Stand-Alone Labs

Lab 1: Connecting to a Router

Objective: Become familiar with the Cisco Router.
Lab Equipment: Router 1 from the eRouters menu

Background Reading: Lab Primer Lesson 1: Introduction to the Cisco Router Command-Line Interface

1. When the lab has finished loading, the Router 1 window will open, and the text “Press Enter to Start” will appear.

2. Click inside the Router 1 window, and press the ENTER key to get started. You are now connected to Router 1 and are at the user mode prompt. The prompt is broken into two parts: the host name and the mode. Router is Router 1’s host name, and the > prompt indicates user mode.

Press Enter to get Started
Router>

3. Next, type the enable command to get to the privileged mode prompt.

Router>enable
Router#

4. To return to user mode, simply type disable. From user mode, type logout or exit to exit the router.

Router#disable
Router>exit
Router con0 is now available
Press RETURN to get started

Lab 2: Introduction to the Basic User Interface

Objective: Become familiar with the command-line interface (CLI), user and privileged mode, and basic help and show commands.
Lab Equipment: Router 1 from the eRouters menu

Background Reading: Lab Primer Lesson 1: Introduction to the Cisco Router Command-Line Interface

1. Press the ENTER key to get to the router prompt.

Router>

2. The interface is now in user mode. At the user mode prompt, type the command that is used to view all the commands available in user mode.

Router>? 

3. Type the command used to enter privileged mode.

Router>enable
Router#

4. Type the command that will allow you to view the available commands in privileged mode.

Router#?
5. Type the command that will allow you to see all of the show commands.
   \texttt{Router#show ?}

6. Type the command that will allow you to see the active, or running, configuration.
   \texttt{Router#show running-config}

7. At the MORE prompt, press the SPACEBAR key to view the next page of information.
   \texttt{SPACEBAR}

8. Finally, type one of the commands that will log you out of the router.
   \texttt{Router#exit}
   OR
   \texttt{Router#disable}

**Lab 3: Introduction to the Basic Show Commands**

**Objective:** Become familiar with the basic show commands.

**Lab Equipment:** Router 1 from the eRouters menu

**Background Reading:** Lab Primer Lesson 2: Basic Commands

1. Press ENTER to get to the router prompt.
   \texttt{Router>}

2. Enter privileged mode.
   \texttt{Router>?enable}
   \texttt{Router#}

3. Display the active configuration in memory. The currently active configuration script running on the router is referred to as the \texttt{running-config} in the router’s CLI. Note that privileged mode is required in order to access the running configuration. The running configuration script is not automatically saved on a Cisco router and will be lost in the event of power failure. The running configuration must be manually saved with the \texttt{copy} command (discussed in a later lab).
   \texttt{Router#show running-config}

4. Display flash memory. Flash memory is a special kind of memory that contains the operating system image file(s) on the router. Unlike regular router memory, flash memory continues to maintain the file image even after power is lost.
   \texttt{Router#show flash}

5. By default, the router’s CLI maintains in memory the last 10 commands entered. The show history command displays simultaneously all of the past commands still in router memory.
   \texttt{Router#show history}

6. Press the CTRL+P key combination to retrieve the previous command you typed.

7. Press the DOWN ARROW key or press the CTRL+N key combination to see the next command in the history buffer.

8. Use the show protocols command to view the status of the current Layer 3 routed protocols running on your router.
   \texttt{Router#show protocols}
9. The `show version` command is used to obtain critical information, such as router platform type, operating system revision, operating system last boot time and file location, amount of memory, number of interfaces, and configuration register.

   Router#show version

10. Use the `show clock` command to view the router's clock.

   Router#show clock

11. The `show hosts` command displays a cached list of hosts and all of their interfaces’ IP addresses.

   Router#show hosts

12. Use the `show users` command to view a list of all users who are connected to the router.

   Router#show users

13. The `show interfaces` command displays detailed information about each interface.

   Router#show interfaces

14. The `show protocols` command displays the global and interface-specific status of any Layer 3 protocols.

   Router#show protocols

Lab 4: CDP

Objective: Learn how the Cisco Discovery Protocol (CDP) functions and what is required for Cisco devices to be discovered.

Lab Equipment: Router 1 and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 5: CDP

1. On Router 1, enter global configuration mode.

   Router>enable
   Router#conf t
   Router(config)#

2. Change the host name to R1.

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

3. Connect to Router 4, and change the host name to R4.

   Router>enable
   Router#conf t
   Router(config)#hostname R4
   R4(config)#

4. Return to R1, and enable the serial 0 interface. By default, all interfaces are shut down (disabled).

   R1(config)#interface serial 0
   R1(config-if)#no shutdown

5. Now, enable the serial 0 interface on R4.

   R4(config)#interface serial 0
   R4(config-if)#no shutdown
6. Enable the Ethernet 0 interface on R1.
   ```
   R1(config)#interface Ethernet 0
   R1(config-if)#no shutdown
   ```

7. CDP allows devices to share basic configuration information and will operate without any protocol-specific information being configured. CDP, which is enabled by default on all interfaces, is a Data Link protocol that operates at Layer 2 of the OSI model. This is important to understand because CDP is not routable; it can only travel to directly connected devices.
   On R1, type the command that displays the status of all interfaces that are running CDP.
   ```
   R1(config-if)#exit
   R1(config)#exit
   R1#show cdp interface
   ```
   The sample output below shows that both interfaces are up and sending CDP packets:
   ```
   Serial0 is up, line protocol is up
   Encapsulation HDLC
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds
   <output omitted>
   ```

8. Now that the router has interfaces that are broadcasting and receiving CDP updates, you can use CDP to find out about directly connected neighbors.

9. On R1, type the command that provides information about directly connected neighbors.
   ```
   R1#show cdp neighbors
   ```
   Below is some sample output:
   ```
   Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
   S - Switch, H - Host, I - IGMP, r - Repeater
   
   Device ID     Local Interface      Holdtime      Capability      Platform      Port ID
   R4               Serial 0                 148             R                  1700           Serial 0
   ```

9. The first device on the directly connected neighbors list for R1 is R4 via the serial 0 link. R1 is receiving CDP updates from R4; the updates tell R1 to retain the information for a specified amount of time. At the time this command was entered, there were 148 seconds left in the hold time for R1’s update. If that time expires before another update is received, R1’s information will be removed from the table. R4 is a 1000 series router, as indicated in the Platform column. The final column, Port ID, indicates the port on the other device from which the updates are being sent.

9. On R1, type the command that provides more detailed information about directly connected neighbors.
   ```
   R1#show cdp neighbor detail
   ```
   Below is some sample output:
   ```
   Device ID: R4
   Entry address(es):
   ```
Platform: cisco 2501, Capabilities: Router
Interface: Serial0, Port ID (outgoing port): Serial0
Holdtime : 162 sec

Version:
Cisco Internetwork Operating System Software
Software, Version 12.0(16), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 02-Mar-01 17:34 by dchih

The `show cdp neighbor detail` command shows devices one at a time. It is used to display Network layer address information. The command also displays IOS version information. Notice that the devices are listed in order. If you wanted to find out information about a device further down the list, you would need to scroll down using the SPACEBAR.

10. On R1, type the command to provide information about the specific device R4.
   `R1#show cdp entry R4`
   
   Below is some sample output:
   
   Device ID: R4
   Entry address(es):
   Platform: cisco 1000, Capabilities: Router
   Interface: Serial0, Port ID (outgoing port): Serial0
   Holdtime : 148 sec

   Version:
   Cisco Internetwork Operating System Software
   Software, Version 12.0(16), RELEASE SOFTWARE (fc2)
   Copyright (c) 1986-2001 by cisco Systems, Inc.
   Compiled Fri 02-Mar-01 17:34 by dchih

   R1#

   The `show cdp entry` command provides the same information as the `show cdp neighbor detail` command, but it allows a single device to be specified. Also, notice that this is one of the only case-sensitive commands that exist.

11. On R1, type the command that shows how often CDP updates are being sent and how long a recipient should retain the update.
   `R1#show cdp`
   
   Below is some sample output:
   
   Global CDP information:
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisements is enabled
12. On R1, adjust the number of seconds between CDP updates to 45.
   R1#conf t
   R1(config)#cdp timer 45
   Besides the update interval, the holdtime value may also be adjusted. This value tells the
   recipient of the update how long to retain the CDP information in the update. It is also a
   global parameter.

13. On R1, type the command to adjust the holddown timer to 60 seconds.
   R1#conf t
   R1(config)#cdp holdtime 60

14. On R1, type the command that will allow you to verify that the changes have been made.
   R1#show cdp
   Below is some sample output:
   R1#sh cdp
   Global CDP information:
   Sending CDP packets every 45 seconds
   Sending a holdtime value of 60 seconds
   Sending CDPv2 advertisements is enabled
   R1#

15. If there are no other directly connected Cisco devices on the network, or if you want to
    conserve bandwidth, you can disable CDP.
    On R1, type the command that disables CDP for the entire router.
    R1#conf t
    R1(config)#no cdp run
    At times, you may wish to disable CDP for a specific interface for security reasons, or
    simply because the interface has very low bandwidth.

16. On R1, type the command that turns CDP back on for the entire router.
    R1#conf t
    R1(config)#cdp run

17. On R1, disable CDP for only the specific interface Ethernet 0.
    R1(config)#interface Ethernet 0
    R1(config-if)#no cdp enable

18. On R1, verify that Ethernet 0 is no longer sending CDP updates. (If the Ethernet 0
    interface does not show up as an entry in the output, you can conclude that it is not
    sending CDP updates.)
    R1#show cdp interface
    Below is sample output from the command:
    R1#show cdp interface
    Serial0 is up, line protocol is up
    Encapsulation HDLC
    Sending CDP packets every 45 seconds
    Holdtime is 60 seconds
Lab 5: Extended Basics

Objective: View and configure some basic areas of the router.

