
Southern Polytechnic State University

Electrical and Computer Engineering Technology Program

ECET 4820 Laboratory Exercise: Cisco Router Configuration

Objective:

Students will learn how to configure a Cisco 2600 or 2800 series router so that it can route IP packets between local area networks via a wide area network.

Background:

One major role of a router is to segment an organization's internal network, or Intranet. In this case, a router will interface to one or more local area networks (LANs), providing connections between them. Routing between LANs may be done through a single router in the case of small Intranets, or in the case of larger networks, several routers can be used to interface to the LANs with a backbone network connecting the routers. In addition, an Intranet uses one or more routers to provide a connection to the WAN. This exercise will focus on the function of routers within an Intranet, where the Intranet is acting as a WAN.

Manufacturers design routers for the particular role they will fill. These roles are changing rapidly as the demand for LAN and WAN infrastructure capacity increases. Nevertheless, routers are essentially designed to operate at the Network layer of the OSI model (layer 3) and the Internet layer of the TCP/IP protocol (layer 3). They provide numerous functions during the process of routing packets, which can essentially be divided into those concerned with making next-hop routing decisions, protocol translation, firewall functions, and the encapsulation/decapsulation of packets.

Routers use routing tables to determine where to send incoming packets. In the case of a static routing algorithm, the next hop is pre-determined and is only changed manually by a network administrator. Dynamic routing algorithms require routers in the network to exchange topology and congestion information with each other periodically in order to determine the route to a destination. Routing tables are then adjusted to minimize routing delays through the network. This exercise will examine the routing Information Protocol (RIP).

The Cisco router operating system and configuration file is stored in a memory configuration much the same as in a personal computer. One difference is that the router does not require as much RAM or ROM as a PC. Another is that the router's operating system and configuration file can be loaded from a remote TFTP file server. This is done for the purposes of redundancy and centralized configuration management.

The Cisco router has four types of memory: 1) ROM is used to store a simple, low-level operating system called RXBOOT that handles automatic loading of the main operating system and permits configuration of the router via an external interface; 2) RAM is used to store the main operating system and configuration files during operation as well as the routing table and data queues; 3) non-volatile RAM (NVRAM) that is used to store the configuration files; and 4) Flash memory stores the boot image, which is a compressed version of the main operating system. The flash memory is non-volatile and acts like a PC's hard disk drive.

Upon power-up, the Cisco router's low-level operating system performs some diagnostic tests. In its default boot sequence, the router attempts to find the operating system image, called the Internet Operating System or IOS, in flash memory and loads it into RAM. Once in RAM, the boot image is uncompressed. In the rare case that the IOS is not in flash, the router will attempt to load it from the designated TFTP server. The router will then try to load the configuration file from NVRAM. If this

fails, it will attempt to load the configuration from the TFTP server. After the configuration file is loaded, the router begins normal operation.

Overview:

Several Cisco routers will be configured as a corporate Intranet. Each has two Ethernet LAN interfaces and two serial WAN interfaces. The 2600 series has 10/100 fast Ethernet interfaces and the 2800 series has two 10/100/1000 gigabit interfaces. Fig. 1 shows how the Intranet will be connected. First, teams of students will log on to one of the Cisco routers through its console port. Next, the command line interface (CLI) will be used to configure one of the router's Ethernet interfaces. Once this is done, the rest of the configuration will be done via Telnet through the Ethernet interface. Initially the routers will be running its operating system boot image and a basic configuration file without all interfaces configured.

Students will create a new router configuration in order to implement the network topology shown in Fig. 1. The following tasks will be performed:

1. Log on to the router.
2. Experiment with Cisco's context-sensitive help and investigate the command history.
3. Verify router configuration.
4. Examine the routing table and check dynamic routing.
5. Configure the network interfaces.

IP addresses will be assigned to both Ethernet interfaces (F 0/0 and F 0/1) and both serial interfaces (S 0/0 and S 0/1) for each router. The synchronous serial interfaces will be set up to run Point-to-Point Protocol (PPP) at 2.0 Mbps as the Layer 2 protocol.

