

Chapter 1 — Routing Concepts

1.0.1.2 Class Activity– Do We Really Need a Map?

Objectives

Describe the primary functions and features of a router.

Scenario

Using the Internet and Google Maps, located at <http://maps.google.com>, find a route between the capital city of your country and some other distant town, or between two places within your own city. Pay close attention to the driving or walking directions Google Maps suggests.

Notice that in many cases, Google Maps suggests more than one route between the two locations you chose. It also allows you to put additional constraints on the route, such as avoiding highways or tolls.

- Copy at least two route instructions supplied by Google Maps for this activity. Place your copies into a word processing document and save it for to use with the next step.
- Open the .pdf accompanying this modeling activity and complete it with a fellow student. Discuss the reflection questions listed on the .pdf and record your answers.

Be prepared to present your answers to the class.

Resources

- Internet connection
- Web browser
- Google Maps, <http://maps.google.com/>

Reflection

1. What do the individual driving, or walking based on your criteria you input, and non-highway directions look like? What exact information do they contain? How do they relate to IP routing?
-

2. If Google Maps offered a set of different routes, what makes this route different from the first? Why would you choose one route over another?

3. What criteria can be used to evaluate the usefulness of a route?

4. Is it sensible to expect that a single route can be “the best one”, i.e. meeting all various requirements? Justify your answer.

5. As a network administrator or developer, how could you use a network map, or routing table, in your daily network activities?

1.1.1.9 Lab – Mapping the Internet

Objectives

Part 1: Determine Network Connectivity to a Destination Host

Part 2: Trace a Route to a Remote Server Using Tracert

Background / Scenario

Route tracing computer software lists the networks that data traverses from the user's originating end device to a distant destination device.

This network tool is typically executed at the command line as:

```
tracert <destination network name or end device address>
```

(Microsoft Windows systems)

or

```
traceroute <destination network name or end device address>
```

(UNIX, Linux systems, and Cisco devices, such as switches and routers)

Both **tracert** and **traceroute** determine the route taken by packets across an IP network.

The **tracert** (or **traceroute**) tool is often used for network troubleshooting. By showing a list of routers traversed, the user can identify the path taken to reach a particular destination on the network or across inter-networks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of hops the data traveled from source to destination.

The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks, such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Command-line based route tracing tools are usually embedded with the operating system of the end device. This activity should be performed on a computer that has Internet access and access to a command line.

Required Resources

PC with Internet access

Part 1: Determine Network Connectivity to a Destination Host

To trace the route to a distant network, the PC used must have a working connection to the Internet. Use the **ping** command to test whether a host is reachable. Packets of information are sent to the remote host with instructions to reply. Your local PC measures whether a response is received to each packet, and how long it takes for those packets to cross the network.

- a. At the command-line prompt, type **ping www.cisco.com** to determine if it is reachable.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

- b. Now ping one of the Regional Internet Registry (RIR) websites located in different parts of the world to determine if it is reachable:

Africa: **www.afrinic.net**

Australia: **www.apnic.net**

South America: **www.lacnic.net**

North America: **www.arin.net**

Note: At the time of writing, the European RIR www.ripe.net does not reply to ICMP echo requests.

The website you selected will be used in Part 2 for use with the **tracert** command.

Part 2: Trace a Route to a Remote Server Using Tracert

After you determine if your chosen websites are reachable by using **ping**, you will use **tracert** to determine the path to reach the remote server. It is helpful to look more closely at each network segment that is crossed.

Each hop in the **tracert** results displays the routes that the packets take when traveling to the final destination. The PC sends three ICMP echo request packets to the remote host. Each router in the path decrements the time to live (TTL) value by 1 before passing it onto the next system. When the decremented TTL value reaches 0, the router sends an ICMP Time Exceeded message back to the source with its IP address and the current time. When the final destination is reached, an ICMP echo reply is sent to the source host.

For example, the source host sends three ICMP echo request packets to the first hop (192.168.1.1) with the TTL value of 1. When the router 192.168.1.1 receives the echo request packets, it decrements the TTL value to 0. The router sends an ICMP Time Exceeded message back to the source. This process continues until the source hosts sends the last three ICMP echo request packets with TTL values of 8 (hop number 8 in the output below), which is the final destination. After the ICMP echo request packets arrive at the final destination, the router responds to the source with ICMP echo replies.

For hops 2 and 3, these IP addresses are private addresses. These routers are the typical setup for point-of-presence (POP) of ISP. The POP devices connect users to an ISP network.

A web-based whois tool is found at <http://whois.domaintools.com/>. It is used to determine the domains traveled from the source to destination.

- a. At the command-line prompt, trace the route to www.cisco.com. Save the **tracert** output in a text file. Alternatively, you can redirect the output to a text file by using **>** or **>>**.

```
C:\Users\User1> tracert www.cisco.com
```

or

```
C:\Users\User1> tracert www.cisco.com > tracert-cisco.txt
```

```
Tracing route to e144.dscb.akamaiedge.net [23.67.208.170]
over a maximum of 30 hops:
```

```
  1      1 ms    <1 ms    <1 ms    192.168.1.1
  2     14 ms     7 ms     7 ms    10.39.0.1
  3     10 ms     8 ms     7 ms    172.21.0.118
  4     11 ms    11 ms    11 ms    70.169.73.196
  5     10 ms     9 ms    11 ms    70.169.75.157
  6     60 ms    49 ms     *      68.1.2.109
  7     43 ms    39 ms    38 ms    Equinix-DFW2.netarch.akamai.com [206.223.118.102]
  8     33 ms    35 ms    33 ms    a23-67-208-170.deploy.akamaitechnologies.com
[23.67.208.170]
```

Trace complete.

- b. The web-based tool at <http://whois.domaintools.com/> can be used to determine the owners of both the resulting IP address and domain names shown in the tracert tools output. Now perform a **tracert** to one of RIR web sites from Part 1 and save the results.

Africa: **www.afrinic.net**

Australia: **www.apnic.net**

Europe: **www.ripe.net**

South America: **www.lacnic.net**

North America: **www.arin.net**

List the domains below from your tracert results using the web-based whois tool.

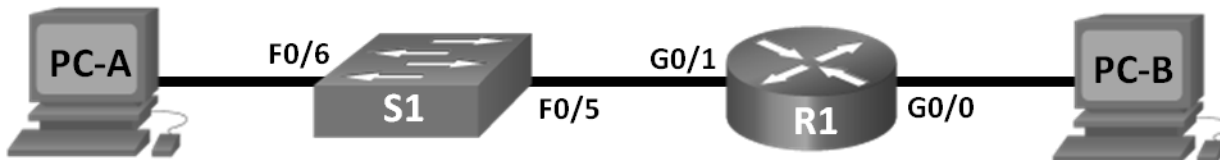
- c. Compare the lists of domains crossed to reach the final destinations.

Reflection

What can affect **tracert** results?

1.1.4.6 Lab – Configuring Basic Router Settings with IOS CLI

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

- Cable equipment to match the network topology.
- Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

- Assign static IPv4 information to the PC interfaces.
- Configure basic router settings.
- Verify network connectivity.
- Configure the router for SSH.