Lab Equipment: Router 1 from the eRouters menu

Background Reading: Lab Primer Lesson 1: Introduction to the Cisco Router Command-Line Interface

1. Press ENTER to get to the router prompt.
   Router>

2. Enter the command that is used to view all the commands available in user mode.
   Router>? 

3. Enter privileged mode. This is the mode that gives you complete control of the router.
   Router>enable
   Router# 

4. View the commands available in privileged mode.
   Router#?

5. Enter the command that provides access to global configuration mode.
   Router#config terminal
   Router(config)#

6. The router’s host name is used for local identification. When you log on to the router, you see its host name in front of the prompt (either the > or the # prompt). The host name can be used to identify the location or function of the router. Set the router’s host name to Krang.
   Router(config)#hostname Krang
   Krang(config)#

7. The enable password controls access to privileged mode. This is a very important password because when it is configured, only those who know the password can make configuration changes in privileged mode. Set the enable password to boson.
   Krang(config)#enable secret boson

8. Test the password. Exit the router, and try to enter privileged mode. Notice that you have to provide the password in order to enter privileged mode. Now, type the conf term command and proceed with the instructions in the next step.
   Krang(config)#exit
   Krang#exit
   Krang>enable
   Password:
   Krang#config terminal
   Krang(config)#

9. The only problem with the enable password is that it appears in plain text in the router’s configuration file. If you need to obtain assistance in troubleshooting a problem, you may inadvertently compromise the security of your system by revealing the password. Set the enable secret password to cisco.
   Krang(config)#enable secret cisco
10. Now, test this password by logging out of the router and then typing `enable` at the user mode prompt. The enable secret password overrides the enable password. If you have set both passwords, you must use the enable secret password to enter privileged mode. The enable password is still configured but is now deactivated.

   ```
   Krang(config)#exit
   Krang#exit
   Krang>enable
   Password:
   Krang#
   ```

### Lab 6: Banner MOTD

**Objective:** Configure a banner Message of the Day (MOTD). The MOTD is displayed when a user logs on to the router. The banner can also be used to display information about the router itself or to display a security message.

**Lab Equipment:** Router 1 from the eRouters menu

1. Connect to Router 1, and enter privileged mode.
   ```
   Router>enable
   Router#
   ```

2. Enter configuration mode.
   ```
   Router#config t
   Router(config)#
   ```

3. Type the command to enter the banner message, and press ENTER. After you type `banner motd`, enter a delimiting character so the router knows when you are finished entering text for the banner. The easiest one to use is the letter Z.
   ```
   Router(config)#banner motd z
   Enter the text followed by the 'z' to finish
   ```

4. Now, all text that you type, until you type the letter Z, will be stored as the banner. Type the text “You do not have permission to be here. This router eats hackers for lunch! z”, and press ENTER. This will set the banner.

   ```
   You do not have permission to be here. This router eats hackers for lunch! z
   ```

5. To view the banner, exit configuration mode, and then exit the router. Press ENTER to display the banner.

   ```
   Router(config)#exit
   Router#exit
   Router>exit
   Press RETURN to get started.
   You do not have permission to be here. This router eats hackers for lunch!
   ```
Lab 7: Copy Command

Objective: Become familiar with the router configuration and the copy commands available in the Cisco IOS.

Lab Equipment: Router 1 from the eRouters menu

Background Reading: Lab Primer Lesson 1: Introduction to the Cisco Router Command-Line Interface

1. Connect to Router 1, and enter privileged mode.
   Router>enable
   Router#

2. Display the active configuration in memory. The currently active configuration script running on the router is referred to as the running-config in the router’s CLI. Note that privileged mode is required to display the active configuration. The running configuration script is not automatically saved on a Cisco router and will be lost in the event of power failure. The running configuration must be manually saved with the copy command.
   Router#show running-config

3. Try to display the configuration stored in NVRAM (known as the startup-config). You have not saved the configuration, so there is not one to show.
   Router#show startup-config

4. Copy the current active configuration to NVRAM. The current active configuration is in RAM; it should be saved so that the router will still boot up with the configuration in the event of a power outage.
   Router#copy running-config startup-config

5. Now, show the configuration stored in NVRAM.
   Router#show startup-config

6. If you decide that you would like to configure the router from scratch, you can erase the startup configuration and reload the router. This will enable you to completely delete all configurations on the router so that you can start from scratch. Type the command that will delete the configuration file in NVRAM. When prompted, confirm that you do want to erase the NVRAM file system by pressing the Y key.
   Router#erase startup-config

7. Now, type the command to reload the router, and press the Y key when prompted to confirm the reload.
   Router#reload

8. After the router reboots, look at the startup configuration file again. Because you did not save it before you reloaded, there is nothing there.
   Router>enable
   Router#show startup-config

9. Now, change the host name of the router to Boson.
   Router#config terminal
   Router(config)#hostname Boson
   Boson(config)#exit
   Boson#
10. Save your router configuration, and reload the router. Again, press the Y key when prompted to confirm the reload.
   Boson#copy run start
   Boson#reload

11. After the router reloads, the host name of Boson appears in the prompt. If you run the show startup-config command, nothing appears.
   Boson>enable
   Boson#show startup-config

Lab 8: Introduction to Interface Configuration

Objective: Learn to enable interfaces on a router, and learn what is required for an interface to be up.

Lab Equipment: Router 1 and Router 2 from the eRouters menu

Background Reading: Lab Primer Lesson 4: Router Interfaces

1. On Router 1, enter global configuration mode.
   Router>enable
   Router#conf t
   Router(config)#
   Router(config)#hostname Router1

2. Type the command to enter interface configuration mode for Ethernet 0.
   Router1(config)#interface Ethernet 0
   Router1(config-if)#

3. Display all the commands available in interface configuration mode by typing ?.
   Router1(config-if)#?

4. The shutdown command shuts down the selected interface. You can often achieve the opposite of a command by typing no in front of it. Execute the command on Router 1 Ethernet 0 to enable the interface.
   Router1(config-if)#no shutdown

5. Add a description for this interface.
   Router1(config-if)#description Ethernet interface on Router 1

6. To view the interface description, exit back to privileged mode, and run the show interface command. You should see the description under Ethernet 0.
   Router1(config-if)#end
   Router1#show interface

7. Connect to Router 2, and assign it a host name of Router2.
   Router#conf t
   Router(config)#hostname Router2

8. Now, access the Ethernet 0 interface, and enable the interface.
   Router2(config)#interface Ethernet 0
   Router2(config-if)#no shutdown
9. Now that the interfaces on both sides of the Ethernet connection are enabled, they should be able to see one another through CDP. Use the `show cdp neighbor` command on Router2 to view all directly connected Cisco routers.

   ```
   Router2(config-if)#end
   Router2#show cdp neighbor
   ```

### Lab 9: Introduction to IP

**Objective:** Configure Routers 1, 2, and 4 with Internet Protocol (IP) addresses, and ping between them to test connectivity.

**Lab Equipment:** Router 1, Router 2, and Router 4 from the eRouters menu

**Background Reading:** Lab Primer Lesson 3: Basic IP Configuration and Verification, and the “Ping” topic from Lab Primer Lesson 2: Basic Commands

1. Connect to Router 1, and assign it a host name of `Router1`.
   ```
   Router>enable
   Router#conf t
   Router(config)#hostname Router1
   Router1(config)#
   ```
2. Enter interface configuration mode for the Ethernet 0 interface.
   ```
   Router1(config)#interface ethernet 0
   Router1(config-if)#
   ```
3. Type the command that will set the IP address on the Ethernet 0 interface to 10.1.1.1 255.255.255.0, and enable the interface.
   ```
   Router1(config-if)#ip address 10.1.1.1 255.255.255.0
   Router1(config-if)#no shutdown
   ```
4. Set the IP address on the serial 0 interface of Router1 to 172.16.10.1 255.255.255.0, and enable the interface.
Router1(config)#interface serial 0
Router1(config-if)#ip address 172.16.10.1 255.255.255.0
Router1(config-if)#no shut

5. Connect to Router 2, and assign it a host name of Router2.
   Router>enable
   Router#conf t
   Router(config)#hostname Router2
   Router2(config)#

6. Set the IP address for the Ethernet 0 interface to 10.1.1.2 255.255.255.0, and enable the interface.
   Router2(config)#interface Ethernet 0
   Router2(config-if)#ip address 10.1.1.2 255.255.255.0
   Router2(config-if)#no shutdown

7. Connect to Router 4, and assign it a host name of Router4.
   Router>enable
   Router#conf t
   Router(config)#hostname Router4

8. Configure an IP address of 172.16.10.2 255.255.255.0 on the serial 0 interface, and enable the interface.
   Router4(config)#interface serial 0
   Router4(config-if)#ip address 172.16.10.2 255.255.255.0
   Router4(config-if)#no shutdown

9. From Router1, try to ping Router2’s Ethernet interface.
   Router1#ping 10.1.1.2

10. Try to ping Router4’s serial 0 interface.
    Router1#ping 172.16.10.2

11. Verify that the lines and protocols are up for all of Router1’s interfaces.
    Router1#show ip interface brief

12. Display Router1’s running configuration, and verify that the IP addresses appear.
    Router1#show running-config

13. Display detailed IP information about each interface on Router1.
    Router1#show ip interface

Lab 10: ARP

Objective: Configure Routers 1 and 2 with IP addresses, and ping between them to test connectivity. Then view the entries stored in the Address Resolution Protocol (ARP) table.

Lab Equipment: Router 1 and Router 2 from the eRouters menu

Background Reading: Lab Primer Lesson 6: ARP

1. Connect to Router 1, and type the command to view the ARP table.
   Router>enable
   Router#show arp
2. Assign an IP address of 10.1.1.1 255.255.255.0 to the Ethernet 0 interface of Router 1.
   
   Router#conf terminal
   Router(config)#interface Ethernet 0
   Router(config-if)#ip address 10.1.1.1 255.255.255.0
   Router(config-if)# no shutdown
   Router(config-if)#exit

3. View the ARP table again.
   
   Router(config)#exit
   Router#show arp

4. Now, connect to Router 2, and configure its Ethernet 0 interface with an IP address of 10.1.1.2 /24.
   
   Router#conf terminal
   Router(config)#interface Ethernet 0
   Router(config-if)#ip address 10.1.1.2 255.255.255.0
   Router(config-if)# no shutdown
   Router(config-if)#exit

5. A connection should now exist between the Router 1 and Router 2 Ethernet interfaces. To ensure that the connection is functional, ping the IP address of Router 1’s Ethernet 0 IP address from Router 2.
   
   Router(config)#exit
   Router#ping 10.1.1.1

6. View the ARP table on Router 2, and notice the entry.
   
   Router#show arp

7. Now, clear the ARP table.
   
   Router#clear arp

8. View the ARP table one last time, and notice what entries are there.
   
   Router#show arp

Lab 11: Creating a Host Table

Objective: Become familiar with the router’s host table. Host tables can be used to set names for commonly used IP addresses, which helps with troubleshooting.

Lab Equipment: Router 1 from the eRouters menu

1. Connect to Router 1, and set the host name to California.
   
   Router>enable
   Router#config t
   Router(config)#hostname California
   California(config)#

2. Configure an IP address of 195.42.36.10 255.255.255.240 on the Ethernet 0 interface; be sure to enable the interface.
   
   California(config)#interface ethernet 0
Stand-Alone Labs

3. Connect to Router 2, and set the host name to Tampa.
   
   Router>enable
   Router#config t
   Router(config)#hostname Tampa
   Tampa(config)#

4. Configure an IP address of 195.42.36.12 255.255.255.240 on the Ethernet 0 interface; be sure to enable the interface.
   
   Tampa(config)#interface ethernet 0
   Tampa(config-if)#ip address 195.42.36.12 255.255.255.240
   Tampa(config-if)#no shutdown
   Tampa(config-if)#exit

5. Exit interface mode. You do not want to have to type California's Ethernet 0 IP address every time you try to ping it from Tampa, so set a host table entry for California using the IP address 195.42.36.10.
   