6. Save the configuration, re-boot the router, and check the configuration.
7. Create standard and extended access lists.

Procedure:

Logistics

1. You will work in teams during this exercise. Your instructor will assign you to a workstation and a router. Enter the name of your router below (London, Paris, or Washington).

Router Name: _____

Physical Configuration

2. The routers and workstations are to be connected together as shown in Fig. 1. This may already be done. If it is, verify the configuration. Complete the steps below as necessary. Ask your instructor whether or not you should perform any configurations via the console port. **Most likely you will not.** The routers may already have one of their Ethernet interfaces configured, so you can skip over step a) and access your router via Telnet. Tables 1 and 2 show the IP address scheme for the network.

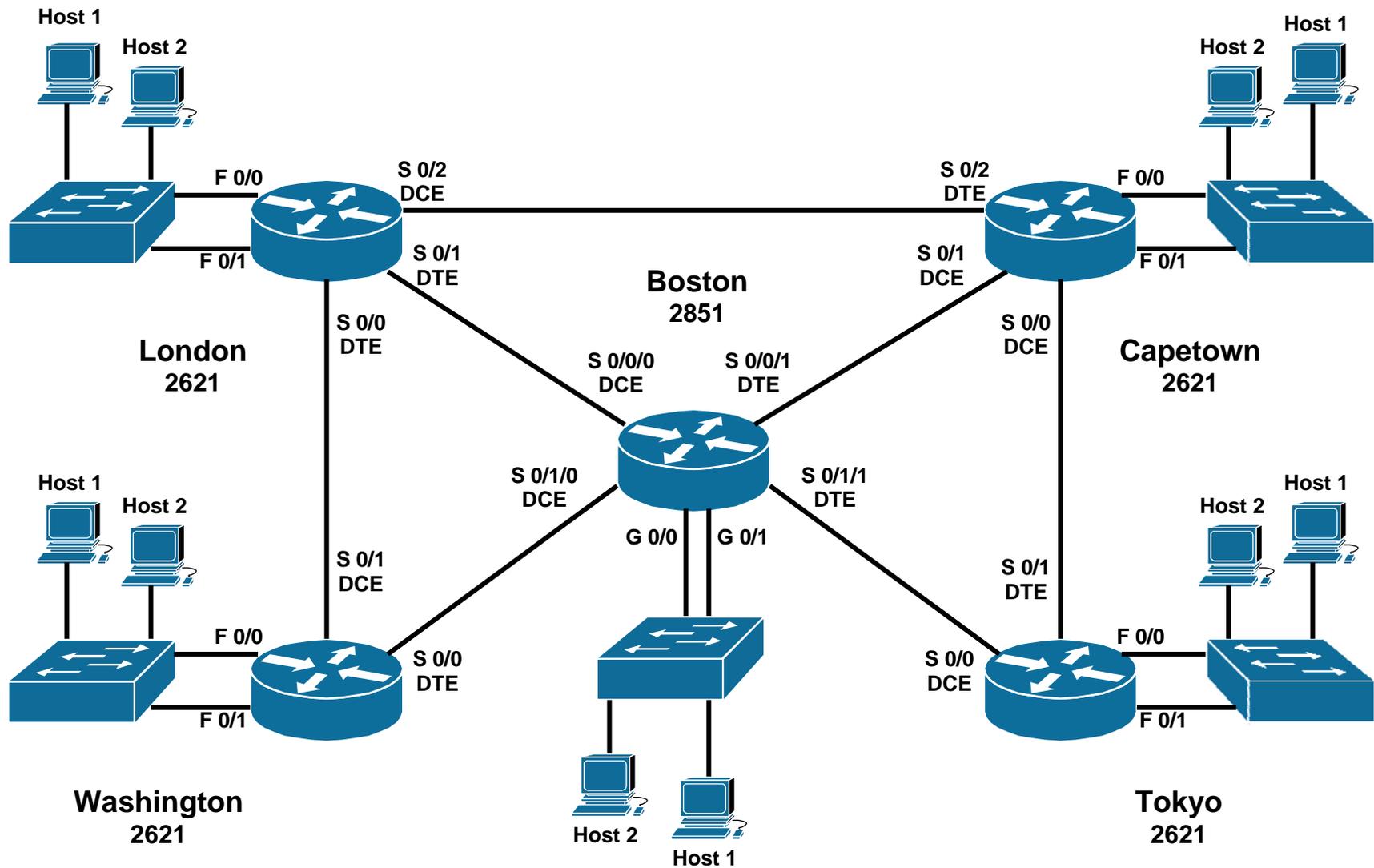


Fig. 1. Lab network configuration.

Table 1. 2600 Series Router Addresses.

Location	S 0/0	S 0/1	S 0/2	S 0/3	F 0/0	F 0/1	Host 1	Host 2
Washington	10.10.1.1 /24	10.10.2.1 /24			192.168.10.1 /24	192.168.11.1 /24	192.168.10.2 /24	192.168.11.2 /24
London	10.10.2.2 /24	10.10.3.1 /24	10.10.4.1 /24		192.168.30.1 /24	192.168.31.1 /24	192.168.30.2 /24	192.168.31.2 /24
Tokyo	10.10.7.1 /24	10.10.6.2 /24			192.168.40.1 /24	192.168.41.1 /24	192.168.40.2 /24	192.168.41.2 /24
Capetown	10.10.6.1 /24	10.10.5.1 /24	10.10.4.2 /24		192.168.50.1 /24	192.168.51.1 /24	192.168.50.2 /24	192.168.51.2 /24

Table 2. 2800 Series Router Addresses.

Location	S 0/0/0	S 0/0/1	S 0/1/0	S 0/1/1	G 0/0	G 0/1	Host 1	Host 2
Boston	10.10.3.2 /24	10.10.5.2 /24	10.10.1.2 /24	10.10.7.2 /24	192.168.20.1 /24	192.168.21.1 /24	192.168.20.2 /24	192.168.21.2 /24

