2.

```
R2#show ip route
```

Are there any OSPF entries in the routing table now? __________

What is the metric value of the OSPF route to R1 Ethernet network 192.168.1.128?

____

____

What is the VIA address in the OSPF route? ___________________________________

Are routes to all networks shown in the routing table? __________

What does the **O** mean in the first column of the routing table?

____

Step 8: Test network connectivity

Ping Host 2 from Host 1.

Was it successful? __________

If the answer is no, troubleshoot to find the error. Ping again until successful.

Step 9: Reflection

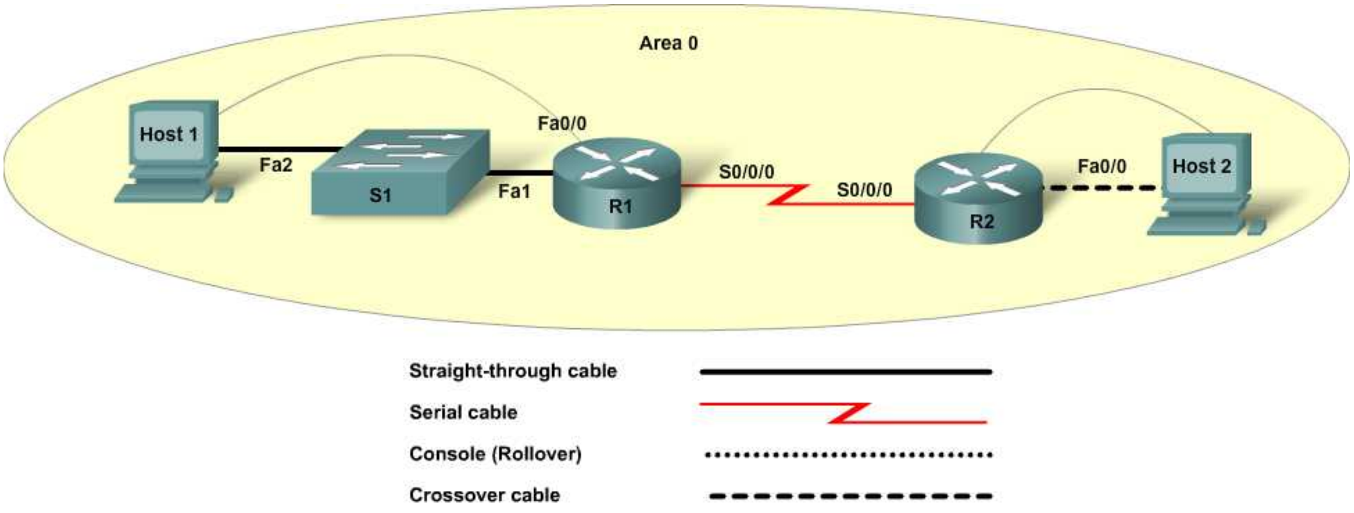
a. What is an advantage of using OSPF as the routing protocol in a network?

____

b. What is a disadvantage of using OSPF as the routing protocol in a network?

____

Lab 6.2.2 Configuring OSPF Authentication



Device	Host Name	Fast Ethernet 0/0 / NIC Address	Serial 0/0/0 Address	Serial 0/0/0 Interface Type	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.0.1/24	192.168.2.1/30	DCE	cisco	class
Router 2	R2	192.168.1.1/24	192.168.2.2/30	DTE	cisco	class
Switch 1	S1				cisco	class
Host 1		192.168.0.10				
Host 2		192.168.1.10				

Objectives

- Perform basic router configuration.
- Perform basic single area OSPF configuration.
- Configure OSPF authentication.
- Verify OSPF authentication.

Background / Preparation

In this lab, you will cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed in the addressing table may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, or any combination can be used.

The information in this lab applies to 1841 routers. Other routers may be used; however, command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two routers. each with a serial connection and an Ethernet interface
- Two Windows-based PCs, each with a terminal emulation program, and each set up as a host
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Two straight-through Ethernet cables
- One crossover Ethernet cable
- One 2-part (DTE/DCE) serial cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router 1 Serial 0/0/0 interface to Router 2 Serial 0/0/0 interface using a serial cable.

b. Connect Router 1 Fa0/0 interface to Switch 1 Fa0/1 port using a straight-through cable.

c. Connect each PC with a console cable to perform configurations on the router and switches.

d. Connect Host 1 to the Switch 1 Fa0/2 port using a straight-through cable.

e. Connect a crossover cable between Host 2 and the Fa0/0 interface of Router 2.

Step 2: Perform basic configuration on the routers

a. Connect a PC to the console port of the routers to perform configurations using a terminal emulation program.

b. Configure Router 1 with a hostname, console, Telnet, and privileged passwords according to the table diagram.

c. Configure Router 2 with a hostname, console, Telnet, and privileged passwords according to the table diagram.

Step 3: Configure and verify OSPF on the routers

a. Configure single area OSPF on R1 and R2. All interfaces will belong to Area 0.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.0.0 0.0.0.255 area 0
R1(config-router)#network 192.168.2.0 0.0.0.3 area 0
R1(config-router)#end

R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#network 192.168.2.0 0.0.0.3 area 0
R2(config-router)#end
```

b. Verify the OSPF configuration using the **show ip route** command on both routers.

```
R1#show ip route

R2#show ip route
```

Does the 192.168.1.0/24 network appear in the routing table of R1? __________

Does the 192.168.0.0/24 network appear in the routing table of R2? __________

Step 4: Configure and verify OSPF authentication

OSPF allows for both plain text authentication and encrypted authentication. Because plain text authentication is as insecure as having no authentication, Message Digest 5 (MD5) authentication is used.

Configuring OSPF authentication is a two-step process. First, it is enabled on a router for an area, and then it is configured on the interfaces in that area.

a. Enable MD5 authentication in Area 0 on both routers.

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest

R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
```

b. Enable OSPF authentication on S0/0/0 of R1.

```
R1(config)#interface s0/0/0
R1(config-if)#ip ospf message-digest-key 10 md5 secretpassword
```

c. Using the **show ip ospf neighbor** command, view the neighbors known to R1.

```
R1#show ip ospf neighbor
```

Does R1 show any OSPF neighbors?

____

Why or why not?

____

d. Watch the terminal output from R1 for several seconds.

What OSPF message was displayed when the MD5 authentication was set on R1 S0/0/0?

____

e. Enable OSPF authentication on S0/0/0 of R2.

```
R2(config)#interface s0/0/0
R2(config-if)#ip ospf message-digest-key 10 md5 secretpassword
```

f. Now, recheck the neighbour status between R1 and R2.

```
R1#show ip ospf neighbor
```

Do R1 and R2 have a neighbor relationship established now? __________

What OSPF console message did you see after the MD5 authentication was set on R2 S0/0?

____

g. Ping from Host 1 to Host 2 to verify connectivity.

Can Host 1 ping Host 2? __________

Step 5: Reflection

a. Why would OSPF authentication be configured in a network?

____

____

____

____

b. Can one OSPF area have different OSPF configuration parameters than another area?

____

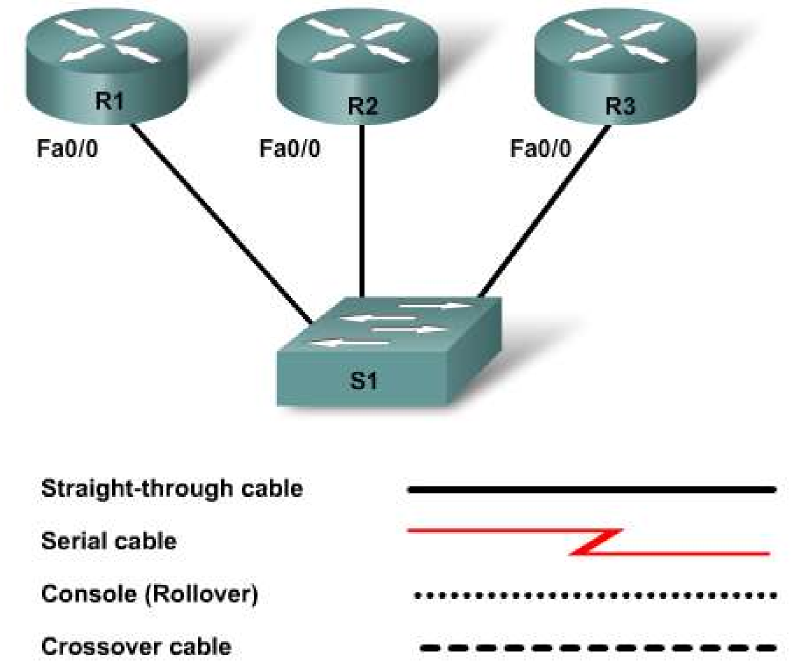
____

c. Can a single OSPF router have multiple authentication passwords configured?

____

____

Lab 6.2.3 Controlling a DR/BDR Election



Device	Fast Ethernet 0/0 IP Address	Loopback0 IP Address	Network Statements
R1	192.168.1.1/24	10.0.3.1/32	192.168.1.0
R2	192.168.1.2/24	10.0.2.1/32	192.168.1.0
R3	192.168.1.3/24	10.0.1.1/32	192.168.1.0

Objectives

- Configure OSPF routing on all routers.
- Verify OSPF routing using **show** commands.
- Configure loopback addresses to dictate DR/BDR election.
- Verify DR/BDR election.

Background / Preparation

This lab focuses on the configuration of multiple OSPF routers attached to a muti-access Ethernet network to control the outcome of the DR/BDR election. The lab uses Cisco IOS commands.

Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to 1841 routers. Other routers may be used; however, command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0, Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. Any Cisco Catalyst switch may be utilized. The default configuration of the switch will perform properly for this exercise.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Three Cisco routers with at least 1 FastEthernet interface (preferably the same model number and IOS version)
- One Windows-based PC with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the routers
- Three straight-through Ethernet cables to connect the routers to the switch

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

Connect each of the router Fa0/0 interfaces to any port on the switch using a straight-through cable.

Step 2: Perform basic configuration on the routers.

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. Configure Routers 1, 2, and 3 with a hostname, and console, Telnet, and privileged passwords according to the table diagram.

Step 3: Configure single area OSPF routing on the routers

Configure basic OSPF routing on the routers. All networks are in Area 0.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0

R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0

R3(config)#router ospf 1
R3(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

Step 4: Verify current OSPF operation

a. Now that the Ethernet interfaces and OSPF have been configured, OSPF should be operational between the routers. Because this is a multi-access network, a DR/BDR election should have occurred.

b. Use the **show ip ospf neighbor** command on all the routers to verify operation. The output should be similar to what is shown below.

```
R1#show ip ospf neighbor

Neighbor ID   Pri   State       Dead Time   Address        Interface
192.168.1.2     1   FULL/BDR    00:00:38    192.168.1.2    FastEthernet0/0
192.168.1.3     1   FULL/DR     00:00:35    192.168.1.3    FastEthernet0/0
```

Do all routers show that they have established a neighbor relationship with the other routers?

____

c. Use the **show ip ospf neighbor detail** command on R1 to determine which routers are the DR and BDR.

Which router is the DR? ___________

Which router is the BDR? __________

What factor determined which router was the DR and which was the BDR in this scenario?

____

Step 5: Configure router loopback interfaces

a. Configuring loopback interfaces for OSPF operation serves two purposes:

1) Because loopback interfaces are logical interfaces and never go down, it ensures that the router ID will never change.

2) Configuring loopback interfaces allows control over the DR/BDR election.

b. Configure the loopback interfaces as shown in the addressing table on the first page.

```
R1(config)#interface loopback 0
R1(config-if)#ip address 10.0.3.1 255.255.255.255
R1(config-if)#end

R2(config)#interface loopback 0
R2(config-if)#ip address 10.0.2.1 255.255.255.255
R2(config-if)#end

R3(config)#interface loopback 0
R3(config-if)#ip address 10.0.1.1 255.255.255.255
R3(config-if)#end
```

c. Use the **show ip ospf neighbor detail** command on R1 to view the DR/BDR status.

Have the DR and BDR routers changed? __________

d. Once elected, the DR and the BDR do not change unless the interfaces all cycle or the OSPF processes are reset. Use the **clear ip ospf 1 process** command on all routers to reset the OSPF processes.

NOTE: If the **clear ip osfp 1 process** command does not result in the loopback addresses determining the router ID and DR/BDR status, use the **reload** command from the privileged EXEC prompt on each router. Be sure to save the configuration on each router before issuing the **reload** command.

e. After the processes have been reset, use the **show ip ospf neighbor detail** command to recheck the DR/BDR status.

```
R1#show ip ospf neighbor detail
 Neighbor 10.0.1.1, interface address 192.168.1.3
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 192.168.1.1 BDR is 192.168.1.2
    Options is 0x52
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:34
    Neighbor is up for 00:11:55
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec

 Neighbor 10.0.2.1, interface address 192.168.1.2
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 192.168.1.1 BDR is 192.168.1.2
    Options is 0x52
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:31
    Neighbor is up for 00:11:57
    Index 1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Which router is now the DR? ____________

Which router is now the BDR? ___________

What factor determined which router was elected as the DR?

____

Step 6: Use router interface priority to determine DR election

a. Another method that is used to determine the DR/BDR election is router interface priority. Use the **show ip ospf interface** command to determine the default priority settings on the routers.

```
R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 10.0.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.0.3.1, Interface address 192.168.1.1
  Backup Designated router (ID) 10.0.2.1, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.0.1.1
    Adjacent with neighbor 10.0.2.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

What is the default interface priority for the Fa0/0 interfaces? ____________

b. Configure interface priorities on R1 and R2 to determine the DR/BDR election results.

```
R1(config)#interface fa0/0
R1(config-if)#ip ospf priority 25
R1(config-if)#end

R2(config)#interface fa0/0
R2(config-if)#ip ospf priority 50
R2(config-if)#end
```

c. Use the **show ip ospf neighbor** command to determine the DR and BDR.

Have the DR and the BDR changed? __________

d. Use the **clear ip ospf 1 process** command on all of the routers to reset the OSPF processes.

e. Again use the **show ip ospf neighbor** command to determine which router is the DR and which is the BDR.

Which router is now the DR? ___________

Which router is now the BDR? __________

f. Use the **show ip ospf interface** command again on R1 and R2 to confirm the priority settings and DR/BRD status on the routers.

```
R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 10.0.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 25
  Designated Router (ID) 10.0.2.1, Interface address 192.168.1.2
  Backup Designated router (ID) 10.0.3.1, Interface address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 10.0.1.1
    Adjacent with neighbor 10.0.2.1  (Designated Router)
  Suppress hello for 0 neighbor(s)

R2#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.2/24, Area 0
  Process ID 1, Router ID 10.0.2.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 50
  Designated Router (ID) 10.0.2.1, Interface address 192.168.1.2
  Backup Designated router (ID) 10.0.3.1, Interface address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
```

```
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 2
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 10.0.1.1
  Adjacent with neighbor 10.0.3.1  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

Did the interface priority override the router ID in determining the DR/BDR? __________

Step 7: Reflection

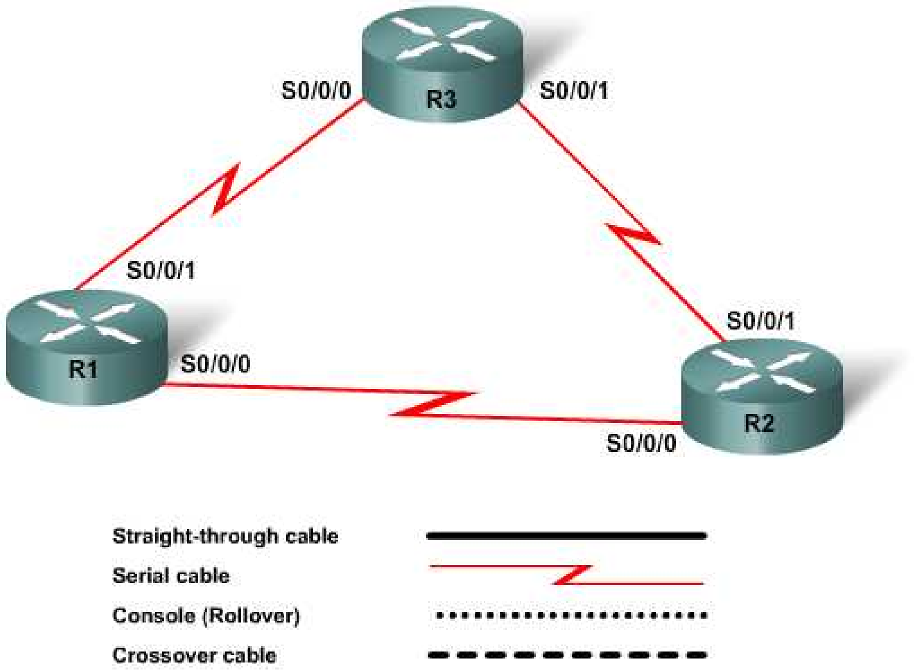
List the criteria used from highest to lowest for determining the DR on an OSPF network.

____

____

____

Lab 6.2.3 Configuring OSPF Parameters



Device	Interface	IP Address	Routing Protocol	Interface Type
R1	**S0/0/0**	192.168.1.1/30	OSPF area 0	DCE
	S0/0/1	192.168.2.1/30	OSPF area 0	DTE
R2	**S0/0/0**	192.168.1.2/30	OSPF area 0	DTE
	S0/0/1	10.0.0.1/30	OSPF area 0	DCE
R3	**S0/0/0**	192.168.2.2/30	OSPF area 0	DCE
	S0/0/1	10.0.0.2/30	OSPF area 0	DTE

Objectives

- Configure OSPF routing on all routers.
- Verify OSPF routing using **show** commands.
- Configure loopback OSPF cost parameters to influence route selection.

Background / Preparation

This lab focuses on the configuration of multiple OSPF routers attached to a muti-access Ethernet network to control the outcome of the DR/BDR election. The lab uses Cisco IOS commands.

Any router that meets the interface requirements displayed in the addressing table may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0, Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. Any Cisco Catalyst switch may be utilized. The default configuration of the switch will perform properly for this exercise.

The following resources are required:

- Three Cisco routers with at least 2 serial interfaces (preferably the same model number and IOS version)
- One Windows-based PC with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cables to configure the routers
- Three serial crossover cables to connect the routers

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

Using a crossover serial cable, connect the serial interface of each router to the other routers, as shown in the topology diagram. Note the DTE vs. DCE end of the connection.

Step 2: Perform basic configuration on the routers

a. Connect a PC to the console port of the routers to perform configurations using a terminal emulation program.

b. Configure Routers 1, 2, and 3 with a hostname, console, Telnet, and privileged passwords according to the table and topology diagram.

Step 3: Configure single area OSPF routing on the routers

Configure basic OSPF routing on the routers. All networks are in Area 0.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.2.0 0.0.0.3 area 0
R1(config-router)#end

R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.3 area 0
R2(config-router)#network 10.0.0.0 0.0.0.3 area 0
R2(config-router)#end
```

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.2.0 0.0.0.3 area 0
R3(config-router)#network 10.0.0.0 0.0.0.3 area 0
R3(config-router)#end
```

Step 4: Verify current OSPF operation

Now that the serial interfaces and OSPF have been configured, OSPF should be operational between the routers.

a. Use the **show ip route** command on all the routers to verify operation. The outputs should be similar to what is shown below. All networks should be listed in the routing table of each router.

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 1 subnets
O       10.0.0.0 [110/128] via 192.168.2.2, 00:10:38, Serial0/0/1
                 [110/128] via 192.168.1.2, 00:10:38, Serial0/0/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial0/0/0
     192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, Serial0/0/1
```

Do all routers show that they have paths to all other networks? __________

b. Use the **show interfaces serial 0/0/0** command to determine the bandwidth settings on the serial interfaces.

```
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.1.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  <*** output omitted ***>
```

What is the current bandwidth setting of the interface? ____________________

Do the interface bandwidth values match the clock rates set by the configuration__________

What path(s) would R1 take to get to the 10.0.0.0 network?

____

Step 5: Configure serial interface bandwidth settings

The metric used by OSPF is cost. On Cisco routers, cost is derived from the bandwidth setting on the interfaces.

a. Configure the bandwidth on the serial 0/0 interface of R1.

```
R1(config)#interface serial 0/0/0
R1(config-if)#bandwith 64
R1(config-if)#end
```

b. Use the **show interfaces serial 0/0/0** command on R1.

What is the bandwidth on S0/0 now? ____________________

c. Again use the **show ip route** command on R1.

Has the routing table changed? __________

Which path to the 10.0.0.0 network is now preferred?

____

Why is that path preferred? ___________________________

What is the cost shown to the 10.0.0.0 network? __________

How is this cost calculated? ____

____

____

Step 6: Use ospf cost to determine route selection

Another method that is used to determine the path chosen by OSPF is to dictate the cost of an interface.

a. Use the **show ip ospf interface** command to determine the current cost for both R1 serial interfaces.

```
R1#show ip ospf interface
Serial0/1 is up, line protocol is up
  Internet Address 192.168.2.1/30, Area 0
  Process ID 1, Router ID 192.168.2.1, Network Type POINT_TO_POINT,
Cost: 64
     <*** output omitted ***>

Serial0/0 is up, line protocol is up
  Internet Address 192.168.1.1/30, Area 0
  Process ID 1, Router ID 192.168.2.1, Network Type POINT_TO_POINT,
Cost: 1562
        <*** output omitted ***>
```

What is the cost for interface S0/0/0? __________

What is the cost for interface S0/0/1? __________

b. On R1, configure the cost of the S0/1 interface with the **ip ospf cost** command.

```
R1(config)#interface s0/0/1
R1(config)#ip ospf cost 2000
```

c. Use the **show ip route** command on R1.

Has the routing table changed? __________

Which path to the 10.0.0.0 network is now preferred by R1? __________

Why is that path preferred? ____

What is the cost shown to the 10.0.0.0 network now? __________

How is this cost calculated? ____

____

____

Step 7: Reflection

a. What determines the path chosen by OSPF?

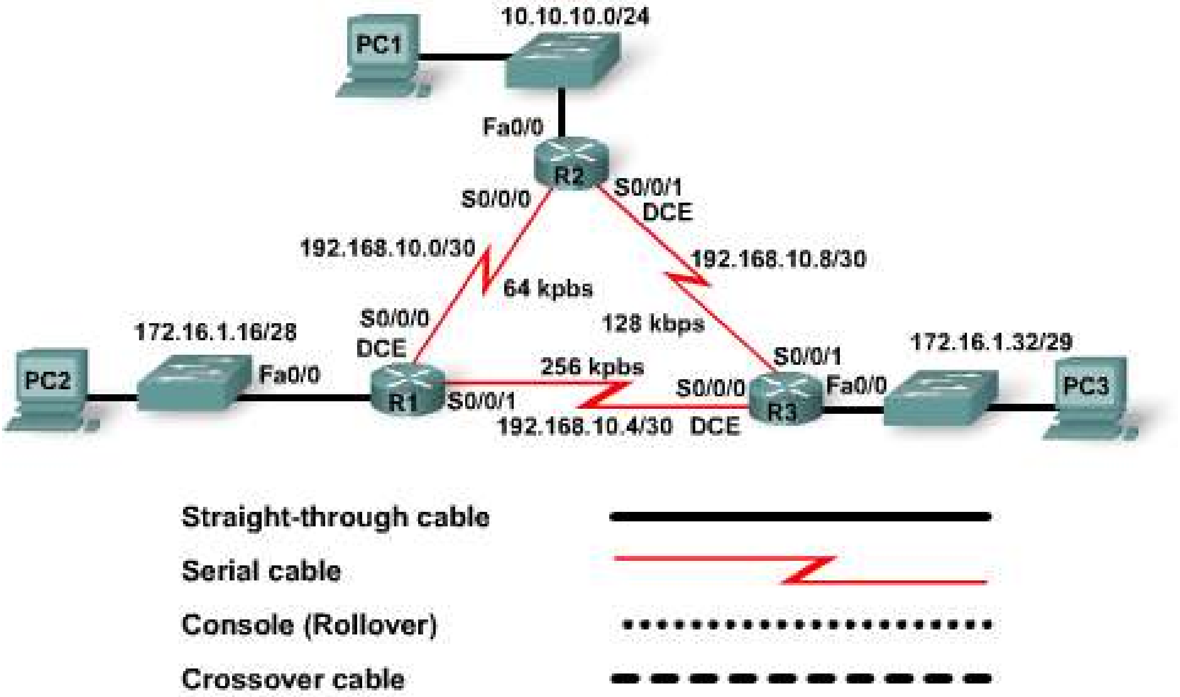
____

____

b. What has a more direct effect on the OSPF cost of a link: the bandwidth setting or the `ip ospf cost` setting?

____

Lab 6.2.4 Part A: Configuring and Verifying Point-to-Point OSPF



Device	Interface	IP Address	Subnet Mask	Default Gateway	Enable Secret Password	Enable, vty, and Console Passwords
R1	Fa0/0	172.16.1.17	255.255.255.240	N/A	class	cisco
	S0/0/0	192.168.10.1	255.255.255.252	N/A		
	S0/0/1	192.168.10.5	255.255.255.252	N/A		
R2	Fa0/0	10.10.10.1	255.255.255.0	N/A	class	cisco
	S0/0/0	192.168.10.2	255.255.255.252	N/A		
	S0/0/1	192.168.10.9	255.255.255.252	N/A		
R3	Fa0/0	172.16.1.33	255.255.255.248	N/A	class	cisco
	S0/0/0	192.168.10.6	255.255.255.252	N/A		
	S0/0/1	192.168.10.10	255.255.255.252	N/A		
PC1	NIC	172.16.1.20	255.255.255.240	172.16.1.17		
PC2	NIC	10.10.10.10	255.255.255.0	10.10.10.1		
PC3	NIC	172.16.1.35	255.255.255.248	172.16.1.33		

Objectives

- Configure OSPF routing on all routers in a point-to-point WAN environment that includes LANs.
- Configure OSPF router IDs.
- Configure interface bandwidth and cost.
- Verify OSPF routing using **`show`** commands.

Background / Preparation

In this lab you will learn how to configure the routing protocol OSPF using the network shown in the topology diagram. The segments of the network have been subnetted using VLSM. OSPF is a classless routing protocol that provides subnet mask information in its routing updates. This allows VLSM subnet information to be propagated throughout the network.

This lab uses an 1841 router and Cisco IOS commands. Any router that meets the interface requirements displayed in the addressing table may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to 1841 routers. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0, Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Three Cisco 2960 switches or other comparable switch (optional if using crossover cables between the PCs and routers)
- Three Cisco 1841 or comparable routers with 2 serial interfaces and 1 FastEthernet interface (preferably the same model number and IOS version)
- Three Windows-based PCs with a terminal emulation program and set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switches
- Six straight-through Ethernet cables to connect the router to the switch and the switch to the hosts
- Three serial crossover cables to connect the routers

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Fa0/0 interface of each router to the Fa0/1 interface of each switch using a straight-through cable.

b. Connect each host to the Fa0/2 switch port of each switch using a straight-through cable.

c. Connect serial cables from each router to the other router as shown in the topology.

Step 2: Perform basic configurations on the routers

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On all routers, configure the hostname, passwords, and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram.

Step 3: Configure the router interfaces

Step 4: Verify IP addressing and interfaces

a. Use the **`show ip interface brief`** or the **`show protocols`** command to verify that the IP addressing is correct and that the interfaces are active.

b. After all interfaces are verified, be sure to save the running configuration to the NVRAM of the router.

Step 5: Configure Ethernet interfaces of PC1, PC2, and PC3

a. Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from the addressing table.

b. Test the PC configuration by pinging the default gateway from each PC.

Step 6: Configure OSPF on Router 1

a. Configure OSPF on the R1 router. Enter a process ID of 1 for the *`process-ID`* parameter.

```
R1(config)#router ospf 1
```

b. Configure the network statement for the LAN. When you are in the Router OSPF configuration submode, configure the LAN 172.16.1.16/28 to be included in the OSPF updates that are sent out of R1. Use an area ID of 0 for the OSPF *`area-id`* parameter. Zero will be used for the OSPF area ID in all **`network`** statements in this topology.

```
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
```

c. Configure the router to advertise the 192.168.10.0/30 network attached to the Serial 0/0/0 interface.

```
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
```

d. Configure the router to advertise the 192.168.10.4/30 network attached to the Serial 0/0/1 interface.

```
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0
```

e. Return to privileged EXEC mode and save the configuration.

Step 7: Configure OSPF on the R2 router

a. Enable OSPF routing on the R2 router using the **`router ospf`** command. Use a process ID of 1.

```
R2(config)#router ospf 1
```

b. Configure the router to advertise the LAN network 10.10.10.0/24 in the OSPF updates.

```
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
```

c. Configure the router to advertise the 192.168.10.0/30 network attached to the Serial 0/0/0 interface.

```
R2(config-router)#network 192.168.10.0 0.0.0.3 area 0
R2(config-router)#
00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0
from EXCHANGE to FULL, Exchange Done
```

When the network for the serial link from R1 to R2 is added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

d. Configure the router to advertise the 192.168.10.8/30 network attached to the Serial 0/0/1 interface. When you are finished, return to privileged EXEC mode.

```
R2(config-router)#network 192.168.10.8 0.0.0.3 area 0
R2(config-router)#end
R2#
```

Step 8: Configure OSPF on the R3 router

Configure OSPF on the R3 router using the `router` **`ospf`** **and** **`network`** commands. Use a process ID of 1. Configure the router to advertise the three directly connected networks. When you are finished, return to privileged EXEC mode.

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.32 0.0.0.7 area 0
R3(config-router)#network 192.168.10.4 0.0.0.3 area 0
R3(config-router)#
00:17:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0
from LOADING to FULL, Loading Done
R3(config-router)#network 192.168.10.8 0.0.0.3 area 0
R3(config-router)#
00:18:01: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on Serial0/0/1
from EXCHANGE to FULL, Exchange Done
R3(config-router)#end
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

When the networks for the serial links from R3 to R1 and R3 to R2 are added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

Step 9: Configure OSPF router IDs

a. The OSPF router ID is used to uniquely identify the router in the OSPF routing domain. A router ID is an IP address. Cisco routers derive the router ID in one of three ways, and with the following precedence:

1) IP address configured with the OSPF **`router-id`** command

2) Highest IP address of any of the router loopback addresses

3) Highest active IP address on any of the router physical interfaces

b. Examine the current router IDs in the topology.

Because no router IDs or loopback interfaces have been configured on the three routers, the router ID for each router is determined by the highest IP address of any active interface.

What is the router ID for R1? ________________________________

What is the router ID for R2? ________________________________

What is the router ID for R3? ________________________________

c. The router ID can also be seen in the output of the **show ip protocols**, **show ip ospf**, and **show ip ospf interfaces** commands.

```
R3#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.10
R3#show ip ospf
 Routing Process "ospf 1" with ID 192.168.10.10
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

<output omitted>

R3#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.33/29, Area 0
  Process ID 1, Router ID 192.168.10.10, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.10.10, Interface address 172.16.1.33
  No backup designated router on this network
<output omitted>
```

d. Use loopback addresses to change the router IDs of the routers in the topology.

```
R1(config)#interface loopback 0
R1(config-if)#ip address 10.1.1.1 255.255.255.255

R2(config)#interface loopback 0
R2(config-if)#ip address 10.2.2.2 255.255.255.255

R3(config)#interface loopback 0
R3(config-if)#ip address 10.3.3.3 255.255.255.255
```

e. Reload the routers to force the new router IDs to be used. When a new router ID is configured, it is not used until the OSPF process is restarted. Make sure that the current configuration is saved to NRAM, and then use the **reload** command to restart each of the routers.