   Tampa(config)#ip host California 195.42.36.10
   Tampa(config)#exit

6. Now you should be able to ping California’s Ethernet 0 IP address from Tampa just by typing ping California.
   
   Tampa#ping California

7. Use the show hosts command to verify that the entry is stored in the router’s host table.
   
   Tampa#show hosts

Lab 12: Static Routes

Objective: Configure Routers 1, 2, and 4 with IP addresses, and then add static routes for all routers.

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Goals:

- Set the host name, and bring up the interfaces.
- Ping the directly connected interfaces.
- Configure static routes for the topology.
- Verify that you can ping all routers.

1. Configure Routers 1, 2, and 4 to the specifications outlined in the table and diagram below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 2</th>
<th>Router 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router2</td>
<td>Router4</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>10.1.1.1 /24</td>
<td>10.1.1.2 /24</td>
<td>12.5.10.1/24</td>
</tr>
<tr>
<td>Serial 0</td>
<td>12.5.10.1/24</td>
<td>12.5.10.2 /24</td>
<td></td>
</tr>
</tbody>
</table>
2. On each router, verify that you can ping the directly connected neighbors.
   Router1#ping 10.1.1.2
   Router1#ping 12.5.10.2
   Router2#ping 10.1.1.1
   Router4#ping 12.5.10.1

3. Now you need to establish static routes on each router to any location that is not directly connected. Router1 is directly connected to both Router2 and Router4, so it will not need any static routes.

   On Router4, enter global configuration mode, and think about what the static route command should be. You know that you currently cannot reach Router2 because it is not directly connected. Off of Router4’s serial interface is network 12.5.10.0, which is connected to Router1. Router1 is also connected to network 10.1.1.0, which you would also like to access. In this case, you will need a static route for network 10.1.1.0. On Router4, what command should you use to establish a static route to network 10.1.1.0?

   Router4#conf term
   Router4(config)#ip route 10.1.1.0 255.255.255.0 12.5.10.1

   You established a route to network 10.1.1.0. Now, whenever a packet of information leaves Router4 destined for network 10.1.1.0, it will first be sent to IP address 12.5.10.1 on Router1.

4. Now, try to ping Router1’s serial 0 interface, Router1’s Ethernet 0 interface, and Router2’s Ethernet 0 interface.
   Router4#ping 12.5.10.1
   Router4#ping 10.1.1.1
   Router4#ping 10.1.1.2

   Consider why the ping to 10.1.1.2 (Router2’s Ethernet 0 interface) was unsuccessful. A packet leaves Router4’s serial 0 interface destined for 10.1.1.2. Because the destination address is on the 10.1.1.0 network and the static route on Router4 stipulates that traffic destined for that network should first be sent to 12.5.10.1, the packet will travel to
12.5.10.1. When the packet reaches Router1, the router sends the packet out the interface that is directly connected to the 10.1.1.0 network. Router2 picks up that packet on its Ethernet 0 interface and attempts to send a response packet to confirm receipt. Router2 examines the source IP address of the received packet, which is 12.5.10.2 (Router4’s serial 0 interface). Router2 does not have a route to network 12.5.10.0, so it drops the packet. This is why the ping was not successful.

5. Just to make sure the static route on Router4 worked, view the routing table to see if the static route has been added there.

   Router4#show ip route

6. To enable Router4 to ping 10.1.1.2, connect to Router2 and configure a static route back to Router4’s network. Type the command that will set a static route on Router2 for the network 12.5.10.0.

   Router2#config term
   Router2(config)#ip route 12.5.10.0 255.255.255.0 10.1.1.1
   Router2(config)#exit

   Consequently, any data sent to network 12.5.10.0 will go to 10.1.1.1 first.

7. Connect to Router4 again, and make sure you can ping Router1’s serial 0 interface, Router1’s Ethernet 0 interface, and Router2’s Ethernet 0 interface.

   Router4#ping 12.5.10.1
   Router4#ping 10.1.1.1
   Router4#ping 10.1.1.2

8. Examine the routing table on Router2.

   Router2#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
          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, * - candidate default
          U - per-user static route

   Gateway of last resort is not set

   C 10.1.1.0/24 is directly connected, 10.1.1.2
   S 12.5.10.0/24 [1/0] via 10.1.1.1

   In the S 12.5.10.0/24 [1/0] via 10.1.1.1 line of output, the S denotes the static route. Next, the destination network and its subnet information (12.5.10.0/24) are displayed. The [1/0] represents the administrative distance, which is 1 by default, and the metric (hop count in this case), which is 0. The word via signals the next hop address the packet should be sent to, which in this case is 10.1.1.1.
Lab 13: RIP

Objective: Configure Routers 1, 2, and 4 with IP addresses and the Routing Information Protocol (RIP).

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 7: Routing Protocols

Goals:
- Set the host name and bring up the interfaces.
- Configure RIP.
- Select the directly connected networks.
- Display the routing table.
- Display the RIP protocol information.

1. Configure Routers 1, 2, and 4 to the specifications outlined in the table and diagram below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Host Name</th>
<th>Ethernet 0</th>
<th>Serial 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router 1</td>
<td>Router1</td>
<td>10.1.1.1 /24</td>
<td>172.16.10.1 /24</td>
</tr>
<tr>
<td>Router 2</td>
<td>Router2</td>
<td>10.1.1.2 /24</td>
<td>172.16.10.2 /24</td>
</tr>
<tr>
<td>Router 4</td>
<td>Router4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. On each router, verify that you can ping the directly connected neighbors.
   - `Router1#ping 10.1.1.2`
   - `Router1#ping 172.16.10.2`
   - `Router2#ping 10.1.1.1`
   - `Router4#ping 172.16.10.1`
3. Add RIP to Router1.
   Router1#
   Router1#configure terminal
   Router1(config)#router rip
   Router1(config-router)#

4. Add the network(s) to which Router1 is directly connected.
   Router1(config-router)#network 10.0.0.0
   Router1(config-router)#network 172.16.0.0

5. Add RIP to Router2.
   Router2#
   Router2#configure terminal
   Router2(config)#router rip
   Router2(config-router)#

6. Add the network(s) to which Router2 is directly connected.
   Router2(config-router)#network 10.0.0.0

   Router4#
   Router4#configure terminal
   Router4(config)#router rip
   Router4(config-router)#

8. Add the network(s) to which Router4 is directly connected.
   Router4(config-router)#network 172.16.0.0

9. Now, RIP should be running on all three routers. See if you can ping between routers that are not directly connected. For instance, from Router2 you should now be able to ping Router4’s serial 0 interface.
   Router2#ping 172.16.10.2

10. Connect to Router4, and ping Router2’s Ethernet 0 interface.
    Router4#ping 10.1.1.2

    If you can ping both devices, then you have correctly configured routing. If the pings were not successful, trace back through the steps.

11. Now, issue the command to display the routing table on Router4.
    Router4#show ip route

12. Finally, display specific IP routing protocol information on Router4.
    Router4#show ip protocol
Lab 14: Troubleshooting RIP

Objective: Configure IP addresses on Routers 1, 2, and 4 with Routing Information Protocol (RIP) as the routing protocol. Then observe routing activity using the debug ip rip command, and examine routes using the show ip route command.

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 7: Routing Protocols

1. Configure Routers 1, 2, and 4 to the specifications outlined in the table below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 2</th>
<th>Router 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router2</td>
<td>Router4</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>192.168.1.1 /24</td>
<td>192.168.1.2 /24</td>
<td></td>
</tr>
<tr>
<td>Serial 0</td>
<td>192.168.2.1 /24</td>
<td></td>
<td>192.168.2.2 /24</td>
</tr>
</tbody>
</table>

2. Use the proper network statements to configure RIP on all routers.
   
   Router1#config
   Router1(config)#router rip
   Router1(config-router)#network 192.168.1.0
   Router1(config-router)#network 192.168.2.0
   Router1(config-router)#exit
   Router1(config)#exit
   Router1#

   Router2#config
   Router2(config)#router rip
   Router2(config-router)#network 192.168.1.0
   Router2(config-router)#exit
   Router2(config)#exit
   Router2#

   Router4#config
   Router4(config)#router rip
   Router4(config-router)#network 192.168.2.0
   Router4(config-router)#exit
   Router4(config)#exit
   Router4#

3. Use the show ip route command to confirm that the routes are being received on all routers.
   
   Router1#show ip route
   Router2#show ip route
   Router4#show ip route

4. Once the routers have received the routes, execute the debug ip rip command at the privileged mode prompt on Router1.
   
   Router1#debug ip rip
Observe the output on Router1’s terminal screen. (The output could take up to 60 seconds to appear.)

5. To turn off the debug command, use the no keyword in front of the command (i.e., no debug ip rip).
   `Router1#no debug ip rip`

6. View the routing table entries on Router2 and Router4. Notice the administrative distances and metrics for these routes.
   `Router2#show ip route`
   `Router4#show ip route`

7. Make sure you can ping all devices on the network from every other device. If all pings do not succeed, then you will need to troubleshoot the router configurations to ensure you configured all settings correctly.
   `Router1#ping 192.168.1.2`
   `Router1#ping 192.168.2.2`
   `Router2#ping 192.168.1.1`
   `Router2#ping 192.168.2.2`
   `Router4#ping 192.168.2.1`
   `Router4#ping 192.168.1.2`

Lab 15: IGRP

Objective: Configure Routers 1, 2, and 4 with IP addresses and Interior Gateway Routing Protocol (IGRP).

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 7: Routing Protocols

Goals:
- Set the host name, and bring up the interfaces.
- Configure IGRP.
- Select the directly connected networks.
- Display the routing table.
- Display the IGRP protocol information.