- a) Connecting your workstation to the Cisco router console port as in Fig. 2.
 - i) Connect the Cisco serial cable to the router console port.
 - ii) Connect the other end to the Cisco crossover adapter.
 - iii) Connect the adapter to the workstation serial port, using a 25-pin to 9-pin serial port adapter if necessary.

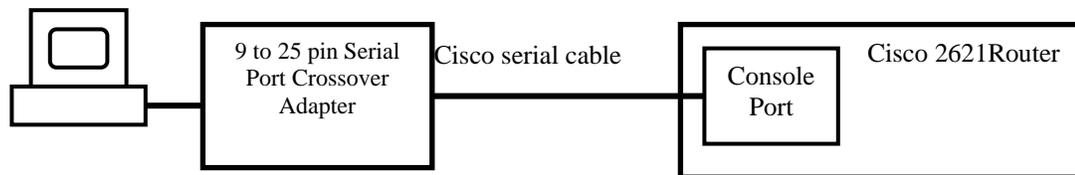


Fig. 2. Console port connection.

- b) Connecting your workstation to the Ethernet.
 - i) Telnet access requires that a workstation be connected to the router through the network. Also, the workstation can be connected to the router Ethernet port directly or through the lab patch panel and Ethernet switch.
 - ii) If connecting directly, run a *crossover* patch cable from the workstation Ethernet card to your router's Ethernet port.
 - iii) If connecting through the Ethernet switch, use normal patch cables to connect your workstation to the switch and then from the switch to the router's Ethernet port.
- c) Configuring TCP/IP on your workstation.
 - i) To communicate to your router through the Ethernet, you need to configure TCP/IP on your workstation.
 - ii) Boot your workstation to the operating system designated by your instructor.
 - iii) Set up TCP/IP using the IP address and subnet mask shown in Fig. 1 for your workstation. For example, one of the London router's workstations has IP address 192.168.30.2 and subnet mask 255.255.255.0 and it is connected to London's F0/0 Ethernet interface.
 - iv) Use your router's Ethernet address that is connected to your workstation as the default gateway. For example, the default gateway for the workstation in the step above is 192.168.30.1.
- d) Connecting the router serial ports.
 - i) The router serial ports should already be connected properly.