When the router is reloaded, what is the router ID for R1? ________________________

When the router is reloaded, what is the router ID for R2? ________________________

When the router is reloaded, what is the router ID for R3? ________________________

f. Use the **show ip ospf neighbors** command to verify that the router IDs have changed.

```
R1#show ip ospf neighbor

Neighbor ID    Pri   State     Dead Time   Address         Interface
10.3.3.3         0   FULL/-    00:00:30    192.168.10.6    Serial0/0/1
10.2.2.2         0   FULL/-    00:00:33    192.168.10.2    Serial0/0/0

R2#show ip ospf neighbor

Neighbor ID    Pri   State     Dead Time   Address         Interface
10.3.3.3         0   FULL/-    00:00:36    192.168.10.10   Serial0/0/1
10.1.1.1         0   FULL/-    00:00:37    192.168.10.1    Serial0/0/0

R3#show ip ospf neighbor

Neighbor ID    Pri   State     Dead Time   Address         Interface
10.2.2.2         0   FULL/-    00:00:34    192.168.10.9    Serial0/0/1
10.1.1.1         0   FULL/-    00:00:38    192.168.10.5    Serial0/0/0
```

g. Use the **router-id** command to change the router ID on the R1 router.

NOTE: Some IOS versions do not support the **router-id** command. If this command is not available, continue to Step 10.

```
R1(config)#router ospf 1
R1(config-router)#router-id 10.4.4.4
```

Reload or use the **clear ip ospf process** command for this to take effect.

If this command is used on an OSPF router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the **clear ip ospf process** command.

```
R1#(config-router)#end
R1#clear ip ospf process
Reset ALL OSPF processes? [no]:yes
R1#
```

h. Use the **show ip ospf neighbor** command on router R2 to verify that the router ID of R1 has been changed.

```
R2#show ip ospf neighbor

Neighbor ID    Pri   State      Dead Time   Address         Interface
10.3.3.3         0   FULL/-     00:00:36    192.168.10.10   Serial0/0/1
10.4.4.4         0   FULL/-     00:00:37    192.168.10.1    Serial0/0/0
```

i. Remove the configured router ID with the **no** form of the **router-id** command.

```
R1(config)#router ospf 1
R1(config-router)#no router-id 10.4.4.4
```

Reload or use the **clear ip ospf process** command for this to take effect.

j. Restart the OSPF process using the **`clear ip ospf process`** command.

   Restarting the OSPF process forces the router to use the IP address configured on the Loopback 0 interface as the router ID.

```
R1(config-router)#end
R1#clear ip ospf process
Reset ALL OSPF processes? [no]:yes
```

Step 10: Verify OSPF operation

a. On the R1 router, use the **`show ip ospf neighbor`** command to view the information about the OSPF neighbor routers R2 and R3. You should be able to see the neighbor ID and IP address of each adjacent router as well as the interface that R1 uses to reach that OSPF neighbor.

```
R1#show ip ospf neighbor
Neighbor ID    Pri   State     Dead Time   Address         Interface
10.2.2.2         0   FULL/-    00:00:32    192.168.10.2    Serial0/0/0
10.3.3.3         0   FULL/-    00:00:32    192.168.10.6    Serial0/0/1
R1#
```

b. On the R1 router, use the **`show ip protocols`** command to view information about the routing protocol operation.

   The information that was configured in the previous steps, such as protocol, process ID, neighbor ID, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown.

```
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.16 0.0.0.15 area 0
    192.168.10.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2         110      00:11:43
    10.3.3.3         110      00:11:43
  Distance: (default is 110)
```

   The output specifies the process ID used by OSPF. The process ID must be the same on all routers for OSPF to establish neighbor adjacencies and share routing information.

Step 11: Examine OSPF routes in the routing tables

View the routing table on the R1 router. OSPF routes are denoted in the routing table with an **O**.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.1/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/65] via 192.168.10.2, 00:01:02, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
O       172.16.1.32/29 [110/65] via 192.168.10.6, 00:01:12, Serial0/0/1
     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/128] via 192.168.10.6, 00:01:12, Serial0/0/1
                     [110/128] via 192.168.10.2, 00:01:02, Serial0/0/0
R1#
```

Unlike RIPv2 and EIGRP, OSPF does not automatically summarize at major network boundaries.

Step 12: Configure OSPF cost

a. Use the **`show ip route command`** on the R1 router to view the OSPF cost to reach the 10.10.10.0/24 network.

```
R1#show ip route

<output omitted>

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.1/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/65] via 192.168.10.2, 00:16:56, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
O       172.16.1.32/29 [110/65] via 192.168.10.6, 00:17:06, Serial0/0/1
     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/128] via 192.168.10.6, 00:17:06, Serial0/0/1
                     [110/128] via 192.168.10.2, 00:16:56, Serial0/0/0
R1#
```

The path cost of 65 to the 10.10.10.0 network results from a WAN serial link cost of 64 plus the LAN FastEthernet link cost of 1.

b. Use the **show interfaces serial0/0/0** command on the R1 router to view the bandwidth of the Serial 0/0/0 interface.

```
R1#show interfaces serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 192.168.10.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0

<output omitted>
```

On most serial links, the bandwidth metric defaults to 1544 Kbits. This translates to an OSPF cost of 64 (100,000,000/1,544,000). If this is not the actual bandwidth of the serial link, the bandwidth needs to be changed so that the OSPF cost can be calculated correctly.

c. Use the **show ip ospf interface** command to see the OSPF cost currently associated with interfaces that are participating in OSPF updates. Because the bandwidth of the FastEthernet interface is 100,000,000 bps, its cost is 1 (100,000,000/100,000,000).

```
R1#show ip ospf interface <some output omitted>
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.10.5/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.3.3.3
  Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)

FastEthernet0/0 is up, line protocol is up
  Internet Address 172.16.1.17/28, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.1, Interface address 172.16.1.17
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

d. Use the **bandwidth** command to change the bandwidth of the serial interfaces of the R1 and R2 routers to the actual bandwidth, 64 kbps.

```
R1 router:
R1(config)#interface serial0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#interface serial0/0/1
R1(config-if)#bandwidth 64

R2 router:
R2(config)#interface serial0/0/0
R2(config-if)#bandwidth 64
R2(config-if)#interface serial0/0/1
R2(config-if)#bandwidth 64
```

e. Use the **`show ip ospf interface`** command on the R1 router to verify the cost of the serial links. The cost of each of the serial links is now 1562, the result of the calculation: 10^8/64,000 bps.

```
R1#show ip ospf interface

<output omitted>

Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.10.5/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT-TO-POINT,

<output omitted>
```

f. Use the **`ip ospf cost`** command to configure the OSPF cost on the R3 router.

g. An alternative to using the **`bandwidth`** command is to use the **`ip ospf cost`** command, which allows you to directly configure the cost. Use the **`ip ospf cost`** command to change the bandwidth of the serial interfaces of the R3 router to 1562.

```
R3(config)#interface serial0/0/0
R3(config-if)#ip ospf cost 1562
R3(config-if)#interface serial0/0/1
R3(config-if)#ip ospf cost 1562
```

h. Use the **`show ip ospf interface`** command on the R3 router to verify that the cost of each of the serial links is now 1562.

```
R3#show ip ospf interface

<output omitted>
Serial0/0/1 is up, line protocol is up
  Internet address is 192.168.10.10/30, Area 0
  Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.10.6/30, Area 0
  Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT-TO-POINT,

<output omitted>
```

Step 13: Reflection

What are some advantages of using OSPF as a routing protocol?

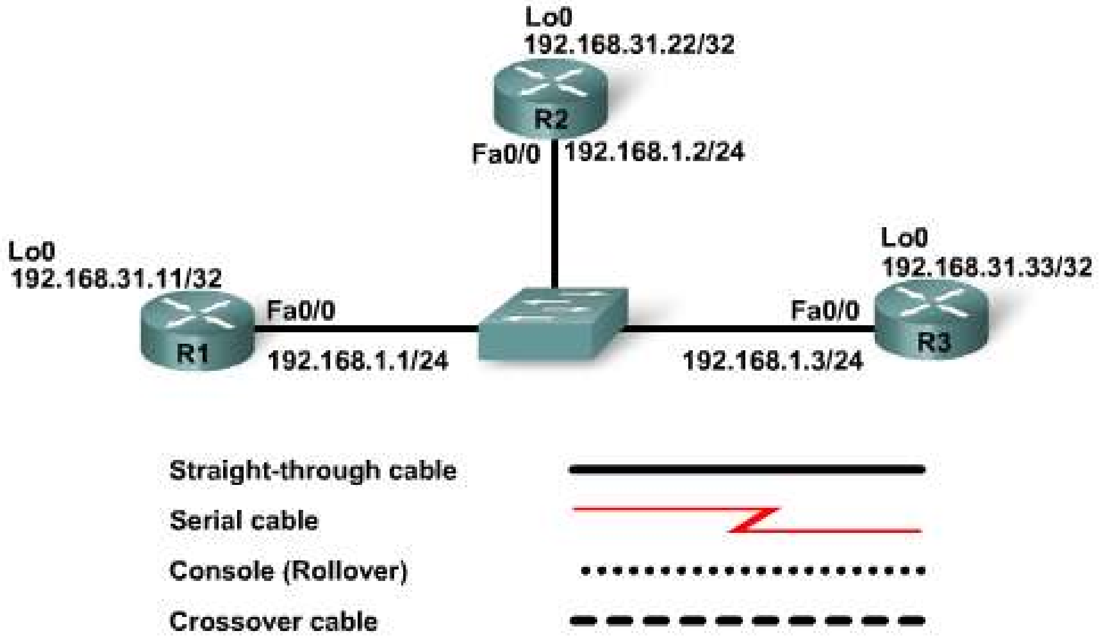
____

____

____

____

Lab 6.2.4 Part B: Configuring and Verifying Multi-access OSPF



Device	Interface	IP Address	Subnet Mask	Default Gateway	Enable Secret Password	Enable, vty, and Console Passwords
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A	class	cisco
	Loopback1	192.168.31.11	255.255.255.255	N/A		
R2	Fa0/0	192.168.1.2	255.255.255.0	N/A	class	cisco
	Loopback1	192.168.31.22	255.255.255.255	N/A		
R3	Fa0/0	192.168.1.3	255.255.255.0	N/A	class	cisco
	Loopback1	192.168.31.33	255.255.255.255	N/A		

Objectives

- Configure OSPF on a multi-access network.
- Configure OSPF priority.
- Control the OSPF election process.
- Verify the OSPF configuration and DR/BDR/DROTHER status.

Background / Preparation

In this lab, you will learn to configure OSPF on a multi-access Ethernet network. You will also learn to use the OSPF election process to determine the designated router (DR), backup designated router (BDR), and DRother states. This lab uses 1841 routers and Cisco IOS commands.

The information in this lab applies to 1841 routers. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0, Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Three Cisco 1841 or comparable routers with 1 FastEthernet interface (preferably the same model number and IOS version)
- Three Windows-based PCs with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the router
- Three straight-through Ethernet cables to connect the routers to the switch

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

Connect the Fa0/0 interface of each router to the switch using a straight-through cable. Three routers are sharing a common Ethernet multi-access network, 192.168.1.0/24. Each router will be configured with an IP address on the FastEthernet interface and a loopback address for the router ID.

Step 2: Perform basic configurations on the routers

Step 3: Configure and activate Ethernet and Loopback addresses

Step 4: Verify IP addressing and interfaces

a. Use the **`show ip interface brief`** or the **`show protocols`** command to verify that the IP addressing is correct and that the interfaces are active.

b. After all interfaces are verified, be sure to save the running configuration to the NVRAM of the router.

Step 5: Configure OSPF on the DR router

The DR and BDR election process takes place as soon as the first router has its interface enabled for OSPF on the multi-access network. If OSPF is already configured for an interface, this can happen as the routers are powered on. It can also happen when the OSPF **`network`** command for that interface is configured. If a new router enters the network after the DR and BDR have already been elected, it will not become the DR or BDR even if it has a higher OSPF interface priority or router ID than the current DR or BDR.

a. Configure the OSPF process on the router with the highest router ID first to ensure that this router becomes the DR.

   Based on the loopback addresses assigned in Step 3, which router should be come the DR? _____

b. Use the **`router ospf`** command in global configuration mode to enable OSPF on the R3 router. Enter a process ID of 1 for the *`process-ID`* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *`area-id`* parameter in the **`network`** statement.

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.1.0 0.0.0.255 area 0
R3(config-router)#end
```

c. Use the **`show ip ospf interface`** command to verify that the OSPF has been configured correctly and that R3 is the DR.

```
R3#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.3/24, Area 0
  Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

NOTE: Wait at least 40 seconds for a hello packet to be sent in order to see the state change. If a state says WAITING, wait longer because it will change to a DR.

What type of network has OSPF detected for this interface? ________________________________

What is the IP address of this interface? _____________________________________

What is the OSPF cost for this interface? ____________________________________

What is the router ID of this router? _____________________________________

Step 6: Configure OSPF on the BDR router

a. Configure the OSPF process on the router with the second highest router ID to ensure that this router becomes the BDR. Use the **router ospf** command in global configuration mode to enable OSPF on the R2 router. Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement.

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#end
```

It may take up to 40 seconds for the R3 router to send a hello packet.

What console message was displayed as a result of the OSPF commands on R2 and what does this mean?

____

____

b. Use the **show ip ospf interface** command to verify that the OSPF has been configured correctly and that R2 is the BDR.

```
R2#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.2/24, Area 0
  Process ID 1, Router ID 192.168.31.22, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
  Backup Designated Router (ID) 192.168.31.22, Interface address
192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

c. Use the **show ip ospf neighbors** command in global configuration mode to view information about the other routers in the OSPF area.

Notice that R3 is the DR.

```
R2#show ip ospf neighbor
Neighbor ID     Pri   State     Dead Time   Address       Interface
192.168.31.33     1   FULL/DR   00:00:33    192.168.1.3   FastEthernet0/0
```

Step 7: Configure OSPF on the DRother router

a. Configure the OSPF process on the router with the lowest router ID last. This router will be designated as DRother instead of DR or BDR. Use the **router ospf** command in global configuration mode to enable OSPF on the R1 router. Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#end

00:16:08: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from LOADING to FULL, Loading Done
00:16:12: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on
FastEthernet0/0 from EXCHANGE to FULL, Exchange Done
```

An adjacency is formed with the R2 and R3 routers. It may take up to 40 seconds for both the R2 and R3 routers to each send a hello packet.

b. Use the **show ip ospf interface** command to verify that the OSPF has been configured correctly and that R1 is a DRother.

```
R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
  Backup Designated Router (ID) 192.168.31.22, Interface address
192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.31.33  (Designated Router)
    Adjacent with neighbor 192.168.31.22  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

c. Use the **show ip ospf neighbors** command in global configuration mode to view information about the other routers in the OSPF area.

Notice that R3 is the DR and R2 is the BDR.

```
R1#show ip ospf neighbor
Neighbor ID    Pri   State         Dead Time   Address         Interface
192.168.31.22    1   FULL/BDR      00:00:35    192.168.1.2     FastEthernet0/0
192.168.31.33    1   FULL/DR       00:00:30    192.168.1.3     FastEthernet0/0
```

Step 8: Use the OSPF priority to determine the DR and BDR

a. Use the **ip ospf priority interface** command to change the OSPF priority of the R1 router to 255. This is the highest possible priority.

```
R1(config)#interface fastEthernet0/0
R1(config-if)#ip ospf priority 255
R1(config-if)#end
```

b. Use the **ip ospf priority interface** command to change the OSPF priority of the R3 router to 100.

```
R3(config)#interface fastEthernet0/0
R3(config-if)#ip ospf priority 100
R3(config-if)#end
```

c. Use the **ip ospf priority interface** command to change the OSPF priority of the R2 router to 0. A priority of 0 causes the router to be ineligible to participate in an OSPF election and become a DR or BDR.

```
R2(config)#interface fastEthernet0/0
R2(config-if)#ip ospf priority 0
R2(config-if)#end
```

d. Shut down and re-enable the FastEthernet0/0 interfaces to force an OSPF election. As the interfaces are shut down, the OSPF adjacencies are lost.

R1:

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from FULL to Down: Interface down or detached
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on
FastEthernet0/0 from FULL to Down: Interface down or detached
```

R2:

```
R2(config)#interface fastethernet0/0
R2(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
02:17:06: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on
FastEthernet0/0 from FULL to Down: Interface down or detached
02:17:06: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on
FastEthernet0/0 from FULL to Down: Interface down or detached
```

R3:

```
R3(config)#interface fastethernet0/0
R3(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from FULL to Down: Interface down or detached
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on
FastEthernet0/0 from FULL to Down: Interface down or detached
```

e. Re-enable the FastEthernet 0/0 interface on the R2 router.

```
R2(config-if)#no shut
R2(config-if)#end
```

f. Re-enable the FastEthernet 0/0 interface on the R1 router.

```
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

02:31:43: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from EXCHANGE to FULL, Exchange Done
```

An adjacency is formed with the R2 router. It may take up to 40 seconds for the R2 router to send a hello packet.

g. Use the **`show ip ospf neighbor`** command on the R1 router to view the OSPF neighbor information for that router.

Even though the R2 router has a higher router ID than R1, the R2 router has been set to a state of DRother because the OSPF priority has been set to 0.

```
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address       Interface
192.168.31.22     0   FULL/DROTHER    0:00:33    192.168.1.2   FastEthernet0/0
R1#
```

h. Re-enable the FastEthernet 0/0 interface on the R3 router.

```
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

02:37:32: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on
FastEthernet0/0 from LOADING to FULL, Loading Done
02:37:36: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on
FastEthernet0/0 from EXCHANGE to FULL, Exchange Done
```

An adjacency is formed with the R1 and R2 routers. It may take up to 40 seconds for both the R1 and R2 routers to each send a hello packet.

i. Use the **show ip ospf interface** command on the R3 router to verify that R3 has become the BDR.

```
R3#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.3/24, Area 0
  Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State BDR, Priority 100
  Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1

<output omitted>
```

Step 9: Reflection

a. When the OSPF process starts, what happens if there is no active interface on the router?

____

b. What can be done to ensure there will be an active interface on a router?

____

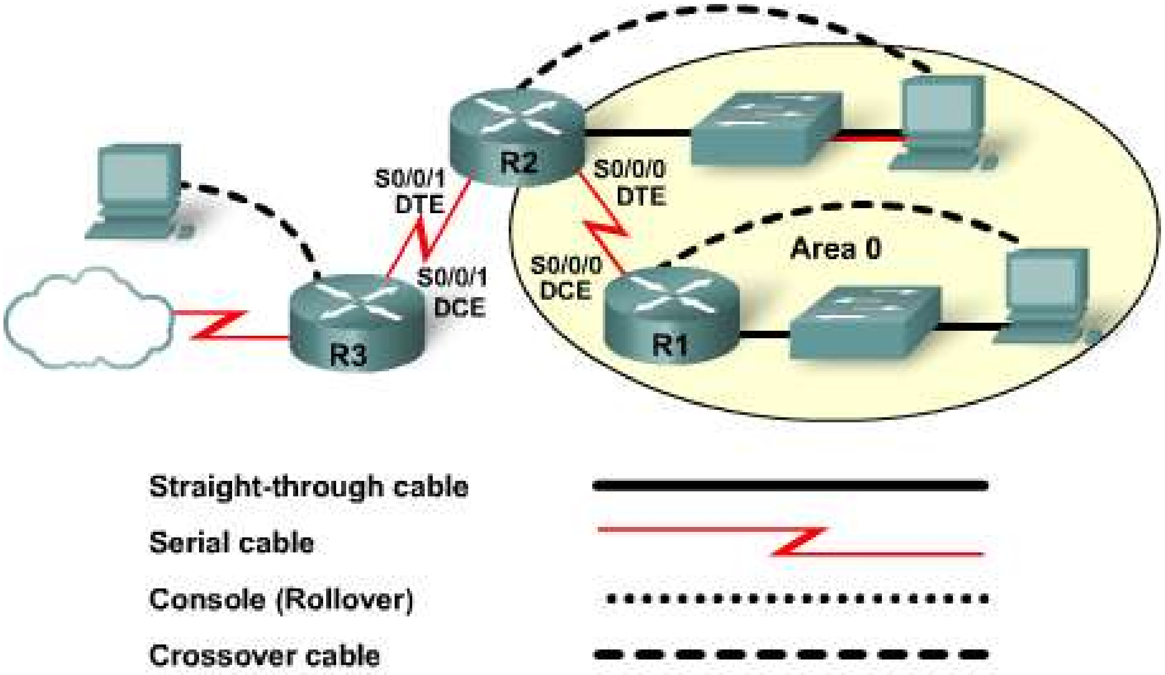
c. How are the DR and BDR elected in an OSPF network?

____

____

d. What OSPF interface priority value prevents a router from being elected as a DR? __________

Lab 6.3.1 Configuring and Propagating an OSPF Default Route



Device	Router Name	IP Address/Mask	Lookback Address/Mask	Network Statements	Enable Secret Password	Enable, vty, and Console Passwords
R1	**R1**	**Fa0/0** 192.168.1.129/26 **S0/0/0** = DCE 192.168.1.1/30	192.168.31.11/32	192.168.1.0	class	cisco
R2	**R2**	**Fa0/0** 192.168.0.1/24 **S0/0/0** 192.168.1.2/30 **S0/0/1** 200.20.20.2/30	192.168.31.22/32	192.168.1.0 192.168.0.0	class	cisco
R3	**ISP**	**S0/0/1** = DCE 200.20.20.1/30	138.25.6.33/32		class	cisco

Objectives

- Set up an IP addressing scheme for the OSPF area.
- Configure and verify OSPF routing.
- Configure the OSPF network so that all hosts in the OSPF area can connect to outside networks.

Background / Preparation

This lab focuses on the basic configuration of the Cisco 1800 series or comparable router using Cisco IOS commands. The information in this lab applies to other routers; however, command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0, Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0 or FastEthernet 0/0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Two Cisco 2960 switches or other comparable switches
- Three Cisco 1841 or comparable routers with 2 serial interfaces and 1 FastEthernet interface
- Three Windows-based PCs, each with a terminal emulation program and set up as a host
- At least one RJ-45-to-DB-9 connector console cable to configure the routers
- Four straight-through Ethernet cables to connect the routers to the switches and the switches to the hosts
- Three serial cables to connect the routers

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

Connect each of the routers, switches, and hosts as shown in the topology diagram.

Step 2: Perform basic configurations on the routers

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Routers 1, 2, and 3, configure the hostname, console, Telnet, privileged passwords, and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram.

Step 3: Configure the ISP router

a. Configure serial and loopback interfaces on Router 3.

```
R3(config)#interface s0/0/1
R3(config-if)#ip address 200.20.20.1 255.255.255.252
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config-if)#interface lo0
R3(config-if)#ip address 138.25.6.33 255.255.255.255
R3(config-if)#exit
```

b. On Router 3, configure a default route to both the 192.168.0.0 and the 192.168.1.0 networks.

```
R3(config)#ip route 192.168.1.0 255.255.255.0 200.20.20.2
R3(config)#ip route 192.168.0.0 255.255.255.0 200.20.20.2
```

Step 4: Configure the Area 0 OSPF routers

a. Configure loopback, FastEthernet, and serial interfaces on Router 1 and Router 2.

```
R1(config)#interface loopback 0
R1(config-if)#ip address 192.168.31.11 255.255.255.255
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#interface fa 0/0
R1(config-if)#ip address 192.168.1.129 255.255.255.192
R1(config-if)#no shutdown

R2(config)#interface loopback 0
R2(config-if)#ip address 192.168.31.22 255.255.255.255
R2(config-if)#interface serial 0/0/0
R2(config-if)#ip address 192.168.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#interface serial 0/0/1
R2(config-if)#ip address 200.20.20.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#interface fa 0/0
R2(config-if)#ip address 192.168.0.1 255.255.255.0
R2(config-if)#no shutdown
```

b. Save the running configuration to the NVRAM of each router.

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. At this point, the workstations will not be able to communicate with each other.

Step 6: Verify connectivity

Ping from R2 to both the ISP and R1 routers.

Were the pings successful? __________

If the pings were not successful, troubleshoot the router configurations until the ping is successful.

Step 7: Configure OSPF routing on both Area 0 routers

a. Configure OSPF routing on each router. Use OSPF process number 1 and ensure that all networks are in Area 0.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.128 0.0.0.127 area 0
R1(config-router)#network 192.168.1.0 0.0.0.3 area 0

R2(config)#router ospf 1
R2(config-router)#network 192.168.0.0 0.0.0.255 area 0
R2(config-router)#network 192.168.1.0 0.0.0.3 area 0
```

Did the IOS version automatically add any lines under router OSPF 1? __________

b. Show the routing table for R1.

Are there any entries in the routing table? __________

Step 8: Test network connectivity

Ping the R1 host from the R2 host.

Was it successful? __________

If the ping is not successful, troubleshoot as necessary.

Step 9: Observe OSPF traffic

a. At the privileged EXEC mode, enter the command **`debug ip ospf events`** and observe the output. You may have to wait at least 40 seconds for the hello packet to be sent before observations can be recorded.

   Is there OSPF traffic? __________

   What type of OSPF traffic is observed on the network? _______________________

b. Turn off debugging by entering **`no debug ip ospf events`** or **`undebug all`**.

Step 10: Create a default route to the ISP

On R2 only, enter a static default route.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 200.20.20.1
```

Step 11: Verify the default static route

Verify the default static route by looking at the R2 routing table.

Is the default route in the routing table? __________

Step 12: Verify connectivity from the R2 router

a. Verify connectivity from R2 by pinging the ISP Serial 0/0/1 interface from the R2 router.

   Is the ping successful? __________

b. Next, on the host attached to R2, open a command prompt and ping the Serial 1 interface on the ISP router.

   Is the ping successful? __________

c. This time, ping the loopback interface address of the ISP router, which represents the ISP connection to the Internet.

   Is the ping successful? __________

All of these pings should be successful. If they are not, troubleshoot the configurations on the host and on the R2 and ISP routers.

Step 13: Verify connectivity from the R1 router.

Verify the connection between the ISP and R1 by pinging the Serial 0/0/1 interface of the ISP router on R2.

Is the ping successful? __________

If yes, why? ____

If not, why not? ____

Step 14: Redistribute the static default route

Propagate the gateway of last resort to the other routers in the OSPF domain. At the configure router prompt on R2, enter **`default-information originate`**.

```
R2(config-router)#default-information originate
```

Is there now a default route on R1? __________

What is the address of the gateway of last resort? __________________

There is an O*E2 entry in the routing table. What type of route is this?

______________________________ ___________________ ________

Can the ISP server address at 138.25.6.33 be pinged from both workstations? __________

If no, troubleshoot both hosts and all three routers.

Step 15: Reflection

a. How does OSPF reach networks outside of the domain?

____

____

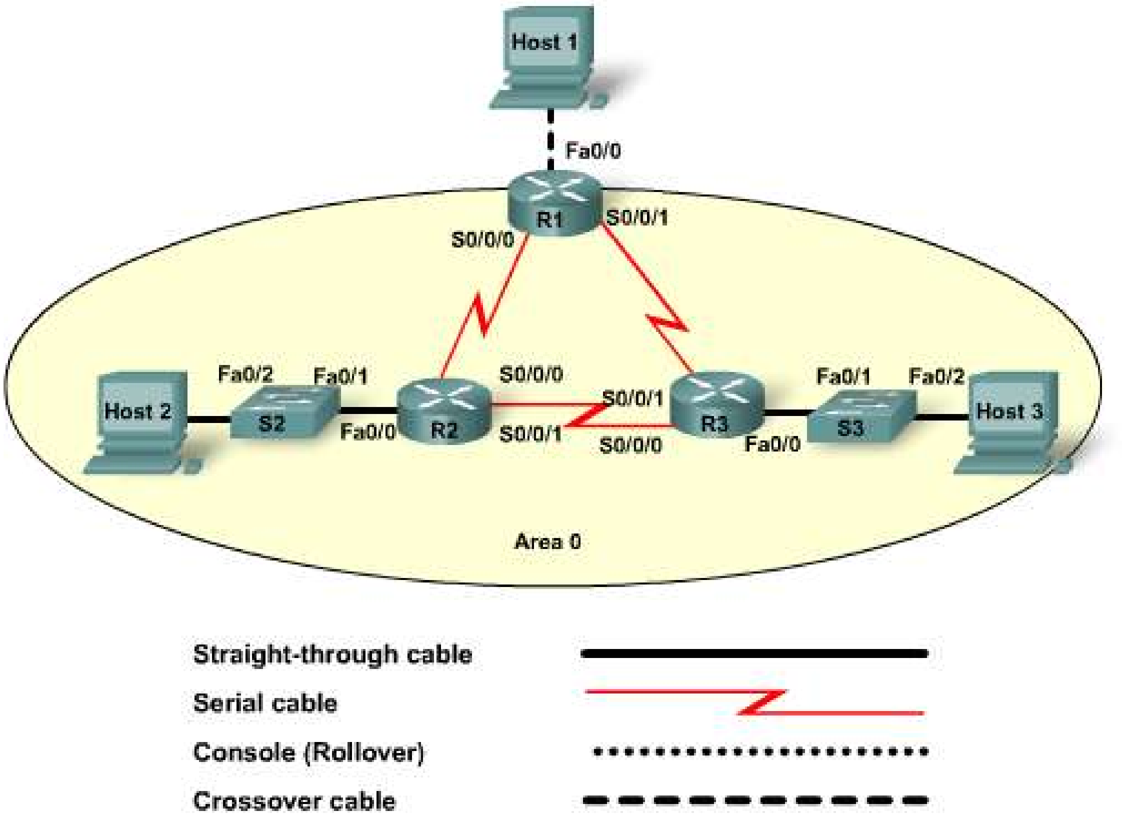
b. What does a router use to generate a gateway of last resort?

____

CCNA Discovery

Introducing Routing and Switching in the Enterprise

Lab 6.3.2 Configuring OSPF Summarization



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Serial 0/0/1 IP Address	Serial 0/0/1 Interface Type	Enable Secret Password	vty, Console Password
Router 1	Border	209.165.201.2 /24	192.168.10.65 /30	DCE	192.168.10.69 /30	DCE	class	cisco
Router 2	R2	192.168.10.1 /28	192.168.10.66 /30	DTE	192.168.10.73 /30	DCE	class	cisco
Router 3	R3	192.168.10.33/28	192.168.10.74 /30	DTE	192.168.10.70 /30	DTE	class	cisco
Switch 2	SW2						class	cisco
Switch 3	SW3						class	cisco

Objectives

- Configure a three-router topology using VLSM.
- Configure OSPF as the routing protocol.
- Configure OSPF summary routes.
- Observe the effect of summarization on the routing table.

Background / Preparation

In this lab, you will set up a network similar to the one in the topology diagram. This topology represents a three-router corporate network using variably-subnetted private IP addressing. From one router, a public network connection to a host PC simulates the corporate network's connection to the ISP. You will configure OSPF as the routing protocol for the corporate network You will also adjust the OSPF configuration to reduce the size of the routing tables. The following resources are required:

- Three Cisco 1841 or comparable routers
- Two Cisco 2960 or other comparable switches
- Three Windows-based PCs, at least one with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable
- Three serial cables
- One crossover Ethernet cable
- Four straight-through Ethernet cables
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router 1 to Routers 2 and 3 with serial cables. Connect Router 2 to Router 3 with a serial cable.

b. Connect the Router 2 Fa0/0 interface to the Switch 2 Fa0/1 interface using a straight-through cable.

c. Connect the Router 3 Fa0/0 interface to the Switch 3 Fa0/1 interface using a straight-through cable.

d. Connect Host 2 to Switch 2 and Host 3 to Switch 3 to the Fa0/2 interface using straight-through cables.

e. Connect Host 1 to the Router 1 Fa0/0 interface using a crossover cable.

f. Connect a PC with a console cable to perform configurations on the routers and switches.

Step 2: Perform basic configurations on the routers

a. Establish a console session with Router 1 and configure hostname, passwords, and interfaces as shown in the addressing table. Save the configuration.

b. Establish a console session with Router 2. Configure hostname, passwords, and interfaces according to the addressing table. Save the configuration.

c. Establish a console session with Router 3. Configure hostname, passwords, and interfaces according to the addressing table. Save the configuration.

Step 3: Perform basic configurations on the switches

a. Establish a console session with Switch 2 and configure hostname and passwords according to the addressing table. Save the configuration.

b. Perform a similar configuration on Switch 3, configuring the hostname and passwords as described for SW 2. Save the configuration.

Step 4: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway for the network on which it resides. Host 1 should be assigned the address 209.165.201.1/24. Host 2 and Host 3 should be assigned IP addresses in the 192.168.10.0/28 and 192.168.10.32/28 networks respectively. All three PCs use the Fa0/0 interface of their attached router as their default gateway.

b. Each workstation should be able to ping the attached router. If the ping is not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned the correct IP address and default gateway.

Step 5: Configure OSPF routing with default summarization

a. On Border, configure OSPF as the routing protocol with a process ID of 1 and advertise the appropriate networks.