1. Configure Routers 1, 2, and 4 to the specifications outlined in the table and diagram below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 2</th>
<th>Router 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router2</td>
<td>Router4</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>10.1.1.1 /24</td>
<td>10.1.1.2 /24</td>
<td>172.16.10.1 /24</td>
</tr>
<tr>
<td>Serial 0</td>
<td>172.16.10.2 /24</td>
<td>172.16.10.2 /24</td>
<td>172.16.10.2 /24</td>
</tr>
</tbody>
</table>
2. After you have configured the correct IP address on each interface, verify that each router can ping its directly connected neighbors.
   Router1#ping 10.1.1.2
   Router1#ping 172.16.10.2
   Router2#ping 10.1.1.1
   Router4#ping 172.16.10.1

3. Access global configuration mode on Router1, and enter the command to configure IGRP as the routing protocol on Router1; use the autonomous system number 100.
   Router1#config terminal
   Router1(config)#router igrp 100
   Router1(config-router)#

4. Add the network(s) to which Router1 is directly connected.
   Router1(config-router)#network 10.0.0.0
   Router1(config-router)#network 172.16.0.0

5. Now, enter global configuration mode on Router2, and add IGRP. Remember to use the same autonomous system number.
   Router2#config terminal
   Router2(config)#router igrp 100
   Router2(config-router)#

6. Add the network(s) to which Router2 is directly connected.
   Router2(config-router)#network 10.0.0.0

7. Now, enter global configuration mode on Router4, and add IGRP. Remember to use the same autonomous system number.
   Router4#config terminal
   Router4(config)#router igrp 100
   Router4(config-router)#
8. Add the network(s) to which Router4 is directly connected.
   Router4(config-router)#network 172.16.0.0
9. IGRP should now be running on all three routers. See if pings are successful between
   routers that are not directly connected. From Router2, you should now be able to ping
   Router4’s serial 0 interface. From Router4, you should be able to ping Router2’s Ethernet
   0 interface.
   Router2#ping 172.16.10.2
   Router4#ping 10.1.1.2
   If you can ping both devices, then you have correctly configured routing. If the pings were
   not successful, trace back through the steps.
10. Now, display the routing table on Router4.
    Router4#show ip route
11. Finally, display specific IP routing protocol information on Router4.
    Router4#show ip protocol

Lab 16: PPP With CHAP Authentication

Objective: Understand how Point-to-Point Protocol (PPP) encapsulation works and how to secure
the connection with Challenge Handshake Authentication Protocol (CHAP).

Lab Equipment: Router 1 and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 8: PPP with CHAP Authentication

1. Enter global configuration mode on Router 1, and change the host name to R1.
   Router>enable
   Router#conf t
   Router(config)#hostname R1
   R1(config)#
2. The enable secret password will be used along with the host name to access the other
   router. Set R1’s enable secret password to sameone.
   R1(config)#enable secret sameone
3. On R1, configure a user name of R4 with the password myboson.
   R1(config)#username R4 password myboson
4. Assign an IP address of 10.1.1.1 255.255.255.0 to R1’s serial 0 interface.
   R1(config)#interface serial 0
   R1(config-if)#ip address 10.1.1.1 255.255.255.0
5. On R1, set the encapsulation for the serial 0 interface to PPP.
   R1(config-if)#encapsulation ppp
6. Next, set PPP authentication to CHAP on the serial 0 interface.
   R1(config-if)#ppp authentication chap
7. Now, make sure the serial 0 interface is enabled.
   R1(config-if)#no shutdown
   R1(config-if)#exit
   R1(config)#

8. Connect to Router 4, and configure a host name of R4.
   Router>enable
   Router#config t
   Router(config)#hostname R4
   R4(config)#

   R4(config)#enable secret myboson

10. Add a user name of R1 with a password of sameone.
    R4(config)#username R1 password sameone

11. Assign an IP address of 10.1.1.2 255.255.255.0 to the serial 0 interface on R4, and then enable the interface.
    R4(config)#interface serial 0
    R4(config-if)#ip address 10.1.1.2 255.255.255.0
    R4(config-if)#no shutdown

12. Configure the serial 0 PPP authentication to CHAP on R4.
    R4(config-if)#ppp authentication chap

13. Enable PPP encapsulation on the serial 0 interface of R4. Now, watch the interface state change to up.
    R4(config-if)#encapsulation ppp
    R4(config-if)#exit
    R4(config)#exit
    R4#

14. To verify that the configuration is correct, ping Router1’s serial 0 interface from Router4.
    R4#ping 10.1.1.1
Lab 17: Connectivity Tests With Traceroute

**Objective:** Learn how to use the `traceroute` command. This command is used to map the IP addresses that a packet travels through to get from one device to another.

**Lab Equipment:** Router 1, Router 2, and Router 4 from the eRouters menu

1. Configure Routers 1, 2, and 4 to the specifications outlined in the table below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 2</th>
<th>Router 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router2</td>
<td>Router3</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>192.168.1.1 /24</td>
<td>192.168.1.2 /24</td>
<td>192.168.1.2 /24</td>
</tr>
<tr>
<td>Serial 0</td>
<td>192.168.2.1 /24</td>
<td>192.168.2.2 /24</td>
<td>192.168.2.2 /24</td>
</tr>
</tbody>
</table>

2. After you have configured the proper IP addresses, enable RIP routing across all three routers. Make sure you use the proper network statements.

```bash
Router1#conf t
Router1(config)#router rip
Router1(config-router)#network 192.168.1.0
Router1(config-router)#network 192.168.2.0
Router1(config-router)#exit
Router1(config)#exit
Router1#

Router2#conf t
Router2(config)#router rip
Router2(config-router)#network 192.168.1.0
Router2(config-router)#exit
Router2(config)#exit
Router2#
```
Router4#config
t
Router4(config)#router rip
Router4(config-router)#network 192.168.2.0
Router4(config-router)#exit
Router4(config)#exit
Router4#

3. From Router1, ping the directly connected routers and their interfaces, which are Router2 Ethernet 0 and Router4 serial 0.
   Router1#ping 192.168.1.2
   Router1#ping 192.168.2.2

4. Because RIP routing is enabled, you should be able to ping non-directly connected routers. Connect to Router2, and ping Router4’s serial 0 interface.
   Router2#ping 192.168.2.2

5. The goal behind the **traceroute** command is to help you troubleshoot and determine the path a packet is taking to reach a destination device. In this example, there are three routers and only one path to any destination. Trace the route from Router2 to Router4’s serial 0 interface.
   Router2#traceroute 192.168.2.2

6. Observe the output from the **traceroute** command. It lists Router1’s Ethernet 0 IP address and then the destination IP address. This means that the packet leaves Router2’s Ethernet 0 interface and passes through Router1’s Ethernet 0 interface before reaching Router4’s serial 0 interface.

**Lab 18: Saving Router Configurations**

**Objective:** Learn how to back up a router’s configuration in case the configuration is accidentally deleted or the router fails.

**Lab Equipment:** Router 4 from the eRouters menu and PC 1 from the eStations menu

1. Connect to Router 4, and change the host name to **Tampa**.
   Router>enable
   Router#conf t
   Router(config)#hostname Tampa
   Tampa(config)#

2. Assign the IP address of 24.37.2.1 255.255.255.0 to the Ethernet 0 interface, and then enable the interface.
   Tampa(config)#interface ethernet 0
   Tampa(config-if)#ip address 24.37.2.1 255.255.255.0
   Tampa(config-if)#no shutdown

3. Connect to PC 1 by selecting it from the eStations menu. Type the command that will allow you to configure PC 1’s IP address and default gateway. Set the IP address to 24.37.2.252 with a subnet mask of 255.255.255.0. Set the default gateway to Tampa’s Ethernet 0 IP address (24.37.2.1).
   C:> winipcfg
4. From PC 1, ping Tampa’s Ethernet 0 interface to make sure connectivity exists to the default gateway.
   C:> ping 24.37.2.1

5. Connect to Tampa again, exit interface configuration mode, and then exit global configuration mode. Copy the running configuration to the TFTP server on PC 1.
   Tampa(config-if)#exit
   Tampa(config)#exit
   Tampa# copy running-config tftp

6. When prompted for the address or name of the TFTP server, provide PC 1’s IP address (24.37.2.252), press ENTER, and then provide the name of the configuration file that will be stored on PC 1. Name the configuration file Tampa_config.
   24.37.2.252
   Tampa_config
   After you press ENTER, the router will take a few seconds to establish the connection; then you will see it copy the configuration file and tell you how long it took.

7. Next, connect back to PC 1 and type the `show tftp-configs` command in order to display the configurations that are stored on the TFTP server. (Note: This command does not work on real PCs, just in the NetSim program.)
   C:>show tftp-configs
   If you see the configuration in the list, you have successfully completed the lab.
   Note: Lab 19 builds on this lab’s configuration. To complete Lab 19, please continue with the instructions for Lab 19 in this lab. If you load another lab from the Lab Navigator, your changes will be lost and Lab 19 will not work properly.

Lab 19: Loading Router Configurations

Objective: Become familiar with the process of loading router configurations.

Lab Equipment: Router 4 from the eRouters menu (Tampa from Lab 18)

Prerequisite: You must have just completed Lab 18: Saving Router Configurations in order to complete this lab successfully.

1. Now that the configuration is stored on the TFTP server, change the host name of the router. This will prove that the configuration was copied from the TFTP server. Log on to Tampa, and enter global configuration mode.
   Tampa#config t
   Tampa(config)#

2. Change the host name to Bad_Router.
   Tampa(config)#hostname Bad_Router

3. Copy the configuration you stored on the TFTP server into the running configuration on Bad_Router.
   Bad_Router(config)#exit
   Bad_Router#copy tftp running-config
4. When the router prompts you for a name or an IP address, enter the IP address of the TFTP server.

```
Address or name of remote host []? 24.37.2.252
```

5. Enter the name of the configuration file that should be obtained from the TFTP server.

```
Source filename []? Tampa_config
```

6. The router will download the configuration and load it into the running configuration. Afterward, the host name will be restored to what it was when the configuration was saved.

```
Tampa#
```

### Lab 20: Copying and Pasting Configurations

**Objective:** Learn to save, reload, and paste modified configurations from within the Simulator.

**Lab Equipment:** Router1 from the eRouters menu

Cisco Routers use a command-line parsing routine. Each time you press a carriage return, the router parses that command and executes the code that is required to carry out the command. The Simulator works the same way. When you are working with the Simulator, you can easily switch between devices using the menus across the top of the main window. The Simulator offers some built-in saving and loading options.

1. Set the host name of Router 1 to **Router1**.

```
Router> enable
Router(config)# hostname Router1
```

2. Select the **Save Single Device Config** option from the **File** menu. The program will ask for a file name; use **Router1**, and click **Save**. Save the files to a convenient location that you will remember easily.

3. After you have saved the file, exit the Simulator, and then start it again. Reload Stand-Alone Lab 20 from the Lab Navigator.

4. Select the **Load Single Device Config (overwrite)** option from the **File** menu. Select the Router1.rtr file that you just saved, and click **Open**.

5. The program will then open the file and execute all the commands that were previously saved on the device. Once it is finished, you will notice that the host name has been restored.