Booting the Cisco Router

3. The router may already be running the correct configuration for this lab, so you may not need to reboot the router. Ask your instructor if you must reboot your router, which will load and run the

configuration file stored in NVRAM. If it is necessary for you to reboot, follow the instructions below. Otherwise, go to the log on procedure.

- a) If the router is off, turn it on using the power switch on its panel. The boot sequence will take about 3 minutes.

Log on to the Router

There are four basic ways to gain access to the router in order to configure it using the command line interface. The first is a direct connection from a computer to the router. The computer is configured as a terminal using an application like Microsoft's HyperTerminal and connected using a special cable and adapter to the router's console port. The second is through a modem connected directly to the router's modem port. The third is to use Telnet from a host that can reach a network port on the router. The fourth is to use a WWW browser from a host that can reach one of the router's network ports.

Cisco routers use two levels of password access, **user mode** and **privileged mode**. When you first log on to the router you are automatically in user mode. The prompt appears similar to the following:

hostname>

where the > symbol indicates user mode. User mode is limited to functions like checking the router status. To configure the router, you must enter privileged mode by typing **enable** at the user mode prompt. After supplying the enable password, you will see a new prompt similar to:

hostname#

where the # indicates that you are in privileged mode. You can configure the router in this mode. The **disable** command returns you to user mode from privileged.

In this exercise you will only access the router through its console port and the Telnet connection. **Ask your instructor which method to use for the initial router configuration.**

4. Perform the following steps only if you are using the console port interface.

- a) If the terminal emulation program on your computer (i.e. HyperTerminal) has a configuration called **Cisco_2621.ht**, double click on it to connect to the Cisco router.
- b) If the configuration *does not* exist, create one using the setup wizard as follows:
 - i) Double click the **Hyperterm.exe** icon.
 - ii) Type the name **Cisco_2621**. Click **OK**.
 - iii) In the **Connect To** box, choose the COM port of your computer that you will use. This is usually COM1.
 - iv) In the **COM1 Properties** box, choose the following settings:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None

- v) Click **OK**.
- c) Initiate the session by double-clicking on the **Cisco_2621.ht** icon.
 - i) Press **Enter** when the window pops up.
- d) You should see the user mode prompt *hostname>*, where **Name** is the router name.
 - i) Type **enable** in all lower case letters and press **Enter**.
 - ii) The router will respond with the **Password:** prompt. Enter the password given by your instructor and press **Enter**.

**Note: if you do not enter the password within a given time a time out may occur.
Press enter once and wait for the prompt to reappear.**

- e) The router will respond with the privileged mode prompt *hostname#*. You are now successfully logged in to the Cisco router and ready to configure it.
5. Perform the following steps if you are using Telnet.
- a) Open a Command window.
 - b) Establish a session by typing “**telnet address**”, where address is the IP address of the gateway to the router.
 - i) The telnet window appears and you will see **Password:**.
Note: you may see a **Username:** prompt first.
 - ii) Enter the **virtual terminal** username and password designated by your instructor.
 - iii) The router will respond with the user-mode prompt like *hostname>*.
 - c) Enter **enable** at the prompt. The router will respond with the **Password:** prompt. Enter the enable password given by your instructor.

Note: if you do not enter the password in a given time a time out may occur. Press enter once and wait for the prompt to reappear.
 - d) The router will respond with the *hostname#* (or similar) prompt. You are now successfully logged in to the Cisco router and are ready to configure it.