```
Border(config)#router ospf 1
Border(config-router)#network 192.168.10.64 0.0.0.3 area 0
Border(config-router)#network 192.168.10.68 0.0.0.3 area 0
```

From the network commands, which interfaces are participating in OSPF routing?

____

b. Perform a similar configuration on R2, using the same process ID and advertising the appropriate networks. Remember to advertise the FastEthernet interface.

c. On R3, perform a similar configuration, using the same process ID and advertising the appropriate networks.

Step 6: Configure and redistribute a default route for Internet access

a. From the Border router to Host 1, the host simulating the Internet, create a static route to network 0.0.0.0 0.0.0.0, using the **ip route** command and the next hop interface. This will forward any unknown-destination address traffic to the PC simulating the Internet by setting a gateway of last resort on the Border router.

```
Border(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.1
```

b. Border will advertise this route to the other routers if this command is added to its OSPF configuration.

```
Border(config)#router ospf 1
Border(config-router)#default-information originate
```

Step 7: Verify the routing configuration

a. View the routing table on Border.
<<output omitted>>

```
Gateway of last resort is 209.165.201.1 to network 0.0.0.0
     192.168.10.0/24 is variably subnetted, 5 subnets, 2 masks
O       192.168.10.0/27 [110/65] via 192.168.10.66, 00:08:52, Serial0/0/0
O       192.168.10.32/27 [110/65] via 192.168.10.70, 00:09:25, Serial0/0/1
C       192.168.10.64/30 is directly connected, Serial0/0/0
C       192.168.10.68/30 is directly connected, Serial0/0/1
O       192.168.10.72/30 [110/128] via 192.168.10.70, 00:09:25,Serial0/0/1
                         [110/128] via 192.168.10.66, 00:08:52,Serial0/0/0
C    209.165.201.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 209.165.201.1
```

How can you tell from the routing table that the subnetted network shared by the corporate routers has a pathway for traffic destined for the Internet?

____

b. View the routing tables on R2 and R3.

How is the pathway for Internet traffic provided in their routing tables?

____

Step 8: Verify connectivity

a. Simulate sending traffic to the Internet by pinging from the host PCs to 209.165.201.1.

Were the pings successful? __________

b. Verify that hosts within the subnetted network can reach each other by pinging between Host 1 and Host 2.

Were the pings successful? __________

Step 9: Configure OSPF summarization

a. Compute a summary route for the corporate subnetworks. The networks have been assigned contiguously:

192.168.10.0
192.168.10.32
192.168.10.64
192.168.10.68
192.168.10.72

What is the one summary route that can be used to advertise all of these subnets?

____

Which router will be reporting this summary route to the ISP? ______________________

b. Configure the summary route in router configuration mode, starting with **area 0 range** followed by the summary route and its mask.

```
Border(config)#router ospf 1
Border(config-router)#area 0 range 192.168.10.0 255.255.255.128
```

Step 10: Recheck routing tables to verify the summarization

View the effects of summarization using the following commands:

```
Border#show ip ospf summary-address
```

Do the routers still have a route for Internet traffic? __________

Does Border have to report changes in individual subnets to the ISP? __________

If the connection to one particular subnet in this area went down, would the summary route be affected? __________

Think about your answers to the previous questions. What advantage do you see in using summarization in this network?

____

____

Step 11: Reflection

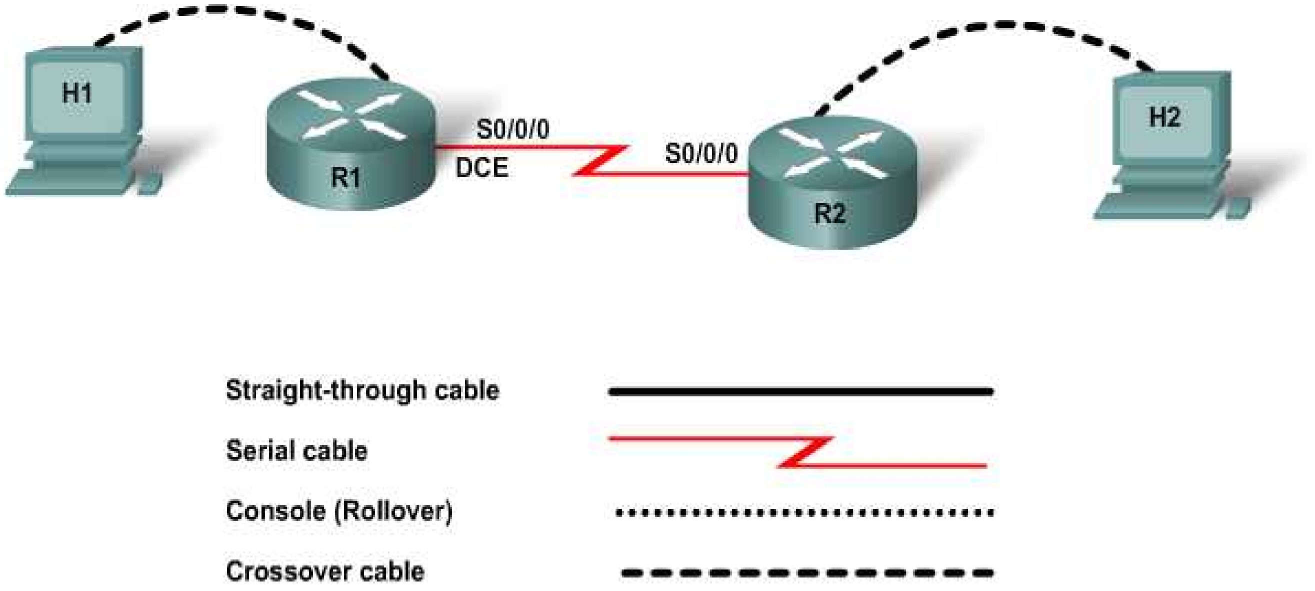
List three effects of using summarization within an OSPF area.

____

____

____

Lab 7.2.3.3 Configuring and Verifying a PPP Link



Device	Host Name	Serial 0/0/0 IP Address	Subnet Mask	Serial 0/0/0 Interface Type	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.15.1	255.255.255.252	DCE	class	cisco
Router 2	R2	192.168.15.2	255.255.255.252	DTE	class	cisco

Objectives

- Configure the serial interfaces on two routers to use PPP.
- Verify and test the link for connectivity.

Background / Preparation

Cable a network similar to the one shown in the topology diagram. Any router that has a single serial interface may be used for this lab. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination are acceptable.

The information in this lab applies to other routers; however, command syntax may vary. Depending on the router model, the interfaces may be identified differently. For example, on some routers, Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The information in this lab applies to routers that use the Serial 0/0/0 notation. If the router in use differs, use the correct notation for the serial interface.

The following resources are required:

Two routers both with a serial interface

Two Windows-based PCs, each with a terminal emulation program

At least one RJ-45-to-DB-9 connector console cable to configure the routers

One 2-part (DTE/DCE) serial cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

Connect Router 1 and Router 2 with a serial cable connecting both Serial 0/0/0 interfaces as shown in the topology diagram.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

On Router 1, configure the hostname, IP addresses, and passwords as provided in the addressing table. Save the configuration.

Step 3: Perform basic configuration on Router 2

On Router 2, configure the hostname, IP addresses, and passwords as provided in the addressing table. Save the configuration.

Step 4: Show the details of Serial 0/0/0 interface on R1

Enter the command **show interface serial 0/0/0** to view the details of the interface.

```
R1#show interface serial 0/0/0
```

What is the status of Serial 0/0/0? __________

Line Protocol is __________

The Internet address is ______________________________

Encapsulation is __________

Step 5: Show the details of Serial 0/0/0 interface on R2

Enter the command **show interface serial 0/0/0** to view the details of the interface.

```
R2#show interface serial 0/0/0
```

What is the status of Serial 0/0/0? __________

Line Protocol is __________

The Internet address is ______________________________

Encapsulation is __________

Step 6: Turn on PPP debugging

Turn on the PPP debug function on both routers by entering **debug ppp negotiation** at the privileged EXEC mode prompt.

```
R1#debug ppp negotiation
R2#debug ppp negotiation
```

NOTE: Debugging output is assigned high priority in the CPU process and can render a system unusable. When working on a live network, use **debug** only during periods of low network traffic.

Step 7: Change the encapsulation type

a. Change the encapsulation type to PPP by entering **encapsulation ppp** at the interface Serial 0/0 configuration mode prompt on both routers.

```
R1(config-if)#encapsulation ppp
R2(config-if)#encapsulation ppp
```

What did the debug function report when the PPP encapsulation was applied to each router?

____

____

____

____

Turn off the debug function by entering **undebug all** at the privileged EXEC mode prompt of both routers.

```
R1#undebug all
R2#undebug all
```

Step 8: Show the details of Serial 0/0/0 interface on R1

Enter the command **show interface serial 0/0/0** to view the details of the interface.

```
R1#show interface serial 0/0/0
```

What is the status of Serial 0/0/0? __________

Line Protocol is __________

The Internet address is ______________________________

Encapsulation is __________

Step 9: Show the details of Serial 0/0/0 interface on R2

Enter the command **show interface serial 0/0/0** to view the details of the interface.

```
R2#show interface serial 0/0/0
```

What is the status of Serial 0/0/0? __________

Line Protocol is __________

The Internet address is ______________________________

Encapsulation is __________

Step 10: Verify that the serial connection is functioning

a. Ping from R1 to R2 to verify that there is connectivity between the two routers.

```
R1#ping 192.168.15.2
R2#ping 192.168.15.1
```

Can the serial interface on the R2 router be pinged from R1? __________

Can the serial interface on the R1 router be pinged from R2? __________

If the answer is no for either question, troubleshoot the router configurations to find the error. Repeat the pings until they are successful.

Step 11: Reflection

a. What command allows you to view the details of a specific interface?

____

____

When should you use the debug function in a router?

____

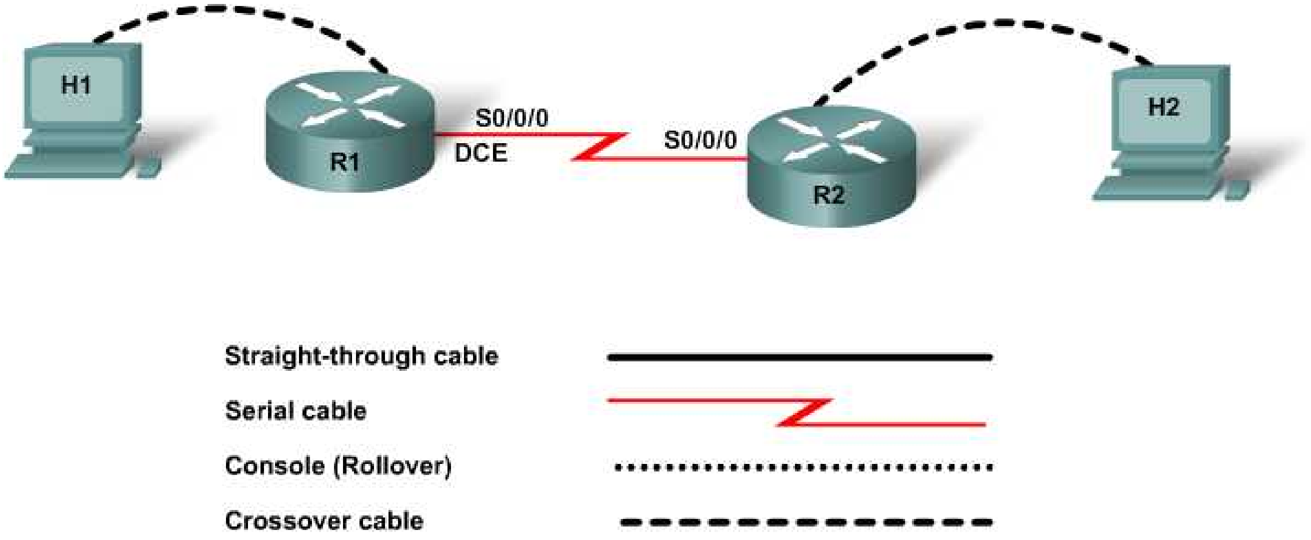
____

____

What is the default serial encapsulation on a Cisco router?

____

Lab 7.2.5.3 Configuring and Verifying PAP and CHAP Authentication



Device	Host Name	Serial 0/0/0 IP Address	Subnet Mask	Serial 0/0/0 Interface Type	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.15.1	255.255.255.0	DCE	class	cisco
Router 2	R2	192.168.15.2	255.255.255.0	DTE	class	cisco

Objectives

- Configure PPP authentication using PAP and CHAP.
- Verify connectivity using **show** and **debug** commands.

Background / Preparation

Cable a network similar to the one shown in the topology diagram. Any router that has a single serial interface may be used for this lab. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination are acceptable.

The information in this lab applies to other routers; however, command syntax may vary. Depending on the router model, the interfaces may be identified differently. For example, on some routers, Serial0 may be Serial0/0 or Serial0/0/0 and Ethernet0 may be FastEthernet0/0. The information in this lab applies to routers that use the Serial0/0/0 notation. If the router in use differs, use the correct notation for the serial interface.

The following resources are required:

- Two routers both with a serial connection
- Two Windows-based PCs, each with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the routers
- One 2-part (DTE/DCE) serial cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

Connect Router 1 and Router 2 with a serial cable connecting both Serial 0/0/0 interfaces as shown in the topology diagram.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Router 1, configure the hostname, IP addresses, and passwords as provided in the addressing table. Save the configuration.

Step 3: Perform basic configuration on Router 2

On Router 2, configure the hostname, IP addresses, and passwords as provided in the addressing table. Save the configuration.

Step 4: Configure PPP encapsulation on both R1 and R2

Change the encapsulation type to PPP by entering **`encapsulation ppp`** at the interface Serial 0/0 configuration mode prompt on both routers.

```
R1(config-if)#encapsulation ppp
R2(config-if)#encapsulation ppp
```

Step 5: Verify PPP encapsulation on R1 and R2

Enter the command **`show interface serial 0/0`** to verify the PPP encapsulation on R1 and R2.

```
R1#show interface serial 0/0/0
R2#show interface serial 0/0/0
```

Is R1 using PPP encapsulation? __________

Is R2 using PPP encapsulation? __________

Step 6: Verify that the serial connection is functioning

Ping from R1 to R2 to verify that there is connectivity between the two routers.

```
R1#ping 192.168.15.2
R2#ping 192.168.15.1
```

Can the serial interface on the R2 router be pinged from R1? __________

Can the serial interface on the R1 router be pinged from R2? __________

If the answer is no for either question, troubleshoot the router configurations to find the error. Repeat the pings until they are successful.

Step 7: Turn on PPP debugging

To display the authentication exchange process as it occurs, issue the command **debug ppp authentication** at the privileged EXEC mode prompt.

```
R1#debug ppp authentication
R2#debug ppp authentication
```

NOTE: Debugging output is assigned high priority in the CPU process and can render a system unusable. When working on a live network, use **debug** only during periods of low network traffic.

Step 8: Configure PPP authentication on R1 with PAP

a. Configure the username and password on the R1 router. The username must be identical to the hostname of the other router. Both the password and usernames are case-sensitive. On the router, define the username and password to expect from the remote router. On Cisco routers, the secret password must be the same for both routers.

```
R1(config)#username R2 password cisco
R1(config)#interface serial 0/0/0
R1(config-if)#ppp authentication pap
```

b. In Cisco IOS releases 11.1 or later, PAP must be enabled on the interface because it is disabled by default. From the Serial 0/0/0 interface configuration mode prompt, enable PAP on the interface.

```
R1(config-if)#ppp pap sent-username R1 password cisco
```

Step 9: Verify that the serial connection is functioning

Verify that the serial connection is functioning by pinging the serial interface of R2.

Was it successful? __________

Why or why not? ____

Step 10: Configure PPP authentication on R2 with PAP

a. Configure the username and password on the R2 router. The username and password must be identical to the hostname and password of the other router. Both the password and user names are case-sensitive. On the router, define the username and password to expect from the remote router. On Cisco routers, the secret password must be the same for both routers.

```
R2(config)#username R1 password cisco
R2(config)#interface serial 0/0/0
R2(config-if)#ppp authentication pap
```

b. In Cisco IOS releases 11.1 or later, PAP must be enabled on the interface because it is disabled by default. From the Serial 0/0/0 interface configuration mode prompt, enable PAP on the interface.

```
R2(config-if)#ppp pap sent-username R2 password cisco
```

What did the debug function report when the PPP authentication was applied?

____

____

____

____

____

Which line reveals the outgoing authentication acknowledgment?

____

Which line reveals the incoming authentication request?

____

Step 11: Verify that the serial connection is functioning

Verify that the serial connection is functioning by pinging the serial interface of R1.

Was it successful? __________

Why or why not? ____

Step 12: Remove PAP from R1 and R2

Remove PAP from R1 and R2 by issuing the command **no** in front of the commands used to configure PAP.

```
R1(config)#interface serial 0/0/0
R1(config-if)#no ppp authentication pap
R1(config-if)#no ppp pap sent-username R1 password cisco
R1(config-if)#exit
R1(config)#no username R2 password cisco

R2(config)#interface serial 0/0/0
R2(config-if)#no ppp authentication pap
R2(config-if)#no ppp pap sent-username R2 password cisco
R2(config-if)#exit
R2(config)#no username R1 password cisco
```

Step 13: Configure PPP authentication on R1 with CHAP

a. If both CHAP and PAP are enabled, the first authentication method specified is requested during the link negotiation phase. If the peer suggests using the second method or simply refuses the first method, the second method is tried.

b. Save the configuration on R1 and R2 and reload both routers.

```
R1#copy running-config startup-config
R1#reload

R2#copy running-config startup-config
R2#reload
```

c. To display the authentication exchange process as it occurs, issue the command **debug ppp authentication** at the privileged EXEC mode prompt.

```
R1#debug ppp authentication
R2#debug ppp authentication
```

d. Configure the username and password on the R1 router. The username must be identical to the hostname of the other router. Both the password and usernames are case-sensitive. Define the username and password to expect from the remote router. On Cisco routers, the secret password must be the same for both routers.

```
R1(config)#username R2 password cisco
R1(config)#interface serial 0/0/0
R1(config-if)#ppp authentication chap
```

Step 14: Configure PPP authentication on R2 with CHAP

Configure the username and password on the R2 router. The passwords must be the same on both routers. The username must be identical to the hostname on the other router. Both the password and user names are case-sensitive. Define the username and password to expect from the remote router.

```
R2(config)#username R1 password cisco
R2(config)#interface serial 0/0/0
R2(config-if)#ppp authentication chap
```

What did the debug function report when CHAP was applied on R2?

____

____

____

____

____

Which authentication method is being used? _____________

What line specifies the incoming authentication request?

____

Which line identifies the outgoing authentication acknowledgment?

____

Step 15: Verify that the serial connection is functioning

Verify that the serial connection is functioning by pinging the serial interface of R1.

Was it successful? __________

Why or why not?

____

____

Step 16: Verify the serial line encapsulation on R1

Enter the command **show interface serial 0/0** to view the details of the interface.

```
R1#show interface serial 0/0/0
```

What is the status of Serial 0/0/0? __________

Line Protocol is __________

Encapsulation is __________

Is the LCP open? __________

How many NCPs have been established? __________

Step 17: Verify the serial line encapsulation on R2

Enter the command **show interface serial 0/0/0** to view the details of the interface.

```
R2#show interface serial 0/0/0
```

What is the status of Serial 0/0/0 __________

Line Protocol is __________

Encapsulation is __________

Is the LCP open? __________

How many NCPs have been established? __________

Step 18: Turn off debugging on both R1 and R2

Turn off all debugging by issuing the **undebug all** command on both R1 and R2.

```
R1#undebug all
R2#undebug all
```

Step 19: Reflection

a. What is an advantage of using CHAP over PAP?

____

____

____

____

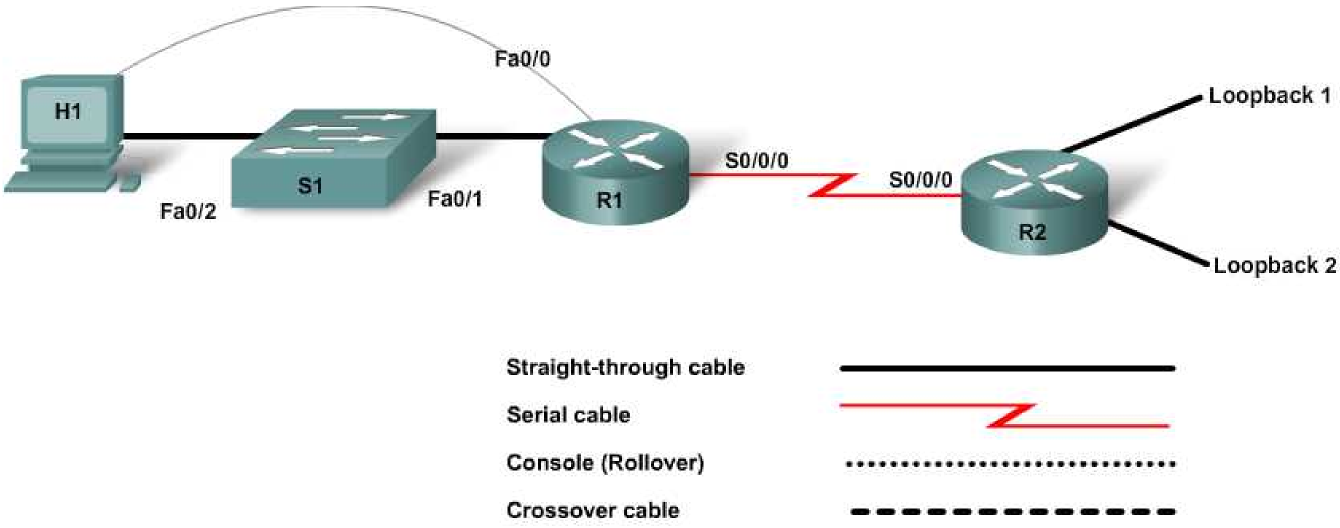
b. Which PPP protocol is used for establishing a point-to-point link?

____

c. Which PPP protocol is used for configuring the various Network Layer protocols?

____

Lab 8.3.3 Configuring and Verifying Standard ACLs



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Loopback Interface Addresses	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.200.1/24	192.168.100.1/30	DCE	n/a	class	cisco
Router 2	R2	n/a	192.168.100.2/30	DTE	Lo0 192.168.1.1 Lo1 192.168.2.1	class	cisco
Switch 1	S1	n/a	n/a	n/a	n/a	class	cisco

Objectives

- Configure standard ACLs to limit traffic.
- Verify ACL operation.

Background / Preparation

In this lab you will work with Standard ACLs to control network traffic based on host IP addresses. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab is based on the 1841 series router. Other routers may be used; however, command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two Cisco 1841 series routers or equivalent, each with a serial and an Ethernet interface
- One Windows-based PC with a terminal emulation program and set up as a host
- At least one RJ-45-to-DB-9 console cable to configure the routers and switch
- Two straight-through Ethernet cables
- One 2-part DTE/DCE serial crossover cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

c. Connect a console cable to the PC to perform configurations on the routers and switch.

d. Connect H1 to the Fa0/2 port of Switch 1 using a straight-through cable.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Router 1, configure the hostname, interfaces, passwords, and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram. Save the configuration.

Step 3: Perform basic configuration on Router 2

Perform basic configuration on Router 2 and save the configuration.

Step 4: Perform basic configuration on Switch 1

Configure Switch 1 with a hostname and passwords according to the addressing table and topology diagram.

Step 5: Configure the host with IP address, subnet mask, and default gateway

a. Configure the host with the proper IP address, subnet mask, and default gateway. The host should be assigned the address 192.168.200.10/24 and the default gateway of 192.168.200.1.

b. The workstation should be able to ping the attached router. If the ping is not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure RIP routing and verify end-to-end connectivity in the network

a. On Router 1, enable the RIP routing protocol and configure it to advertise both connected networks.

b. On Router 2, enable the RIP routing protocol and configure it to advertise all three connected networks.

c. Ping from Host 1 to the two loopback interfaces on Router 2.

Were the pings from Host 1 successful? __________

If the answer is no, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

Step 7: Configure and test a standard ACL

In this lab topology, the loopback interfaces on R2 simulate two Class C networks connected to the router. ACLs will be used to control access to these subnets. The loopback 0 interface will represent a network of management workstations, and the loopback 1 interface will represent a limited-access engineering network.

In this network, it is necessary to have at least one management workstation on the 192.168.200.0/24 subnet along with other user workstations. The management workstation is assigned a static IP address of 192.168.200.10. The user workstations consume the rest of the IP addresses on the network.

The ACL should allow the management workstation access to the networks attached to R2, but not allow access to these networks from the other hosts on the 192.168.200.0 network.

A Standard ACL is being used and will be placed on R2, because R2 is closest to the destination.

a. Create a Standard ACL on R2 to be used for access to the attached networks. This ACL will allow the 192.168.200.10 host access and deny all others.

```
R2(config)#access-list 1 permit 192.168.200.10
R2(config)#access-list 1 deny any
```

NOTE: The implicit **deny** at the end of an access control list performs this same function. However, adding the line to the ACL helps document it and is considered good practice. By explicitly adding this statement, the number of packets matching the statement are tallied, and the administrator can see how many packets were denied.

b. After the ACL has been created, it must be applied to an interface on the router. Use the Serial 0/0/0 interface to allow control to both the 192.168.1.0 and 192.168.2.0 networks. Potential traffic would be flowing into the interface; therefore, apply the ACL in the inbound direction.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group 1 in
```

c. Now that the ACL has been created and applied, use the **show access-lists** command on R2 to view the ACL.

Are there any matches for either ACL statement? __________

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.200.10
    20 deny   any
```

Does the output of the **show access-lists** command display the ACL that was created?

____

Does the output of the **show access-lists** command display how the ACL is applied?

____

d. Use the **show ip interface s0/0/0** command to display the application of the ACL.

What does the output of the **show ip interface** command tell you about the ACL?

____

Step 8: Test the ACL

a. From Host 1, ping the 192.168.1.1 loopback address.

Is the ping successful? __________

b. From Host 1, ping the 192.168.2.1 loopback address.

Is the ping successful? __________

c. Issue the **show access-list** command again.

How many matches are there for the first ACL statement (`permit`)? __________

```
R2#show access-lists
Standard IP access list 1
    permit 192.168.200.10 (16 matches)
    deny   any
```

How many matches are there for the second ACL statement (`deny`)? __________

d. View the routing table on R2 using the **`show ip route command`**.

What route is missing from the routing table? ____

The route is missing from the routing table because the ACL only permits packets from 192.168.200.10. RIP update packets from R1 are sourced from the router Serial 0/0/0 interface 192.168.100.1 and are denied by the ACL. Because R1 RIP updates advertising the 192.168.200.0 network are blocked by the ACL, R2 has no knowledge of the 192.168.200.0 network. The pings that were done earlier were not blocked by the ACL. They failed because R2 could not return the echo reply; R2 did not know how to get to the 192.168.200.0 network.

This example shows why ACLs must be programmed carefully and tested thoroughly for functionality.

e. Recreate the ACL on R2 to allow for routing updates to be received from R1.

```
R2(config)#no access-list 1
R2(config)#access-list 1 permit 192.168.200.10
R2(config)#access-list 1 permit 192.168.100.1
R2(config)#access-list 1 deny any
```

f. Ping 192.168.1.1 and 192.168.2.1 from Host 1.

Are the pings now successful? ___________

g. Change the IP address on Host 1 to 192.168.200.11.

h. Again ping 192.168.1.1 and 192.168.2.1 from Host 1.

Are the pings successful? __________

Display the ACL again using the **`show access-lists`** command.

Are there matches for the 192.168.100.1 ACL statement? __________

NOTE: You can clear the ACL counters using the **`clear ip access-list counters`** command from the privileged EXEC prompt.

Step 9: Reflection

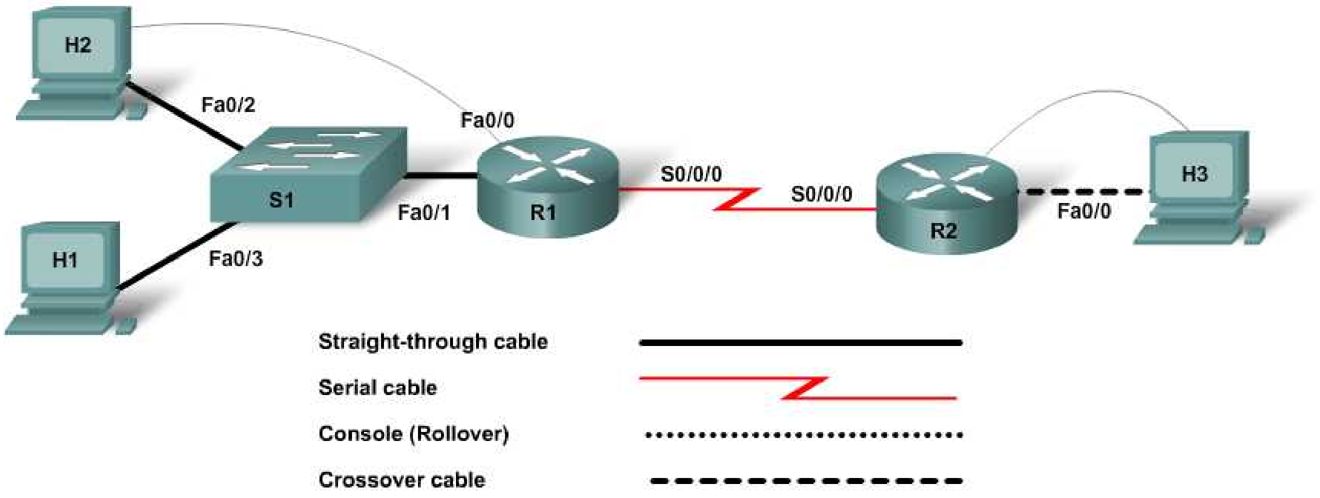
a. Why is careful planning and testing of access control lists required?

____

b. What is the main limitation of standard ACLs?

____

Lab 8.3.4 Planning, Configuring and Verifying Extended ACLs



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0/ IP Address	Serial 0/0/0 Interface Type	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	192.168.15.1/30	DCE		class	cisco
Router 2	R2	192.168.5.1/24	192.168.15.2/30	DTE		class	cisco
Switch 1	S1					class	cisco
Host 1	H1	192.168.1.10/24			192.168.1.1		
Host 2	H2	192.168.1.11/24			192.168.1.1		
Host 3	H3	192.168.5.10/24			192.168.5.1		

Objectives

- Configure Extended ACLs to control traffic.
- Verify ACL operation.

Background / Preparation

In this lab you will work with Extended ACLs to control network traffic based on host IP addresses. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to 1841 series routers. It also apples to other routers; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or equivalent routers, each with a serial and an Ethernet interface
- Three Windows-based PCs, at least one with a terminal emulation program, and all set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Three straight-through Ethernet cables
- One crossover Ethernet cable
- One 2-part DTE/DCE serial crossover cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

c. Connect a console cable to each PC to perform configurations on the routers and switch.

d. Connect Host 1 to the Fa0/3 port of Switch 1 using a straight-through cable.

e. Connect Host 2 to the Fa0/2 port of Switch 1 using a straight-through cable.

f. Connect a crossover cable between Host 3 and the Fa0/0 interface of Router 2.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Router 1, configure the hostname, interfaces, passwords, and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram. Save the configuration.

Step 3: Perform basic configuration on Router 2

Perform basic configuration on Router 2 and save the configuration.

Step 4: Perform basic configuration on Switch 1

Configure Switch 1 with a hostname, console, Telnet, and privileged passwords according to the addressing table and topology diagram.

Step 5: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure the hosts with IP address, subnet mask, and default gateway according to the addressing table and the topology diagram.

b. Each workstation should be able to ping the attached router. If the pings are not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure RIP routing and verify end to end connectivity in the network

a. On R1, enable the RIP routing protocol and configure it to advertise both connected networks.

b. On R2, enable the RIP routing protocol and configure it to advertise both connected networks.

c. Ping from each host to the other two hosts.

Were the pings successful? __________

If the answer is no, troubleshoot the router and host configurations to find the error. Ping again until they are all successful.

Step 7: Configure Extended ACLs to control traffic

Host 3 in this network contains proprietary information. Security requirements for this network dictate that only certain devices should be allowed access to this machine. Host 1 is the only host that will be allowed to access this computer. All other hosts on this network are used for guest access and should not be allowed access to Host 3. In addition, Host 3 is the only computer in the network that is allowed to access R1 interfaces for remote management. Extended ACLs will be used to control access on this network.

a. Itemize the list of requirements for clarity:

1) Host 1 can access Host 3. All other hosts (on that network only) cannot access Host 3. Any additional hosts added on other networks in the future should be able to access Host 3 because they will not be guest-accessible machines.

2) Host 3 can access the R1 interfaces. All other devices on the network will not have access.

b. Analyze the requirements and determine placement of Extended access control lists.

Based on the requirements, the traffic that needs to be controlled is the traffic traveling out of the R2 Fa0/0 interface and destined for Host 3. Therefore, the access control list should be placed on the R2 Fa0/0 interface.

c. Create an Extended ACL to perform the tasks stated and apply it to R2.