Part 3: Display Router Information

- Retrieve hardware and software information from the router.
- Interpret the output from the startup configuration.
- Interpret the output from the routing table.
- Verify the status of the interfaces.

Part 4: Configure IPv6 and Verify Connectivity

Background / Scenario

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and IPv4 interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and utilize IOS commands to retrieve information from the device to answer questions about the router. In Part 4, you will configure IPv6 on the router so that PC-B can acquire an IP address and then verify connectivity.

For review purposes, this lab provides the commands necessary for specific router configurations.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. Refer to Appendix A for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 ISRs are autosensing and an Ethernet straight-through cable can be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up the Topology and Initialize Devices

Step 1: **Cable the network as shown in the topology.**

- a. Attach the devices as shown in the topology diagram, and cable as necessary.
- b. Power on all the devices in the topology.

Step 2: **Initialize and reload the router and switch.**

Note: Appendix A details the steps to initialize and reload the devices.

Part 2: Configure Devices and Verify Connectivity

Step 1: **Configure the PC interfaces.**

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: **Configure the router.**

- a. Console into the router and enable privileged EXEC mode.

```
Router> enable
```

```
Router#
```

- b. Enter into global configuration mode.

```
Router# config terminal  
Router(config)#
```

- c. Assign a device name to the router.

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

- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

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

- e. Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Besides setting a minimum length, list other ways to strengthen passwords.

- f. Assign **cisco12345** as the privileged EXEC encrypted password.

```
R1(config)# enable secret cisco12345
```

- g. Assign **ciscoconpass** as the console password, establish a timeout, enable login, and add the **logging synchronous** command. The **logging synchronous** command synchronizes debug and Cisco IOS software output and prevents these messages from interrupting your keyboard input.

```
R1(config)# line con 0  
R1(config-line)# password ciscoconpass  
R1(config-line)# exec-timeout 5 0  
R1(config-line)# login  
R1(config-line)# logging synchronous  
R1(config-line)# exit  
R1(config)#
```

For the **exec-timeout** command, what do the **5** and **0** represent?

- h. Assign **ciscovtypass** as the vty password, establish a timeout, enable login, and add the **logging synchronous** command.

```
R1(config)# line vty 0 4  
R1(config-line)# password ciscovtypass  
R1(config-line)# exec-timeout 5 0  
R1(config-line)# login  
R1(config-line)# logging synchronous  
R1(config-line)# exit  
R1(config)#
```


- i. Encrypt the clear text passwords.

```
R1 (config)# service password-encryption
```

- j. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1 (config)# banner motd #Unauthorized access prohibited!#
```

- k. Configure an IP address and interface description. Activate both interfaces on the router.

```
R1 (config)# int g0/0
```

```
R1 (config-if)# description Connection to PC-B
```

```
R1 (config-if)# ip address 192.168.0.1 255.255.255.0
```

```
R1 (config-if)# no shutdown
```

```
R1 (config-if)# int g0/1
```

```
R1 (config-if)# description Connection to S1
```

```
R1 (config-if)# ip address 192.168.1.1 255.255.255.0
```

```
R1 (config-if)# no shutdown
```

```
R1 (config-if)# exit
```

```
R1 (config)# exit
```

```
R1#
```

- l. Set the clock on the router; for example:

```
R1# clock set 17:00:00 18 Feb 2013
```

- m. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
R1#
```

What would be the result of reloading the router prior to completing the **copy running-config startup-config** command?

Step 3: Verify network connectivity.

- a. Ping PC-B from a command prompt on PC-A.

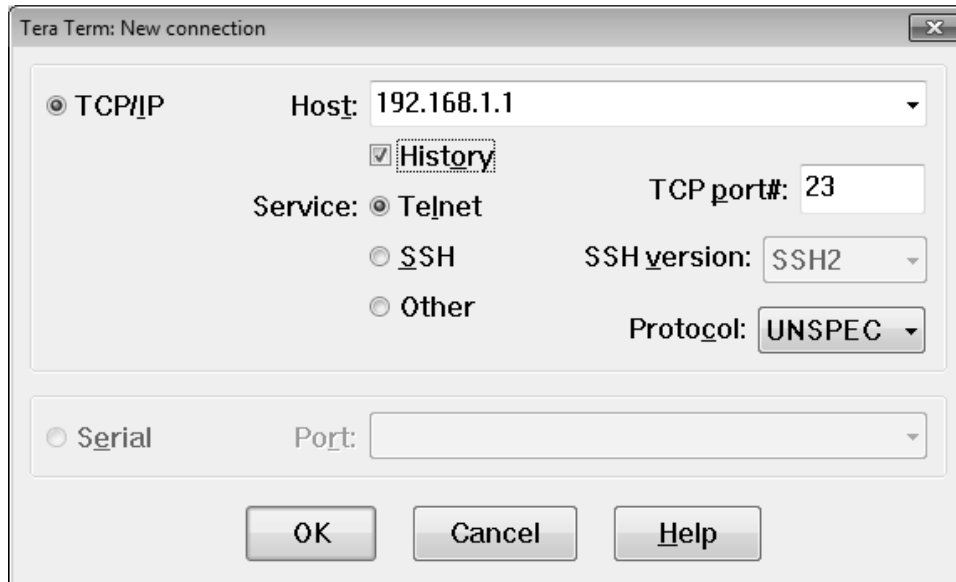
Note: It may be necessary to disable the PCs firewall.

Were the pings successful? _____

After completing this series of commands, what type of remote access could be used to access R1?

- b. Remotely access R1 from PC-A using the Tera Term Telnet client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **Telnet** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? ____

Why is the Telnet protocol considered to be a security risk?

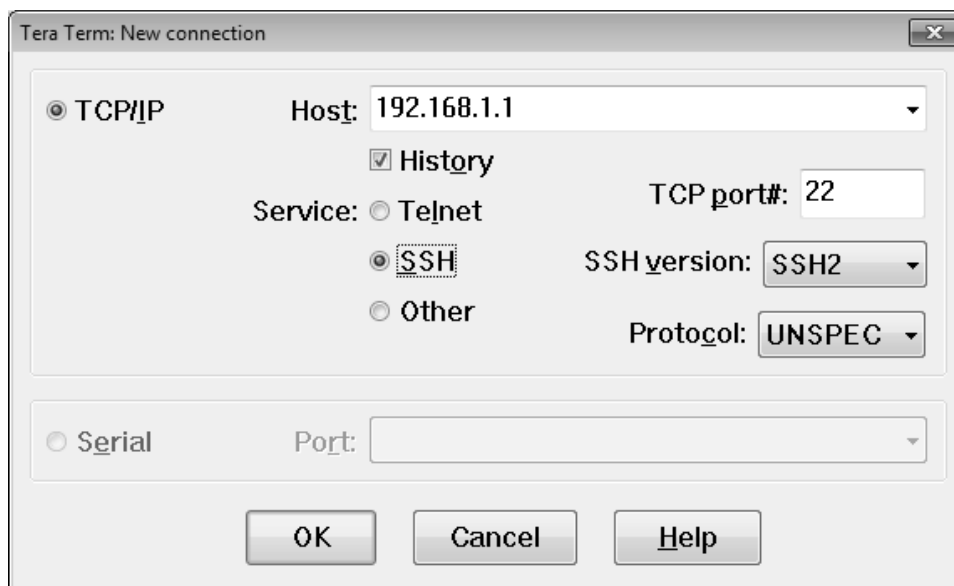
Step 4: Configure the router for SSH access.