The Help Command

6. There are often situations where you do not know the command or the way to use a command. In that case, use the IOS context-sensitive help.
- a) Typing “?” at the prompt lists all of the router commands available at that privilege level. Do this now.
 - i) If you see -- **More--** at the bottom with your cursor next to it, pressing **Enter** displays one more line and pressing the **space bar** displays the next page.
 - ii) From privileged mode, type **disable** to return to user mode and display the list of commands again. You should see a difference in the available commands between the two modes.
 - iii) Return to privileged mode.

- b) If you type “*command ?*”, where *command* is the command you want to learn about, the router shows you the parameters available to you.
- c) Type **show ?**. Determine the appropriate command to display the router’s system hardware and software status. What is the version of the IOS image file?

IOS version: _____

- d) To get an idea of how context-sensitive help works, try the following commands and watch the results.
 - i) Type **show c?**.
 - ii) Type **show cl?**
 - iii) Type **show cloc** followed by **Enter**.

Using the History Buffer

- 7. The router IOS maintains a history of the commands entered during your session. The default size is the last 10 commands.
 - a) Type **show hist**. What is the result?
 - b) At the prompt, press the **up** and **down** arrow keys. What happens?

Checking Router Configuration

- 8. You will check several router configuration parameters. Initially, your router will be fully functional. Later the configuration will be removed and you will have to rebuild it.
 - a) In privileged mode, type **show ip ?**.
 - b) Type the command to show the router IP interface configuration.
 - c) If any interfaces have IP configured, the router will respond by listing the name of the circuit, the circuit number, whether it is up or down, its IP address, its subnet mask, plus many more parameters. You may see an active Ethernet interface, but in most cases you will see “**Internet Protocol processing disabled**” under the interface name. List the names of the interfaces with IP configure and those without IP configured in the table below.

Interfaces With IP Configured	Interfaces Without IP Configured

Display the Routing Table

9. The routing table shows all of the networks that your router can reach either directly or indirectly and the next-hop address needed to reach that network.
 - a) At the *hostname#* prompt, type **show ip route** and press **Enter**.
 - b) The routing table will appear. You should see a response much like that in the table below. The number of destinations and other parameters will vary depending on the router.

Source of Route Info	Destination	Administrative Distance	Next Hop Address	Time Since updated	Interface
R	10.10.2.2/32	[120/1]	10.1.1.1	00:00:08	Serial 0/0
R	10.10.2.0/24	[120/1]	10.1.3.2	00:00:08	Serial 0/1

- c) Have your instructor verify that your table is correct. Once it is verified, enter it below or copy it to a text-editing program and save or print it.

Source of Route Info	Destination	Administrative Distance	Next Hop Address	Time Since updated	Interface
				Omit	

- d) Re-enter the **show ip routes** command after 5 minutes. Did any table entries change? Which ones?

Check RIP Dynamic Routing

10. The instructor will disable one of the router's serial ports. The routers will communicate with each other using RIP and attempt to route around the bad connection. Within a minute the routers will adapt to the changed topology.
- Immediately after your instructor disables the port, enter **show ip route**. What happened to your routing table? Can your router still reach all of the other networks? Check the other groups to see if their tables changed.
 - After 1 minute, re-enter the **show ip route** command. What happened to your routing table? Can your router still reach all of the other networks? Check the other groups to see if their tables changed.
 - After 4 minutes, re-check your routing table. Enter your final routing table below, or copy it to a text-editing program and save or print it.

Source of Route Info	Destination	Administrative Distance	Next Hop Address	Time Since updated	Interface
				Omit	

Checking RIP Route Updates (Demo by Instructor)

11. Routers periodically exchange route information with each other as part of the RIP protocol. The debug command is used to examine the route updates. **The update information is only output to the console port, not over the Ethernet.** This part will be demonstrated by your instructor.
- At the *hostname#* prompt, type **debug ip rip**. You will see the RIP updates
 - How often do the updates arrive from a given router?

Configuring the Router Interfaces

Your instructor will reload your router with a minimal configuration and you will rebuild the configuration to make it fully-functional.