```
R2(config)#access-list 101 permit ip host 192.168.1.10 host
192.168.5.10
R2(config)#access-list 101 deny ip 192.168.1.0 0.0.0.255 host
192.168.5.10
R2(config)#access-list 101 permit ip any any
R2(config)#access-list 101 deny ip any any
```

NOTE: The implicit **deny** at the end of an access control list performs this same function. However, adding the line to the ACL helps document it and is considered good practice. By explicitly adding this statement, the number of packets matching the statement are tallied, and the administrator can see how many packets were denied.

d. Apply the access list on the Fa0/0 interface of R2 in the outbound direction.

```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip access-group 101 out
```

e. Verify the ACL on R2 with the **show access-lists** command.

Does the output of the **show access-lists** command display the ACL that was created?

____

Does the output of the **show access-lists** command display how the ACL is applied?

____

f. Use the **show ip interface fa0/0** command on R2 to display the application of the ACL.

What does the output of the **show ip interface** command tell you about the ACL?

____

Step 8: Test the ACL

a. Ping Host 3 from both Hosts 1 and 2.

Can Host 1 ping Host 3? __________

Can Host 2 ping Host 3? __________

b. To verify that other addresses can ping Host 3, ping Host 3 from R1.

Is the ping successful? __________

c. Display the access control list again with the **show access-lists** command.

What additional information is displayed beyond just the access list statements?

____

d. Remove this access control list before continuing.

Step 9: Configure and test the ACL for the next requirement

a. Host 3 is the only host that should be allowed to connect to R1 for remote management. Create an access control list to meet this requirement. This ACL will need to be placed on R1 because R1 is the destination of the traffic. All other hosts will not be allowed access. This is the only traffic being controlled; all other traffic should be allowed.

```
R1(config)#access-list 101 permit ip host 192.168.5.10 host
192.168.15.1
```

```
R1(config)#access-list 101 permit ip host 192.168.5.10 host 192.168.1.1
R1(config)#access-list 101 deny ip any host 192.168.15.1
R1(config)#access-list 101 deny ip any host 192.168.1.1
R1(config)#access-list 101 permit ip any any
R1(config)#access-list 101 deny ip any any
```

b. Because the source traffic could come from any direction, this ACL needs to be applied to both interfaces on R1. The traffic to be controlled would be inbound to the router.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 101 in
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip access-group 101 in
```

c. Now attempt to telnet to R1 from all hosts and R2. Attempt to telnet to both R1 addresses.

Can you telnet to R1 from any of these devices? If yes, which one(s)? ____________________

d. View the output of the **`show access-lists`** command on R1.

Does the output of the **`show access-lists`** command display that the statements are being matched? __________

Step 11: Reflection

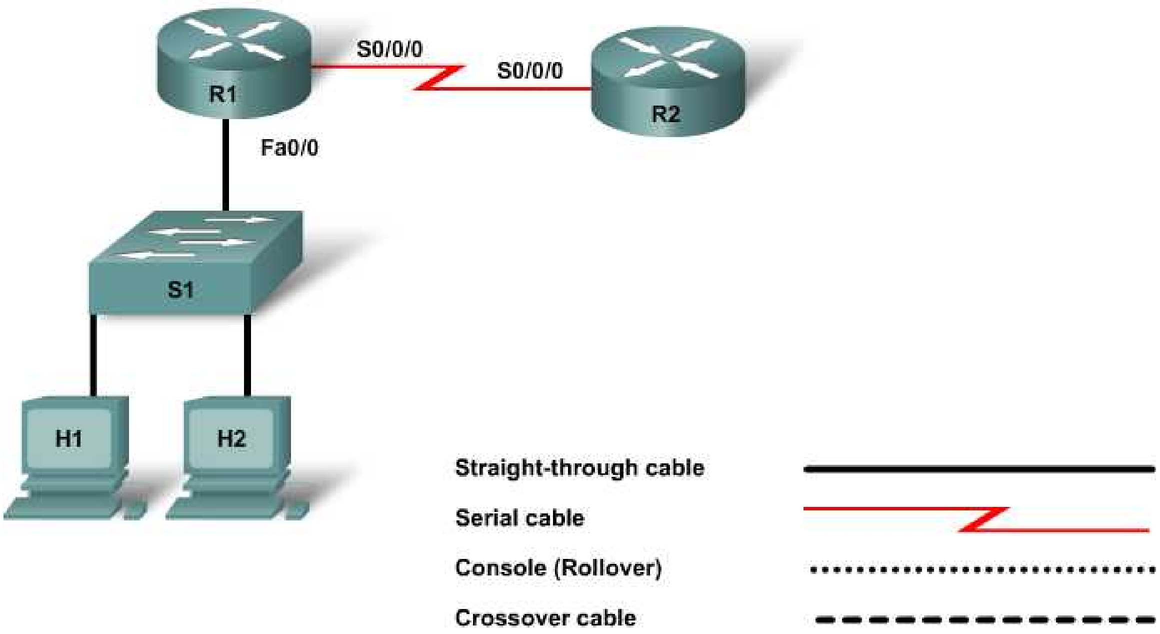
a. Why is careful planning and testing of access control lists required?

____

b. What is an advantage of using Extended ACLs over Standard ACLs?

____

Lab 8.3.5 Configuring and Verifying Extended Named ACLs



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.15.1/24	209.165.201.1/30	DTE		class	cisco
Router 2	R2		209.165.201.2/30	DCE		class	cisco
Switch 1	S1					class	cisco
Host 1	H1	192.168.15.2/24			192.168.15.1		
Host 2	H2	192.168.15.3/24			192.168.15.1		

Objectives

- Create Standard and Extended Named ACLs.
- Test the ACLs to determine whether they achieve the desired results.
- Edit a Named ACL.

Background / Preparation

In this lab you will work with Named Standard and Extended ACLs to control network traffic based on host IP addresses. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to 1841 routers. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or comparable routers, each with a serial connection and an Ethernet interface
- Two Windows-based PCs, both with a terminal emulation program, and both set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Three straight-through Ethernet cables
- One 2-part (DTE/DCE) serial crossover cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable as shown in the diagram and addressing table.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

c. Connect Host 1 to the Fa0/2 port of Switch 1 using a straight-through cable.

d. Connect Host 2 to the Fa0/3 port of Switch 1 using a straight-through cable.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Router 1 configure the hostname, interfaces, passwords, and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram. Save the configuration.

Step 3: Perform basic configuration on Router 2

Step 4: Perform basic configuration on Switch 1

Step 5: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure the hosts IP address, subnet mask, and default gateway according to the addressing table and the topology diagram.

b. Each workstation should be able to ping R1 and each other. If the pings are not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Verify that the network is functioning

a. From the attached hosts, ping the FastEthernet interface of the default gateway router.

Was the ping from Host 1 successful? __________

Was the ping from Host 2 successful? __________

If the answer is no for either question, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

b. Use the command **`show ip interface brief`** and check the status of each interface.

What is the state of the interfaces on each router?

R1:

FastEthernet 0/0: ____________________

Serial 0/0/0: ________________________

Serial 0/0/1: ________________________

R2:

FastEthernet 0/0: ____________________

Serial 0/0/0: ________________________

Serial 0/0/1: ________________________

c. Ping from the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2.

Was the ping successful? __________

If the answer is no, troubleshoot the router configurations to find the error. Ping again until successful.

Step 7: Configure static and default routing on the routers.

a. Configure a default route on R1. Use the next hop interface on R2 as the path.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

b. From one of the host PCs on R1, ping R2.

Why is the ping unsuccessful?

____

c. Configure a static route on R2 to the R1 192.168.15.0 network. Use the next hop interface on R1 as the path.

```
R2(config)#ip route 192.168.15.0 255.255.255.0 209.165.201.1
```

d. From one of the host PCs on R1, ping R2.

Did the ping succeed? __________

If the ping did not succeed, troubleshoot the static and default routes.

Step 8: Configure and test a simple Named Standard ACL

a. Create a Named ACL that allows H2 to reach other hosts on the local network but does not allow H2 to access remote networks. At the configuration prompt, use this command sequence:

```
R1(config)#ip access-list standard H2_no_access
R1(config-std-nacl)#deny host 192.168.15.3
R1(config-std-nacl)#permit any
```

Why do you need the third statement? ____

b. Apply the ACL to the interface.

```
R1(config)#interface fastethernet0/0
R1(config-if)#ip access-group H2_no_access in
```

Describe how you should test this ACL: ____

____

c. Conduct the tests to verify that this ACL achieves its goals. If it does not, troubleshoot by viewing the output of a **show running-config** command to verify that the ACL is present and applied to the correct interface.

Step 9: Create and test a Named Extended ACL

a. Create a Named ACL that does not allow H1 to ping R2 but allows H1 to reach the local network and R1.

```
R1(config)#ip access-list extended H1_limit_access
R1(config-ext-nacl)#deny ip host 198.168.15.2 host 209.165.201.2
R1(config-ext-nacl)#permit ip any any
```

b. Apply the ACL to the interface.

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group H1_limit_access out
```

Describe how you would test this ACL: ____

____

c. Conduct the tests to verify that this ACL achieves its goals. If it does not, troubleshoot by viewing the output of a **show running-config** command to verify that the ACL is present and applied to the correct interface.

Step 10: Edit a Named Standard ACL

a. You have decided to edit the Named Standard ACL. In privileged EXEC mode, view the access list statements.

```
R1#show access-list
Standard IP access list H2_no_access
    10 deny host 192.168.15.3
    20 permit any
```

b. Add a line to this Named Standard ACL to block H1 from reaching R1, but still permit H1 and H2 to reach each other.

Enter configuration commands, one per line. End with **CNTL/Z**.

```
R1(config)#ip access-list standard H2_no_access
R1(config-std-nacl)#15 deny host 192.168.15.2
```

c. View the edited ACL to verify that all statements are present.

```
R1#show access-list
Standard IP access list H2_no_access
    10 deny host 192.168.15.3
    15 deny host 192.168.15.2
    20 permit any
```

If you added a new PC to the topology, attached it to S1, and gave it the IP address 192.168.15.4/24, would it be able to reach R1? __________

Step 11: Reflection

a. Why is it good practice to perform basic configurations and verify connectivity before adding ACLs to routers?

____

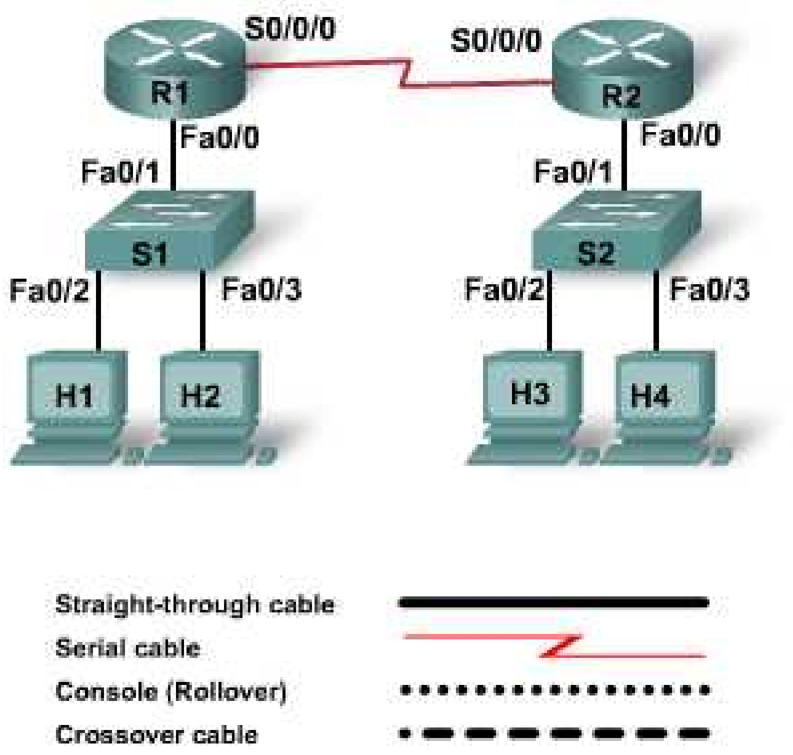
____

b. What advantages do Named ACLs offer?

____

____

Lab 8.3.6 Configuring and Verifying VTY Restrictions



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.15.1/24	192.168.16.1/24	DTE		class	cisco
Router 2	R2	192.168.17.1/24	192.168.16.2/24	DCE		class	cisco
Switch 1	S1					class	cisco
Switch 2	S2					class	cisco
Host 1	H1	192.168.15.2/24			192.168.15.1		
Host 2	H2	192.168.15.3/24			192.168.15.1		
Host 3	H3	192.168.17.2/24			192.168.17.1		
Host 4	H4	192.168.17.3/24			192.168.17.1		

Objectives

- Use access-class and line commands to control Telnet access to a router.
- Test the ACLs to determine whether they achieve the desired results.

Background / Preparation

In this lab you will work with vty ACLs to restrict Telnet access to a router. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Two Cisco 2960 switches or other comparable switches
- Two Cisco 1841 or comparable routers, each with a Serial connection and an Ethernet interface
- Four Windows-based PCs, both with a terminal emulation program, and both set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Six straight-through Ethernet cables
- One 2-part (DTE/DCE) serial crossover cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the S0/0/0 interface of Router 1 to the S0/0/0 interface of Router 2 using a serial cable as shown in the diagram and addressing table.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

c. Connect Host 1 to the Fa0/2 port of Switch 1 using a straight-through cable, and connect Host 2 to the Fa0/3 port of Switch 1 using a straight-through cable.

d. Connect Host 3 to the Fa0/2 port of Switch 2 using a straight-through cable, and connect Host 4 to the Fa0/3 port of Switch 2 using a straight-through cable.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. On Router 1, configure the hostname, interfaces, passwords and message-of-the-day banner and disable DNS lookups according to the addressing table and topology diagram. Save the configuration.

Step 3: Perform basic configuration on Router 2

Step 4: Perform basic configuration on Switch 1 and Switch 2

Step 5: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure the hosts IP address, subnet mask, and default gateway according to the table and the topology diagram.

b. Each workstation should be able to ping the attached router. If the pings were not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure dynamic routing on the routers

a. Configure RIP routing on R1. Advertise the appropriate networks.

b. Configure RIP routing on R2. Advertise the appropriate networks.

Step 7: Verify connectivity

a. If the network has converged, list four destinations that H1 should be able to ping:

____

b. Test connectivity by pinging all the destinations. If any pings fail, troubleshoot the configurations on the routers and host PCs.

c. Check the routing table on R1.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.15.0/24 is directly connected, FastEthernet0/0
R    192.168.17.0/24 [120/1] via 192.168.16.2, 00:00:09, Serial0/0/0
C    192.168.16.0/24 is directly connected, Serial0/0/0
```

How many routes should appear? __________

d. Verify that all routes appear in the routing table. If a route is missing, troubleshoot the router configuration.

e. Telnet from the hosts to both routers. All hosts should be able to Telnet to both routers. If Telnet fails, troubleshoot the router and host configurations.

Step 8: Configure and test an ACL that will limit Telnet access

a. Create a standard ACL that represents the LAN attached to R1.

```
R1(config)#access-list 1 permit 192.168.15.0 0.0.0.255
```

b. Now that you have defined the LAN traffic, you must apply it to the vty lines. This allows users from this LAN to Telnet to this router, but will block users from other LANs from accessing Telnet on this router.

```
R1(config)#line vty 0 4
R1(config-line)#access-class 1 in
R1(config-line)#end
```

Which PCs should be able to Telnet to R1 and which should not?

____

c. Test the restriction.

Step 9: Create vty restrictions for R2

a. Create a Standard ACL that will not allow hosts on the R1 LAN to Telnet to R2 but will allow hosts on the R2 LAN to Telnet to their attached router.

```
R2(config)#access-list 2 permit 192.168.17.0 0.0.0.255
R2(config)#line vty 0 4
R2(config-line)#access-class 2 in
R2(config-line)#end
```

b. Conduct the tests to verify that this ACL achieves its goals. If it does not, troubleshoot by viewing the output of a **`show running-config`** command to verify that the ACL is present and applied correctly.

Step 10: Reflection

Why is the vty restriction ACL a good practice when configuring a router?

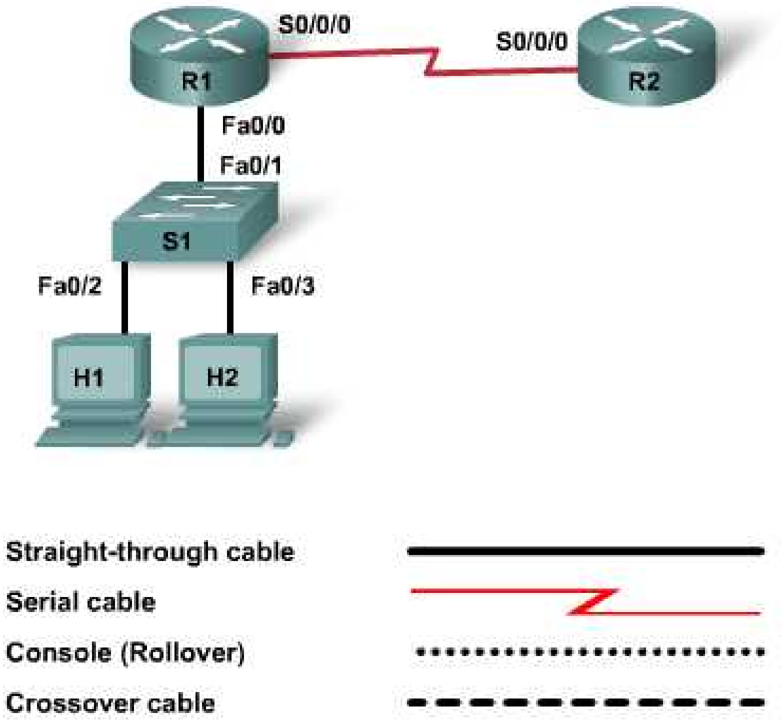
____

____

____

____

Lab 8.4.3 Configuring an ACL with NAT



Device	Host Name	FastEthernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	209.165.201.1/30	DTE		class	cisco
Router 2	R2		209.165.201.2/30	DCE		class	cisco
Switch 1	S1					class	cisco
Host 1	H1	192.168.1.2/24			192.168.1.1		
Host 2	H2	192.168.1.3/24			192.168.1.1		

Objectives

- Configure NAT and PAT and verify functionality.
- Configure and apply an ACL to an interface where NAT occurs.
- Observe the effects of ACL placement when using NAT.

Background / Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 series of routers. It also applies to other routers; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two 1841 or equivalent series routers, each with a serial connection and an Ethernet interface
- Two Windows-based PCs, both with a terminal emulation program, and both set up as hosts
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Three straight-through Ethernet cables
- One 2-part (DTE/DCE) serial cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable as shown in the diagram and addressing table.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

c. Connect each PC with a console cable to perform configurations on the router and switches.

d. Connect Host 1 to the Fa0/2 port of Switch 1 using a straight-through cable.

e. Connect Host 2 to the Fa0/3 port of Switch 1 using a straight-through cable.

Step 2: Perform basic configuration on Router 1

a. Connect a PC to the console port of the router to perform configurations using a terminal emulation program.

b. Configure Router 1 with a hostname, interfaces, console, Telnet, IP addresses, and privileged passwords according to the addressing table and topology diagram. Save the configuration.

Step 3: Perform basic configuration on Router 2

Perform basic configuration on Router 1 as the gateway router with a hostname, interfaces, console, Telnet, and privileged passwords according to the addressing table and topology diagram. Save the configuration.

Step 4: Perform basic configuration on Switch 1

a. Configure Switch 1 with a hostname and console, telnet and privileged passwords according to the table and topology diagram.

Step 5: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway.

b. Each workstation should be able to ping the attached router. If the ping was not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure static and default routes on the routers

a. Configure a static route on router R2 to reach the private network on R1. Use the next hop interface on R1 as the path.

```
R2(config)#ip route 192.168.1.0 255.255.255.0 209.165.201.1
```

b. Configure a default route on router R1 to forward any unknown destination traffic to the next hop interface on R2.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

Step 7: Verify that the network is functioning

a. From the attached hosts, ping the FastEthernet interface of the default gateway router.

Was the ping from Host 1 successful? __________

Was the ping from Host 2 successful? __________

If the answer is no for either question, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

b. From each host, ping the Serial 0/0/0 interface of R2.

Each ping should be successful. If it is not, troubleshoot the static and default route configurations to find the error. Ping again until they are both successful.

Step 8: Configure NAT and PAT on R1

a. Define an access list that matches the inside private IP addresses.

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

b. Define the PAT translation from inside the list to outside.

```
R1(config)#ip nat inside source list 1 interface s0/0/0 overload
```

c. Specify the interfaces.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip nat outside
```

Where will the private IP address of a host be translated? ___________________________

____

Step 9: Test and verify the configuration

a. Ping PC2 from PC1.

Was it successful? ________

b. Ping the serial interface on R2 from PC1 and PC2.

Was it successful? _______

c. Verify that NAT translations are taking place by using the command **show ip nat translations** (a sample output is shown).

```
Pro  Inside global    Inside local   Outside local     Outside global
icmp 209.165.201.1:2  192.168.1.2:2  209.165.201.2:2   209.165.201.2:2
icmp 209.165.201.1:3  192.168.1.2:3  209.165.201.2:3   209.165.201.2:3
icmp 209.165.201.1:4  192.168.1.2:4  209.165.201.2:4   209.165.201.2:4
icmp 209.165.201.1:5  192.168.1.2:5  209.165.201.2:5   209.165.201.2:5
icmp 209.165.201.1:10 192.168.1.3:10 209.165.201.2:10  209.165.201.2:10
icmp 209.165.201.1:7  192.168.1.3:7  209.165.201.2:7   209.165.201.2:7
icmp 209.165.201.1:8  192.168.1.3:8  209.165.201.2:8   209.165.201.2:8
icmp 209.165.201.1:9  192.168.1.3:9  209.165.201.2:9   209.165.201.2:9
```

How does the output indicate that PAT is being used?

____

Step 10: Configure and apply an ACL designed to filter traffic from one host

a. Prevent PC1 from reaching R2, while allowing other traffic to flow freely.

```
R1(config)#access-list 10 deny 192.168.1.2
R1(config)#access-list 10 permit any
```

b. Apply the ACL to the serial interface of R1.

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 10 out
```

Step 11: Test the effects of the ACL on network traffic

a. Ping from PC1 to PC2, and from PC1 to its default gateway.

Were the pings successful? __________

b. Ping from PC1 to the serial interface of R2.

Was the ping successful? __________

c. Ping from PC2 to the serial interface of R2.

Was the ping successful? __________

Is the ACL producing the desired results? __________

What would you expect to see if you viewed the NAT translation table?

____

Step 12: Move the ACL and retest

a. Remove the ACL from the serial interface of R1.

```
R1(config)#interface s0/0/0
R1(config-if)#no ip access-group 10 out
```

b. Place the ACL on the FastEthernet interface instead.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 10 in
```

c. Retest the ACL using the pings from Step 11.

Describe the results this time.

____

Is the ACL producing the desired results? __________

Step 13: Reflection

a. What is the role of the serial interface IP of R1 in NAT and PAT? (Refer back to the output shown in Step 9.)

____

____

b. List, in the order in which they occurred, the changes that happened to the PC1 IP address when the ACL was placed on the R1 serial interface.

____

____

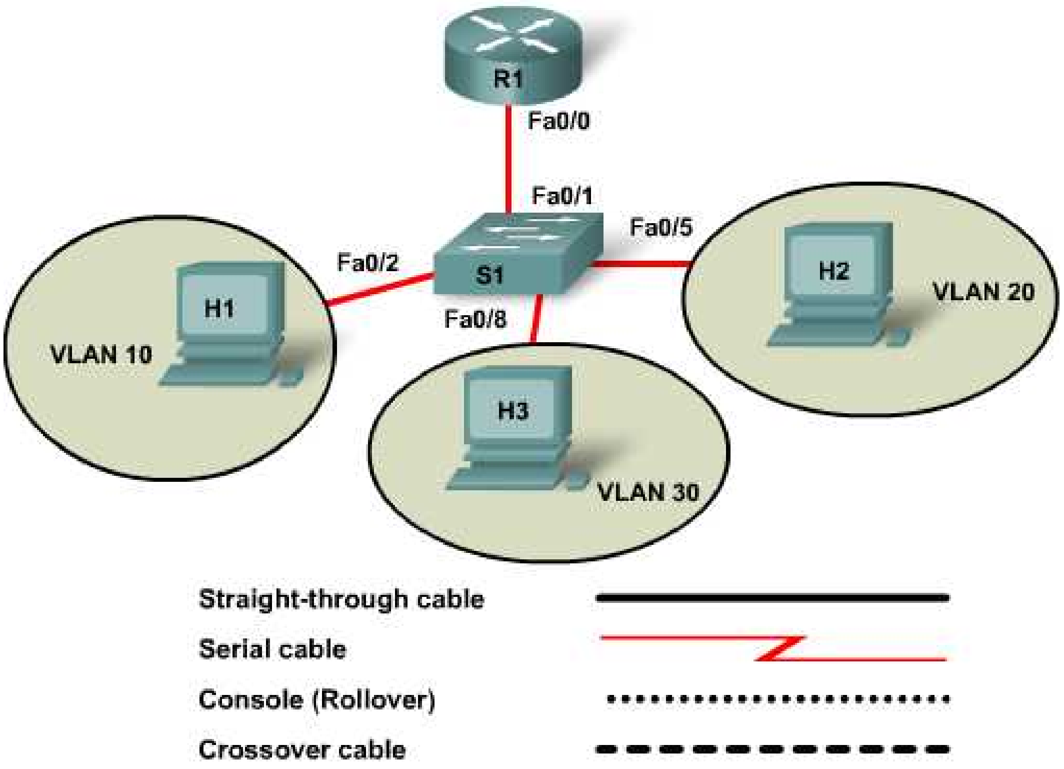
____

c. Why did moving the ACL to the FastEthernet interface produce the desired results?

____

____

Lab 8.4.5 Configuring and Verifying ACLs to filter Inter-VLAN Traffic



Device	Host Name	FastEthernet IP Address	Default Gateway IP Address	VLAN Names and Numbers	Switch Port Assignments	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	Fa0/0: none Fa0/0.1: 192.168.1.1/24 Fa0/0.2: 192.168.2.1/24 Fa0/0.3: 192.168.3.1/24 Fa0/0.4: 192.168.4.1/24				class	cisco
Switch 1	S1	192.168.1.2/24	192.168.1.1	VLAN 1 Native VLAN 10 Servers VLAN 20 Users1 VLAN 30 Users2	Fa0/1 Fa0/2 Fa0/5 Fa0/8	class	cisco
Host 1	H1	192.168.2.10/24	192.168.2.1				
Host 2	H2	192.168.3.10/24	192.168.3.1				
Host 3	H3	192.168.4.10/24	192.168.4.1				

Objectives

- Configure VLANs on a switch.
- Configure and verify trunking.
- Configure a router for inter-VLAN routing.
- Configure, apply, and test an ACL to filter inter-VLAN traffic.

Background / Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may also work; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 or comparable switch
- One Cisco 1841 or comparable router
- Three Windows-based PCs, each with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the router and switch
- Four straight-through Ethernet cables

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

b. Connect PCs with console cables to perform configurations on the router and switch.

c. Connect the host PCs with straight-through cables to the following switch ports: Host 1, to Fa0/2; Host 2, to Fa0/5; Host 3, to Fa0/8.

Step 2: Perform basic configuration on Router 1

Step 3: Configure R1 to support inter-VLAN traffic

The FastEthernet 0/0 interface on R1 will be subinterfaced to route traffic from each of the three VLANs. Each subinterface IP address will become the default gateway for its designated VLAN.

```
R1#configure terminal
R1(config)#interface fastethernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/0.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.2
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.3
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.3.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.4
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.4.1 255.255.255.0
R1(config-subif)#end
R1#copy running-config startup-config
```

Why is the **`no shutdown`** command performed only on interface FastEthernet 0/0?

____

Why is it necessary to specify the encapsulation type on each subinterface?

____

Step 4: Perform basic configuration on Switch 1

Step 5: Create, name, and assign ports to three VLANs on S1

This network contains one VLAN for the server farm and two VLANs for user groups.

Why is it good practice to place the server farm in a separate VLAN?

____

a. Enter the following commands to create the three VLANs:

```
S1(config)#vlan 10
S1(config)#name Servers
S1(config)#vlan 20
S1(config)#name Users1
S1(config)#vlan 30
S1(config)#name Users2
```

b. Assign a port to each VLAN, according to the addressing table.

```
S1#configure terminal
S1(config)#interface fastethernet0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10

S1(config)#interface fastethernet0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20

S1(config)#interface fastethernet0/8
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
```

NOTE: For the purposes of this lab, only one representative interface is assigned to each VLAN. When assigning multiple ports to a VLAN, use the **range** parameter. For example, if assigning ports 0/2 through 0/4 to VLAN 10, use this command sequence:

```
S1(config)#interface range fastethernet 0/2 - 4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
```

Step 6: Create the trunk on S1

Enter the following command to establish interface Fa0/1 as a trunk port:

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#end
```

Why is it not necessary to specify which trunking protocol (dot1q, ISL) will be used?