6. Two other options under the **File** menu offer similar functionality: the **Save Multi Devices Configs** option and the **Load Multi Devices Configs** option. These two options respectively will save and load the configurations for all the devices.

7. Saved files can be edited easily. Minimize the program, and double-click the Router1.rtr file that you just saved to your computer. When the operating system asks you which program you would like to use to open the file, select Microsoft Notepad.

8. Notepad will launch with Router1’s running configuration displayed. You will see the **hostname** command a few lines down. Change this line from **hostname Router1** to **hostname Miami**. Save your changes.

9. Now, repeat step 4, and observe the host name change.
10. If you have created a configuration that you want to paste into the routers, the program offers a tool to allow you to do this.

11. First, make sure Router1 is open. Select the Paste Real Router Configs option from the File menu. This will open a window that will allow you to paste configuration files you would like to have executed on Router1. In the empty text box, type the following:

```
hostname Router1
interface Ethernet 0
ip address 1.1.1.1 255.255.255.0
no shutdown
exit
exit
```

12. After you have typed the commands above, click the OK button. The router will quickly execute the commands. Notice that the host name of the router will change back to Router1.

13. Execute the show ip interface brief command on Router1 to see that the IP address has been set for Ethernet 0.

Lab 21: ISDN

Objective: Learn how to set up Integrated Services Digital Network (ISDN) on Cisco routers.

Lab Equipment: Router 1 and Router 2 from the eRouters menu

1. Connect to Router 1, and assign it a host name of Router1.
   - `Router>enable`
   - `Router#conf t`
   - `Router(config)#hostname Router1`

2. Connect to Router 2, and assign it a host name of Router2.
   - `Router>enable`
   - `Router#conf t`
   - `Router(config)#hostname Router2`

3. Now, set up the connection between Router1 and Router2 using the BRI ports. Assign the BRI 0 interface of Router1 an IP address of 42.34.10.1 with a 255.255.255.0 subnet mask, enable the interface, and then exit interface configuration mode.
   - `Router1(config)#interface BRI0`
   - `Router1(config-if)#ip address 42.34.10.1 255.255.255.0`
   - `Router1(config-if)#no shut`
   - `Router1(config-if)#exit`
   - `Router1(config)#`

4. Now, connect to Router2, and assign its BRI 0 interface an IP address of 42.34.10.121 with a 255.255.255.0 subnet mask. Enable the interface, and then exit interface configuration mode.
   - `Router2(config)#interface BRI0`
   - `Router2(config-if)#ip address 42.34.10.121 255.255.255.0`
   - `Router2(config-if)#no shut`
   - `Router2(config-if)#exit`
   - `Router2(config)#`
5. Return to Router1, and start to configure ISDN. First, specify the ISDN switch type that will be used. If you use the Simulator defaults, the switch type is basic-ni. There are two different ways to configure the ISDN switch type that the router should use. You can specify the command globally for all BRI interfaces on the router, or you can make the switch type interface-specific. In this instance, specify the switch type globally on your router.

```
Router1(config)#isdn switch-type basic-ni
```

6. Configure some specific information for this BRI interface. First, assign it the ISDN Service Profile Identifier (SPID). Set the SPID on the BRI interface of Router1 by using the `isdn spid` command. A SPID is a number supplied by the ISP to identify the line configuration of the BRI service. Each SPID points to line setup and configuration information on the ISP's ISDN switch. If you use the defaults for the ISDN switch, the SPID for Router1 will be 32177820010100.

```
Router1(config)#interface bri 0
Router1(config-if)#isdn spid 32177820010100
```

7. Now that you have configured the switch type and SPID, Layer 1 connectivity should exist. Layer 1 connectivity occurs between the ISDN switch and the router. To verify that Layer 1 connectivity exists, use the `show isdn status` command at the privileged mode prompt. Make sure that the Layer 2 state is `Multiple_Frame_Established`.

```
Router1(config-if)#exit
Router1(config)#exit
Router1#show isdn status
```

8. Now, configure the number that will need to be dialed on the ISDN switch to establish a Layer 3 connection; this is called the dialer string. Set the dialer string on Router1’s BRI 0 interface. If you are using the default configuration, use 7782001.

```
Router1#config t
Router1(config)#interface bri 0
Router1(config-if)#dialer string 7782001
```

9. Because ISDN costs money when the connection is up, the connection should only be active when it is being used. You can use dialer groups and dialer lists to accomplish this. A dialer list either permits or denies traffic. Specify a dialer list of `protocol ip permit`; consequently, all IP traffic will be permitted. To set up a dialer list, use the `dialer-list` command in global configuration mode.

```
Router1(config-if)#exit
Router1(config)#dialer-list 1 protocol ip permit
```

10. The dialer list must be associated with an interface. Add the dialer list to the ISDN BRI 0 interface by using the `dialer-group` command.

```
Router1(config)#interface bri 0
Router1(config-if)#dialer-group 1
```

11. Now that you have set up ISDN on Router1, you need to perform the same steps for Router2, but with some slight modifications. Connect to Router2, and specify the ISDN switch type that you will be using. If you use the Simulator defaults, the switch type is basic-ni. Specify the switch type in global configuration mode on the router.

```
Router2(config)#isdn switch-type basic-ni
```
12. Next, provide the SPID for this interface. If you use the Simulator defaults for the ISDN switch, the SPID for Router 2 will be 32177820020100.
   
   ```
   Router2(config)#interface bri 0
   Router2(config-if)#isdn spid1 32177820020100
   ```

13. Now that you have set up the switch type and SPID, Layer 1 connectivity should be established. To verify that Layer 1 connectivity exists, use the `show isdn status` command at the privileged mode prompt. Make sure that the Layer 2 state is `Multiple Frame Established`.
   
   ```
   Router2(config-if)#exit
   Router2(config)#exit
   Router2#show isdn status
   ```

14. Now, configure the dialer string that you will need to dial on the ISDN switch in order to establish a Layer 3 connection. Set the dialer string on Router2's BRI 0 interface. If you are using the default configuration, use 7782002.
   
   ```
   Router2(config)#interface bri 0
   Router2(config-if)#dialer string 7782002
   ```

15. Configure the dialer list named `protocol ip permit` on Router2 to permit all IP traffic.
   
   ```
   Router2(config-if)#dialer-list 1 protocol ip permit
   ```

16. Use the `dialer-group 1` command to add the dialer list to the ISDN BRI 0 interface.
   
   ```
   Router2(config-if)#dialer-group 1
   ```

17. Now that both routers are configured for ISDN, see if you can ping the router on the other side of the connection. From Router2, ping Router1's BRI 0 interface (IP address 42.34.10.1).
   
   ```
   Router2(config-if)#exit
   Router2(config)#exit
   Router2#ping 42.34.10.1
   ```

18. If the ping is successful, ISDN is working. Verify this by issuing the `show isdn status` command on Router2.
   
   ```
   Router2#show isdn status
   ```

Examine the Layer 3 settings; there should be one active Layer 3 call. You should also see that the SPID is valid in Layer 2. This information is useful for troubleshooting.

19. Finally, view the configuration changes you have made by displaying the running configuration.
   
   ```
   Router2#show running-config
   ```
Lab 22: Introduction to the Switch

Objective: View some basic areas of a Cisco Catalyst 1900 switch.

Lab Equipment: Switch 1 from the eSwitches menu

Background Reading: Lab Primer Lesson 11: Switches

1. Connect to Switch 1. You should see the user mode prompt.
   >

2. Enter the command to display the IOS version of the switch.
   >show version

   What version of the IOS is running? _______________________

   What is the model number of the switch? ________________

   What is the Base Ethernet Address of the switch? _____________

3. Display the interfaces of the switch.
   >show interfaces

   How many of the interfaces are 10 Mbps? ________________

   How many ports are 100 Mbps Fast Ethernet? ________________

4. Enter the command to view the MAC address table.
   >show mac-address-table

   How many dynamic entries have been learned? _______________

5. Display the running configuration.
   >show running-config

Lab 23: Introduction to Basic Switch Commands

Objective: Become familiar with the basic configuration of the Cisco Catalyst 1912 switch.

Lab Equipment: Switch 1 from the eSwitches menu

Background Reading: Lab Primer Lesson 11: Switches

1. Connect to Switch 1. You should see the user mode prompt.
   >

2. Display the list of commands available at this prompt.
   >?

3. Now, enter privileged mode.
   >enable
   #

4. Display the available commands in privileged mode.
   #?

5. Enter configuration mode.
   #config terminal
   (config)#
6. The host name is used for local identification. When you log on to the switch, you see the host name in front of the prompt (if a host name has been configured). The host name can be used to identify the location or function of the switch. Set the switch’s host name to **Boson**.

   ```
   (config)#hostname Boson
   Boson(config)#
   ```

7. The enable password controls access to privileged mode. This is a very important password because when it is configured, only those who know the password can make configuration changes in privileged mode.

   There is a difference in the syntax used to set the password for a router and the syntax used to set the password for a switch. On the 1900 series switch, levels need to be set when a password is declared. The different levels allow different sets of people to enter different commands on the switch. The password levels range from 1 to 15. Level 1 allows the user to log in to the router and use very basic `show` commands. Level 15 allows the user to do anything. The levels in between can be customized by the network administrator to allow certain commands.

   On Switch1, set the enable password to **Krang**.

   ```
   Boson(config)#enable password level 15 Krang
   ```

8. Test the password by first exiting the switch and then trying to enter privileged mode. Notice that you have to provide the enable password in order to get into privileged mode.

   Now, type `conf term` and proceed with the lab instructions in the next step.

   ```
   Boson(config)#exit
   Boson#exit
   Boson>enable
   Password: 
   Boson#conf term
   Boson(config)#
   ```

9. The only problem with the enable password is that it appears in plain text in the switch’s configuration file. If you need to obtain assistance while troubleshooting a problem, you may inadvertently compromise the security of your system by revealing the password. Set the enable secret password to **cisco**. Do not forget to use the level commands.

   ```
   Boson(config)#enable secret level 15 cisco
   ```

10. You can now test this password by logging out of the switch and then trying to access privileged mode. The enable secret password overrides the enable password. If you have set both passwords, the enable secret password is the password you should use to enter privileged mode. The enable password is now deactivated.