12. You will set up both Ethernet ports and both serial ports using IOS commands. Cisco names its interfaces as follows.

Interface Type	Cisco Name
10BaseT	Ethernet or E
100BaseTX	FastEthernet or F
1000BaseTX	GigabitEthernet or G
Serial	Serial or S

Interfaces are identified by their location in the router using the designation **network-module-slot/interface-card-slot/port** or if built into the chassis then **interface-card-slot/port**, where **interface-card-slot** is the slot number and **port** is the interface number in that slot. Numbering starts at 0. For example, F 0/0 identifies the first 100BaseTX interface in slot 0. S 1/1 identifies the second serial interface (interface 1) in the second slot (slot 1). Also, the dual serial interface cards installed in the 2800 series router HWIC slots use the three number designation with the left-most number always 0. For example: **S 0/1/1**.

Important: Refer to Tables 1 and 2 for the IP addresses and subnet masks for your router's interfaces.

- a) Make sure you are in privileged mode. Then type **confi g t** (or config terminal). You should see the prompt **hostname(config)#**.
- b) If you are using a telnet connection, you are doing so through FastEthernet interface **F 0/0** (or **G 0/0**) and can skip the next step.
- c) Configuring the Ethernet interface F 0/0 (G 0/0). **Skip this step if you are using a telnet connection.**
 - i) Then type **int F 0/0**; then press **Enter** . The prompt should appear as **hostname(config-if)#**.
 - ii) After this, type **ip address address mask**; then press **Enter**. Address is the IP address in dotted decimal format and mask is the subnet mask.
- d) Configuring the Ethernet interface F 0/1 (G 0/1).
 - i) Then type **int F 0/1**; then press **Enter** .
 - ii) After this, type **ip address address mask**; then press **Enter**.
- e) Configuring the serial port S 0/1. To configure this port, we do the same as the Ethernet port.
 - i) Type **int S 0/1**; then press **Enter** .
 - ii) After this, type **ip address address mask**; then press **Enter**.
 - iii) Next type **encapsulation ppp**, then press **Enter**. This sets up the PPP data link protocol on your serial interface.

iv) If Fig 1. says this is a DCE interface on your router, you must set the clock rate. Your interface will clock the corresponding DTE interface on the other router. If it is, do the step below.

- Type **clockrate 2000000** then press **Enter**.

Important: a DCE interface has a different cable connected to it than a DTE interface. In the lab, they have been properly marked.

Important: only configure a clock rate on the DCE interfaces.

Important: the 2800 series router automatically detects whether the cable connected to its serial interface is a DTE or DCE cable. In the case of the DTE cable, it automatically removes a clockrate specification and in the case of a DCE cable, it automatically assigns a clockrate that you can modify using the clock rate command.

f) Configuring the serial port S 0/0.

i) Type **int S 0/0**; then press **Enter** .

ii) After this, type **ip address address mask**; then press **Enter**.

iii) Next type **encapsulation ppp**, then press **Enter**. This sets up the PPP data link protocol on your serial interface.

iv) If Fig 1. says this is a DCE interface on your router, you must set the clock rate. Your interface will clock the corresponding DTE interface on the other router. If it is, do the step below.

- Type **clockrate 2000000** then press **Enter**. This sets the data rate to 2Mbps.

Important: only configure a clock rate on the DCE interfaces.

g) After this press **Ctrl** key and press **z** at the same time. This will take you to the enable prompt **hostname#**.

Configuring RIP Routing Protocol

13. **Ask your instructor if you are to perform this task.** If so, you will configure the router to run the RIP (Routing Information Protocol), which is a suitable protocol for small networks. Once RIP is started, it is necessary to tell the router which networks it is connected to.

a) At the **hostname#** prompt, type **config t**. You should see the **hostname(config)#** prompt.

b) Type **router rip**. This starts RIP with its default settings. The router will respond with the prompt **hostname(config-router)#**.

c) Determine the networks to which your router is connected. For example, 10.0.0.0, 192.168.30.0, 192.168.31.0, etc. These must be the Class A, B, or C address, not a subnetted version. **Ask your instructor if you have difficulty.**

d) Type **network address**, where address is the network address as defined in c) above. Repeat for all of the networks your router is connected to.

c) Type **Ctrl-z** to exit configuration mode.