- a. Enable SSH connections and create a user in the local database of the router.

```
R1# configure terminal
R1(config)# ip domain-name CCNA-lab.com
R1(config)# username admin privilege 15 secret adminpass1
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
R1(config)# crypto key generate rsa modulus 1024
R1(config)# exit
```

- b. Remotely access R1 from PC-A using the Tera Term SSH client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? _____

Part 3: Display Router Information

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

Step 1: Establish an SSH session to R1.

Using Tera Term on PC-B, open an SSH session to R1 at IP address 192.168.0.1 and log in as **admin** with the password **adminpass1**.

Step 2: Retrieve important hardware and software information.

- a. Use the **show version** command to answer questions about the router.

What is the name of the IOS image that the router is running?

How much non-volatile random-access memory (NVRAM) does the router have?

How much Flash memory does the router have?

- b. The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (|) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version | include register** to answer the following question.

What is the boot process for the router on the next reload?

Step 3: Display the startup configuration.

Use the **show startup-config** command on the router to answer the following questions.

How are passwords presented in the output?

Use the **show startup-config | begin vty** command.

What is the result of using this command?

Step 4: **Display the routing table on the router.**

Use the **show ip route** command on the router to answer the following questions.

What code is used in the routing table to indicate a directly connected network?

How many route entries are coded with a C code in the routing table? _____

Step 5: Display a summary list of the interfaces on the router.

Use the **show ip interface brief** command on the router to answer the following question.

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

Part 4: Configure IPv6 and Verify Connectivity

Step 1: Assign IPv6 addresses to R1 G0/0 and enable IPv6 routing.

Note: Assigning an IPv6 address in addition to an IPv4 address on an interface is known as dual stacking, because both the IPv4 and IPv6 protocol stacks are active. By enabling IPv6 unicast routing on R1, PC-B receives the R1 G0/0 IPv6 network prefix and can autoconfigure its IPv6 address and its default gateway.

- a. Assign an IPv6 global unicast address to interface G0/0, assign the link-local address in addition to the unicast address on the interface, and enable IPv6 routing.

```
R1# configure terminal
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ipv6 unicast-routing
R1(config)# exit
```

- b. Use the **show ipv6 int brief** command to verify IPv6 settings on R1.

If no IPv6 address is assigned to G0/1, why is it listed as [up/up]?

- c. Issue the **ipconfig** command on PC-B to examine the IPv6 configuration.

What is the IPv6 address assigned to PC-B?

What is the default gateway assigned to PC-B? _____

Issue a ping from PC-B to the R1 default gateway link local address. Was it successful? _____

Issue a ping from PC-B to the R1 IPv6 unicast address 2001:db8:acad:a::1. Was it successful? _____

Reflection

1. In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?

2. In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What **show** command could the technician use to troubleshoot this issue?

3. After configuring IPv6 on the R1 G0/0 PC-B LAN, if you were to ping from PC-A to the PC-B IPv6 address, would the ping succeed? Why or why not?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table 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 Cisco IOS commands to represent the interface.

Appendix A: Initializing and Reloading a Router and Switch

Step 1: Initialize and reload the router.

- a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- b. Type the **erase startup-config** command to remove the startup configuration from NVRAM.

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

- c. Issue the **reload** command to remove an old configuration from memory. When prompted to **Proceed with reload**, press Enter to confirm the reload. (Pressing any other key aborts the reload.)

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may be prompted to save the running configuration prior to reloading the router. Type **no** and press Enter.

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


- d. After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

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

- e. You are prompted to terminate autoinstall. Type **yes** and then press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Step 2: Initialize and reload the switch.

- a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable
```

```
Switch#
```

- b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
```

```
Directory of flash:/
```

```

 2  -rwx          1919   Mar 1 1993 00:06:33 +00:00  private-config.text
 3  -rwx          1632   Mar 1 1993 00:06:33 +00:00  config.text
 4  -rwx         13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
 5  -rwx       11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
 6  -rwx           616   Mar 1 1993 00:07:13 +00:00  vlan.dat
```

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

- c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
```

```
Delete filename [vlan.dat]?
```

- d. You are prompted to verify the filename. At this point, you can change the filename or just press Enter if you have entered the name correctly.

- e. You are prompted to confirm deleting this file. Press Enter to confirm deletion. (Pressing any other key aborts the deletion.)

```
Delete flash:/vlan.dat? [confirm]
```

```
Switch#
```

- f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to confirm removing the configuration file. Press Enter to confirm to erase this file. (Pressing any other key aborts the operation.)

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

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

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#
```

- g. Reload the switch to remove any old configuration information from memory. You are prompted to confirm reloading the switch. Press Enter to proceed with the reload. (Pressing any other key aborts the reload.)

```
Switch# reload
```

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

Note: You may be prompted to save the running configuration prior to reloading the switch. Type **no** and press Enter.

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

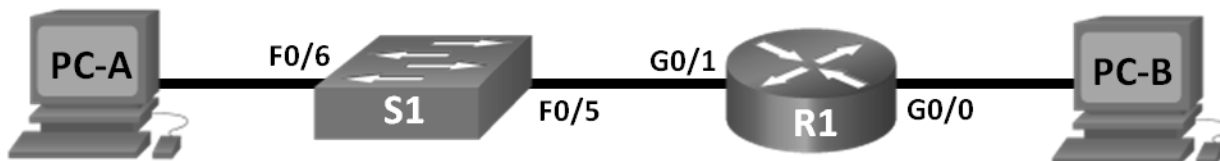
- h. After the switch reloads, you should be prompted to enter the initial configuration dialog. Type **no** and press Enter.

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

```
Switch>
```

1.1.4.7 Lab – Configuring Basic Router Settings with CCP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Configure Router to Allow CCP Access

Part 4: (Optional) Install and Set Up CCP on PC-A

Part 5: Configure R1 Settings Using CCP

Part 6: Use CCP Utilities

Background / Scenario

Cisco Configuration Professional (CCP) is a PC-based application that provides GUI-based device management for Integrated Services Routers (ISRs). It simplifies the configuration of routing, firewall, VPN, WAN, LAN, and other settings through menus and easy-to-use wizards.

In this lab, you will configure the router settings using the configuration from the previous lab in this chapter. Layer 3 connectivity must be established between the PC running CCP (PC-A) and R1 before CCP can establish a connection. In addition, HTTP access and authentication must be configured on R1.

You will download and install CCP on the PC and then use it to monitor R1's interface status, configure an interface, set the date and time, add a user to the local database, and edit vty settings. You will also use some of the utilities included in CCP.