    ```
    Boson(config)#exit
    Boson#exit
    Boson>enable
    Password: 
    Boson#
    ```
Lab 24: Frame Relay

**Objective:** Learn to establish a Frame Relay connection.

**Lab Equipment:** Router 1 and Router 2 from the eRouters menu

**Background Reading:** Lab Primer Lesson 9: Frame Relay

1. Connect to Router 1, and configure the host name to **R1**.
   
   ```
   Router>enable
   Router#conf t
   Router(config)#hostname R1
   R1(config)#
   ```

2. Assign an IP address of 10.1.1.1 255.255.255.0 to the serial 0 interface, and enable the interface.
   
   ```
   R1(config)#interface serial 0
   R1(config-if)#ip address 10.1.1.1 255.255.255.0
   R1(config-if)#no shut
   ```

3. Now, connect to Router 2 and change the host name to **R2**.
   
   ```
   Router>en
   Router#conf t
   Router(config)#hostname R2
   R2(config)#
   ```

4. Assign an IP address of 10.1.1.2 255.255.255.0 to the serial 0 interface, and enable the interface.
   
   ```
   R2(config)#interface serial 0
   R2(config-if)#ip address 10.1.1.2 255.255.255.0
   R2(config-if)#no shut
   ```

5. On R1, set the encapsulation for the serial 0 interface to Frame Relay. Notice that the interface is still down.
   
   ```
   R1(config-if)#encapsulation frame-relay
   ```

6. Next, set the Frame Relay interface data-link connection identifier (DLCI) for the connection from R1 to R2. Because the default Frame Relay network is being used, the DLCI will be **102**.
   
   ```
   R1(config-if)#frame-relay interface-dlci 102
   ```

7. On R2, set the encapsulation for the serial 0 interface to Frame Relay. Notice that the serial 0 interface is still down.
   
   ```
   R2(config-if)#encapsulation frame-relay
   ```

8. Now, set the Frame Relay interface DLCI for the connection from R2 to R1. Because the default Frame Relay network is being used, the DLCI will be **201**.
   
   ```
   R2(config-if)#frame-relay interface-dlci 201
   ```

You should have seen the output from the router saying that the DLCI changed to the active state. This means you have established a connection from R1 through the Frame Relay switch to R2.
9. From R2, verify that the configuration is correct by first trying to ping the serial 0 IP address on R1.
   \texttt{R2(config-if)#exit}
   \texttt{R2(config)#exit}
   \texttt{R2#ping 10.1.1.1}

10. Next, use the Frame Relay show commands to prove that the connection is active. The show frame-relay lmi command displays the Local Management Interface (LMI) traffic that has been exchanged between the router and the Frame Relay switch.
   \texttt{R2#show frame-relay lmi}

11. The show frame-relay traffic command displays the global Frame Relay statistics since the last reload of the router.
   \texttt{R2#show frame-relay traffic}

12. The show frame-relay map command displays the mappings of the Layer 2 DLCI to the Layer 3 IP address.
   \texttt{R2#show frame-relay map}

13. The show frame-relay PVC command displays all of the permanent virtual circuit (PVC) mappings for the router. These mappings are only locally significant between the router and the Frame Relay switch.
   \texttt{R2#show frame-relay pvc}

---

**Lab 25: Frame Relay Hub-and-Spoke Topology**

**Objective:** Learn to configure a hub-and-spoke topology.

**Lab Equipment:** Router 1, Router 2, Router 3, and Router 4 from the eRouters menu

**Background Reading:** Lab Primer Lesson 9: Frame Relay

Your company’s corporate office is in Dallas, and its sales offices are in San Francisco, New York, and Tampa. You want to implement a hub-and-spoke topology in which all of the sales offices connect to the corporate office to send all data, including communications between sales offices.
1. First, assign the host names of Dallas, San_Francisco, New_York, and Tampa to Router 1, Router 2, Router 3, and Router 4, respectively.

2. Now, enter interface configuration mode for the serial 0 interface on Dallas, and set the encapsulation type to Frame Relay. Be sure to enable the interface.

   Dallas(config)#interface serial 0
   Dallas(config-if)#encapsulation frame-relay
   Dallas(config-if)#no shutdown

3. Next, create a subinterface for the connection from Dallas to the San Francisco sales office.

   Dallas(config-if)#exit
   Dallas(config)#interface serial 0.100 point-to-point
   Dallas(config-subif)#

4. Assign the subinterface the DLCI number for the connection from Dallas to San Francisco, and configure the subinterface with the appropriate IP address. Remember to enable the subinterface.

   Dallas(config-subif)#frame-relay interface-dlci 102
   Dallas(config-subif)#ip address 172.16.1.1 255.255.255.0
   Dallas(config-subif)#no shutdown

5. Create a subinterface for the connection from Dallas to the sales office in New York.

   Dallas(config-subif)#exit
   Dallas(config)#interface serial 0.200 point-to-point
   Dallas(config-subif)#

6. Add the correct DLCI for the connection from Dallas to New_York, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.

   Dallas(config-subif)#frame-relay interface-dlci 103
   Dallas(config-subif)#ip address 172.16.2.1 255.255.255.0
   Dallas(config-subif)#no shutdown

7. Create a subinterface for the connection from Dallas to the sales office in Tampa.

   Dallas(config-subif)#exit
   Dallas(config)#interface serial 0.300 point-to-point
   Dallas(config-subif)#

8. Add the correct DLCI for the Dallas to Tampa connection, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.

   Dallas(config-subif)#frame-relay interface-dlci 104
   Dallas(config-subif)#ip address 172.16.3.1 255.255.255.0
   Dallas(config-subif)#no shutdown

9. Access the serial 0 interface on San_Francisco, set the encapsulation to Frame Relay, and enable the interface.

   San_Francisco(config)#interface serial 0
   San_Francisco(config-if)#encapsulation frame-relay
   San_Francisco(config-if)#no shutdown
10. Because subinterfaces are not necessary for single connections, add the appropriate DLCI value.
   \texttt{San\_Francisco(config-if)#frame-relay interface-dlci 201}

11. Set the IP address for this interface, and enable the interface.
   \texttt{San\_Francisco(config-if)#ip address 172.16.1.2 255.255.255.0}
   \texttt{San\_Francisco(config-if)# no shutdown}

12. Access the serial 0 interface on New\_York, and set the encapsulation to Frame Relay.
   \texttt{New\_York(config)#interface serial 0}
   \texttt{New\_York(config-if)#encapsulation frame-relay}

13. Add the appropriate DLCI value.
   \texttt{New\_York(config-if)#frame-relay interface-dlci 301}

14. Set the IP address for this interface, and enable the interface.
   \texttt{New\_York(config-if)#ip address 172.16.2.2 255.255.255.0}
   \texttt{New\_York(config-if)# no shutdown}

15. Access the serial 0 interface on Tampa, and set the encapsulation to Frame Relay.
   \texttt{Tampa(config)#interface serial 0}
   \texttt{Tampa(config-if)#encapsulation frame-relay}

16. Add the appropriate DLCI value.
   \texttt{Tampa(config-if)#frame-relay interface-dlci 401}

17. Configure the IP address for this interface, and enable the interface.
   \texttt{Tampa(config-if)#ip address 172.16.3.2 255.255.255.0}
   \texttt{Tampa(config-if)# no shutdown}

18. Now, all interfaces should be up and up. To confirm this, connect to Dallas and try to ping each of the three sales offices.
   \texttt{Dallas(config-subif)#exit}
   \texttt{Dallas(config)#exit}
   \texttt{Dallas#ping 172.16.1.2}
   \texttt{Dallas#ping 172.16.2.2}
   \texttt{Dallas#ping 172.16.3.2}

**Lab 26: Frame Relay Full Mesh Topology**

**Objective:** Learn to configure a full mesh topology.

**Lab Equipment:** Router 1, Router 2, Router 3, and Router 4 from the eRouters menu

**Background Reading:** Lab Primer Lesson 9: Frame Relay

Again, the company's corporate office is in Dallas and its sales offices are in San Francisco, New York, and Tampa. The sales offices should be able to access all company resources. You want to establish a full mesh topology in which a point-to-point Frame Relay connection links the corporate office to each sales office and links each sales office to every other sales office.
The difference between the Frame Relay hub-and-spoke topology and the full mesh topology is that, with a full mesh topology, every sales office has a direct connection to every other sales office and the corporate office. This is a very redundant topology so if one of the connections fails, data can still be transferred to every site by using a different path.

1. First, assign the host names of Dallas, San_Francisco, New_York, and Tampa to Router 1, Router 2, Router 3, and Router 4, respectively.

2. Now, enter interface configuration mode for the serial 0 interface on Dallas, and set the encapsulation type to Frame Relay. Be sure to enable the interface.
   - Dallas(config)#interface serial 0
   - Dallas(config-if)#encapsulation frame-relay
   - Dallas(config-if)#no shutdown

3. Next, create a subinterface for the connection between Dallas and the San Francisco sales office.
   - Dallas(config-if)#exit
   - Dallas(config)#interface serial 0.100 point-to-point
   - Dallas(config-subif)#

4. Assign the subinterface the DLCI number for the connection from Dallas to San Francisco, and configure the subinterface with the appropriate IP address. Remember to enable the subinterface.
   - Dallas(config-subif)#frame-relay interface-dlci 102
   - Dallas(config-subif)#ip address 172.16.1.1 255.255.255.0
   - Dallas(config-subif)#no shutdown

5. Create a subinterface for the connection from Dallas to the sales office in New York.
   - Dallas(config-subif)#exit
   - Dallas(config)#interface serial 0.200 point-to-point
   - Dallas(config-subif)#
6. Add the correct DLCI for the connection from Dallas to New_York, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.
   Dallas(config-subif)#frame-relay interface-dlci 103
   Dallas(config-subif)#ip address 172.16.2.1 255.255.255.0
   Dallas(config-subif)#no shutdown

7. Create a subinterface for the connection from Dallas to the sales office in Tampa.
   Dallas(config-subif)#exit
   Dallas(config)#interface serial 0.300 point-to-point
   Dallas(config-subif)#

8. Add the correct DLCI for the connection from Dallas to Tampa, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.
   Dallas(config-subif)#frame-relay interface-dlci 104
   Dallas(config-subif)#ip address 172.16.3.1 255.255.255.0
   Dallas(config-subif)#no shutdown

9. Access the serial 0 interface of San_Francisco, set the encapsulation to Frame Relay, and enable the interface.
   San_Francisco(config)#interface serial 0
   San_Francisco(config-if)#encapsulation frame-relay
   San_Francisco(config-if)#no shutdown

10. Create the first subinterface for the connection from San_Francisco to the corporate office in Dallas.
    San_Francisco(config-if)#interface serial 0.100 point-to-point
    San_Francisco(config-subif)#

11. Add the correct DLCI for the connection from San_Francisco to Dallas, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.
    San_Francisco(config-subif)#frame-relay interface-dlci 201
    San_Francisco(config-subif)#ip address 172.16.1.2 255.255.255.0
    San_Francisco(config-subif)#no shutdown

12. Create a subinterface for the connection from San_Francisco to New_York.
    San_Francisco(config-subif)#exit
    San_Francisco(config)#interface serial 0.200 point-to-point

13. Add the correct DLCI value for the connection from San_Francisco to New_York, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.
    San_Francisco(config-subif)#frame-relay interface-dlci 203
    San_Francisco(config-subif)#ip address 172.16.4.1 255.255.255.0
    San_Francisco(config-subif)#no shutdown

14. Create the subinterface for the connection from San_Francisco to Tampa.
    San_Francisco(config-subif)#exit
    San_Francisco(config)#interface serial 0.300 point-to-point
15. Add the correct DLCI value for the San_Francisco to Tampa connection, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.