Saving Your Router Configuration and Rebooting Your Router.

14. When setting up the Cisco router like you have done here, the changes do not take place immediately. One has to save the configuration in a start file and the router must be rebooted using this file for the changes to take effect. To do this one has to do this.
- a) **Have your instructor verify your configuration.**
 - b) At the *hostname#* prompt type **copy run start** and then press **enter twice**.
 - c) After this, the router should say **building configuration** and the router will copy the currently running configuration that you created to NVRAM.
 - i) Type **reload** at the command prompt.
 - ii) The router will then reboot.
 - iii) The telnet window should then be closed.
 - iv) Once this is done, you must log back into the router.

Check Your Router's Configuration

15. Always test your configuration after rebooting to make sure that everything works. The more extensive the changes, the more testing you need to do.
- a) At the *hostname#* prompt, type **show ip int** followed by **Enter**.
 - b) From the data displayed on the screen, can you tell whether or not your configuration was implemented? Check to see that the interface is **up** and the line protocol is **up**.
 - i) If a serial interface says line protocol is down, you did not set up PPP properly.
 - ii) If a serial interface is down, the DTE/DCE clocking is wrong.
 - c) **Have your instructor verify that your interface configuration information is correct.** Once it is verified, enter it below.

Circuit	State	IP Address	Mask	Clockrate (if applicable)

- d) Type **show run** (abbreviation for **show running-config**). Do you see all of configuration information you entered?

Testing the Intranet Connections

16. As part of any network configuration procedure, you must determine that all connections are correct. Once all of the routers have been rebooted, it takes about 30 seconds for them to exchange RIP routing information. After the routing tables are stable, the reachable networks should be listed in the table.
- Verify that all of the networks in Fig. 1 appear in the routing table. If not, identify which ones are not there.
 - From the list of missing networks, identify the router(s) to which these networks are *directly* connected. The group responsible for this router must fix its configuration prior to moving to the next step.

Saving Your Configuration to a TFTP Server

17. In most network implementations, you will want to back up your router configurations on a server so they can be downloaded to the router as needed. You can save many different configurations as you experiment with them. The trivial file transfer protocol (TFTP) is very similar to file transfer protocol (FTP), but without all of the available commands. Both of these protocols are part of the TCP/IP suite. By starting a TFTP server on your administrator's workstation, you can upload or download the router's configuration very easily. The only requirement is that the router can reach the server via a network connection. Once the TFTP server is started, it is pointing to a home directory that it will use for uploads and downloads. You can change that directory in the TFTP application window.
- From your workstation, start the TFTP server. Click **Start**→**Programs**→**TFTP Server**.
 - From a telnet session with your router, enter the privileged mode. You should have a prompt like *hostname#*.
 - Save your router's configuration to your workstation by typing **copy running-config tftp** at the prompt. You will have to supply the TFTP server's IP address and a file name. Use the name **router-mm-dd-yy.cfg**, where mm-dd-yy corresponds to today's date.
 - Check to see if your file appears in the TFTP server's directory.
 - Have your instructor verify your results.**

Creating and Using Standard Access Lists

Access lists are configured on Cisco routers and applied to interfaces as a means of controlling network traffic. They are important components of firewalls. For example, they can be used to deny access to the network by a particular workstation, or they can be used to deny any http traffic from entering your network. The network administrator first creates an access list consisting of a series of *permit* and/or *deny* statements that apply to IP addresses or upper layer protocols. The list is then applied to the desired router interface.

Standard access lists deal only with IP source or destination addresses in incoming or outgoing packets. *Extended access lists* are used to filter packets based on the upper layer protocols, not just the IP address.