Note: Router configurations performed using CCP generate IOS CLI commands. CCP can be very useful for configuring more complex router features because it does not require specific knowledge of the Cisco IOS command syntax.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: PC system requirements for CCP version 2.6 are:

- 2 GHz processor or faster
- 1 GB DRAM minimum; 2 GB recommended
- 400 MB of available hard disk space
- Internet Explorer 6.0 or above
- Screen resolution of 1024x768 or higher
- Java Runtime Environment (JRE) version 1.6.0_11 or later.
- Adobe Flash Player version 10.0 or later, with Debug set to No

Note: The Gigabit Ethernet interfaces on Cisco 1941 ISRs are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up the Topology and Initialize Devices

Step 1: **Cable the network as shown in the topology.**

- a. Attach the devices shown in the topology diagram, and cable as necessary.
- b. Power on all the devices in the topology.

Step 2: **Initialize and reload the router and switch.**

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will configure basic settings, such as the interface IP addresses (G0/1 only), secure device access, and passwords. Refer to the Topology and Addressing Table for device names and address information.

Step 1: Configure the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

Note: Do NOT configure interface G0/0 at this time. You will configure this interface using CCP later in the lab.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter into global configuration mode.
- c. Disable DNS lookup.
- d. Assign a device name to the router.
- e. Require that a minimum of 10 characters be used for all passwords.
- f. Assign **cisco12345** as the privileged EXEC encrypted password.
- g. Assign **ciscoconpass** as the console password and enable login.
- h. Assign **ciscovtypass** as the vty password and enable login,
- i. Configure **logging synchronous** on the console and vty lines.
- j. Encrypt the clear text passwords.
- k. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- l. Configure the IP addresses, an interface description, and activate G0/1 interface on the router.
- m. Save the running configuration to the startup configuration file.

Step 3: Verify network connectivity.

Verify that you can ping R1 G0/1 from PC-A.

Part 3: Configure the Router to Allow CCP Access

In Part 3, you will set up the router to allow CCP access by enabling HTTP and HTTPS server services. You will also enable HTTP authentication to use the local database.

Step 1: Enable HTTP and HTTPS server services on the router.

```
R1(config)# ip http server
R1(config)# ip http secure-server
```

Step 2: Enable HTTP authentication to use the local database on the router.

```
R1(config)# ip http authentication local
```

Step 3: Configure the router for CCP access.

Assign a user in the router local database for accessing CCP using username **admin** and password **admin-pass1**.

```
R1 (config)# username admin privilege 15 secret adminpass1
```

Part 4: (Optional) Install and Set Up CCP on PC-A**Step 1: Install CCP.**

Note: This step can be skipped if CCP is already installed on PC-A.

- a. Download CCP 2.6 from Cisco's website:

<http://software.cisco.com/download/release.html?mdfid=281795035&softwareid=282159854&release=2.6&rellifecycle=&relind=AVAILABLE&reltype=all>

- b. Choose the **cisco-config-pro-k9-pkg-2_6-en.zip** file.

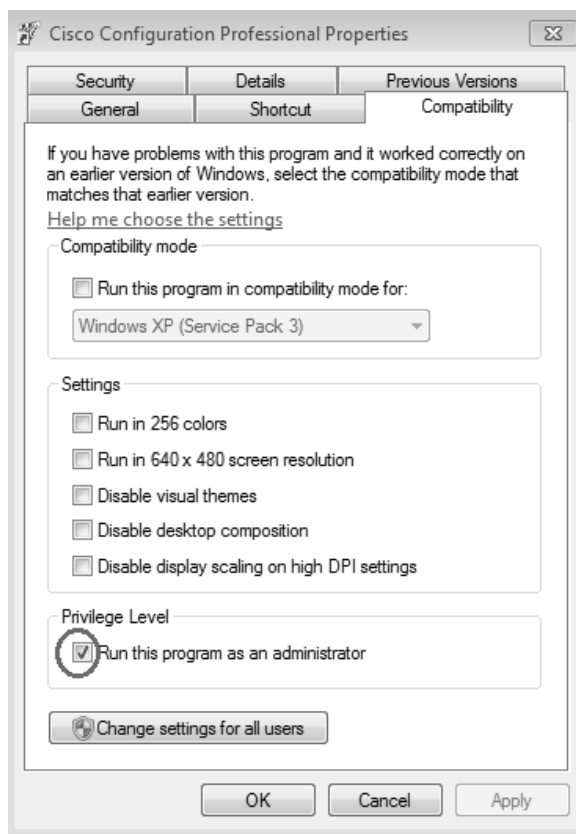
Note: Verify that you select the correct CCP file and not CCP Express. If there is a more current release of CCP, you may choose to download it; however, this lab is based on CCP 2.6.

- c. Agree to the terms and conditions, and download and save the file to the desired location.
- d. Open the zip file and run the CCP executable.
- e. Follow the on-screen instructions to install CCP 2.6 on your PC.

Step 2: Change settings to run as the administrator.

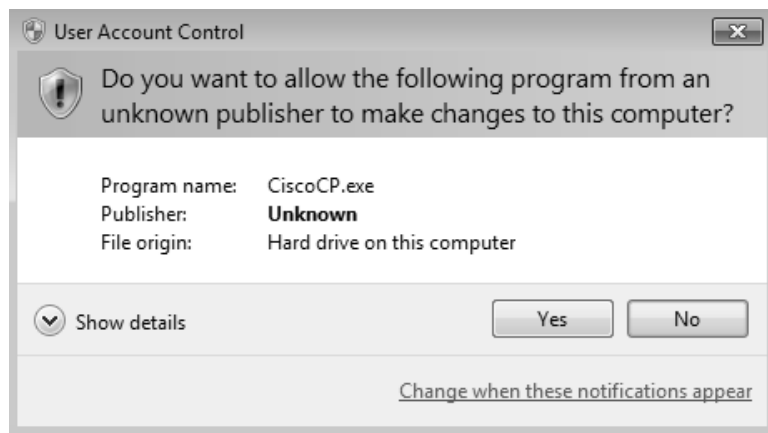
CCP may fail to launch correctly if it is not run as an administrator. You can change the launch settings so that it automatically runs in administrator mode.

- a. Right-click the **CCP** desktop icon (or click the **Start** button) and then right-click **Cisco Configuration Professional**. In the drop-down list, select **Properties**.
- b. In the Properties dialog box, select the **Compatibility** tab. In the Privilege Level section, click the **Run this program as an administrator** checkbox, and then click **OK**.