San_Francisco(config-subif)#frame-relay interface-dlci 204
San_Francisco(config-subif)#ip address 172.16.6.1 255.255.255.0
San_Francisco(config-subif)#no shutdown

16. Access the serial 0 interface of New_York, set the encapsulation to Frame Relay, and enable the interface.

New_York(config)#interface serial 0
New_York(config-if)#encapsulation frame-relay
New_York(config-if)#no shutdown

17. Create the first subinterface for the connection from New_York to the corporate office in Dallas.

New_York(config-if)#exit
New_York(config)#interface serial 0.100 point-to-point

18. Add the correct DLCI value for the connection from New_York to Dallas, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.

New_York(config-subif)#frame-relay interface-dlci 301
New_York(config-subif)#ip address 172.16.2.2 255.255.255.0
New_York(config-subif)#no shutdown

19. Create the subinterface for the connection from New_York to San_Francisco.

New_York(config-subif)#exit
New_York(config)#interface serial 0.200 point-to-point

20. Add the correct DLCI value for the connection from New_York to San_Francisco, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.

New_York(config-subif)#frame-relay interface-dlci 302
New_York(config-subif)#ip address 172.16.4.2 255.255.255.0
New_York(config-subif)#no shutdown

21. Create the subinterface for the connection from New_York to Tampa.

New_York(config-subif)#exit
New_York(config)#interface serial 0.300 point-to-point

22. Add the correct DLCI value for the New_York to Tampa connection, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.

New_York(config-subif)#frame-relay interface-dlci 304
New_York(config-subif)#ip address 172.16.5.1 255.255.255.0
New_York(config-subif)#no shutdown

23. Access the serial 0 interface on Tampa, set the encapsulation to Frame Relay, and enable the interface.

Tampa(config)#interface serial 0
Tampa(config-if)#encapsulation frame-relay
Tampa(config-if)#no shutdown
24. Create the first subinterface for the connection from Tampa to the corporate office in Dallas.
   Tampa(config-if)#exit
   Tampa(config)#interface serial 0.100 point-to-point

25. Add the correct DLCI value for the Tampa to Dallas connection, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.
   Tampa(config-subif)#frame-relay interface-dlci 401
   Tampa(config-subif)#ip address 172.16.3.2 255.255.255.0
   Tampa(config-subif)#no shutdown

26. Create the subinterface for the connection from Tampa to San_Francisco.
   Tampa(config-subif)#exit
   Tampa(config)#interface serial 0.200 point-to-point

27. Add the correct DLCI value for the Tampa to San_Francisco connection, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.
   Tampa(config-if)#frame-relay interface-dlci 402
   Tampa(config-subif)#ip address 172.16.6.2 255.255.255.0
   Tampa(config-subif)#no shutdown

28. Create the subinterface for the connection from Tampa to New_York.
   Tampa(config-subif)#exit
   Tampa(config)#interface serial 0.300 point-to-point

29. Add the correct DLCI value for the Tampa to New_York connection, and configure the appropriate IP address for the subinterface. Remember to enable the subinterface.
   Tampa(config-subif)#frame-relay interface-dlci 403
   Tampa(config-subif)#ip address 172.16.5.2 255.255.255.0
   Tampa(config-subif)#no shutdown

30. Now, all interfaces should be up and up. To test the configuration, connect to Dallas and try to ping each of the three sales offices.
   Dallas(config-subif)#exit
   Dallas(config)#exit
   Dallas#ping 172.16.1.2
   Dallas#ping 172.16.2.2
   Dallas#ping 172.16.3.2

31. Connect to San_Francisco, and try to ping the other three offices.
   San_Francisco(config-subif)#exit
   San_Francisco(config)#exit
   San_Francisco#ping 172.16.1.1
   San_Francisco#ping 172.16.4.2
   San_Francisco#ping 172.16.6.2
Lab 27: Standard Access Lists

Objective: Gain experience configuring standard access lists.

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 10: Access Lists

If you feel confident about configuring IP addresses and RIP, establish the configuration in the table below, and then continue with step 10.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 2</th>
<th>Router 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router2</td>
<td>Router4</td>
</tr>
<tr>
<td>Enable RIP</td>
<td>on E0 and S0</td>
<td>on E0</td>
<td>on S0</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>24.17.2.1 255.255.255.240</td>
<td>24.17.2.2 255.255.255.240</td>
<td></td>
</tr>
<tr>
<td>Serial 0</td>
<td>24.17.2.17 255.255.255.240</td>
<td>24.17.2.18 255.255.255.240</td>
<td></td>
</tr>
</tbody>
</table>

1. Connect to Router 1, assign it a host name of Router1, and set the IP address on the Ethernet 0 interface to 24.17.2.1 255.255.255.240. Set the IP address on the serial 0 interface to 24.17.2.17 255.255.255.240. Remember to enable both interfaces.

   Router> enable
   Router#config t
   Router(config)#hostname Router1
   Router1(config)#interface ethernet0
   Router1(config-if)#ip address 24.17.2.1 255.255.255.240
   Router1(config-if)#no shutdown
   Router1(config-if)#exit
   Router1(config)#interface serial0
   Router1(config-if)#ip address 24.17.2.17 255.255.255.240
   Router1(config-if)#no shutdown
   Router1(config-if)#exit

2. Connect to Router 2, assign it a host name of Router2, and set the IP address on the Ethernet 0 interface to 24.17.2.2 255.255.255.240. Remember to enable the interface.

   Router> enable
   Router#config t
   Router(config)#hostname Router2
   Router2(config)#interface ethernet0
   Router2(config-if)#ip address 24.17.2.2 255.255.255.240
   Router2(config-if)#no shutdown
   Router2(config-if)#exit
   Router2(config)#exit

3. From Router2, ping Router1’s Ethernet 0 interface to ensure a connection exists.

   Router2#ping 24.17.2.1
4. Connect to Router 4, assign it a host name of **Router4**, and set the IP address on the serial 0 interface to 24.17.2.18 255.255.255.240. Then ping Router1’s serial 0 interface.

   ```
   Router>enable
   Router#config t
   Router(config)#hostname Router4
   Router4(config)#interface serial0
   Router4(config-if)#ip address 24.17.2.18 255.255.255.240
   Router4(config-if)#no shutdown
   Router4(config-if)#exit
   Router4(config)#exit
   Router4#ping 24.17.2.17
   ```

5. Now that IP addresses have been configured on all interfaces, you need to implement a routing protocol to facilitate communication between Router2 and Router4. Enable Routing Information Protocol (RIP) on Router1, and add the network for Ethernet 0 and serial 0.

   ```
   Router1#config t
   Router1(config)#router rip
   Router1(config-router)#network 24.0.0.0
   Router1(config-router)#exit
   Router1(config)#exit
   ```

6. On Router2, enable RIP and add the network for Ethernet 0.

   ```
   Router2#config t
   Router2(config)#router rip
   Router2(config-router)#network 24.0.0.0
   Router2(config-router)#exit
   Router2(config)#exit
   ```

7. On Router4, enable RIP and add the network for serial 0.

   ```
   Router4#config t
   Router4(config)#router rip
   Router4(config-router)#network 24.0.0.0
   Router4(config-router)#exit
   Router4(config)#exit
   ```

8. Verify that you can ping Router2’s Ethernet 0 interface from Router4.

   ```
   Router4#ping 24.17.2.2
   ```

9. Now, configure a standard access list to block Router4 from being able to ping Router2. You should configure this access list on Router2. First, connect to Router2 and enter global configuration mode.

   ```
   Router2#config t
   Router2(config)#
   ```

10. Create access list 1 to block the single IP address 24.17.2.18. Here are three ways to accomplish this:

   ```
   Router2(config)#access-list 1 deny host 24.17.2.18
   OR
   ```
**Router2(config)#access-list 1 deny 24.17.2.18 0.0.0.0**

**OR**

**Router2(config)#access-list 1 deny 24.17.2.18**

11. Next, issue the **access-list 1 permit any** command.

**Router2(config)#access-list 1 permit any**

12. Now you need to apply the access list to the Ethernet 0 interface. You must specify the direction of traffic flow upon which the access list should apply. The in parameter configures the access list to apply to packets coming in from the network and traveling to the router. The out parameter configures the access list to apply to packets traveling from the router out the interface to the network. In this scenario, you should use the in parameter.

**Router2(config)#interface ethernet0**

**Router2(config-if)#ip access-group 1 in**

**Router2(config-if)#exit**

*Note:* This completes the Standard Access Lists lab. Please continue on to Lab 28: Verify Standard Access Lists without accessing the Lab Navigator.

---

**Lab 28: Verify Standard Access Lists**

**Objective:** Verify that the standard access list created in the previous lab is configured correctly.

**Lab Equipment:** Router 2 and Router 4 from the eRouters menu

**Background Reading:** Lab Primer Lesson 10: Access Lists

**Prerequisite:** You must have just completed Lab 27: Standard Access Lists in order to complete this lab successfully.

1. First, see if you can still ping Router2 from Router4. Connect to Router4, and try to ping Router2’s Ethernet 0 interface (24.17.2.2).

   **Route4>enable**

   **Route4#ping 24.17.2.2**

   If you see **UUUUU**, indicating that the ping was not successful, then your access list is working correctly.

2. Now, connect to Router2 and view the running configuration in order to verify that the access list is running on the interfaces.

   **Router2>enable**

   **Router2#show running-config**

3. You can also view which access lists are applied to the interfaces by using the **show ip interface** command.

   **Router2#show ip interface**

4. The **show access-lists** command will display which access lists have been created on the router. It will also tell you which lines have been used and how many packets have been either permitted or denied.

   **Router2#show access-lists**

   *Note:* Continue on to Lab 29: Extended Access Lists without accessing the Lab Navigator. This will save you the trouble of configuring the same IP addresses again.
Lab 29: Extended Access Lists

Objective: Gain experience configuring extended access lists.

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 10: Access Lists

1. If you have just completed Lab 28: Verifying Standard Access Lists, then all you need to do is execute the `no ip access-group 1 in` command on the Ethernet 0 interface of Router2, and then start this lab at step 10.