____

Step 7: Configure the hosts

Configure each host with the proper IP address, subnet mask, and default gateway according to the addressing table.

Predict: If the configurations are correct, to which devices should a user at PC1 be able to ping successfully?

____

Step 8: Verify that the network is functioning

a. From each attached host, ping the other two hosts and each of the router sub-interface IP addresses.

Were the pings successful? __________

If the answer is no, troubleshoot the router, switch and host configurations to find the error.

b. From the switch S1, ping the router default gateway 192.168.1.1.

Were the pings successful? __________

c. Use the command **show ip interfaces brief** and check the status of each interface or sub-interface.

What is the state of the interfaces?

R1:

FastEthernet 0/0: __________

FastEthernet 0/0.1: __________

FastEthernet 0/0.2: __________

FastEthernet 0/0.3: __________

FastEthernet 0/0.4: __________

S1:

Interface VLAN1: __________

d. Ping again until successful.

Step 9: Configure, apply, and test an Extended ACL to filter inter-VLAN traffic

Members of the Users1 VLAN should not be able to reach the server farm, but members of the other VLAN should be able to reach each other and the router. Users1 should be able to reach VLANs other than the server farm.

a. Create the extended ACL statements:

```
R1(config)#access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.2.0
0.0.0.255
R1(config)#access-list 100 permit ip any any
```

R1 has a FastEthernet 0/0 interface and four subinterfaces. Where should this ACL be placed, and in which direction? Why?

____

b. Apply the ACL, and test by pinging from PC2 to PC1 and to PC3.

If the ACL is working properly, pings from PC2 to PC1 should fail. All other pings should succeed. If results fail to meet these criteria, troubleshoot the ACL syntax and placement.

Step 10: Reflection

a. Why is it good practice to perform and verify basic and VLAN-related configurations before creating and applying an ACL?

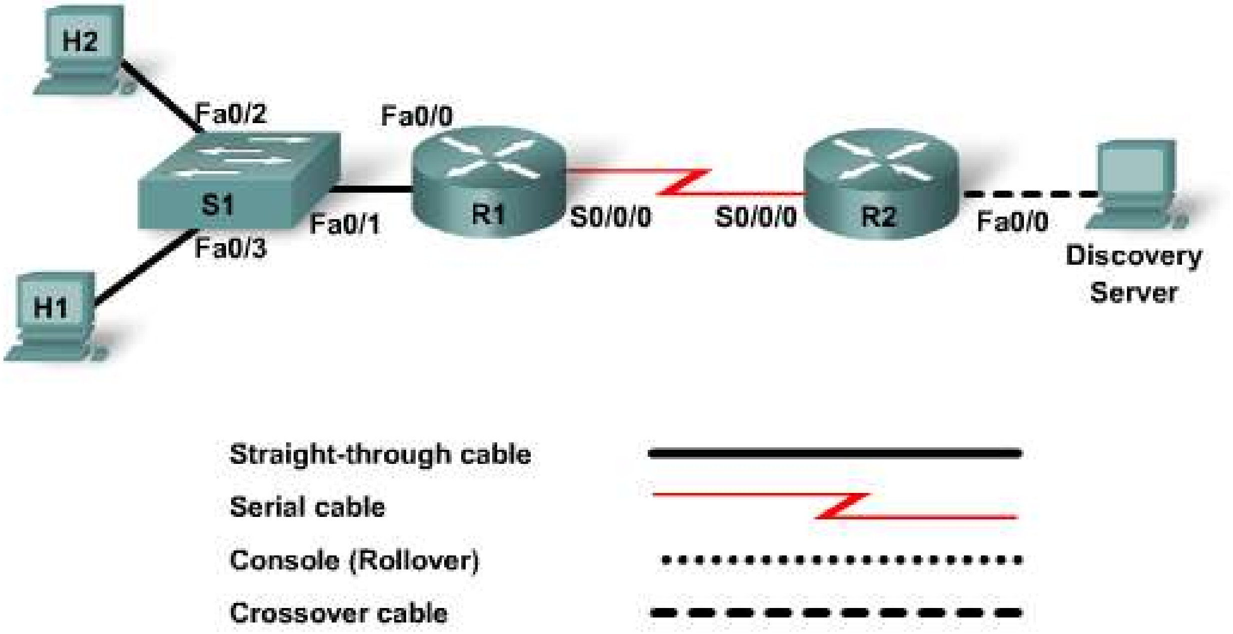
____

____

b. What results would have been produced if the ACL had been placed on subinterface FastEthernet 0/0.3 going out and PC2 pinged PC3?

____

Lab 8.5.1 Configuring ACLs and Verifying with Console Logging



Device	Host Name	FastEthernet 0/0 Interface IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Network Statements	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	192.168.5.1/30	DCE	192.168.1.0 192.168. 5.0	class	cisco
Router 2	R2	172.17.0.1/16	192.168.5.2/30	DTE	192.168. 5.0 172.17.0.0	class	cisco
Switch 1	S1					class	cisco
Host 1	Host 1	192.168.1.5/24 GW=192.168.1.1					
Host 2	Host 2	192.168.1.6/24 GW=192.168.1.1					
Discovery Server	Server	172.17.1.1/16 GW=172.17.0.1					

Objectives

- Configure and verify ACLs to control traffic.
- Verify ACLs using the logging capabilities of the router.

Background / Preparation

Cable a network similar to the one shown in the topology diagram. Any router that meets the interface requirements displayed in the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The command syntax given in the lab may vary. For example, the interfaces may differ due to the router model. On some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or equivalent routers, both with a Serial connection and an Ethernet interface
- Two Windows-based PCs, each with a terminal emulation program and set up as a host
- One PC to act as the Discovery Server
- One Discovery Live CD for the server
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Three straight-through Ethernet cables
- One crossover Ethernet cable
- One DTE/DCE serial cable

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

NOTE: This lab makes use of the Discovery Server Live CD. For detailed instructions on the installation and configuration of the Discovery Server Live CD, please refer to the lab manual that is located on Academy Connection in the Tools Section.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port on Switch 1 using a straight-through cable.

c. Connect Host 1 to the Fa0/3 port on Switch 1 using a straight-through cable.

d. Connect Host 2 to the Fa0/2 port on Switch 1 using a straight-through cable.

e. Connect the Discovery Server to the Fa0/0 interface of Router 2 using a crossover cable.

Step 2: Perform basic configuration on Router 1

Step 3: Perform basic configuration on Router 2

Step 4: Perform basic configuration on Switch 1

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway.

   1) Host 1 should be assigned 192.168.1.5 /24 and the default gateway of 192.168.1.1.

   2) Host 2 should be assigned 192.168.1.6 /24 and the default gateway of 192.168.1.1.

   3) The server should be assigned 172.17.1.1 and a default gateway of 172.17.0.1.

b. Each host should be able to ping the other hosts. If the ping is not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway. Do not configure ACLs until each host can ping the other hosts.

Step 6: Configure and apply ACLs

ACLs will be configured to control what services Hosts 1 and 2 can access from the server. An ACL will be created that allows Host 1 web (HTTP) and FTP access to the server but denies Host 2. Host 2 will be allowed to telnet to the server, but this service is denied to Host 1. These ACLs will be configured and verified with **show** commands and logging.

a. Create an ACL based on the requirements previously outlined. This ACL is applied to R1.

```
R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any
```

b. Apply the ACL to the FastEthernet 0/0 interface on R1 in the inbound direction.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 110 in
```

c. From Host 1, open a web browser and attempt to connect to the web and FTP services on the server. In the web browser address textbox, enter **http://172.17.1.1**.

   Is the web connection from Host 1 successful? __________

d. In the web browser address textbox, enter **ftp://172.17.1.1**.

   Is the FTP connection from Host 1 successful? __________

e. Attempt to connect to the web and FTP services on the server from Host 2.

   Are you able to connect from Host 2? __________

f. Attempt to telnet to the server from Host 1 and Host 2?

   Is the Telnet connection from Host 1 successful? __________

   Is the Telnet connection from Host 2 successful? __________

g. Use the command **show access-lists** to display the access control list and associated statistics.

What information can be obtained from the command output?

____

```
R1#show access-lists
Extended IP access list 110
    10 permit tcp host 192.168.1.5 host 172.17.1.1 eq www (3 matches)
    20 permit tcp host 192.168.1.5 host 172.17.1.1 eq ftp (9 matches)
    30 permit tcp host 192.168.1.6 host 172.17.1.1 eq telnet (3 matches)
    40 deny ip any any (92 matches)
```

The output of the **show access-lists** command displays the number of times each `access-list` line was matched. In many troubleshooting scenarios, however, this is not enough information. For example, the output shown above indicates that the **deny ip any any** line had 92 matches. But it does not tell you what type of traffic was sent and from what sources the traffic was denied. If there is an error in an access control list that is blocking traffic to or from a destination that the ACL was not meant to block, more information is necessary. Logging can be useful in this type of environment.

The same ACL will be configured on R1; this time, the logging option will be enabled.

NOTE: Turning on the logging option of an access control list is similar to using a **debug** command. In a production network, this option can place a heavy load on router resources and slow down the network or even cause it to fail. In a production network this feature must be used with caution.

h. Remove the ACL on R1 and recreate it with the logging option.

```
R1(config)#no access-list 110

R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www log
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp log
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet log
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any log
```

i. Attempt to telnet from Host 1 to the server.

After verifying that Host 1 is unable to make the connection, view the output from the console connection on R1. The output should look similar to this sample:

```
*Oct 18 01:10:57.466: %SEC-6-IPACCESSLOGP: list 110 denied tcp
192.168.1.5(1097) -> 172.17.1.1(23), 1 packet
```

The line displayed is the result of adding the **log** option to an `access-list` line. It displays a date and a time (`01:10:57.466`), the process that generated the console message (`%SEC-6-IPACCESSLOGP`), and detailed information about the message (`list 110 denied tcp 192.168.1.5(1097) -> 172.17.1.1(23), 1 packet`).

In this example, the logging option indicates that an access-list line had a match, and it also indicates the exact source and destination of the matched packet.

j. Attempt to ping as well as use Telnet, web, and FTP connections from Host 1 and Host 2 to the Discovery Server.

Is a log message created each time a connection is attempted? __________

Do the console messages indicate which packets are allowed by the ACL as well as those that are denied? __________

If you attempt connections very rapidly, a message similar to this one may appear:

```
*Oct 18 01:26:39.638: %SEC-6-IPACCESSLOGRL: access-list logging rate-
limited or missed 1 packet
```

This message indicates that the IOS sensed either that a console rate was too high or that the console was too busy to process all the packets. In this example, it indicates that it missed one packet. To avoid this situation in a production network, limit the number of `access-list` lines for which logging is enabled.

Step 7: Reflection

a. What is an advantage of using the logging option on an ACL versus the information provided by the **`show access-lists`** command?

____

b. What is a major concern of enabling the logging feature of an access control list?

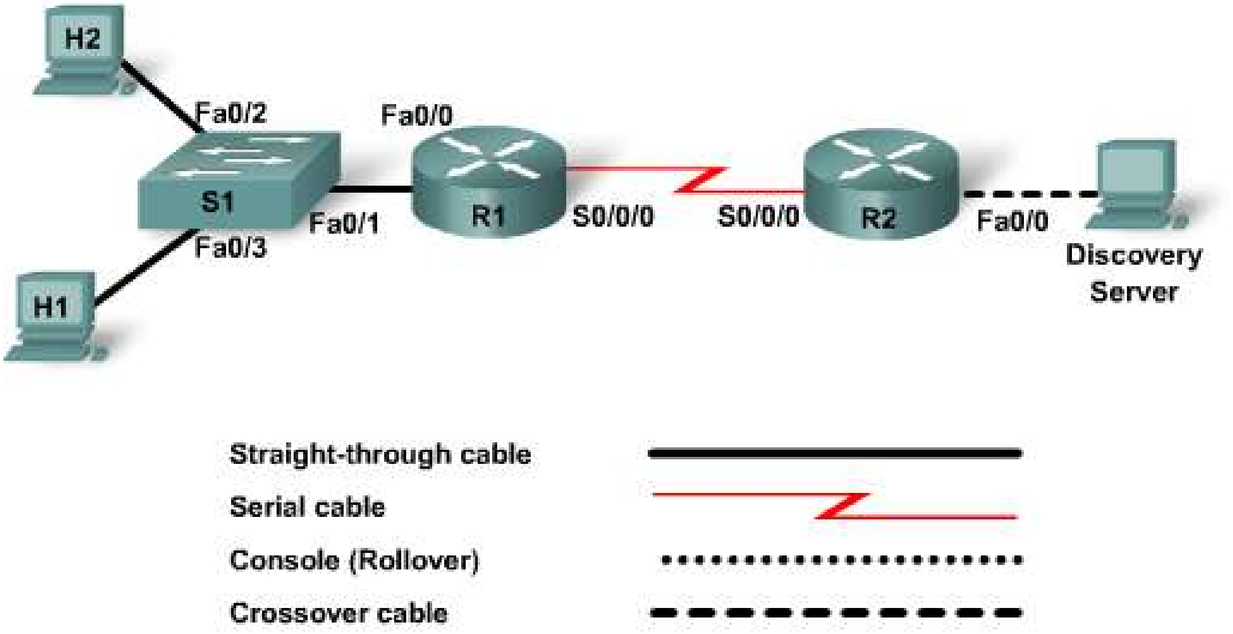
____

c. Would you normally log more than one line? Why or why not?

____

d. If the network is not performing as expected (e.g. routing updates not occurring, name resolution not occurring) which ACL statement would you log? ____________________________________

Lab 8.5.2 Configuring ACLs and Recording Activity to a Syslog Server



Device	Host Name	Fast Ethernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Network Statements	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	192.168.15.1/30	DCE	192.168.1.1 192.168.15.0	class	Cisco
Router 2	R2	172.17.0.1/16	192.168.15.2/30	DTE	192.168.15.0 172.17.0.0	class	Cisco
Switch 1	S1					class	Cisco
Host 1	H1	192.168.1.5/24 DG: 192.168.1.1					
Host 2	H2	192.168.1.6/24 DG: 192.168.1.1					
Discovery Server	Server	172.17.1.1 DG: 172.17.0.1					

Objectives

- Configure and verify ACLs to control traffic.
- Verify ACLs using a syslog server.

Background / Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed in the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The command syntax given in the lab may vary. For example, the interfaces may differ due to the router model. On some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Two Cisco 2960 switch or other comparable switch
- Two Cisco 1841 or comparable routers, each with a serial connection and an Ethernet interface
- Two Windows-based PCs, each with a terminal emulation program and set up as a host
- One Discovery Live CD for the server
- One PC to use as the Discovery Server
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Three straight-through Ethernet cables
- One crossover Ethernet cable
- One DTE/DCE serial cable
- Kiwi Syslog Daemon (downloadable from www.kiwisyslog.com or check with your instructor)

NOTE: Make sure that the routers and switch have been erased and have no startup configurations. Instructions for erasing both the switch and router are provided at the end of this lab.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM for basic router configuration, refer to the instructions at the end of this lab or contact your instructor if necessary.

NOTE: This lab makes use of the Discovery Server Live CD.   For detailed instructions on the installation and configuration of the Discovery Server Live CD, please refer to the lab manual that is located on Academy Connection in the Tools Section.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port on Switch 1 using a straight-through cable.

c. Connect Host 1 to the Fa0/3 port on Switch 1 using a straight-through cable.

d. Connect Host 2 to the Fa0/2 port on Switch 1 with a straight-through cable.

e. Connect the Discovery Server with a crossover cable to the Fa0/0 interface of Router 2.

Step 2: Perform basic configuration on Router 1

Step 3: Perform basic configuration on Router 2

Step 4: Perform basic configuration on Switch 1

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway.

1) Host 1 should be assigned 192.168.1.5 /24 and the default gateway of 192.168.1.1.

2) Host 2 should be assigned 192.168.1.6 /24 and the default gateway of 192.168.1.1.

3) The server should be assigned 172.17.1.1 and a default gateway of 172.17.0.1.

b. Each host should be able to ping the other hosts. If the ping is not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure and apply ACLs

ACLs will be configured to control what services Hosts 1 and 2 can access from the server. An ACL will be created that allows Host 1 web (HTTP) and FTP access to the server but denies Host 2. Host 2 will be allowed to telnet to the server, but this service is denied to Host 1. These ACLs will be configured and verified with **show** commands and logging. Logging will be enabled on the access control list statements.

a. Create an ACL based on the requirements previously outlined. This ACL is applied to R1.

```
R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www log
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp log
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet log
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any
```

b. Apply the ACL to the FastEthernet 0/0 interface on R1 in the inbound direction.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 110 in
```

c. From Host 1, open a web browser and attempt to connect to the web and FTP services on the server. In the web browser address textbox, enter **http://172.17.1.1**.

Is the web connection from Host 1 successful? __________

d. In the web browser address textbox, enter **ftp://172.17.1.1**.

Is the FTP connection from Host 1 successful? __________

e. Attempt to connect to the web and FTP services on the server from Host 2.

Are you able to connect from Host 2? __________

f. Attempt to telnet to the server from Host 1 and Host 2.

Is the Telnet connection from Host 1 successful? __________

Is the Telnet connection from Host 2 successful? __________

When these connections are attempted, console messages appear on R1 indicating the `access-list` lines matched by the various types of packets transmitted.

Step 7: Configure the syslog service on Host 2

Using the logging option in an `access-list` line provides helpful information but also has its disadvantages:

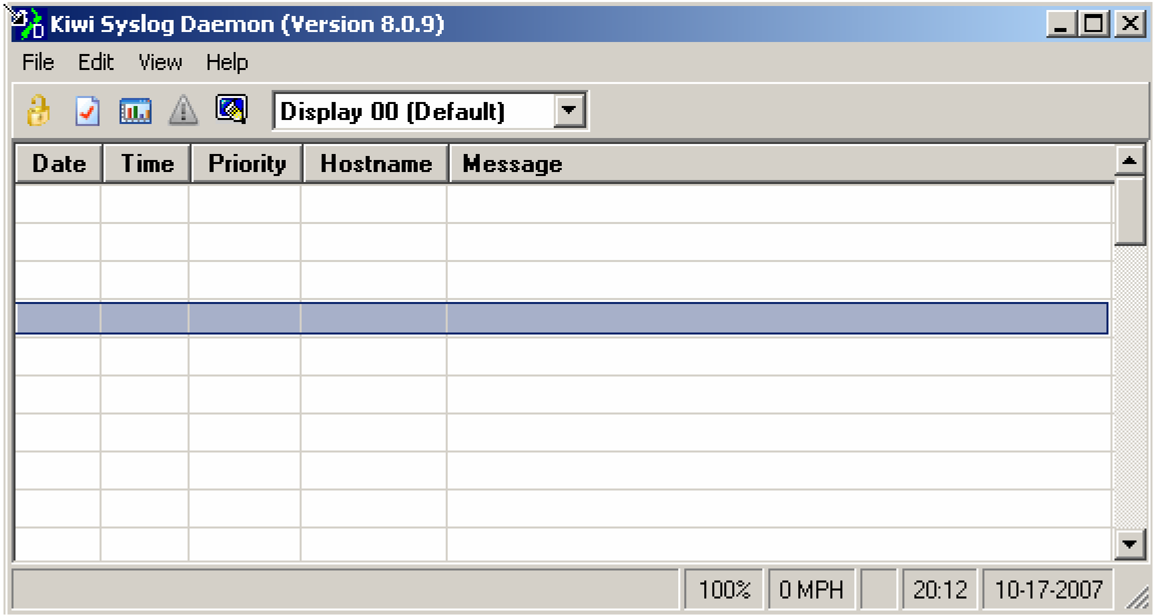
- It can require a lot of router resources.
- It also requires that a router console connection be active at all times or else messages are missed.

A solution that helps with both of these disadvantages is to log the messages to a syslog server. Logging messages to a syslog server reduces the load on the router and provides a destination for the messages. In addition, management tools are available to analyze syslog output to help detect patterns or problems.

Install the Kiwi Syslog Daemon on Host 2. If you need assistance with this, contact your instructor.

NOTE: A number of commercial and open source syslog servers are available. In this lab, the Kiwi syslog server is used. This software may be downloaded from www.kiwisyslog.com.

When the syslog server is running on the server, it should produce a display similar to this one:



The syslog service needs to be configured on the router. To do this properly involves setting the time and date on the router, enabling the timestamp service on the router, and configuring the router to send console messages to the syslog server.

Step 8: Configure the router to properly use the syslog service

Displaying the correct time and date on the syslog messages is vital when using syslog to monitor a network. If the correct time and date of a message is not known, it is sometimes impossible to determine what network event caused the message.

a. Set the correct time and date on the router. Replace the hours, minutes, seconds, month, day, and year variables with the proper values.

```
R1#clock set 15:22:00 may 17 2007
```

b. Configure the correct time zone on the router. Replace the zone name and offset with the correct values for your area.

```
R1(config)#clock timezone cdt -5
```

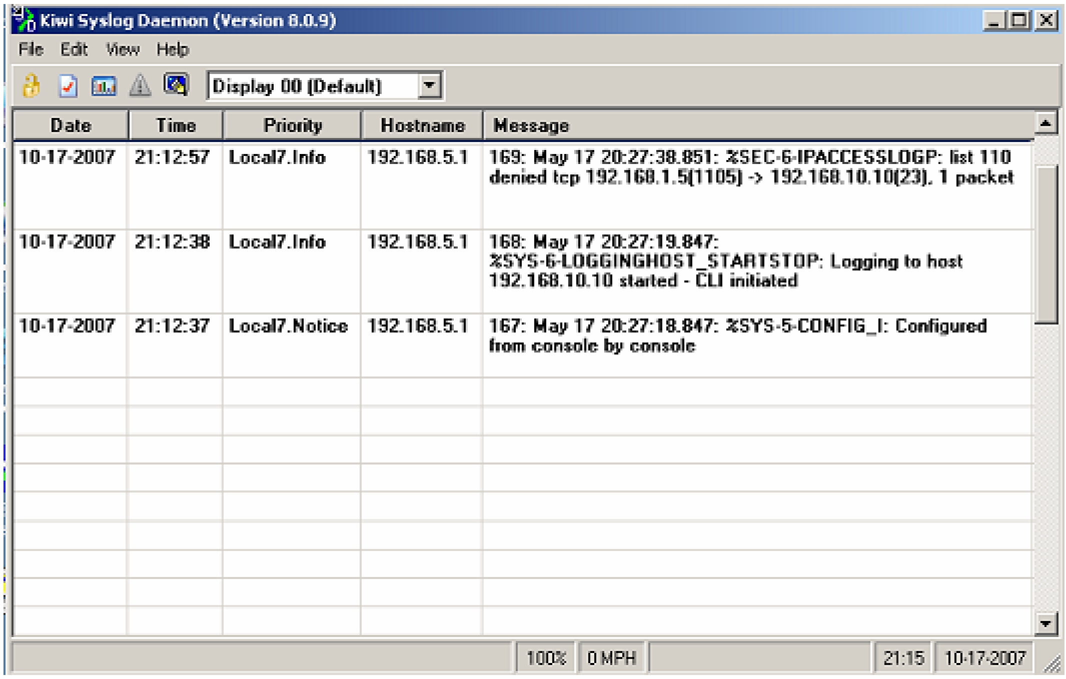
c. Enable the timestamp service on the router.

```
R1(config)#service timestamps
```

d. Configure the syslog service on the router to send syslog messages to the syslog server.

```
R1(config)#logging 192.168.1.6
```

e. Attempt to telnet from Host 1 to the server and then view the syslog display on the server. It should look similar to this example:



Date	Time	Priority	Hostname	Message
10-17-2007	21:12:57	Local7.Info	192.168.5.1	169: May 17 20:27:38.851: %SEC-6-IPACCESSLOGP: list 110 denied tcp 192.168.1.5(1105) -> 192.168.10.10(23), 1 packet
10-17-2007	21:12:38	Local7.Info	192.168.5.1	168: May 17 20:27:19.847: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.10 started - CLI initiated
10-17-2007	21:12:37	Local7.Notice	192.168.5.1	167: May 17 20:27:18.847: %SYS-5-CONFIG_I: Configured from console by console

f. Because logging is turned on at all levels, all console messages appear on the syslog output, including the configuration messages. To control the message display, set the logging level required to generate a message.

NOTE: The time and date appear in both the system message and as a function of the Kiwi syslog server.

g. With the current configuration, syslog messages are displayed on the syslog server and the console. With the syslog server displaying them, console logging can be turned off on router R1.

```
R1(config)#no logging console
```

h. Attempt various Telnet, web, and FTP connections from both hosts to the server and observe the results on the syslog server. In addition to viewing messages from the connection attempts, observe other messages from Hosts 1 and 2, such as NetBIOS broadcasts (UDP port 138).

Step 9: Reflection

a. State the advantages of using a syslog server instead of console logging.

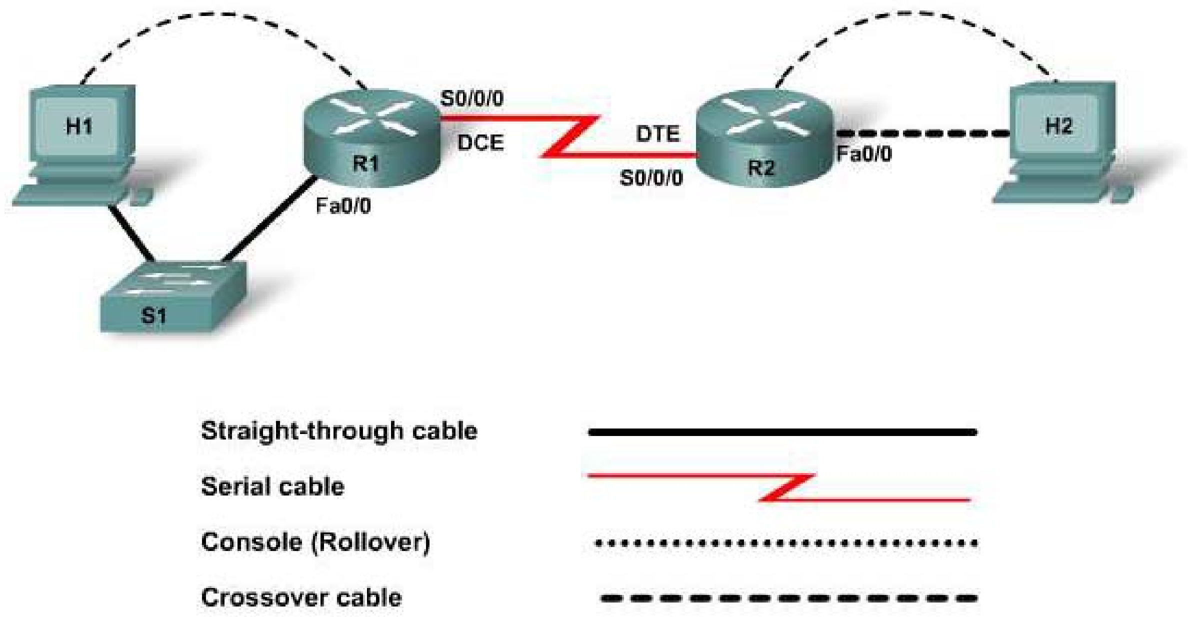
____

____

What factor determines the maximum number of messages stored on the syslog server?

____

Lab 9.3.1 Troubleshooting RIPv2 Routing Issues



Device	Host Name	Fast Ethernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Interface Type	Enable Secret Password	Enable, vty, and Console Password	Default Gateway
Router 1	R1	172.16.0.1/16	172.17.0.1/16	DCE	class	cisco	N/A
Router 2	R2	172.18.0.1/16	172.17.0.2/16	DTE	class	cisco	N/A
Switch 1	S1				class	cisco	N/A
Host 1	H1	172.16.0.2/16					172.16.0.1
Host 2	H2	172.18.0.2/16					172.18.0.1

Objectives

- Configure RIPv2 on routers.
- Discover where communication is not possible.
- Implement solutions to network errors.
- Examine the routing configuration with the **`show ip protocols`** command.
- Examine routing tables using the **`show ip route`** command.
- Observe routing activity using the **`debug ip rip`** command.

Background / Preparation

In this lab, you will learn how to troubleshoot the routing protocol RIPv2 using the network shown in the topology diagram. This lab uses an 1841 router and Cisco IOS commands. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0, Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch (optional if using crossover cables between the PCs and routers)
- Two Cisco Routers with 2 serial interfaces and 1 FastEthernet interface (preferably the same model number and IOS version)
- Two Windows-based PCs, each with a terminal emulation program and set up as a host
- At least one RJ-45-to-DB-9 connector console cable to configure the routers and switch
- Two straight-through Ethernet cables to connect from the router to the switch and the switch to the host
- One crossover cable to connect to the router
- One 2-part (DTE/DCE) serial cable

NOTE: Make sure that the routers have been erased and have no startup configurations. For instructions on erasing and reloading a switch and a router please refer to the Lab Manual. The Lab Manual can be found and downloaded on the Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM for basic router configuration, refer to the instructions provided in the Lab Manual which can be found and downloaded on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Fa0/0 interface of Router 1 to the Fa0/1 interface of Switch 1 using a straight-through cable.

c. Connect Host H1 to the console of Router 1 using a rollover cable to perform configurations.

d. Connect Host H1 to the Fa0/2 interface of Switch 1 using a straight-through cable.

e. Connect Host H2 Fa0/0 interface of the Router 2 using a crossover cable.

f. Connect Host H2 to the console of Router 2 using a rollover cable to perform configurations.

Step 2: Load the preconfigurations for R1 and R2

a. See your instructor to obtain the preconfigurations for this lab.

b. Connect the PCs to the console ports of the routers for loading the preconfigurations using a terminal emulation program.

c. Transfer the configuration from H1 to Router 1:

1) In the terminal emulation program on H1, choose **Transfer > Send Text File**.

2) Locate the file for the configuration of Router 1 provided by your instructor and choose **Open** to start the transfer of the preconfiguration to Router 1.

3) When the transfer is complete, save the configuration.

d. Repeat the transfer process from H2 to Router 2:

4) In the terminal emulation program on H2, choose **Transfer > Send Text File**.

5) Locate the file for the configuration of Router 2 provided by your instructor, and choose **Open** this start the transfer of the preconfiguration to Router 2.

6) When the transfer is complete, save the configuration.

Step 3: Configure the hosts with IP address, subnet mask, and default gateway

e. Configure each host with the proper IP address, subnet mask, and default gateway.

1) H1 should be assigned 172.16.0.2 with a subnet mask of 255.255.0.0 and the default gateway of 172.16.0.1.

2) H2 should be assigned 172.18.0.2 with a subnet mask of 255.255.0.0 and the default gateway of 172.18.0.1.

Can H1 ping the FastEthernet interface of R1? __________

If the answer is no, troubleshoot as necessary to determine the problem. Use commands such as **`show ip interface brief,`** etc., to identify the problems.

Why or why not? ____

If a problem is found, enter the commands to correct the problem.

Each workstation should be able to ping the attached router. If the ping was not successful, troubleshoot further. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 4: Check connectivity between hosts H1 and H2

a. Ping from Host H1 to Host H2. Is the ping successful? _______

If the answer is no, troubleshoot as necessary to determine the problem. Use commands such as **`show ip interface brief, on R1 and R2,`** to identify the problems.

Are all necessary interfaces up? __________

Step 5: Show the routing tables for each router

From the enable or privileged EXEC mode of both routers, examine the routing table entries, using the **`show ip route`** command on each router.

What are the entries in the R1 routing table?

____

____

____

What are the entries in the R2 routing table?