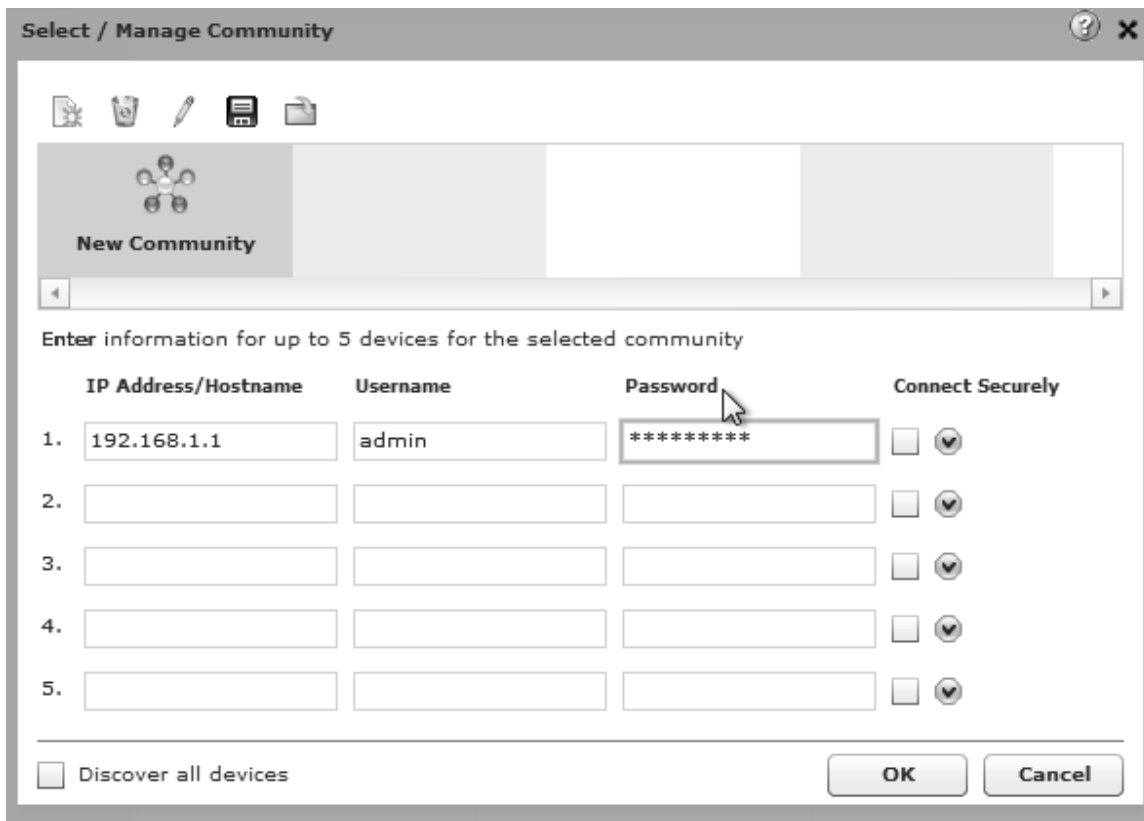


Step 3: Create or manage communities.

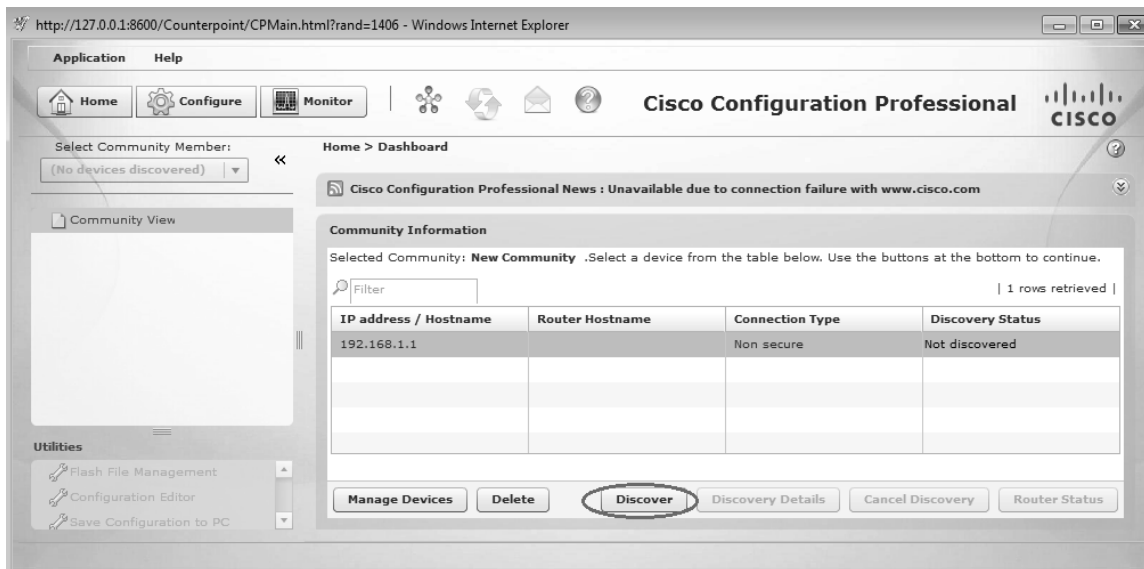
- a. On PC-A, start CCP. (Double-click the CCP desktop icon or click **Start > Cisco Configuration Professional**.)
- b. If you receive a security warning message prompting to allow the CiscoCP.exe program to make changes to the computer, click **Yes**.



- c. When CCP starts, the **Select / Mange Community** dialog box displays. Enter the IP address for R1 G0/1, and the username **admin** and password **adminpass1** that you added to the local database during the router configuration in Part 2. Click **OK**.



d. In the Community Information window, click **Discover**.



If you have configured the router correctly, the Discovery Status changes from **Not discovered** to **Discovered**, and R1 appears in the Router Hostname column.

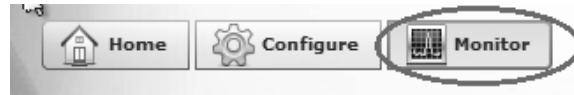
Note: If there is a problem with your configuration, you will see a "Discovery failed" status. Click **Discovery Details** to determine why the discovery process failed and then troubleshoot the problem.

Part 5: Configure R1 Settings Using CCP

In Part 5, you will use CCP to display information about R1, configure interface G0/0, set the date and time, add a user to the local database, and change your vty settings.

Step 1: View the status of the interfaces on R1.

- a. On the CCP toolbar, click **Monitor**.



- b. In the left navigation pane, click **Router > Overview** to display the Monitor Overview screen in the right content pane.

The screenshot shows the Cisco Configuration Professional (CCP) interface. The left navigation pane has 'Router > Overview' selected. The main content area displays the 'Monitor Overview' screen for the router. The interface status section shows a table of interfaces:

Interface	IP	Status	Bandwidth Usage	Description
Embedded-Service-Engine	no ip address	Down	0 %	
GigabitEthernet0/0	no ip address	Down	0 %	

- c. Use the up and down arrows to the right of the interface list to scroll through the list of interfaces for the router.

The close-up screenshot shows the 'Interface Status' section of the CCP interface. It displays the total number of interfaces up and down, and a table of interfaces with scroll arrows on the right side.