There are two important considerations when creating an access list. First, *access list statements are processed in the order they appear in the list*. Make sure you get the order right. Second, *all Cisco*

access lists have an implicit “**deny all**” statement added to the end by the router. So any packet that does not meet any of the conditions in the access list is automatically denied by the router. Therefore, it is important to put a “permit all” statement at the end. Note: since the deny all statement is implicit, you will not see it at the end when you display the list.

18. You will create a standard access list to deny any traffic coming from one of the Ethernet interfaces on your router from being forwarded to the router’s other Ethernet interface. Standard access lists are given numbers 1-99.

a) From your router’s *hostname#* prompt, type **config t**.

b) Type **access-list 1 deny XX.YY.0.0 0.0.255.255**.

i) The **XX.YY.0.0** is the network number, including subnet, of the network on your router that you are denying traffic from entering your other subnet.

ii) Here you have entered a deny as the first line of access list number 1.

iii) The **0.0.255.255** is a wild card mask (not a subnet mask). The 0’s indicate that the packet address must match these positions. The 1’s indicate that they do not have to match these positions. So, your wild card mask is telling the deny statement to look at the first two octets of the packet’s address.

c) Type **access-list 1 permit any**.

i) Here you are permitting any other traffic through and avoiding the implicit deny all.

19. Now that you have your list, apply it to the interface you want to keep the traffic out of. For example, if you are denying traffic from 172.25.0.0 on interface **f 0/0** from entering the 172.26.0.0 network on interface **f 0/1**, apply the access list to **f 0/1** and make it an *outbound* list. By making it an outbound list, it affects traffic coming through your router, hitting the 172.26.0.0 interface, and attempting to go *out* the interface to the 172.26.0.0 subnet.

a) From the *hostname(config)#* prompt, type **interface f 0/X**, where X is either 1 or 0 as desired. This command puts you in the mode of configuring that interface.

b) At the *hostname(config-if)#* prompt, type **ip access-group 1 out**.

c) Verify that your access list exists and is applied to the interface by doing the following.

i) Return to the *hostname#* prompt.

ii) Type **show run** to display the running configuration.

iii) Scroll down the configuration output until you see the interface that you applied the access list to. Do you see the line indicating that access list 1 is applied to the interface?

iv) Now scroll down until you see the access list itself. Do you see the permit and deny commands you entered?

d) Test your access lists by pinging from each of your workstations to the other.

Important: be sure you are pinging from your workstations, and not from a telnet session of the router!

e) **Have your instructor verify your results.**

20. Now remove the access list from your interface and remove the list from the configuration.

- a) At the *hostname(config-if)#* prompt, type **no ip access-group 1 out**.
- b) At the *hostname(config)#* prompt, type **no access-list 1**.

Exiting out of the Routers

21. Type **exit** at each prompt until you log yourself out and then close the hyperterminal or telnet window.

Questions:

1. What are the meanings of the parameters in the routing table (Source of Route, Destination, Administrative Distance, Next Hop Address, Time Since updated, Interface)? Do not discuss each table entry.
2. What is the difference between the privileged and user modes?
3. How does RIP respond when a router serial port connection is cut?
4. Which is the most flexible way to access your router: the console or telnet? Which is most secure?
5. Did the results from ping verify your routing table? Why or why not?
6. You have a network consisting of a number of workstations and two web servers, all connected through an Ethernet switch to your gateway router. The gateway router has another interface connected to an outside network. You want one web server to only be accessed from your internal network, but the other can be accessed from the outside or inside. How might you use an access list on your gateway router to implement this web server configuration?

Your explanation does not have to include the specific commands; just discuss how you would restrict the traffic. Assume both networks connected to the router use public IP addresses and that no network address translations are being performed by the router.

Conclusions:

Bring together the concepts illustrated in the lab and make conclusions as to what they mean, and what you learned.

References

- [1] S. McQuerry, *Interconnecting Cisco Network Devices*, Indianapolis, IN, Cisco Press, 2000.