____

____

____

What is missing from the touting tables? ____

Step 4: Verify that routing updates are being sent

a. Type the command **`debug ip rip`** at the privileged EXEC mode prompt of R1. Wait for at least 45 seconds.

Was there any output from the debug command on R1? __________

What is missing from the debug output on R1? ____

____

b. Use the **`show ip protocol`** command on R1 to determine the problem. Review the topology diagram and the networks that should be associated with each router interface.

What problem is occurring?

____

____

c. Make corrections to the configuration as necessary.

Was there any output from the debug command? __________

What did the output show? ____

____

d. To turn off debug on R1. For example, **`no debug ip rip`**. To turn off all **`debug`** commands, enter **`undebug all`**.

e. Use the **`show ip protocol`** command on R1 to verify the proper RIP V2 configuration.

Step 5: Show the routing tables for each router

From the enable or privileged EXEC mode of both routers, examine the routing table entries, using the **`show ip route`** command on each router.

What are the entries in the R1 routing table?

____

____

____

What are the entries in the R2 routing table?

____

____

____

Step 6: Show the RIP routing table entries for each router

a. Enter the **`show ip route rip`** command on both routers.

b. List the routes shown in the routing table.

____

____

What is the administrative distance of these routes? __________

Step 7: Test network connectivity

From H1, is it possible to ping the FastEthernet interface of R2? __________

From H1, is it possible to ping Host H2? __________

From H2, is it possible to ping the FastEthernet interface of R1? __________

From H2, is it possible to ping Host H1? __________

If the answer is no, troubleshoot to find the error. Ping again until successful.

Step 8: Reflection

a. What does **`ping`** test?

____

____

b. When should the **`show ip protocols`** and **`show ip route`** commands be used?

____

____

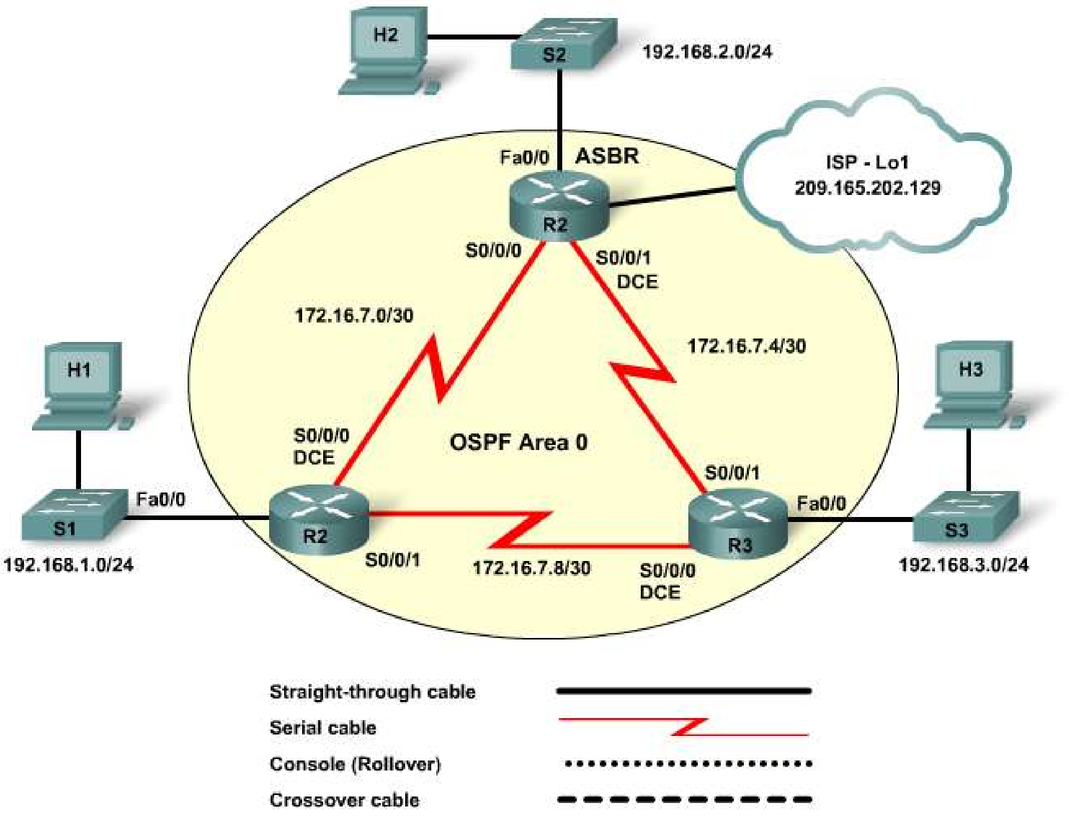
c. When should the **`debug ip rip`** command be used?

____

____

____

Lab 9.3.3 Troubleshooting OSPF Routing Issues



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	**Fa0/0**	192.168.1.1	255.255.252.0	N/A	class	cisco
		S0/0/0	172.16.7.1	255.255.255.252	N/A		
		S0/0/1	172.16.7.9	255.255.255.252	N/A		
		Lo1	10.1.1.1	255.255.255.255	N/A		
Router 2	R2	**Fa0/0**	192.168.2.1	255.255.254.0	N/A	class	cisco
		S0/0/0	172.16.7.2	255.255.255.252	N/A		
		S0/0/1	172.16.7.5	255.255.255.252	N/A		
Router 3	R3	**Fa0/0**	192.168.3.1	255.255.255.0	N/A	class	cisco
		S0/0/0	172.16.7.10	255.255.255.252	N/A		
		S0/0/1	172.16.7.6	255.255.255.252	N/A		
Host 1	H1	**NIC**	192.168.1.11	255.255.255.0	192.168.1.1		
Host 2	H2	**NIC**	192.168.2.22	255.255.255.0	192.168.2.1		
Host 3	H3	**NIC**	192.168.3.33	255.255.255.0	192.168.3.1		

Objectives

- Load the routers with preconfigurations.
- Discover where communication is not possible.
- Gather information about OSPF and other misconfigured portion of the network.
- Analyze information using **show** and **debug** commands to determine connectivity issues.
- Propose solutions to network errors.
- Implement solutions to network errors and verify.

Background / Preparation

In this lab, you will build a full-mesh single-area OSPF network using point-to-point WAN links. Router R2 is the Autonomous System Border Router (ASBR) that provides a connection to the Internet through the ISP and propagates a default route to the other routers in Area 0. You will load preconfigurations onto each of the routers, which have intentional errors in them, resulting in connectivity problems. You will use **show** and **debug** commands to troubleshoot and identify problems. Then you will correct the misconfigurations to achieve full network connectivity.

Cable a network similar to the one shown in the topology diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers can be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Three Cisco 2960 switches or other comparable switch. Crossover cables may be used between the hosts and routers and the switches omitted.
- Three routers, each with 2 serial interfaces and an Ethernet interface
- Three Windows-based PCs, each with a terminal emulation program and set up as a host
- At least one RJ-45-to-DB-9 connector console cable to configure the routers
- Six straight-through Ethernet cables (or 3 crossover cables if omitting switches)
- Three 2-part (DTE/DCE) serial cables
- Preconfiguration files (with errors) for each of the three routers (obtain from instructor)

NOTE: Make sure that the routers have been erased and have no startup configurations. For instructions on erasing and reloading a switch and a router, please refer to the Lab Manual. The Lab Manual can be found and downloaded on the Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM for basic router configuration, refer to the instructions provided in the Lab Manual which can be found and downloaded on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Fa0/0 interface of each router to the Fa0/1 interface of each switch using a straight-through cable.

b. Connect each host to the Fa0/2 switch port of each switch using a straight-through cable.

c. Connect serial cables from each router to the other routers according to the topology diagram.

Step 2: Load the preconfiguration on R1

a. See your instructor to obtain the preconfigurations for this lab.

b. Connect a Host H1 to the console port of Router 1 for loading the preconfigurations using a terminal emulation program.

c. Transfer the configuration from H1 to Router 1:

1) In the terminal emulation program on the PC, choose **Transfer > Send Text File**.

2) Locate the file for the configuration of Router 1 provided by your instructor and choose **Open** to start the transfer of the preconfiguration to Router 1.

3) When the transfer is complete, save the configuration.

Step 3: Load the preconfiguration on R2

Copy the preconfiguration on R2 using the process detailed in Step 2.

Step 4: Load the preconfiguration on R3

Copy the preconfiguration on R3 using the process detailed in Step 2.

Step 5: Troubleshoot Router R1 Issues

You are a network administrator, located at the same site as the R1 router, and a user calls the help desk stating that they cannot connect to a file server. You determine that the user is on the 192.168.1.0 network (R1) and that the server is on the 192.168.3.0 network (R3). You visit the user and begin troubleshooting.

a. Begin troubleshooting at host H1 connected to the R1 router.

From the host H1, is it possible to ping H2? __________

From the host H1, is it possible to ping H3? __________

From the host H1, is it possible to ping the ISP Loopback interface on R2? __________

From the host H1, is it possible to ping the default gateway on R1? __________

b. Examine the R1 router to find possible configuration errors. Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces that are in use with this topology?

____

c. Check to see if there are routes to the other networks by examining the output of the **`show ip route`** command.

Is there an OSPF route to the 192.168.2.0 (H2) network? __________

Is there an OSPF route to the 192.168.3.0 (H3) network? __________

d. Check the OSPF neighbor adjacencies on R1 using the **`show ip ospf neighbors`** command.

Has R1 established an adjacency with R2? __________

Has R1 established an adjacency with R3?

What is the neighbor ID of R2? ______________________________

e. Use the **`show protocols`** command to display the IP address, slash notation, subnet mask, and the status of all Internet Protocol interfaces on R1.

Are there any issues associated with IP addressing? __________ If so, what are they?

____

____

f. If there are any problems with the configuration of the interfaces, record the commands that will be necessary to correct the configuration errors.

____

____

____

g. If you have recorded any commands above, apply them to the router configuration now and save the configuration.

Did you notice any console messages on R1? __________

h. Issue the **`show protocols`** command again to verify interface addressing configuration changes.

i. Check the neighbor adjacencies on R1 again using the **`show ip ospf neighbors`** command.

Has R1 established an adjacency with R2? __________

Has R1 established an adjacency with R3? __________

What is the neighbor ID of R2? ______________________

What is the neighbor ID of R3? ______________________

j. Use test pings again to recheck connectivity from H1 to other hosts.

From the host H1, is it possible to ping H2? __________

From the host H1, is it possible to ping H3? __________

From the host H1, is it possible to ping the ISP Loopback interface on R2? __________

Did the R1 interface configuration change you made correct the connectivity problem from H1 to H3?

____

k. Continue with your troubleshooting by rechecking to see which OSPF routes R1 has learned using the **`show ip route`** command.

Is there a route to the 192.168.3.0 (H3) network now? __________

l. Use the **`debug ip ospf packet`** command to verify that hello packets are being exchanged between R1 and neighbors R2 and R3.

Are hello packets (t:1) being received from both R2 and R3? __________

What is the router ID of R3? _________________________

What does this tell you about the R3 interface fa0/0 and its status?

____

____

m. Turn off debugging using either the **`undebug ip ospf packet`** or **`undebug all`** command.

R1 Troubleshooting Review:

Let’s review what you have determined so far in your R1 troubleshooting.

- You were unable to ping from host H1 on the 192.168.1.0 network to host H3 on the 192.168.3.0 network.
- You determined that the IP address on R1 S0/0/1 was on a different network and corrected it so that R1 and R3 could become neighbors.
- The **`show ip route`** command on R1 reveals that the OSPF route to the 192.168.3.0 network is missing from the routing table but there are other OSPF routes present.
- The **`show ip ospf neighbors`** output shows R2 and R3 as fully adjacent neighbors with R1.
- The **`debug ip ospf packet`** output shows that hello packets are being exchanged between R1 and R3 and that R3 interface Fa0/0 (IP address 192.168.3.1) is up.

Next you will telnet to R3 to examine its configuration.

Step 6: Troubleshoot Router R3 Issues

a. To help diagnose potential problems with R3, telnet from R1 to the R3 router using the IP address of the R3 S0/0/0 interface (172.16.7.10) and enter the vty password (**cisco**) for R3 when prompted. Enter privileged EXEC mode (password **class**).

```
R1>telnet 172.16.7.10
Trying 172.16.7.10 ... Open
User Access Verification
Password:
R3>enable
Password:
R3#
```

b. While connected to R3 via Telnet, use the **`show ip route`** command to see which OSPF routes R3 has learned.

Is there a route to the R1 192.168.1.0 network in the R2 routing table to ensure that packets have a return route to H1? __________

Is there an entry for 192.168.3.0 network in the R3 routing table? __________

What kind of router entry is it? _____________

c. Use the **`show ip protocols`** command to determine which networks R3 is advertising.

d. List the networks R3 is advertising:

____

____

____

Is there a problem with the OSPF networks being advertised? __________If so, what?

____

____

____

e. If there are any problems with the OSPF configuration, record any commands that will be necessary to correct the configuration errors. Apply the configuration changes now and save the configuration.

____

____

____

____

f. Use the **show ip protocols** command again to verify that R3 is advertising the correct networks now.

g. End the Telnet session on router R3 and return to R1 using the **quit** command.

```
R3#quit
[Connection to 172.16.7.10 closed by foreign host]
```

h. Check to see which OSPF routes R1 has learned now using the **show ip route** command.

   Are all routes to the 192.168.x.0 LAN networks present now? __________

i. Ping from H1 to H3 to verify that you have corrected the problem.

   Are you able to ping H3? __________

j. If you are unable to ping H3, continue troubleshooting until you are successful.

Step 7: Troubleshoot Router R2 Issues – Part A

You have resolved the problems with access to the file server on the 192.168.3.0 network. Another user calls the help desk stating that they cannot connect to the Internet. You determine that the user is on the 192.168.3.0 network (R3) and that the ISP server is 209.165.202.129 (R2 Loopback1 - Simulated ISP). Router R2 is the Autonomous System Border Router (ASBR), and access to the ISP for all hosts in Area 0 is though router R2. You try some test pings from various network locations to the R2 router. You are able to telnet from a host on the 192.168.1.0 network to the R2 router to investigate the problem.

a. Because you are located at the same site as the R1 router, perform some test pings from host H1 to R2 IP addresses.

   From the host H1, is it possible to ping H2 (192.168.2.22)? __________

   From the host H1, is it possible to ping the R2 LAN default gateway (192.168.2.1)? __________

   From the host H1, is it possible to ping the simulated ISP Loopback interface on R2 (209.165.202.129)? __________

b. To help diagnose potential problems with R2, telnet from R1 to the R2 router using the IP address of the R2 S0/0/0 interface (172.16.7.2) and enter the vty password (**cisco**) when prompted. Enter privileged EXEC mode (password **class**).

```
R1>telnet 172.16.7.2
Trying 172.16.7.2 ... Open
User Access Verification
Password:
R2>enable
Password:
R2#
```

c. To see console messages from R2 while connected from R1 via telnet, issue the **terminal monitor** command from the R2 privileged prompt. Without this command, no R2 console messages or debug output can be viewed remotely from R1.

```
R2#terminal monitor
```

   Did any console messages display for R2 after issuing the **terminal monitor** command? __________ If so, what did they say?

____

____

What does this message mean? ____

____

d. Stop the terminal monitoring of R2 using the command **`terminal no monitor`** at the privileged prompt. This will stop the repetitive display of error messages.

```
R2#terminal no monitor
```

e. While telnetted in to R2, issue the **`show ip ospf`** command to see what OSPF areas are defined.

What OSPF areas are defined on Router R2 and how many interfaces are in each area?

____

How many OSPF areas should be defined on router R2?

____

____

f. While remotely connected via Telnet to R2, issue the **`show ip ospf interface`** command to see the OSPF-related interface information.

Fill in the following table based on the output from this command.

Interface Type/Number	IP Address/Mask	Network Type	Area

Is there a problem with the OSPF network areas defined for the R2 networks? __________If so, what?

____

g. Issue the **`show ip ospf neighbor`** command on R2.

```
R2#show ip ospf neighbor
Neighbor ID     Pri   State      Dead Time   Address         Interface
192.168.1.1       0   FULL/  -   00:00:32    172.16.7.1      Serial0/0/0
```

Why is only router R1 a neighbor of R2?

____

h. Display the R2 routing table using the **`show ip route`** command.

What router is the next hop to the 192.168.1.0 network and what is the OSPF Cost?

____

What router is the next hop to the 192.168.3.0 network and what is the OSPF Cost?

____

Why is the route from R2 to the R3 LAN higher than the cost to the R1 LAN?

____

____

Will the OSPF area mismatch problem on the R2-R3 WAN prevent pings to the LAN hosts from reaching their destination in this topology? __________ Why or why not?

____

____

____

i. If there are any problems with the OSPF configuration, record the commands that will be necessary to correct the configuration errors. Apply the configuration changes now and save the configuration.

```
R2#configure terminal
R2(config)#router ospf 1
R2(config-router)#no network 172.16.7.4 0.0.0.3 area 10
R2(config-router)#network 172.16.7.4 0.0.0.3 area 0
```

j. Issue the **`show ip protocols`** command to verify that the proper networks are being advertised in the correct areas for R2.

k. As a final check, issue the **`show ip route`** command to verify that R2 now has a route to the R3 LAN via R3 (172.16.7.6) with a cost of 65 that uses the previously unavailable R2-R3 WAN link.

Step 8: Troubleshoot Router R2 Issues – Part B

Although you resolved the problem with OSPF area mismatch on the R2 WAN link, many of your users still cannot connect to the ISP through R2. You suspect that the problem is still with R2 but is not related to the OSPF area mismatch problem solved earlier.

a. To verify this, issue more test pings to the ISP.

From the host H1, is it possible to ping the simulated ISP Loopback interface on R2 (209.165.202.129)? __________

From the host H2, is it possible to ping the simulated ISP Loopback interface on R2 (209.165.202.129)? __________

From the host H3, is it possible to ping the simulated ISP Loopback interface on R2 (209.165.202.129)? __________

b. You note that only users on the R2 LAN can access the Internet and users on R2 and R3 LANs cannot. Issue the **`show ip route`** command to verify the R2 routing table entries.

`Is there a static default route to the ISP?` __________

c. Suspend the Telnet session from R1 to R2 by simultaneously pressing the keystroke combination of **`Ctrl+Shift+6`** and, while holding these keys down, press the letter **`x`**. This will return you to R1 but will leave the Telnet session to R2 active.

d. Issue the **`show ip route`** command on R1.

Is there a static default route in the routing table and is the gateway of last resort set? __________

e. Press **Enter** twice to resume the Telnet connection from R1 to R2.

```
R1#
[Resuming connection 1 to 172.16.7.2 ... ]
R2#
```

f. Telnet from R2 to the R3 router using the IP address of the R3 S0/0/1 interface (172.16.7.6) and enter the vty password (**cisco**) when prompted. Enter privileged EXEC mode (password **class**).

```
R2>telnet 172.16.7.6
Trying 172.16.7.6 ... Open
User Access Verification
Password:
R3>enable
Password:
R3#
```

g. Issue the **show ip route** command on R3.

Is there a static default route in the routing table and is the gateway of last resort set? __________

h. Type **quit** to end the session on R3 and to return to R2.

```
R3#quit
[Connection to 172.16.7.6 closed by foreign host]
```

i. Issue the **show running-config** command on R2 to verify the OSPF routing statements.

Based on the **show running-config** output for router R2, is there a default route? _________

Router R2 is the ASBR and needs to provide a default route to the other Area 0 routers. Why is the default route not being propagated to the other two routers R1 and R3?

____

j. If there are any problems with the OSPF configuration, record the commands that will be necessary to correct the configuration errors. Apply the configuration changes now and save the configuration.

```
R2#configure terminal
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

k. Issue the **show running-config** command again on R2 to verify the routing OSPF statements.

l. Type **quit** to end the session on R2 and return to R1.

```
R2#quit
[Connection to 172.16.7.2 closed by foreign host]
```

m. On R1, issue the **show ip route** command to view the routing table entries.

Is there a static default route in the routing table and is the gateway of last resort set? __________

n. Telnet from R1 to the R3 router using the IP address of the R3 S0/0/0 interface (172.16.7.10) and enter the vty password (**cisco**) when prompted. Enter privileged EXEC mode (password **class**).

```
R1>telnet 172.16.7.10
Trying 172.16.7.10 ... Open
User Access Verification
Password:
R3>enable
Password:
R3#
```

o. Issue the **show ip route** command on R3.

Is there a static default route in the routing table and is the Gateway of last resort set? __________

p. As a final test, issue more pings to the ISP.

From the host H1, is it possible to ping the simulated ISP Loopback interface on R2 (209.165.202.129)? __________

From the host H2, is it possible to ping the simulated ISP Loopback interface on R2 (209.165.202.129)? __________

From the host H3, is it possible to ping the simulated ISP Loopback interface on R2 (209.165.202.129)? __________

Step 9: Reflection

A number of configuration errors appeared in the preconfigurations that were provided for this lab. Use this space below to write a brief description of the errors that you found on each router.

____

____

____

____

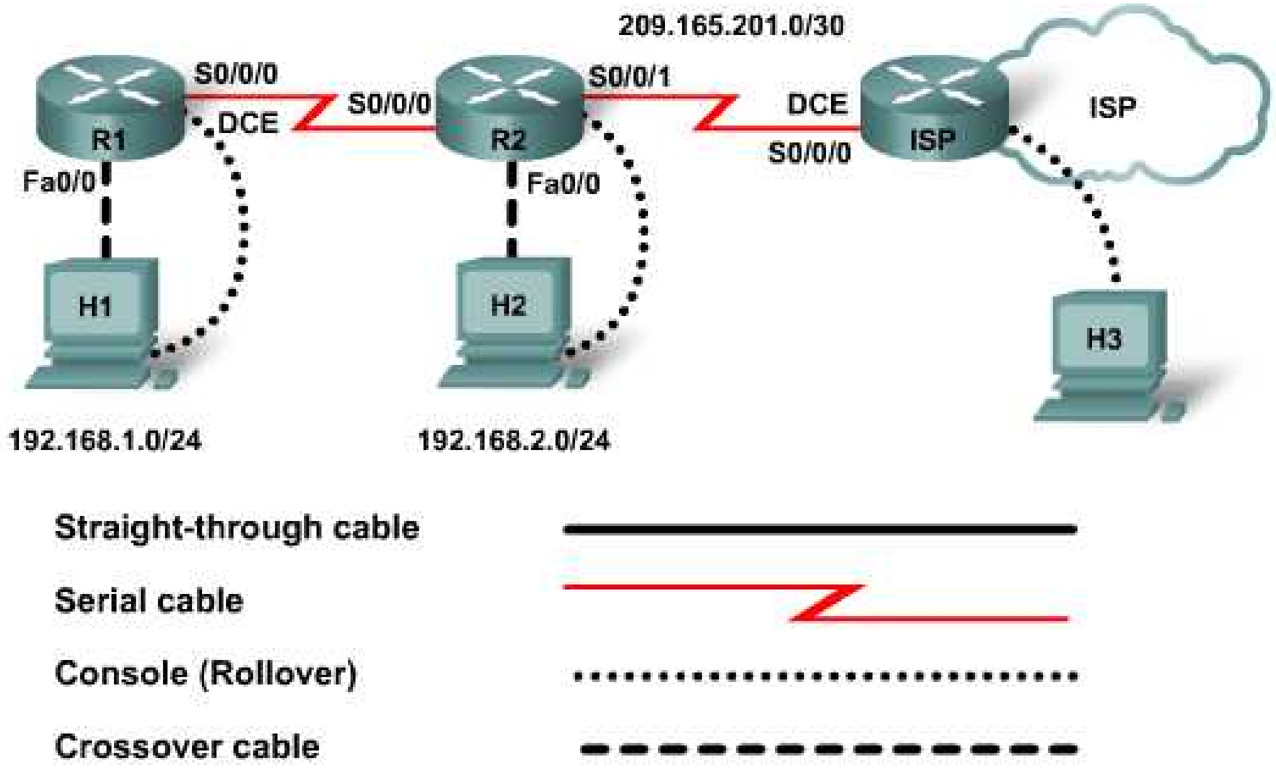
____

____

____

____

Lab 9.3.4 Troubleshooting Default Route Redistribution with EIGRP



Device	Host Name	Fast Ethernet 0/0 IP Address	Serial 0/0/0 IP Address	Serial 0/0/0 Type	Serial0/0/1 IP Address	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.1.1/24	172.30.1.1/30	DCE	NA	class	cisco
Router 2	R2	192.168.2.1/16	172.30.1.2/16	DTE	209.165.201.1/30	class	cisco
ISP	ISP	NA	209.165.201.2/30	DCE	NA	class	cisco
PC1	H1	192.168.1.2/24					
PC2	H2	192.168.2.2/24					
PC3	H3	NA					

Objectives

- Configure EIGRP on routers.
- Discover connectivity issues and implement solutions to network errors.
- Examine the topology tables with the **`show ip eigrp topology`** command.
- Examine the statistics using the **`show ip eigrp traffic`** command.
- Examine routing tables using the **`show ip route`** command.
- Observe routing activity using the **`debug ip eigrp`** command.

Background / Preparation

In this lab, you will learn how to troubleshoot the routing protocol EIGRP using the network shown in the topology diagram. This lab uses an 1841 router and Cisco IOS commands. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0, Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- Three Cisco Routers with 2 serial interfaces and 1 FastEthernet interface (preferably the same model number and IOS version)
- One Windows-based PC, with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the routers
- Three 2-part (DTE/DCE) serial cables
- Two crossover cables for the hosts to router connections

NOTE: Make sure that the routers have been erased and have no startup configurations. For instructions on erasing and reloading a switch and a router please refer to the Lab Manual. The Lab Manual can be found and downloaded on the Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM for basic router configuration, refer to the instructions provided in the Lab Manual, which can be found and downloaded on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Serial 0/0/0 interface of Router 1 to the Serial 0/0/0 interface of Router 2 using a serial cable.

b. Connect the Serial 0/0/1 interface of Router 2 to the Serial 0/0/0 interface of the ISP router using a serial cable.

c. Connect Host H1 to the console of Router 1 using a rollover cable to perform configurations and use a crossover cable to connect the NIC of H1 to the Fa0/0 of R1.

d. Connect Host H2 to the console of Router 2 using a rollover cable to perform configurations and use a crossover cable to connect the NIC of H2 to the Fa0/0 of R2.

e. Connect Host H3 to the console of ISP using a rollover cable to perform configurations.

Step 2: Load the preconfigurations for R1, R2, and ISP

a. See your instructor to obtain the preconfigurations for this lab.

b. Connect the PC to the console ports of the routers for loading the preconfigurations using a terminal emulation program.

c. Transfer the configuration from H1 to Router 1:

1) In the terminal emulation program on H1, choose **Transfer > Send Text File**.

2) Locate the file for the configuration of Router 1 provided by your instructor and choose **Open** to start the transfer of the preconfiguration to Router 1.

3) When the transfer is complete, save the configuration.

d. Repeat the transfer process from H2 to Router 2:

1) In the terminal emulation program on H2, choose **Transfer > Send Text File**.

2) Locate the file for the configuration of Router 2 provided by your instructor, and choose **Open** to start the transfer of the preconfiguration to Router 2.

3) When the transfer is complete, save the configuration.

e. Repeat the transfer process from H3 to ISP:

1) In the terminal emulation program on H3, choose **Transfer > Send Text File**.

2) Locate the file for the configuration of ISP provided by your instructor, and choose **Open** to start the transfer of the preconfiguration to ISP.

3) When the transfer is complete, save the configuration.

Step 3: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway.

1) H1 should be assigned 192.168.1.2 with a subnet mask of 255.255.255.0 and the default gateway of 192.168.1.1.

2) H2 should be assigned 192.168.2.2 with a subnet mask of 255.255.255.0 and the default gateway of 192.168.2.1.

Can H1 ping the FastEthernet interface of R1? __________

If the answer is no, troubleshoot as necessary to determine the problem. Use commands such as **show ip interface brief,** etc., to identify the problems.

H1 should be able to ping the attached router. If the ping was not successful, troubleshoot further. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 4: Check connectivity between hosts H1 and H2

a. Ping from Host H1 to Host H2.

Is the ping successful? __________

If the answer is no, troubleshoot as necessary to determine the problem. Use commands such as **show ip interface brief** on R1 and R2 to identify the problems.

Are all necessary interfaces up? __________

b. If no, make the necessary corrections to have all interfaces up.

What must be done? ______________

____

Both workstations should be able to ping the attached router. If the ping was not successful, troubleshoot further. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 5: Show the routing tables for each router

From the enable or privileged EXEC mode of both routers, examine the routing table entries, using the **show ip route** command on each router.

What are the entries in the R1 routing table?

____

____

What are the entries in the R2 routing table?

____

____

____

What is missing from the routing tables? ____

Step 6: Verify that routing updates are being sent

a. Type the commands **debug ip eigrp** and **clear ip route *** at the privileged EXEC mode prompt of R1. Wait for at least 45 seconds.

Was there any output from the debug commands on R1? __________

What is missing from the debug output on R1? ____

____

b. On R1, use the **show ip protocols** command to determine the problem. Review the topology diagram and the networks that should be associated with each router interface.

What problem is occurring?

____

____

c. On R2, use the **`show ip protocols`** and **`show ip route`** commands to determine the problem. Review the topology diagram and the networks that should be associated with each router interface.

What problem is occurring?

____

____

d. Make corrections to the configuration as necessary.

Step 7: Show the routing tables for each router

From the enable or privileged EXEC mode of both routers, examine the routing table entries, using the **`show ip route`** command on each router.

What are the entries in the R1 routing table?

____

____

____

____

What does **D*EX** mean in the output? ____

What are the entries in the R2 routing table?

____

____

____

____

What is the address type in the 0.0.0.0 route? ______________________________

What does the **D** mean in the first column of the routing table? _________________

What is the administrative distance of 192.168.1.0 network? ___________________

Step 8: Show the EIGRP topology table entries for each router

a. To view the topology table, issue the **`show ip eigrp topology`** command on R1.

How many routes are in passive mode? ____

b. To view more specific information about a topology table entry, use an IP address with this command:

```
R1#show ip eigrp topology 192.168.2.0
```

Based on the output of this command, how does R1 know about the 192.168.2.0 network?

____

____

Step 9: Show the EIGRP traffic entries for R1

Issue the **`show ip eigrp traffic`** command on R1.

What were the results?

____

____

____

Are updates being sent and received? __________

Step 10: Test network connectivity

From H1, is it possible to ping the FastEthernet interface of R2? __________

From H1, is it possible to ping Host H2? __________

From H1, is it possible to ping the S0/0/0 of the ISP? __________

From H2, is it possible to ping the FastEthernet interface of R1? __________

From H2, is it possible to ping Host H1? __________

From H2, is it possible to ping the S0/0/0 of the ISP? ________

If any answer is no, troubleshoot to find the error. Ping again until successful.

Step 11: Reflection

a. What does **`ping`** test?

____

____

b. When should the **`show ip protocols`** and **`show ip eigrp topology`** commands be used?

____

____

____

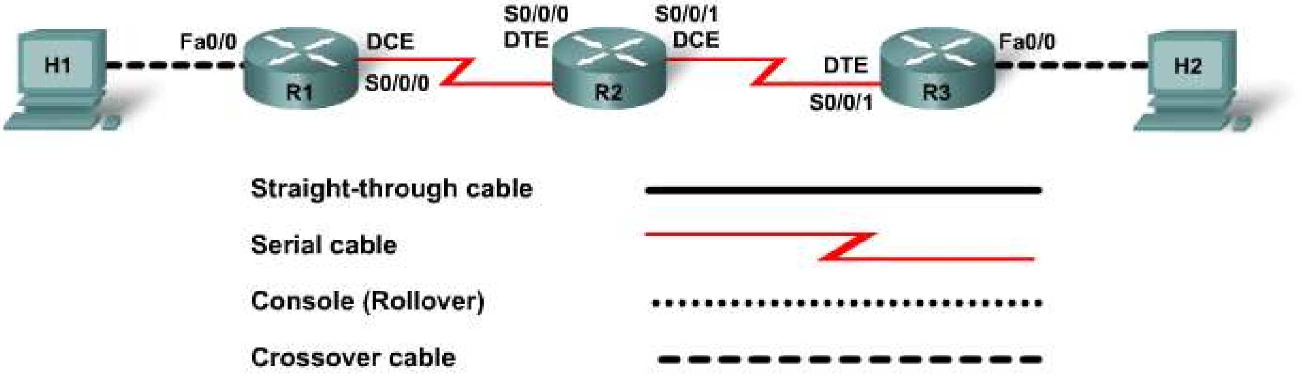
c. When should the **`debug ip eigrp`** command be used?

____

____

____

Lab 9.3.4 Troubleshooting OSPF Default Route Redistribution



Device	Host Name	Fast Ethernet 0/0 Interface IP Address	Serial 0/0/0 IP Address	Serial 0/0/1 IP Address	Enable Secret Password	Enable, VTY, and Console Password
Router 1	R1	192.168.1.1/24	192.168.5.1/30		class	cisco
Router 2	GW		192.168.5.2/30	172.16.1.1/30	class	cisco
Router 3	ISP	10.0.1.1/24		172.16.1.2/30	class	cisco
Host 1	H1	192.168.1.5/24 GW=192.168.1.1				
Host 2	H2	10.0.1.10/24 GW=10.0.1.1				

Objectives

- Set up network as shown in the topology diagram.
- Configure and verify single-area OSPF routing.
- Configure OSPF default route redistribution.
- Use IOS commands to troubleshoot and verify route redistribution.

Background / Preparation

Cable a network similar to the one shown in the topology diagram. Any router that meets the interface requirements displayed in the diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax given in the lab may vary. Depending on the router model, the interfaces may differ. For example, the interfaces may differ due to the router model. On some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0.

The following resources are required:

- Three Cisco routers, two with a serial connection and an Ethernet interface, and one with two serial interfaces
- One Windows-based PC with a terminal emulation program set up as a host
- At least one RJ-45-to-DB-9 connector console cable to configure the routers
- Two crossover Ethernet cables
- Two DTE/DCE serial cables

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Cable the network as shown in the topology diagram.

b. Connect Host 1 to the console port of Router 1 using a console cable to perform configurations.

Step 2: Perform basic configuration on Router 1

Configure Router 1 with a hostname, assign IP addresses to interfaces, assign privileged passwords, and configure for secure console and Telnet access according to the addressing table and topology diagram. Configure OSPF to advertise networks between routers. Save the configuration. This router will serve as an internal router to the network.

Step 3: Perform basic configuration on Router 2

Perform basic configuration on Router 2 with a hostname, assign IP addresses to interfaces, assign privileged passwords, and configure for secure console and Telnet access according to the addressing table and topology diagram. Configure OSPF to advertise networks between routers 1 and 2. Save the configuration. This router will serve as the router connecting the network to the ISP.

Step 4: Perform basic configuration on Router 3

Perform basic configuration on Router 3 with a hostname, assign IP addresses to interfaces, assign privileged passwords, and configure for secure console and Telnet access according to the addressing table and topology diagram. OSPF will not be configured on this router. Save the configuration. This router will serve as the ISP side router.

Step 5: Configure the hosts with IP address, subnet mask, and default gateway

a. Configure Host 1 and Host 2 with the proper IP address, subnet mask, and default gateway.

   1) Host 1 should be assigned 192.168.1.5 /24 and the default gateway of 192.168.1.1.

   2) Host 2 should be assigned 10.0.1.10 /24 and the default gateway of 10.0.1.1.

b. Each host should be able to ping its default gateway. If the ping is not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Configure default routing

In this scenario, the devices will have the following functions:

- Router 1 (R1) will be an internal enterprise network router.
- Router 2 (GW) is to serve as the gateway router connecting the network to the ISP.
- Router 3 (ISP) represents the ISP side of the Internet connection.
- Host 1 represents an internal network host.
- Host 2 (or loopback interface) connected to Router 3 represents a resource on the Internet.

This enterprise network is single-homed, meaning that it only has one connection to the Internet. Therefore, there is no need to run a routing protocol between the enterprise network and the ISP. Static routing will be used here.

After a default route to the ISP has been created on the GW router, it is desired to redistribute that default route into the rest of the enterprise network rather than configuring default routes on all enterprise routers.

a. Create a static route on the ISP router to the enterprise network.