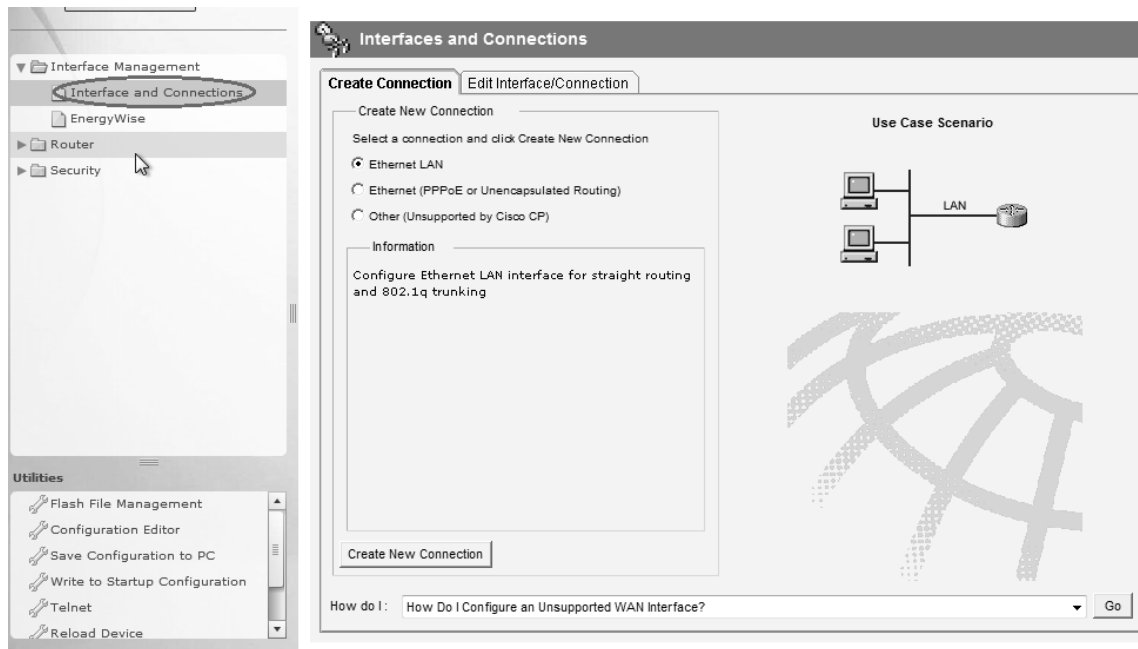
Interface	IP	Status	Bandwidth Usage	Description
GigabitEthernet0/0	no ip address	Down	0 %	
GigabitEthernet0/1	192.168.1.1	Up	0 %	

Step 2: Use the Ethernet LAN wizard to configure interface G0/0.

- a. On the CCP toolbar, click **Configure**.



- b. In the left navigation pane, click **Interface Management > Interface and Connections** to display the Interfaces and Connections screen in the right content pane.

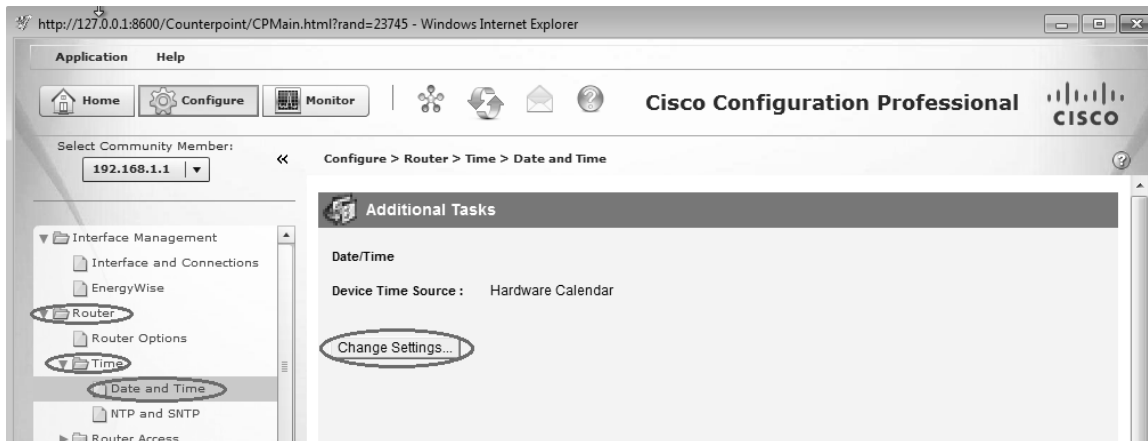


- c. Click **Create New Connection** to start the Ethernet LAN wizard.
- d. When you are prompted to enable AAA on the router, click **No**.
- e. Click **Next** to be guided through the Layer 3 Ethernet interface creation process.
- f. Keep the **Configure this interface for straight routing** radio button selected and click **Next**.
- g. Enter **192.168.0.1** in the IP address field and **255.255.255.0** in the Subnet mask field and click **Next**.
- h. Keep the **No** radio button selected on the DHCP server screen and click **Next**.
- i. Review the summary screen and click **Finish**.
- j. Click the **Save running config to device's startup config** check box, and then click **Deliver**. This adds the commands shown in the preview window to the running configuration, and then saves the running configuration to the startup configuration on the router.
- k. The Commands Delivery Status window displays. Click **OK** to close this window. You will be routed back to the Interfaces and Connections screen; G0/0 should have turned green and displayed as Up in the Status column.

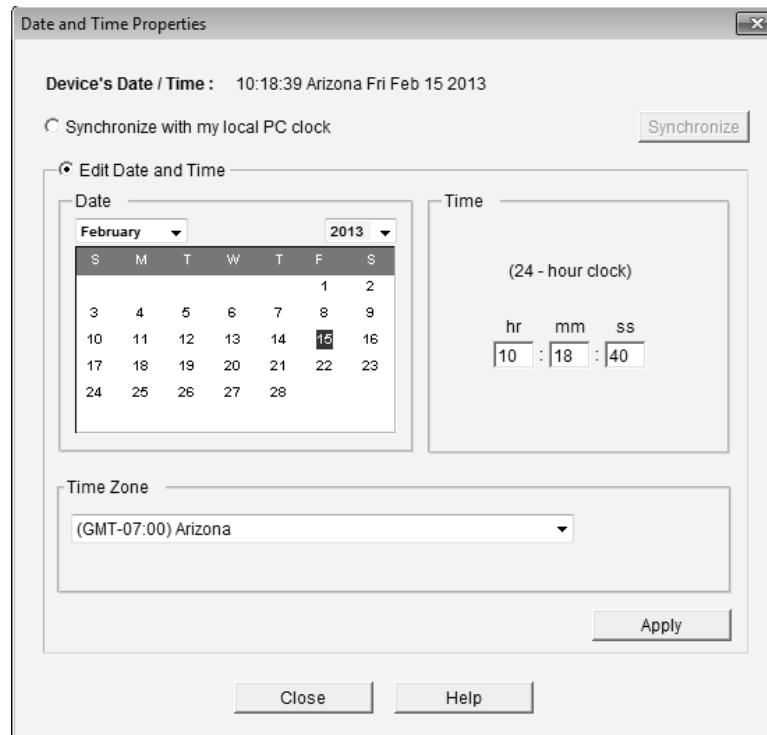
Interface	IP	Type	Slot	Status	Description
Embedded-Service-Engi	no IP address	Embedded-Service-Engin	0	Down	
GigabitEthernet0/0	192.168.0.1	GigabitEthernet	0	Up	
GigabitEthernet0/1	192.168.1.1	GigabitEthernet	0	Up	Connection to S1 F0/5
Serial0/0/0	no IP address	Serial	0	Down	
Serial0/0/1	no IP address	Serial	0	Down	

Step 3: Set the date and time on the router.

- In the left navigation pane, select **Router > Time > Date and Time** to display the Additional Tasks > Date/Time screen in the right content pane. Click **Change Settings...**



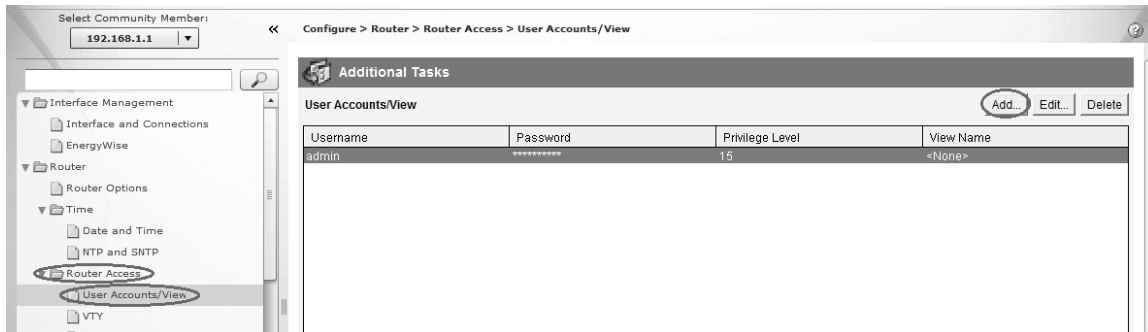
- In the Date and Time Properties window, edit the Date, Time, and Time Zone. Click **Apply**.



- In the Router's clock configured window, click **OK**. In the Date and Time Properties window, click **Close**.

Step 4: Add a new user account to the local database.

- a. In the left navigation pane, select **Router > Router Access > User Accounts/View** to display the Additional Tasks > User Accounts/View screen in the content pane on the right. Click the **Add...** button.



- b. Enter **ccpadmin** in the Username: field. Enter **ciscoccpass** in the New Password: and Confirm New Password: fields. Select **15** in the Privilege Level: drop-down list. Click **OK** to add this user to the local database.

Add an Account ✕

Enter the username and password

Username:

Password:

New Password:

Confirm New Password:

Encrypt password using MD5 hash algorithm

Privilege Level: ▼

Associate a View with the user

View Name: ▼

- c. In the Deliver Configuration to Device window, click the **Save running config to device's startup config** check box, and then click **Deliver**.

- d. Review the information in the Commands Delivery Status window, and click **OK**. The new user account should now appear in the content pane on the right.

Additional Tasks			
User Accounts/View			
Username	Password	Privilege Level	View Name
admin	*****	15	<None>
ccpadmin	*****	15	<None>

Step 5: Edit vty line settings.

- a. In the left navigation pane, select **Router Access > VTY** to display the Additional Tasks > VTYS screen in the content pane on the right. Click **Edit...**

Item Name	Item Value
Line Range	0-4
Input Protocols Allowed	ssh
Output Protocols Allowed	None
EXEC timeout	5
Inbound Access-class	None
Outbound Access-class	None

- b. In the Edit VTY Lines window, change the Time out: field to **15** minutes. Click the **Input Protocol > Telnet** check box. Review the other options available. Also select the **SSH** checkbox. Then click **OK**.

Line Range

Lines: --

Time out: minutes

Input Protocol

Telnet SSH all

Output Protocol

Telnet SSH all

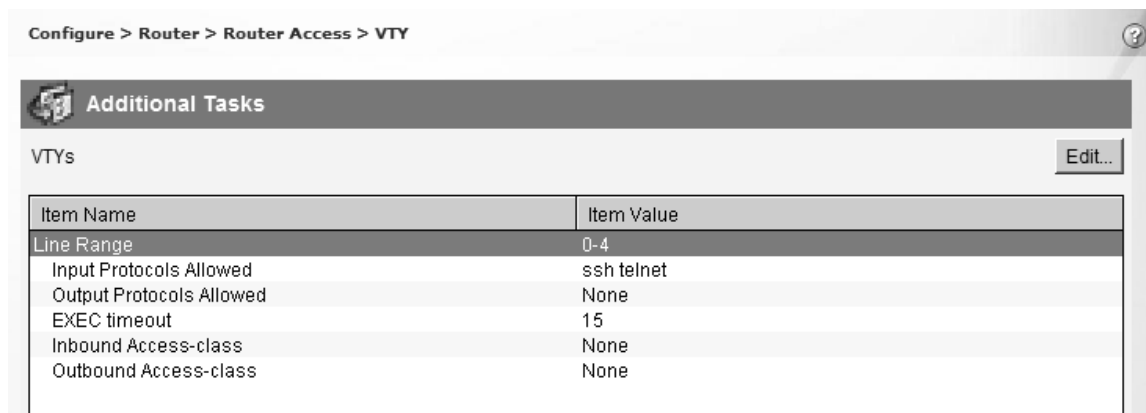
Access Rule

Inbound: ... ▾

Outbound: ... ▾

OK Cancel Help

- c. Review the commands that will be delivered to the running configuration on the Deliver Configuration to Device screen and click **Deliver**. In the Commands Delivery Status window, click **OK**. The content pane on the right should reflect the changes to the EXEC timeout value.

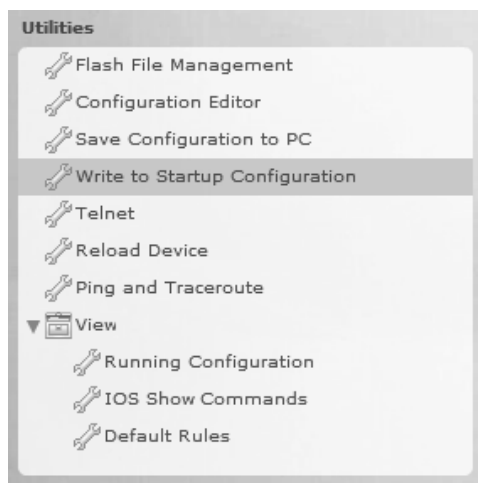


Part 6: Use CCP Utilities

In Part 6, you will use the Utilities pane to save the router's running configuration to the startup configuration. The Ping utility will be used to test network connectivity, and the View utility will be used to show the router's running configuration. Finally, you will close CCP.

Step 1: Save the router's running configuration to the startup configuration.

- a. At the bottom of the left navigation pane, locate the Utilities pane. Click **Write to Startup Configuration**.



- b. The content pane displays a confirmation screen. Click **Confirm**. An Information window displays, letting you know that the configuration was saved successfully. Click **OK**.

Step 2: Use the Ping utility to test connectivity to PC-B.

- a. In the Utilities pane, click **Ping and Traceroute** to display the Ping and Traceroute screen in the content pane. Enter **192.168.0.3** in the Destination*: field and then click **Ping**. Use the scrollbar to the right of the results box to view the results of your ping.