```
ISP(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1
```

b. Create a default route on the GW router to the ISP router.

```
GW(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

c. Use the **show ip route** command on the GW router to observe the result from configuring the default route.

```
GW#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0/1
     192.168.5.0/30 is subnetted, 1 subnets
C       192.168.5.0 is directly connected, Serial0/0/0
O    192.168.1.0/24 [110/782] via 192.168.5.1, 00:13:39, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 172.16.1.2
GW#
```

The output of the **show ip route** command should indicate that a gateway of last resort has been identified.

d. Test the functionality by pinging from the GW router to Host 2.

Was the ping successful? __________

e. Test the current overall connectivity by pinging from Host 1 to Host 2.

Was the ping successful? __________

Explain the results.

____

f. The OSPF process does not automatically propagate the default route into the OSPF routing domain. Router R2 must be configured to redistribute the default route into the OSPF routing process. This can be done with the **redistribute static** command or with the **default-information originate** command. The **redistribute static** option must be considered carefully because, by default, it redistributes all static routes configured into the OSPF domain. This may or may not be desirable in a given scenario. In this scenario, use the **default-information originate** option.

```
GW(config-router)#default-information originate
```

g. Test the functionality by pinging from Host 1 to Host 2.

Was the ping successful? __________

h. Use the **show ip route** command on router R1 to observe the default route.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.5.2 to network 0.0.0.0
     192.168.5.0/30 is subnetted, 1 subnets
C       192.168.5.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.5.2, 00:02:56, Serial0/0/0
```

The output displays the default routing information. What type of OSPF route was generated on Router 1? ____

What type of OSPF router did Router 2 become? ____________________

Step 7: Troubleshooting default routing

Default routing is susceptible to many of the same issues that can cause problems with any OSPF route propagation. In this lab, some typical problems will be injected, and troubleshooting methods will be explored.

Router R2 has been configured with a default route. Even though it is a default route, the same reachability rules apply that apply to any route.

a. Shut down the S0/0/1 interface on Router ISP and observe the routing table on Router R1.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     192.168.5.0/30 is subnetted, 1 subnets
C       192.168.5.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

b. Observe that the default route is no longer present. Whenever a configuration like the one used in this lab is present and a default route is not appearing, first check whether other routers are also not receiving the default route. If multiple routers are not receiving the default route, go to the source of the default route – the GW router in this lab – and begin troubleshooting there. First, check the routing table on the GW router.

```
GW#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     192.168.5.0/30 is subnetted, 1 subnets
C       192.168.5.0 is directly connected, Serial0/0/0
O    192.168.1.0/24 [110/782] via 192.168.5.1, 00:23:27, Serial0/0/0
```

Because the default route does not appear in the routing table of the GW router, it cannot be advertised to other routers.

c. Troubleshooting becomes more difficult when the GW router is configured to always send the default routing information. Configure this option on the GW router now.

```
GW(config-router)#default-information originate always
```

d. Recheck the routing table on Router 1.

Is the default route present? __________

e. Attempt to ping from Host 1 to Host 2.

Was the ping successful? __________

In this scenario, checking the routing tables on routers in the network does not provide any helpful information. In this case, using **traceroute** from a host on the network would provide better information about how far the pings are going.

f. Display the routing table on router GW.

```
GW#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     192.168.5.0/30 is subnetted, 1 subnets
C       192.168.5.0 is directly connected, Serial0/0/0
O    192.168.1.0/24 [110/782] via 192.168.5.1, 00:59:29, Serial0/0/0
```

The oddity in this situation is that the default route does not appear on router GW but it is being advertised to router R1.

g. On router ISP, turn the S0/0/1 interface back up.

Other problems with default route advertisements are often due to typical OSPF communication issues. Next, you will inject some OSPF faults and observe the commands used to determine the faults.

h. On router GW, remove the current **network** statement and replace it with:

```
GW(config-router)#network 192.168.5.0 0.0.0.3 area 1
```

i. On R1, enter the **show ip ospf neighbor** command.

Do any neighbors appear? ___________

j. Knowing that OSPF has been configured on both routers, enter the **debug ip ospf events** command on R1 and observe the output.

```
R1#debug ip ospf events
*Mar  1 02:14:44.807: OSPF: Send hello to 224.0.0.5 area 0 on
FastEthernet0/0 from 192.168.1.1
*Mar  1 02:14:46.963: OSPF: Send hello to 224.0.0.5 area 0 on
Serial0/0/0 from 192.168.5.1
*Mar  1 02:14:52.743: OSPF: Rcv pkt from 192.168.5.2, Serial0/0/0, area
0.0.0.0
      mismatch area 0.0.0.1 in the header
```

In the event output, OSPF hellos are being sent and received. The packet received from router GW indicates the mismatched area. This mismatched area prevents the neighbor relationship from forming.

k. Replace the **network** statement on router GW with the correct one. After a brief delay, a console message should appear indicating that the neighbor relationship was re-established.

l. Verify this neighbor relationship with the **show ip ospf neighbor** command.

m. On Router 1, remove the **network** statement for the 192.168.5.0 network.

The output of the **debug ip ospf events** command is still helpful in this situation. In this case, the hint is in what is *not* appearing versus what *is* appearing. Notice that there is never an indication of a hello being sent out the Serial 0/0/0 interface.

n. On Router 1, enter the **`show ip ospf interface`** command. The output will be similar to this:

```
R1#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.5.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.5.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

The Fa0/0 interface information appears in the output but not the S0/0/0 interface information. This absence of information indicates that the S0/0/0 interface has not been configured to participate in the OSPF process.

o. Place the **`network`** statement for the 192.168.5.0 network back into the OSPF routing process, and then shut down the S0/0/0 interface.

p. On Router 1, enter the **`show ip ospf interface`** command.

```
R1#show ip ospf interface
Serial0/0/0 is administratively down, line protocol is down
  Internet Address 192.168.5.1/30, Area 0
  Process ID 1, Router ID 192.168.5.1, Network Type POINT_TO_POINT,
Cost: 64
  Transmit Delay is 1 sec, State DOWN,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.5.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.5.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Even though the serial interface is shut down, it still appears in the command output. This means that the **`show ip ospf interface`** command is showing the *configured* interfaces, not just the *active* interfaces.

Step 8: Reflection

a. Can a default route be advertised by an OSPF router that does not have the next hop in its routing table?

____

b. List three things that can cause OSPF default route propagation to fail?

____

____

____

c. What type of OSPF router does a router that injects a default route into the OSPF process become?

____

____

d. What is an advantage and a disadvantage of using the **`default-information originate`** command over configuring default routes on all routers?

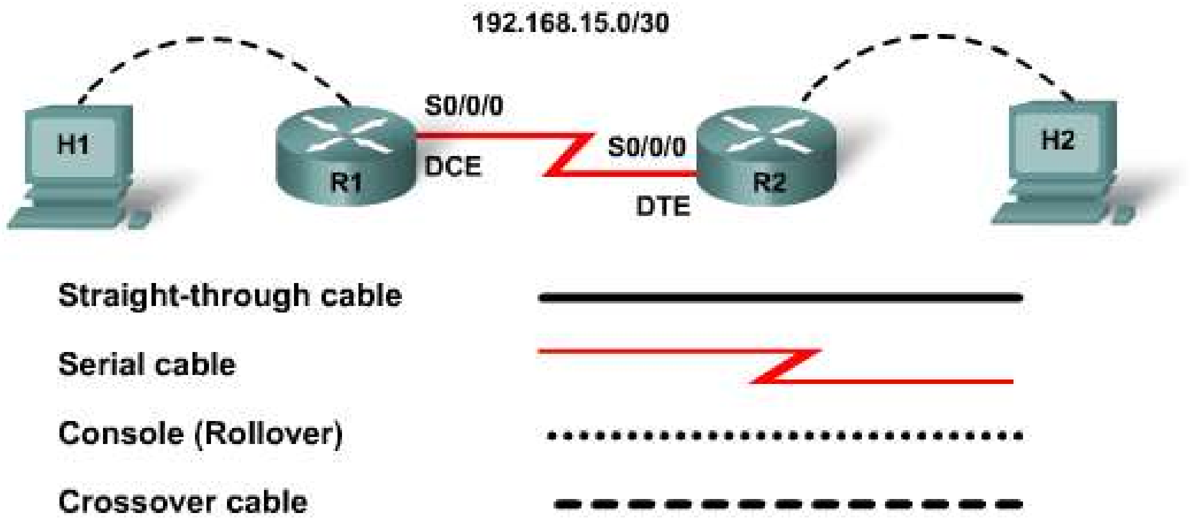
____

____

____

____

Lab 9.4.2 Troubleshooting WAN and PPP Connectivity



Device	Host Name	Serial 0/0/0 IP Address	Subnet Mask	Serial 0/0/0 Interface Type	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	192.168.15.1	255.255.255.252	DCE	class	cisco
Router 2	R2	192.168.15.2	255.255.255.252	DTE	class	cisco

Objectives

- Load the routers with preconfigurations.
- Discover where communication is failing.
- Gather information about the misconfigured portion of the network or any other errors.
- Analyze WAN and PPP related information to determine why communication is failing.
- Propose solutions to network errors.
- Implement solutions to network errors.

Background / Preparation

A small company is having problems in their network. You have been called to troubleshoot their problem. The company is using PPP with PAP authentication. Follow the topology diagram and addressing table to determine the physical setup and find where communication is failing. Use the **show** and **debug** commands to help locate the problems. When problems are found, implement solutions to repair any network errors.

Cable a network similar to the one shown in the topology diagram. Any router that has a single serial interface may be used for this lab. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination are acceptable.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may be identified differently. For example, on some routers, Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The information in this lab applies to routers that use the Serial 0/0/0 notation. If the router in use differs, use the correct notation for the serial interface.

The following resources are required:

- Two Routers, each with one Serial interface
- Two Windows-based PCs, both with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the routers
- One 2-part (DTE/DCE) serial cable

NOTE: Make sure that the routers have been erased and have no startup configurations. For instructions on erasing and reloading a switch and a router please refer to the Lab Manual. The Lab Manual can be found and downloaded on the Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM for basic router configuration, refer to the instructions provided in the Lab Manual, which can be found and downloaded on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

Connect the equipment as shown in the topology diagram.

Step 2: Load the preconfiguration on R1

a. See your instructor for obtaining the preconfigurations for this lab.

b. Connect PC1 to the console port of Router 1 to perform loading the preconfigurations using a terminal emulation program.

c. Transfer the configuration from PC1 to Router 1:

   1) In the terminal emulation program on PC1, choose **Transfer > Send Text File**.

   2) Locate the preconfiguration file and choose **Open** to start the transfer of the preconfiguration to Router 1.

   NOTE: The preconfiguration can also be copied and pasted into the router using the HyperTerminal program. Choose **Edit** and then **Paste to Host**. Before using the **Paste** function, be sure that you are in configuration mode.

3) When the transfer is complete, save the configuration.

Step 3: Load the preconfiguration on R2

Copy the preconfiguration on R2 using the process detailed in Step 2.

Step 4: Troubleshoot R1

a. Enter the command **`show interfaces serial 0/0/0`** to view the details of the interface.

What is the status of Serial 0/0/0? __________

Line Protocol is __________

The Internet address is ____________________________________

The subnet mask is _______________________________________

Encapsulation is __________

Is PPP LCP open? __________

Are there any problems? __________

If yes, what are they?

____

____

____

Issue the **`show controllers serial 0/0/0`** command. What did you find as a result of the command just entered?

____

b. If any errors were found, make the necessary configuration changes to R1.

Step 5: Show the details of Serial interface 0/0/0 on R2

a. Enter the command **`show interface serial 0/0/0`** to view the details of the interface.

What is the status of Serial 0/0/0? __________

Line Protocol is __________

The Internet address is ____________________________________

The subnet mask is _______________________________________

Encapsulation is __________

Is PPP open? __________

Are there any problems? __________

If yes, what are they?

____

____

b. If any errors were found, make the necessary configuration changes to R2.

Step 6: Turn on PPP debugging

a. Turn on the PPP debug function on both routers by entering **debug ppp authentication** at the privileged EXEC mode prompt.

```
R1#debug ppp authentication
R2#debug ppp authentication
```

NOTE: Debugging output is assigned high priority in the CPU process and can render a system unusable. When working on a live network, use only during periods of low network traffic.

What did the debug function report when the PPP encapsulation was applied to the router?

____

____

____

____

____

`Is PPP authenticating?` __________

b. Turn off the debug function by entering **undebug all** at the privileged EXEC mode prompt of both routers.

```
R1#undebug all
R2#undebug all
```

Step 7: Show the details of the configuration on R2

a. Enter the command **show run** to view the details of the interface.

____

____

b. If any errors were found, make the necessary configuration changes to R2.

Step 8: Verify that the serial connection is functioning

a. Ping from R1 to R2 to verify that there is connectivity between the two routers.