Utilities > Ping and Traceroute

Destination*: Advanced ▾
 (IP Address or Hostname)

Ping Traceroute

```

Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
  
```

Clear

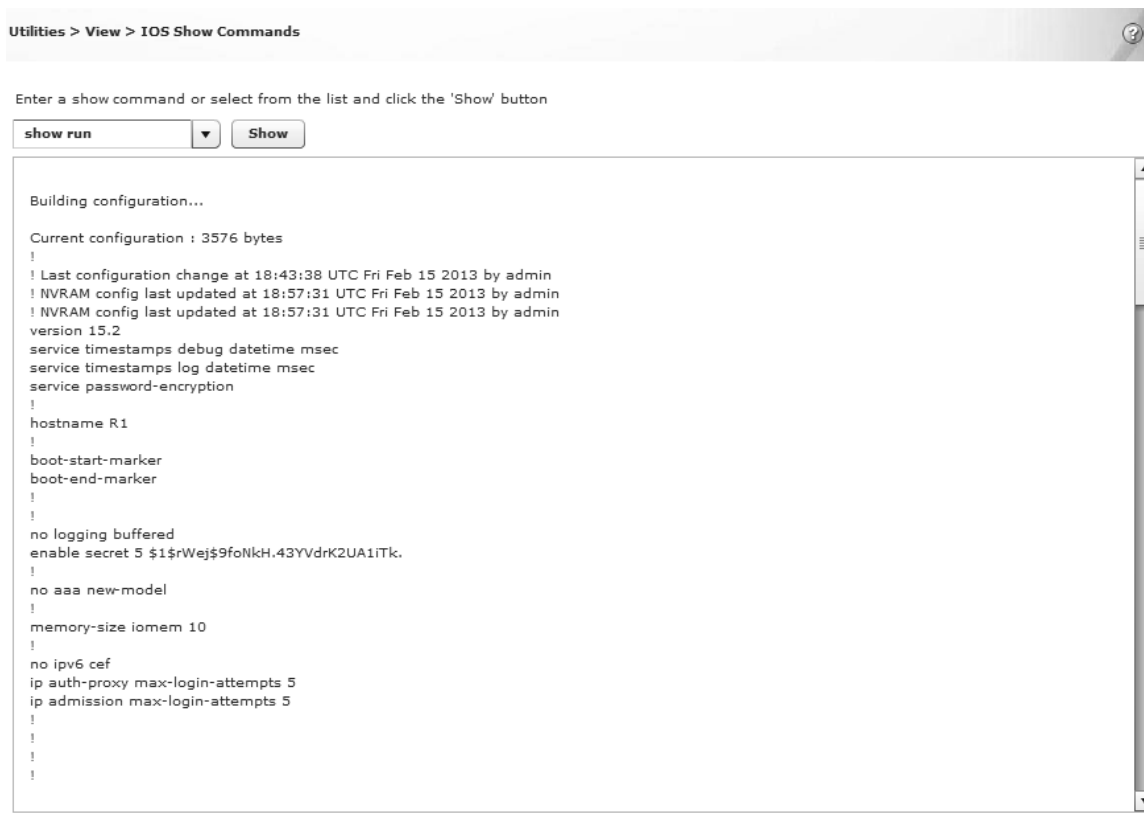
* - indicates mandatory field

Step 3: Use the View utility to show the running configuration for the router.

- In the Utilities pane, click **View > IOS Show Commands** to display the IOS Show Commands screen in the content pane.

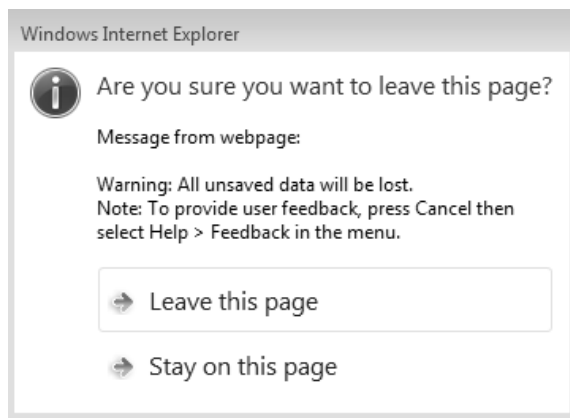


- Select **show run** from the drop-down list and click **Show**. The router's running configuration is displayed in the content pane.



Step 4: Close CCP.

Close the CCP window. When a Windows Internet Explorer confirmation window displays, click **Leave this page**.



Reflection

1. What transport protocol does CCP use to access the router and what commands are used to allow access?

2. What router command tells CCP to use the local database to authenticate?

3. What other **show** commands are available in the Utilities pane of CCP?

4. Why would you want to use CCP instead of the IOS CLI?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table 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 Cisco IOS commands to represent the interface.

1.4.1.1 Class Activity – We Really Could Use a Map!

Objectives

Describe the three types of routes that are populated in a routing table (to include: directly-connected, static, and dynamic).

Scenario

Use the Ashland and Richmond routing tables shown below. With the help of a classmate, draw a network topology using the information from the tables. To assist you with this activity, follow these guidelines:

- Start with the Ashland router - use its routing table to identify ports and IP addresses/networks.
- Add the Richmond router - use its routing table to identify ports and IP addresses/networks.
- Add any other intermediary and end devices, as specified by the tables.

In addition, record answers from your group to the reflection questions provided with this activity.

Be prepared to share your work with another group or the class.

Resources

```
Ashland> show ip route

Codes: L - local, 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, 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

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
D 192.168.3.0/24 [90/2170368] via 192.168.4.2, 01:53:50, GigabitEthernet0/0
192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.4.0/24 is directly connected, GigabitEthernet0/0
L 192.168.4.1/32 is directly connected, GigabitEthernet0/0
D 192.168.5.0/24 [90/3072] via 192.168.4.2, 01:59:14, GigabitEthernet0/0
S 192.168.6.0/24 [1/0] via 192.168.2.2

Ashland>
```

```

Richmond> show ip route

Codes: L - local, 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, 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

S 192.168.1.0/24 [1/0] via 192.168.3.1
D 192.168.2.0/24 [90/2170368] via 192.168.5.2, 01:55:09, GigabitEthernet0/1
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.3.0/24 is directly connected, Serial0/0/0
L 192.168.3.2/32 is directly connected, Serial0/0/0
D 192.168.4.0/24 [90/3072] via 192.168.5.2, 01:55:09, GigabitEthernet0/1
192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.5.0/24 is directly connected, GigabitEthernet0/1
L 192.168.5.1/32 is directly connected, GigabitEthernet0/1
192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.6.0/24 is directly connected, GigabitEthernet0/0
L 192.168.6.1/32 is directly connected, GigabitEthernet0/0

Richmond>

```

Reflection

1. How many directly connected routes are listed on the Ashland router? What letter represents a direct connection to a network on a routing table?

2. Find the route to the 192.168.6.0/24 network. What kind of route is this? Was it dynamically discovered by the Ashland router or manually configured by a network administrator on the Ashland router?

3. If you were configuring a default (static route) to any network from the Ashland router and wanted to send all data to 192.168.2.2 (the next hop) for routing purposes, how would you write it?

4. If you were configuring a default (static route) to any network from the Ashland router and wanted to send all data through your exit interface, how would you write it?

5. When would you choose to use static routing, instead of letting dynamic routing take care of the routing paths for you?

6. What is the significance of the L on the left side of the routing table?