```
R1#ping 192.168.15.2
R2#ping 192.168.15.1
```

Can the serial interface on the R2 router be pinged from R1? __________

Can the serial interface on the R1 router be pinged from R2? __________

b. If the answer for either question is no, troubleshoot the router configurations to find the error. Then do the pings again until the answer to both questions is yes.

Step 9: Reflection

a. The IP address and subnet mask for R1 s0/0/0 is 196.168.15.1 and 255.255.255.252. R2s s0/0/0 interface was misconfigured to 192.168.15.2 and an incorrect subnet mask of 255.255.255.254. If all PPP authentication and all other parameters were configured correctly would R1 have been able to ping R2? Why or why not? ____

b. What command allows you to view the details of a specific interface?

____

c. When should you use the debug function in a router?

____

____

d. What is the default serial encapsulation on a Cisco router? _________________________

e. There were a number of configuration errors in the preconfigurations that were provided for this lab. Use this space below to write a brief description of the errors that you found.

____

____

____

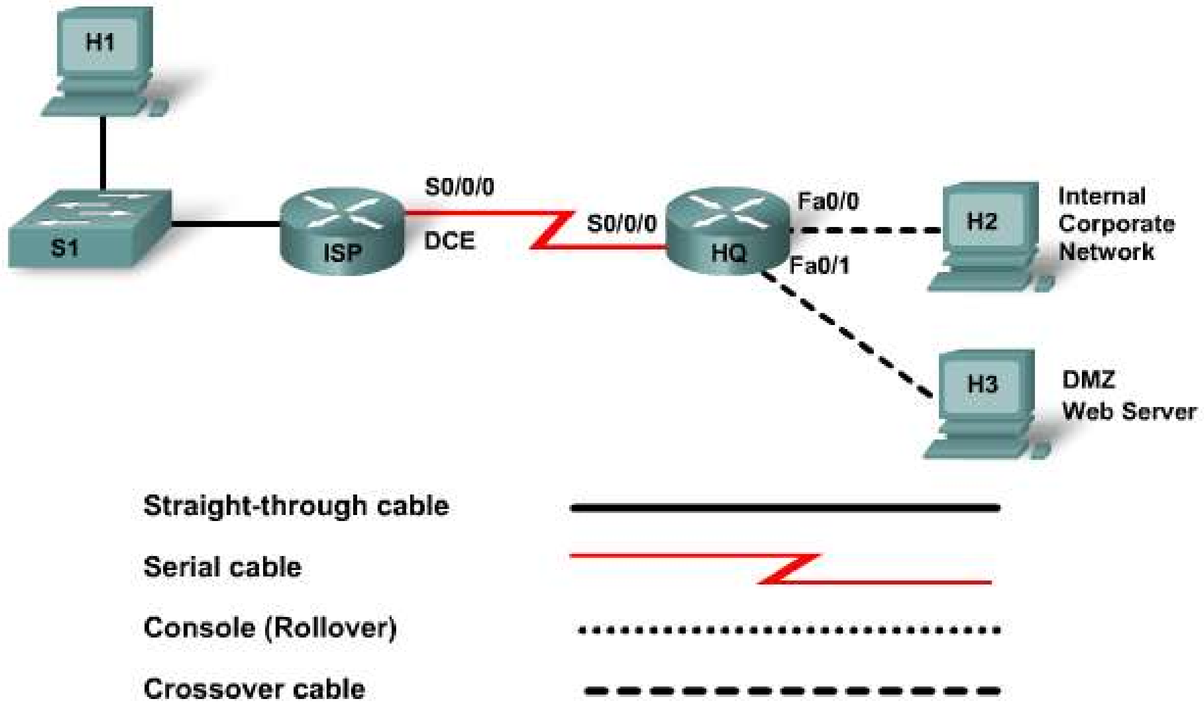
____

____

____

____

Lab 9.5.2 Troubleshooting ACL Configuration and Placement



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway	Enable Secret Password	Enable, vty, and Console Password
Router 1	ISP	**Fa0/0**	172.19.2.1	255.255.255.0	N/A	class	cisco
		S0/0/0	172.16.1.1	255.255.255.252	N/A		
Router 2	HQ	**Fa0/0**	172.18.2.1	255.255.255.0	N/A	class	cisco
		Fa/0/1	172.17.0.1	255.255.0.0	N/A		
		S0/0/0	172.16.1.2	255.255.255.252	N/A		
Host 1	H1	**NIC**	172.19.2.2	255.255.255.0	172.19.2.1		
Host 2	H2	**NIC**	172.18.2.2	255.255.255.0	172.18.2.1		
Web server (Discovery Server)	H3	**NIC**	172.17.1.1	255.255.0.0	172.17.0.1		

Objectives

- Load the routers with preconfigurations.
- Discover where communication is failing.
- Gather information about the misconfigured ACLs.
- Analyze information to determine why communication is not possible.
- Propose solutions to network errors.
- Implement solutions to network errors.

Background / Preparation

A small manufacturing company wants to create an awareness of their products over the Internet. Their immediate requirement is to promote their products to potential customers by providing product overviews, reports, and testimonials. Because they need a secure infrastructure to support their internal and external network requirements, you have implemented a two-tier security architecture consisting of an internal corporate network zone and a Demilitarized Zone (DMZ). The corporate network zone would house private servers and internal clients. The DMZ would house only one external server that would provide World Wide Web services. Since the company can only administer their own HQ router and not that of the ISP, all ACLs must be applied to the HQ router.

- **Access list 101 is implemented to limit the traffic out of the corporate network zone**, which houses private servers and internal clients. No other network should be able to access it. Protecting the corporate network begins by specifying which traffic can exit out of the network. This may sound strange, but it becomes clearer when it is known that most hackers are internal employees.
- **Access list 102 is implemented to limit the traffic into the corporate network.** Traffic entering the corporate network will be coming from either the Internet (ISP) or the DMZ. Only traffic that originated from the corporate network can be allowed back into that network. To make network management and troubleshooting easier, it is also decided to permit ICMP into the network. This will allow internal hosts to receive ICMP messages. At this time, no other traffic is desired into the corporate network.
- **Access list 111 is implemented to control outbound DMZ network traffic.** The DMZ network will house only one external server that will provide World Wide Web services. Other services such as e-mail, FTP, and DNS will be implemented at a later time. The traffic that can exit the network is specified here.
- **Access list 112 is implemented to control inbound DMZ network traffic.** Traffic entering the DMZ network will be coming from the Internet (ISP) or the corporate network requesting World Wide Web services, which must be allowed in. Allow only corporate users ICMP access into the DMZ network. No other traffic is permitted into the DMZ network.
- **Access list 121 is implemented to deter spoofing.** Networks are becoming increasingly prone to attacks from outside users. Hackers maliciously try to break into networks and render networks incapable of responding to legitimate request (Denial of Service (DoS) attacks). The access list should make it difficult for outside users to spoof internal addresses by specifying three common source IP addresses that hackers attempt to forge. These include valid internal private addresses, such as 172.19.2.0, loopback addresses such as 127.0.0.0, and multicast addresses (i.e., 224.x.x.x-239.x.x.x).

Cable a network similar to the one shown in the topology diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may be used; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switch or other comparable switch; alternately, crossover cables may be used between the hosts and routers and the switch omitted.
- One router with one Serial interface and 2 Ethernet interfaces
- One router with one Serial interface and one Ethernet interface
- Two Windows-based PCs, with a terminal emulation program, and set up as hosts
- One Windows-based PC running the Discovery Live CD representing the web server
- RJ-45-to-DB-9 connector console cable to configure the routers
- Two straight-through Ethernet cables
- One 2-part (DTE/DCE) serial cable
- Two crossover cables
- Cisco Discovery Live CD (obtain from instructor)

NOTE: Make sure that the routers have been erased and have no startup configurations. For instructions on erasing and reloading a switch and a router please refer to the Lab Manual. The Lab Manual can be found and downloaded on the Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM for basic router configuration, refer to the instructions provided in the Lab Manual which can be found and downloaded on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Fa0/0 interface of Router 1 to the Fa0/1 interface of the switch using a straight-through cable.

b. Connect each host to the Fa0/2 switch port of the switch using a straight-through cable.

c. Connect serial cables from Router 1 to Router 2 according to the topology diagram.

d. Connect both hosts on Router 2 to the Fa0/0 and Fa0/1 of Router 2 using crossover cables according to the above topology.

Step 2: Load the preconfiguration on ISP

a. See your instructor for obtaining the preconfigurations for this lab.

b. Connect Host 1 to the console port of Router 1 to perform loading the preconfigurations using a terminal emulation program.

c. Transfer the configuration from Host 1 to Router 1:

1) In the terminal emulation program on H1, choose **Transfer > Send Text File**.

2) Locate the preconfiguration file and choose **Open** to start the transfer of the preconfiguration to Router 1.

NOTE: The preconfiguration can also be copied and pasted into the router using the HyperTerminal program. Choose **Edit** and then **Paste to Host**. Before using the **Paste** function, be sure that you are in configuration mode.

3) When the transfer is complete, save the configuration.

Step 3: Load the preconfiguration on HQ

Copy the preconfiguration on HQ using the process detailed in Step 2.

Step 4: Configure hosts H1 and H2

a. Configure the Ethernet interfaces of H1 and H2 with the IP addresses and default gateways from the addressing table.

b. Test the PC configuration by pinging the default gateway from each PC.

Step 5: Configure the web server host H3

a. Load the Discovery LIVE CD on Host H3. The server's Ethernet interface is preconfigured with the IP address and default gateway shown in the addressing table. If using another web server, configure the IP address and subnet mask to match that in the table.

b. Test the PC configuration by pinging the default gateway from the PC.

Step 6: Troubleshoot the HQ router and access list 101

a. Begin troubleshooting with the HQ router.

Access list 101 is implemented to protect the internal corporate network zone, which houses private servers and internal clients. No other network should be able to access it. Protecting the corporate network begins by specifying which traffic can exit out of the network.

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 101. Enter the command **`show access-list 101.`**

What does the information show?

____

____

____

c. Verify reachability by pinging all systems and routers from each system. If a successful ping is not reached by all hosts, there is a problem with the access list.

Can H2 ping the web server? __________

Can H2 ping H1? __________

Can H1 ping the web server? __________

Can H1 ping H2? __________

Are there any problems with access-list 101? __________

If yes, what?

____

____

d. If any errors were found, make the necessary configuration changes to HQ. Remember that access lists have to be deleted and re-entered if there is any discrepancy in the commands.

____

____

____

____

e. Issue the command **`show ip interface fa0/0`**.

Is the access list applied in the correct direction on the Fa0/0 interface? __________

f. Perform the pings from Step 6c again. If the pings are not successful, continue to troubleshoot other access lists.

Step 7: Troubleshoot the HQ router and access list 102

a. Continue troubleshooting with the HQ router.

Access list 102 is implemented to limit the traffic into the corporate network. Traffic entering the corporate network will be coming from either the Internet (ISP) or the DMZ. Only traffic that originated from the corporate network can be allowed back into that network. To make network management and troubleshooting easier, it is also decided to permit ICMP echo replies into the network. This will allow internal hosts to receive replies from external hosts but not allow external hosts to ping internal hosts. At this time no other traffic is desired into the corporate network.

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 102. Enter the command **`show access-list 102.`**

What does the information show?

____

____

____

____

c. Verify reachability by pinging all systems and routers from each system. If the access list is working correctly, H1 cannot ping H2, but all of the other pings should be successful.

Can H2 ping the web server? __________

Can H2 ping H1? __________

Can H1 ping the web server? __________

Can H1 ping H2? __________

Are there any problems with access-list 102? __________

If yes, what?

____

____

d. If any errors were found, make the necessary configuration changes to HQ. Remember to delete the entire access list before making the corrections. The commands must be in logical, sequential order.

____

____

____

____

____

____

____

____

e. H2 should be able to ping H1. However, H1 should not be able to ping H2 at this point. Open a web browser, such as Windows Explorer, Netscape Navigator, or Firefox and enter the address of the web server in the address location. Verify that H2 has web access to the web server.

   Can H2 view the web page on the web server? __________

   Can H1 view the web page on the web server? __________

f. Issue the command **`show ip interface fa0/0`**.

   Is the access list applied in the correct direction on the interface? __________

g. If the web page cannot be viewed, troubleshoot as necessary. If the ping is unsuccessful, continue to troubleshoot the next access control list.

Step 8: Troubleshoot the HQ router and access list 111

a. Continue troubleshooting with the HQ router.

   Access list 111 is implemented to protect the DMZ network. The DMZ network will house only one external server that will provide World Wide Web services. Other services such as email, FTP, and DNS will be implemented at a later time. The HQ router will allow World Wide Web services destined for the web server into the DMZ network. Only corporate users will be allowed ICMP access into the DMZ network. No other traffic is permitted into the DMZ network.

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 111. Enter the command **`show access-list 111.`**

   What does the information show?

   ____

   ____

   ____

   ____

c. Verify reachability by pinging all systems and routers from each system. H1 should not be able to ping H2, but all other pings should be successful if the access list is correct.

   Can H2 ping the web server? __________

   Can H2 ping H1? __________

   Can H1 ping the web server? __________

   Can H1 ping H2? __________

   Are there any problems with access-list 111? __________

   If yes, what?

   ____

   ____

   ____

   ____

d. If any errors were found, make the necessary configuration changes to HQ.

   ____

   ____

   ____

   ____

e. Issue the command **`show ip interface fastethernet0/1`**.

   Is the access list applied in the correct direction on the interface? __________

f. If the pings do not produce the expected results, continue to troubleshoot the next access control list.

Step 9: Troubleshoot the HQ router and access list 112

a. Continue troubleshooting with the HQ router.

   Access list 112 is implemented to protect the DMZ network. Traffic entering the DMZ network will be coming from the Internet (ISP) or the corporate network requesting World Wide Web services, which must be allowed in. Allow only corporate users ICMP access into the DMZ network. No other traffic is permitted into the DMZ network.

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 112. Enter the command **`show access-list 112.`**

   What does the information show?

   ____

   ____

   ____

   ____

c. Verify reachability by pinging all systems and routers from each system. Only H2 should be able to successful ping all locations. If the access list is correct, H1 should not be able to ping the web server or H2.

   Can H2 ping the web server? __________

   Can H2 ping H1? __________

   Can H1 ping the web server? __________

   Can H1 ping H2? __________

   Are there any problems with access-list 112? __________

   If yes, what?

   ____

   ____

d. If any errors were found, make the necessary configuration changes to HQ.

   ____

   ____

   ____

   ____

e. Only H2 should be able to ping all locations. Open a web browser, such as Windows Explorer. Netscape Navigator, or Firefox and enter the address of the web server in the address location. Verify that H1 and H2 have web access to the web server.

   Can H1 view the web page on the web server? __________

   Can H2 view the web page on the web server? __________

   Can H2 ping all locations? __________

f. Issue the command **`show ip interface fastethernet0/1`**.

Is the access list applied in the correct direction on the interface? __________

g. If web browser services are not successful as they should be, troubleshoot as necessary. H2 should now be able to successfully ping all locations. H1 should not be able to ping the web server or H2.

Step 10: Troubleshoot the HQ router and access list 121

a. Continue troubleshooting with the HQ router.

Access list 121 is implemented to deter spoofing. Networks are becoming increasingly prone to attacks from outside users. Hackers maliciously try to break into networks and render networks incapable of responding to legitimate request (Denial of Service (DoS) attacks). The access list should make it difficult for outside users to spoof internal addresses by specifying three common source IP addresses that hackers attempt to forge; valid internal private addresses, such as 172.19.2.0, loopback addresses such as 127.0.0.0, and multicast addresses (i.e., 224.x.x.x-239.x.x.x).

b. Examine the HQ router to find possible configuration errors. Begin by viewing the summary of access list 121. Enter the command **`show access-list 121.`**

What does the information show?

____

____

____

____

c. Verify reachability by pinging all systems and routers from each system. If the access list is correct, only H2 should successfully ping the web server.

Can H2 ping the web server? __________

Can H2 ping H1? __________

Can H1 ping the web server? __________

Can H1 ping H2? __________

Are there any problems with access-list 121? __________

If yes, what?

____

____

____

____

d. Issue the command **`show interface serial0/0/0`**.

Is the access list applied in the correct direction on the interface? __________

e. If any errors were found, make the necessary configuration changes to HQ.

____

____

____

f. Open a web browser such as Windows Explorer or Netscape Navigator or Firefox and enter the address of the web server in the address location. Verify that H1 and H2 still have web access to the web server.

Can H1 view the web page on the web server? __________

Can H2 view the web page on the web server? __________

Step 11: Reflection

There were a number of configuration errors in the preconfigurations that were provided for this lab. Use this space below to write a brief description of the errors that you found.

____

____

____

____

____

____

____

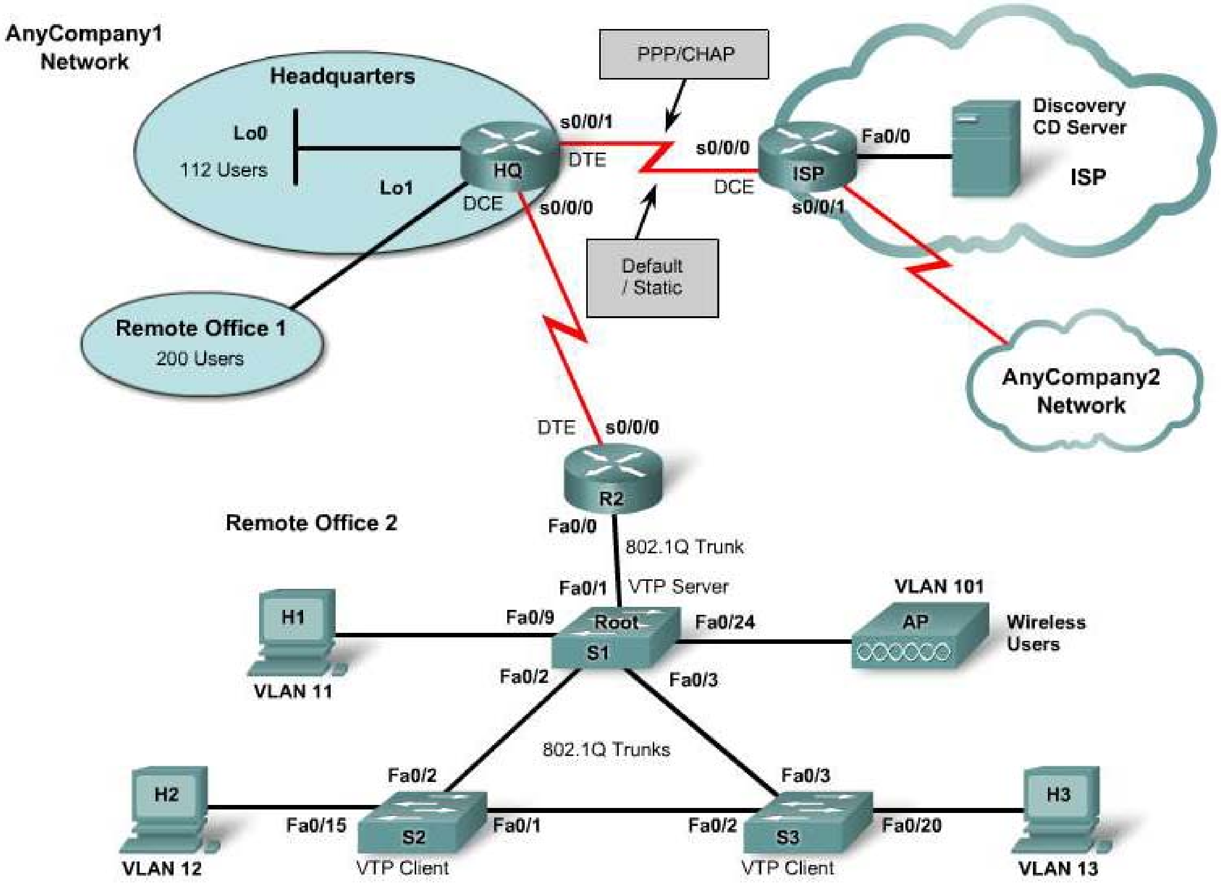
____

____

____

____

Summary Lab 10.0.1 Putting It All Together



Objectives

Part A

- Analyze the customer work order and proposed network design.
- Create a VLSM IP addressing scheme.

Part B

- Build a multilayer network and connect to a simulated ISP.
- Configure basic settings on switches with multiple VLANs and VTP.
- Configure the STP root bridge.
- Configure basic settings on routers and inter-VLAN routing.
- Verify basic connectivity, device configuration, and functionality.

Part C

- Configure multiple routers using OSPF, PAT and a default route.
- Configure WAN link using PPP and authentication.
- Configure multiple switches with port security.
- Configure ACLs to control network access and to secure routers.
- Verify connectivity, device configuration, and functionality.

Background / Preparation

AnyCompany is opening a new branch office (Remote Office 2) and has contracted you to extend the AnyCompany network into the new facilities. Corporate management has also decided that this would be a good time to restructure the existing network to provide increased levels of security and performance.

The existing network consists of a head office, which houses 112 employees, and a business office (remote office 1), which houses 200 employees. The new office space (Remote Office 2) will initially house four distinct groups of employees but will expand as the company grows. For this reason, implement VLANs to help manage the traffic. Also use VTP to simplify the task of managing the VLANs. One of the groups occupying the new office is the sales force. This group requires wireless access to the company network. Because security is of great concern, the wireless network must be on its own VLAN.

Initially the network in Remote Office 2 will consist of five VLANs.

This lab focuses on the configuration of the Cisco 1800 router and 2960 switch, or comparable equipment, using Cisco IOS commands. The information in this lab applies to other routers and switches; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0.

It is recommenced to work in teams of three. Each person can be responsible for one of the three switches and its associated host PC. The team can work together to configure the two company routers.

The following resources are required:

- One ISP router with one serial and one FastEthernet interface (preconfigured by instructor)
- Three Ethernet 2960 switches (or comparable) for Remote Office 2 LAN
- Two 1841 routers (or other routers), one with a FastEthernet interface and one with two serial interfaces
- One Wireless Access Point (optional)
- One Ethernet 2960 switch to connect wired PCs
- Three Windows XP-based PCs to act as wired clients
- One Discovery CD Server, preconfigured by instructor (optional if a Loopback is on ISP router)
- Cat 5 cabling as necessary (straight-through and crossover)
- Two Serial DTE/DCE cables for WAN links
- ISP work order (included in this lab)

Part A – Review the work order and develop the VLSM subnet scheme

Task 1: Review the customer work order and proposed network.

You have received the following work order from your manager at the ISP. Review the work order to get a general understanding of what is to be done for the customer.

ABC-XYZ-ISP Inc.

Official Work Order

Customer: AnyCompany1 or AnyCompany2 **Date:** _____________

(Circle the customer name assigned by your instructor)

Address: 1234 Fifth Street, Anytown

Customer Contact: Fred Pennypincher, Chief Financial Officer

Phone number: 123-456-7890

Description of work to be performed

Review the proposed network topology at the beginning of the lab. The existing network includes Headquarters (HQ) and Remote Office 1 (RO1). You will need to configure the HQ router, build the network for Remote Office 2 (RO2) network and connect it to the HQ router. Equipment for the RO2 network consists of an additional 1841 router, 3 new 2960 switches, and a wireless Access Point (AP). RO2 will use VLANs to separate user departments, a server farm, and wireless users. The RO2 router will route between VLANs and pass traffic to the HQ router to be forwarded to the ISP. The HQ router must use a static address to communicate with the ISP router. The ISP serial interface IP address is:

____

If HQ is connected to the ISP as AnyCompany1, the IP address of the ISP Serial 0 interface is 209.165.201.1/30.

If HQ is connected to the ISP as AnyCompany2, the IP address of the ISP Serial 1 interface is 209.165.202.129/30.

The serial link to the new ISP uses PPP encapsulation with CHAP authentication and static routes. The OSPF routing protocol is to be used between the HQ and RO2 routers and the encapsulation on the WAN link between them is HDLC. Routes from the RO2 network must be summarized and advertised to the HQ router.

You will need to develop a VLSM addressing scheme that will accommodate the existing HQ and RO1 networks as well as the new RO2 network.

Assigned to: Approved by:

Guy Netwiz Bill Broadband, ISP Manager

Task 2: Develop the network scheme

NOTE: Be sure to have the instructor check your work for each step in this task before going on to Task 3.

Step 1: Determine the size of the CIDR address block assigned

a. The customer has been assigned CIDR network address: ______________________________

If network customer is AnyCompany1, use 172.20.0.0/22.

If network customer is AnyCompany2, use 172.20.4.0/22.

b. How many total host IP addresses does this CIDR address block represent?

____

Using this address block, you will develop a VLSM subnet scheme that will allow AnyCompanyX to support existing HQ and RO1 networks as well as the new RO2 network.

Step 2: Determine the size of each VLSM block to accommodate users

a. Based on the CIDR address assigned by the ISP and the number of users in each area or VLAN, optimally subnet this block of addresses to provide sufficient addresses for all offices (HQ, RO1, and RO2) and VLAN requirements.

b. To start, determine the size of the subnet address block required for a network area or group of users. Fill in the table with this information. Look at the number of users for each area or subnet and determine the smallest power of 2 that will cover the requirement. As an example, if 93 addresses were required, a VLSM block of 128 (2^7) would be needed. The next smallest power of 2 is 64 (2^6), which does not cover the requirement. A block of 128 results in some unused addresses but also allows for growth.

Network Area	No. Users / IPs	VLSM block size / No. of IPs (powers of 2)
HQ Network	112	
RO1 Network	200	
RO2 Network / VLANs		
VLAN 1 (Server Farm)	18 users	
VLAN 2 (Native/mgmt -IP)	9 users	
VLAN 11 (Dept 1)	75 users	
VLAN 12 (Dept 2)	112 users	
VLAN 13 (Dept 3)	38 users	
VLAN 101 (wireless)	52 users	
WAN link (RO2 to HQ)	2	
Total users and block sizes for RO2	306	
RO2 block size to subdivide	N/A	
Total users and all VLSM blocks	618	

c. To optimally allocate addresses from the /22 CIDR address, start by sorting the block sizes from largest to smallest. For this lab, add up the individual smaller blocks for each of the VLANs in the RO2 network and allocate a single larger block that will cover all the smaller block requirements. This keeps all of the subnets together for RO2 and aids in route summarization. Use the table below to order the network areas by the VLSM block size. List the large block for the entire RO2 network first, followed by the others. The larger RO2 block will be broken down into smaller subnets later.

Network Area / VLAN	VLSM block size starting with the largest first
RO2 total block size (will be subdivided into smaller blocks)	
RO1 Network	
HQ Network	
RO2 - VLAN 11 (Dept 1)	
RO2 - VLAN 12 (Dept 2)	
RO2 - VLAN 13 (Dept 3s)	
RO2 - VLAN 101 (wireless)	
RO2 - VLAN 1 (Server Farm)	
RO2 - VLAN 2 (Native/mgmt -IP)	
RO2 - HQ Wan link	

Step 3: Determine subnet addresses for the CIDR block

a. Determine which blocks of CIDR address to assign to each area of the network or VLAN. Use the VLSM subnet chart (Appendix A) to enter the subnet information for each of the CIDR blocks.

b. To determine the subnet addresses for the 172.20.0.0/22 or the 172.20.4.0/22 CIDR block, use the subnet calculator tool on the Cisco Network Academy website. With the subnet calculator tool, enter the Base Network Address (172.20.0.0 or 172.20.4.0) and the value of VLSM Mask 1 in dotted decimal, starting with 255.255.252.0 (/22). Click the **Actions** button **Calculate Subnetting using VLSM**. Use the same base address and increase the mask length by one each time to fill in the chart.

NOTE: Entries for the subnet numbers for the /29 and /30 mask are not included in the table. Subdivide one of the /28s to a /30 for the WAN link.

Step 4: Allocate blocks of addresses to each area of the network

a. Fill in the following table based on the subnet information in the CIDR/VLSM Subnet Chart and the sorted table of address requirements. Draw lines around each of the blocks in the address table above, or color them in, and label each one according to the network area or VLAN to which it is assigned.

Network Area / VLAN	**VLSM Block Size (# of addr)**	**Subnet Address and Prefix**	**Useable Address Range**	**Subnet Mask**
RO2 total block size (will be subdivided into smaller blocks)				
RO2 – VLAN 11 (Dept 1)				
RO2 – VLAN 12 (Dept 2)				
RO2 – VLAN 13 (Dept 3)				
RO2 – VLAN 101 (wireless)				
RO2 – VLAN 1 (Server Farm)				
RO2 – VLAN 2 (Native/mgmt – IP)				
RO2 - WAN link				
RO1 Network				
HQ Network				

b. Have the instructor verify that your addressing scheme is accurate and assigns address space efficiently. You should not have any overlapping subnets and should have unused contiguous blocks of addresses that can used for future subnets as the company grows.

Task 3: Determine IP addresses to use for device interfaces

Step 1: Select IP addresses for use when configuring devices

Select addresses from the block assigned to an area of the network and fill in the IP address and subnet mask to be used for each device/interface in the topology. These IP addresses will be used later in Part C when configuring the network equipment.

NOTE: When finished with this Task, check with the instructor before proceeding.

Device Interface / IP Address Chart

Device	Interface	IP Address	Subnet Mask
HQ	Serial 0/0/0		
	Serial 0/0/1		
	Loopback0 (HQ)		
	Loopback1 (RO1)		
R2	Serial 0/0/0		
	FastEthernet 0/0	None	None
	Subint Fa0/0.1		
	Subint Fa0/0.2		
	Subint Fa0/0.11		
	Subint Fa0/0.12		
	Subint Fa0/0.13		
	Subint Fa0/0.101		
ISP	Serial 0/0/0	209.165.201.1 (AnyCompany1) or 209.165.202.129 (AnyCompany2)	255.255.255.252
S1 (RO2)	VLAN 2		
S2 (RO2)	VLAN 2		
S3 (RO2)	VLAN 2		
H1	NIC		
H2	NIC		
H3	NIC		

Step 2: Have the instructor check your work for this task before going on to Part B.

Part B – Physically construct the network and perform basic device configuration

Task 1: Build the network and connect cables to the interfaces and ports indicated

Connect your AnyCompanyX network router HQ to the ISP router. The ISP router and the Discovery CD Server should be preconfigured by the instructor. If ISP router is configured with a Loopback address in lieu of the Discovery CD Server, the HTTP server in the router must be enabled. If you are unsure, check with your instructor.

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

The IP addresses used to configure the devices in the following tasks should be based on your solution for the VLSM scheme.

NOTE: VLAN Mismatch Messages - You may want to wait until after the switches are configured to connect the trunk links. Otherwise, native VLAN mismatch messages come up until all switches are configured.

Task 2: Configure the HQ router

Step 1: Configure the HQ host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the HQ serial and loopback interfaces

The WAN link from HQ to R2 uses default Cisco HDLC encapsulation.

The WAN link from HQ to ISP uses PPP with CHAP authentication.

Step 3: Create CHAP user ID and password

Configure a username for the ISP router on the HQ router with a password of **cisco** for use with CHAP authentication.

Step 4: Save the router running-config configuration to startup-config

Step 5: Copy the router running-config to a text editor and save it for later use, if needed

a. Open a text editor such as Windows Notepad.

b. Issue the **`show running-config`** command.

c. Copy the output and paste it into the text editor.

d. Save the file on the Windows Desktop as **HQ.txt**.

Task 3: Configure the Remote Office 2 router R2

Step 1: Configure the R2 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the RO2 FastEthernet subinterfaces and serial interfaces

a. It is easier to troubleshoot the FastEthernet subinterfaces if the numbers match the VLAN numbers they represent. They should also use 802.1Q encapsulation.

b. VLAN 2 is the native VLAN.

c. The WAN link from HQ to R2 uses default Cisco HDLC encapsulation.

Step 3: Save the router running-config configuration to startup-config

Step 4: Copy the router running-config to a text editor and save it for later use, if needed

a. Open a text editor such as Windows Notepad.

b. Issue the **`show running-config`** command.

c. Copy the output and paste it into the text editor.

d. Save the file on the Windows Desktop as **R2.txt**.

NOTE: If you need to use this file later, you will need to edit it to clean it up and make sure that the necessary interfaces have the **`no shutdown`** command applied to them.

Task 4: Configure the Remote Office 2 switch S1

NOTE: Be sure to erase the startup-config, delete the vlan.dat file, and reload the switch before beginning the configuration.

Step 1: Configure the S1 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the VLANs for Remote office 2 on S1 using the VLAN numbers and names shown in the chart below

Assign ports to each VLAN as indicated. Use the same chart to configure switches S2 and S3:

RO2 VLAN Number	VLAN Name	Ports assigned	Notes
VLAN 1 (default VLAN)	default	Ports 4-5	VLAN 1 cannot be renamed
VLAN 2 (Native/mgmt – IP)	Mgmnt	Port 23	
VLAN 11 (Dept 1 users)	Dept1	Ports 6 to 11	
VLAN 12 (Dept 2 users)	Dept2	Ports 12 to 17	
VLAN 13 (Dept 3 users)	Dept3	Ports 18 to 22	
VLAN 101 (wireless)	Wireless	Port 24	

Step 3: Assign an IP address to the Management VLAN 2 on S1

a. Assign the VLAN 2 address according to the Device Interface / IP Address Chart in Part A, Task 3, Step1.

b. Configure the switch with a default gateway to router R2 for VLAN 2.

Step 4: Configure S1 switch ports Fa0/1, Fa0/2 and Fa0/3 as 802.1Q trunks

The trunks carry VLAN information. Set each trunk to use VLAN 2 as the native VLAN.

Step 5: Configure S1 as the root switch for STP

Change the priority of native VLAN 2 from the default of 32769 to 4096.

Step 6: Configure a VTP domain

a. Configure the AnyCompanyX domain name (where X is 1 or 2) on S1 and a password of **cisco**.

b. Configure S1 as the VTP server.

Step 7: Save the switch running-config configuration to startup-config

Step 8: Copy the switch running-config to a text editor and save it for later use, if needed

Task 5: Configure the Remote Office 2 switch S2

Step 1: Configure the S2 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the VTP domain AnyCompanyX on S2 with S2 as a client using the password of cisco

It is not necessary to configure the VLANs on S2. As a VTP client, the information will be obtained from VTP server S1.

You will, however, need to assign ports to the VLANs according to the chart in Part B, Task 4, Step 2.

Step 3: Assign an IP address to the Management/Native VLAN 2 on S2

a. Use the IP address from the Device Interface / IP Address Chart in Part A, Task 3, Step 1.

b. Configure the switch with a default gateway to router R2 for VLAN 2.

Step 4: Configure Switch ports Fa0/1 and Fa0/2 as 802.1Q trunks to carry VLAN information

Step 5: Save the switch running-config configuration to startup-config and copy the switch running-config to a text editor for later use, if needed

Task 6: Configure the Remote Office 2 switch S3

Step 1: Configure the S3 host name, passwords, no domain lookup, and message-of-the-day

Step 2: Configure the VTP domain AnyCompanyX on S3 in client mode with a password of cisco

In client mode, it is not necessary to configure the VLANs on S3 because the information will be obtained from VTP server S1.

You will, however, need to assign ports to the VLANs according to the chart in Part B, Task 4, Step 2.

Step 3: Assign an IP address to the Management/Native VLAN 2 on S3

a. Use the IP address from the Device Interface / IP Address Chart in Part A, Task 3, Step1.

b. Configure the switch with a default gateway to router R2 for VLAN 2.

Step 4: Configure Switch ports Fa0/2 and Fa0/3 as 802.1Q trunks to carry VLAN information

Step 5: Save the switch running-config configuration to startup-config

Step 6: Copy the switch running-config to a text editor and save it for later use, if needed

Task 7: Configure host IP addresses

Step 1: Configure each host IP address and subnet mask

Use the information in the Device Interface / IP Address Chart in Part A, Task 3, Step 1.

Step 2: Configure the default gateway

Use the VLAN information to determine the default gateway for each host. This is the R2 subinterface address in the Device Interface / IP Address Chart in Part A, Task 3, Step 1.

Task 8: Verify device configurations and basic connectivity

Step 1: Before going on to Lab Part C, verify that the devices are correctly configured

Verify that there is basic connectivity as appropriate between devices for AnyCompanyX. Verify the following items and indicate which command you used:

Item to verify	Command used
Basic configuration of HQ (hostname, passwords, etc)	
Basic configuration of R2 (hostname, passwords, etc)	
Basic configuration of S1 (hostname, passwords, etc)	
Basic configuration of S2 (hostname, passwords, etc)	
Basic configuration of S3 (hostname, passwords, etc)	
Correct subinterfaces created on R2 Fa0/0	

Item to verify	**Command used**
Correct encapsulation on R2 subinterfaces	
Correct VLANs created on each switch	
Ports are in correct VLANs on each switch	
Native VLAN is VLAN 2	
Correct ports are 802.1Q trunks on each switch	
S1 is root switch	
S1 is VTP server	
S2 is VTP client	
S3 is VTP client	
Ping S1 from H1 H2, and H3	
Ping S2 from H1, H2, and H3	
Ping S3 from H1, H2, and H3	
Ping R2 default gateway from H1, H2, and H3	
Ping R2 default gateway from S1, S2, and S3	
Ping from H1 to H2 and H3 (between VLANs)	
Ping HQ from R2	

Part C – Routing, ACLs, and switch security configuration

Task 1: Configure routing for HQ and R2

Step 1: Configure OSPF process 1 for Area 0 on R2

Specify the subnet for each R2 interface using the appropriate wildcard mask.

Step 2: Configure OSPF process 1 for Area 0 on HQ

Step 3: Issue the `show ip route` command on HQ to see the routing table

How many OSPF routes have been learned from R2? __________

Step 4: Configure a default route to the ISP on HQ and propagate this route to R2 using OSPF

Step 5: Verify that R2 has learned about the default route configured on HQ

Use the **`show ip route`** command on R2.

`What is the gateway of last resort for R2?`

____

Step 6: Save the router running-config configuration to startup-config

Task 2: Configure overloaded NAT (PAT) on HQ

Step 1: Configure overloaded NAT (PAT) on HQ

a. Use the IP address on the serial port that connects to the ISP as the overloaded address.

b. Specify the inside and outside NAT interfaces.

Step 2: Ping the Serial 0/0/0 address of the ISP router (209.165.201.1) from the PC Host H1 command prompt

Was the ping successful? __________

Step 3: Open a browser on host H1 and enter the IP address of the ISP router Serial 0/0/0 interface (209.165.201.1)

Were you able to access the HTTP interface using the browser? __________

Step 4: On the HQ router issue the `show ip nat translations` command

```
HQ#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.2:512 172.20.0.2:512     209.165.201.1:512  209.165.201.1:512
tcp 209.165.201.2:1072 172.20.0.2:1072    209.165.201.1:80   209.165.201.1:80
```

For the ping (icmp) entry, what is the inside local address and port number?

____

For the ping (icmp) entry, what is the inside global address and port number?

____

For the browser connection (tcp) entry, what is the inside local address and port number?

____

For the browser connection (tcp), what is the outside global address and port number? _______________

Step 5: Save the router running configuration to NVRAM.

Task 3: Configure port security for the switches

Step 1: Configure switch port security on switches S1, S2, and S3

Connecting any host other than the one connected previously should disable the port.

Step 2: Display the MAC address table entry for Fa0/9

This is the port to which H1 is connected. Use the show **mac-address-table int f0/9** command. You may need to ping from the PC to the switch or other destination to refresh the MAC address table entry.

```
S1#show mac-address-table int f0/9
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  11    000b.db04.a5cd    DYNAMIC     Fa0/9
Total Mac Addresses for this criterion: 1
```

Step 3: Before configuring port security, clear the dynamically learned MAC address entry using the clear mac-address-table dynamic interface command

Step 4: Before configuring port security, shut down the port and then issue the port security commands

a. The **switchport port-security mac-address sticky** command allows the switch to learn the MAC address currently associated with the port. This address will become part of the running comfiguration. If the running–config is saved to the startup-config, the MAC address will be retained when the switch is reloaded.

b. The **switchport port-security** command enables port security on the port using the defaults. The defaults are: 1 MAC address allowed and **shutdown** as the violation action to be taken. Enter **no shutdown** to bring the port back up so that it can learn the MAC address of the PC.

Step 5: Ping from H1 to the VLAN 11 default gateway

Allow some time to pass and then issue the **show running-config** command to see the MAC address that the switch learned.

Step 6: Display the port security for Fa0/9 using the show port-security interface command

What is the Port Status? ____

What is the Security Violation Count? ______________________________

What is the Source Address:Vlan? ________________________________

```
S1#show port-security int fa0/9
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
```

```
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 000b.db04.a5cd:11
Security Violation Count   : 0
```

Step 7: Remove the PC H1 cable from switch port Fa0/9 and connect the cable from PC H2

a. Ping from H2 to any IP address to cause a security violation on port Fa0/9. You should see security violation messages.

b. Issue the **`show port-security interface`** command again for Fa0/9.

What is the Port Status? ____________________________________

What is the Security Violation Count? ___________________________

What is the Source Address:Vlan? ______________________________)

Step 8: Move the cables for the PCs back to their original ports and restore port Fa0/9

a. Clear the sticky address entry for port Fa0/9.

b. To return the interface from `error disable` to `administratively up`, enter the **`shutdown`** command followed by the **`no shutdown`** command.

Step 9: Save the switch running-config configuration to startup-config

Step 10: Repeat Steps 1 through 6 to set port security for the other two switches, S1 and S2, and save the running config to startup-config

Task 4: Verify overall network connectivity before applying ACLs

Step 1: Before configuring ACLs, verify routing, NAT, and basic connectivity for AnyCompanyX and the ISP

Step 2: Verify the following items and indicate which command you used

Item to verify	Command used
Routing configuration of HQ (OSPF/Static)	
Routing configuration of R2 (OSPF/Static/Summary)	
NAT overload on HQ	
Port security on S1, S2, and S3	
Ping from H1, H2 ,and H3 to HQ S0/0/0	
Ping from H1, H2, and H3 to HQ Lo0 (HQ LAN)	
Ping from H1, H2, and H3 to HQ Lo1 (RO1 LAN)	
Ping from H1, H2, and H3 to ISP S0/0/0	
Ping from H1, H2, and H3 to ISP Discovery CD Server	
Web browser from H1, H2, and H3 to ISP router Loopback or Discovery CD Server address	
Telnet from H1, H2, and H3 to HQ and R2	

Task 5: Configure ACL Security on HQ and R2

NOTE: The following commands are based on IP address ranges for one possible solution to the VLSM scheme in part of the lab. Replace the address ranges with those that match the ones that you applied to the Remote Office 2 Hosts and VLANs.

Step 1: Create and apply an Extended Numbered ACL on the edge router (HQ)

a. The ACL allows replies to requests made by internal hosts to enter the network. Allow internal users to **`ping`** or **`trace`** any location on the Internet but do not allow any **`ping`** or **`trace`** access to people external to the enterprise.

b. Apply the ACL to the NAT outside interface of the HQ router to protect the AnyCompanyX network.

c. Test the ACL by pinging from H1, H2, and H3 to the ISP loopback address or the IP address of the Discovery CD Server.

Were the pings successful? __________

d. Using a browser from H1, H2, and H3, enter the ISP router Loopback0 address or the IP address of the Discovery CD Server.

Were you able to access the web interface of the router or the Web page from the server?

____

Step 2: Create and apply an Extended Named ACL on R2

a. The ACL allows web requests and pings to leave the Remote Office 2 network if they originated in VLANs 1, 11, 12, 13, or 101. Telnet traffic is permitted if it originated in VLAN 12, and FTP traffic is permitted if it originated in VLAN 13. All other traffic is denied.

b. On the R2 router, apply the ACL to each Fa0/0 subinterface except Fa0/0.2, the native VLAN.

c. Test the ACL by pinging from H1, H2, and H3 to the ISP loopback address or the IP address of the Discovery CD Server.

Were the pings successful? __________

d. Using a browser from H1, H2, and H3, enter the ISP router Loopback0 address or the IP address of the Discovery CD Server.

Were you able to access the web interface of the router or the Web page from the server?

____

e. Telnet from Host H1 in VLAN 11 to the HQ router using its S0/0/0 IP address.

Were you able to telnet to it? __________

f. Telnet from Host H2 in VLAN 12 to the HQ router using its S0/0/0 IP address.

Were you able to telnet to it? __________

g. Use the **`show access-lists`** command to verify that the ACL is working.

Step 3: Create and apply a standard ACL to control VTY access to the HQ router

a. The ACL should deny hosts from all VLANs on Remote Office 2 except for Host H2 on VLAN 12. This will still allow other hosts on VLAN 12 to access router R2 using telnet.

b. Apply the ACL to VTY lines 0 through 4 on the R2 router.

c. Telnet from Host H2 in VLAN 12 to the HQ router using its S0/0/0 IP address.

Were you able to telnet to it? ___

d. Change the IP address of H2 to another one that is on VLAN 12 and telnet again from Host H2 in VLAN 12 to the HQ router using its S0/0/0 IP address.

   Were you able to telnet to it? ___

e. Use the **`show access-lists`** command to verify that the ACLs are working.

Step 4: On R2 and HQ, save the router running configuration to NVRAM

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (Fa0)	FastEthernet 1 (Fa1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (Fa0/0)	FastEthernet 0/1 (Fa0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
NOTE: To find out exactly how the router is configured, look at the interfaces. Doing this will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in IOS command to represent the interface.				

APPENDIX A

CIDR / VLSM Subnet Chart

Base Address: 172.20.0.0		**Subnet Mask: 255.255.252.0**							
CIDR mask	**/22**	**/23**	**/24**	**/25**	**/26**	**/27**	**/28**	**/29**	**/30**
Dot mask (octets 3&4)	**252.0**	**254.0**	**255.0**	**255.128**	**255.192**	**255.224**	**255.240**	**255.248**	**255.252**
No hosts possible	**1,024**	**512**	**256**	**128**	**64**	**32**	**16**	**8**	**4**
Subnet # (octets 3&4)									

Base Address: 172.20.0.0	**Subnet Mask: 255.255.252.0**					