   `Router2>enable`
   `Router2#conf t`
   `Router2(config)#interface ethernet0`
   `Router2(config-if)#no ip access-group 1 in`

   Note: If you have not completed Lab 28: Verifying Standard Access Lists and you feel confident about configuring IP addresses and RIP, establish the configuration in the table below and then continue with step 10.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 2</th>
<th>Router 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router2</td>
<td>Router4</td>
</tr>
<tr>
<td>Enable RIP</td>
<td>on E0 and S0</td>
<td>on E0</td>
<td>on S0</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>24.17.2.1 255.255.255.240</td>
<td>24.17.2.2 255.255.255.240</td>
<td></td>
</tr>
<tr>
<td>Serial 0</td>
<td>24.17.2.17 255.255.255.240</td>
<td></td>
<td>24.17.2.18 255.255.255.240</td>
</tr>
</tbody>
</table>

2. Connect to Router 1, assign it a host name of Router1, and set the IP address on the Ethernet 0 interface to 24.17.2.1 255.255.255.240. Set the IP address on the serial 0 interface to 24.17.2.17 255.255.255.240. Remember to enable both interfaces.

   `Router>enable`
   `Router#conf t`
   `Router(config)#hostname Router1`
   `Router1(config)#interface ethernet0`
   `Router1(config-if)#ip address 24.17.2.1 255.255.255.240`
   `Router1(config-if)#no shutdown`
   `Router1(config-if)#exit`
   `Router1(config)#interface serial0`
   `Router1(config-if)#ip address 24.17.2.17 255.255.255.240`
   `Router1(config-if)#no shutdown`
   `Router1(config-if)#exit`
   `Router1(config)#exit`
3. Connect to Router 2, assign it a host name of Router2, and set the IP address on the Ethernet 0 interface to 24.17.2.2 255.255.255.240. Remember to enable the interface.

   Router>enable
   Router#config t
   Router(config)#hostname Router2
   Router2(config)#interface ethernet0
   Router2(config-if)#ip address 24.17.2.2 255.255.255.240
   Router2(config-if)#no shutdown
   Router2(config-if)#exit
   Router2(config)#exit

4. Ping Router1's Ethernet 0 interface to ensure that a connection exists.

   Router2#ping 24.17.2.1

5. Connect to Router 4, assign it a host name of Router4, and set the IP address on the serial 0 interface to 24.17.2.18 255.255.255.240. Then ping Router1's serial 0 interface.

   Router>enable
   Router#config t
   Router(config)#hostname Router4
   Router4(config)#interface serial0
   Router4(config-if)#ip address 24.17.2.18 255.255.255.240
   Router4(config-if)#no shutdown
   Router4(config-if)#exit
   Router4(config)#exit
   Router4#ping 24.17.2.17

6. Now you need to implement a routing protocol to facilitate communication between Router2 and Router4. Enable Routing Information Protocol (RIP) on Router1, and add the network for Ethernet 0 and serial 0.

   Router1#config t
   Router1(config)#router rip
   Router1(config-router)#network 24.0.0.0
   Router1(config-router)#exit
   Router1(config)#exit

7. On Router2, enable RIP and add the network for Ethernet 0.

   Router2#config t
   Router2(config)#router rip
   Router2(config-router)#network 24.0.0.0
   Router2(config-router)#exit
   Router2(config)#exit

8. On Router4, enable RIP and add the network for serial 0.

   Router4#config t
   Router4(config)#router rip
   Router4(config-router)#network 24.0.0.0
   Router4(config-router)#exit
   Router4(config)#exit
9. Verify that you can ping Router2’s Ethernet 0 interface from Router4.
   
   Router4#ping 24.17.2.2

10. The extended access lists you create should accomplish two things. First, allow only 
    Telnet traffic from the subnet off of Router1’s serial 0 interface to come into Router1. 
    Next, allow any traffic from Router1’s Ethernet 0 subnet to travel anywhere. Connect to 
    Router1, and enter global configuration mode.
    
    Router1#conf t
    Router1(config)#

11. To allow only Telnet traffic from the 24.17.2.16 subnet, create access list 101. Use the log 
    keyword to display output to the router every time this line on the access list is invoked.
    
    Router1(config)#access-list 101 permit tcp 24.17.2.16 0.0.0.15 any eq telnet log

12. To permit all traffic from the 24.17.2.0 subnet, create access list 102, and use the log 
    keyword.
    
    Router1(config)#access-list 102 permit ip 24.17.2.0 0.0.0.15 any log

13. Now, apply these access lists to the interfaces. First, enter interface configuration mode 
    for the serial 0 interface of Router1, and apply access list 101 inbound.
    
    Router1(config)#interface serial0
    Router1(config-if)#ip access-group 101 in
    Router1(config-if)#exit

14. For Ethernet 0 on Router1, apply access list 102 inbound.
    
    Router1(config)#interface ethernet0
    Router1(config-if)#ip access-group 102 in
    Router1(config-if)#exit

   Note: To make sure the access lists are configured correctly, continue on to Lab 30: Verify 
   Extended Access Lists without accessing the Lab Navigator.

Lab 30: Verify Extended Access Lists

Objective: Verify that the extended access lists created in Lab 29 are configured correctly.

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 10: Access Lists

Prerequisite: You must have just completed Lab 29: Extended Access Lists in order to complete 
this lab successfully.

1. Test whether the extended access lists created in Lab 29 are working properly. Connect 
   to Router4, and try to ping Router1’s serial 0 interface. If the access lists are configured 
   correctly, you should not be able to ping the serial interface.
   
   Router4>enable
   Router4#ping 24.17.2.17
2. Now that you have verified that the access lists are blocking pings to Router1 from the subnet off of Router1’s serial 0 interface, verify that Telnet traffic from that subnet is allowed to reach Router1. Connect to Router1, enable Telnet access, and then set the password to boson.

   Router1(config)#
   Router1(config)#line vty 0 4
   Router1(config-line)#login
   Router1(config-line)#password boson
   Router1(config-line)#exit

3. Connect to Router4 again, and try to telnet into Router1’s serial 0 interface.

   Router4#telnet 24.17.2.17

4. If Telnet access is permitted, you should see the host name in the router prompt change to Router1. Now, press the CTRL+SHIFT+6 key combination followed by the X key to return to Router4. Then type disconnect 1 to close the connection to Router1.

   Router1> Press CTRL+SHIFT+6, then press X
   Router4#disconnect 1

5. Connect to Router2, and see if you can ping Router4’s serial 0 interface.

   Router2#enable
   Router2#ping 24.17.2.18

   Consider why the ping is unsuccessful. The packet starts at Router2, travels through Router1, and reaches Router4. Once it arrives at Router4, it is repackaged and sent back to Router1. When Router4 repackages the packet, the packet’s source IP address becomes the destination IP address, and the destination IP address becomes the source IP address. When the packet encounters the access list on Router1’s serial 0 interface, it is blocked because the packet’s source IP address is Router4’s serial 0 address.

6. See if you can ping Router1’s Ethernet 0 interface from Router2.

   Router2#ping 24.17.2.1

7. Now, try to telnet into Router1’s Ethernet 0 interface from Router2. If Telnet access is permitted, you should see the host name in the router prompt change to Router1. Press the CTRL+SHIFT+6 key combination followed by the X key to return to Router4. Then type disconnect 1 to close the connection to Router1.

   Router2#telnet 24.17.2.1
   Router1> Press CTRL+SHIFT+6, then press X
   Router2#disconnect 1

8. To verify that the access lists are configured on the interfaces, display the running configuration.

   Router1#show running-config

9. You can also view which access lists are applied to the interfaces by using the show IP interface command.

   Router1#show ip interface

10. The show access-lists command displays which access lists have been created on a router. The output of this command also tells you which lines of the access list have been used and how many packets have been permitted or denied.

   Router1#show access-lists
Lab 31: Named Access Lists

Objective: Create a named access list that will deny all ping traffic from PC 1 to Router 1, but will enable all access from Router 4 to Router 1. For this lab, the access list must be added on Router 1.

Lab Equipment: Router 1 and Router 4 from the eRouters menu and PC 1 from the eStations menu

Background Reading: Lab Primer Lesson 10: Access Lists

1. Establish the configurations outlined in the table below. Use the winipcfg command on PC 1 to configure the IP address and default gateway.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 4</th>
<th>PC 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router4</td>
<td>PC 1</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>192.168.1.17 /28</td>
<td>192.168.1.18 /28</td>
<td></td>
</tr>
<tr>
<td>Serial 0</td>
<td>192.168.1.1 /28</td>
<td>192.168.1.2 /28</td>
<td></td>
</tr>
<tr>
<td>Default Gateway</td>
<td></td>
<td></td>
<td>192.168.1.17</td>
</tr>
</tbody>
</table>

2. Configure RIP on the two routers. Be sure to use the proper network statements.
   - Router1(config)#router rip
   - Router1(config-router)#network 192.168.1.0
   - Router4(config)#router rip
   - Router4(config-router)#network 192.168.1.0

3. Use the show ip route command on each router to make sure that the routes have been received.
   - Router1#show ip route
   - Router4#show ip route

4. Verify that you can ping Router1 from PC 1.
   - C:>ping 192.168.1.1

5. Create an access list that prevents ping traffic originating from PC 1 and destined for Router1 from reaching Router1. Typically, this access list could be placed on either Router4 or Router1. It often makes more sense to place the access list on the router closest to the source as possible; this helps keep unnecessary traffic off the backbone. For this example, however, the access list will be placed on Router1 for inbound traffic.
   - Router1(config)#ip access-list extended deny_ping
   - Router1(config-ext-acl)#deny icmp host 192.168.1.18 192.168.1.1 0.0.0.0 log
   - Router1(config-ext-acl)#permit ip any any log

The first statement above defines the access list as extended. The second statement denies any ICMP traffic with a source IP address of 192.168.1.18 that is destined for 192.168.1.1; the wildcard mask of 0.0.0.0 in this line means that the IP address must be matched exactly. Notice how the host command is used for the first part of the access list and the wildcard mask of 0.0.0.0 is used for the second part of the access list. The host command and the wildcard mask of 0.0.0.0 both do the same thing. The log keyword allows you to double-check your work.
6. Next, apply the access list to inbound traffic on the serial 0 interface of Router1.
   Router1(config-ext-acl)#exit
   Router1(config)#interface serial 0
   Router1(config-if)#ip access-group deny_ping in

7. Connect to PC 1 and send a test ping to Router1. Then connect to Router4 and send a
test ping to Router1. Are the pings successful?
   C:>ping 192.168.1.1
   Router4#ping 192.168.1.1

8. Connect to Router1 again; you should see two separate log messages. The first one is
denying the ping from PC 1, and the second is allowing the ping from Router4.

Lab 32: Advanced Extended Access Lists

Objective: Configure extended access lists to filter out network-to-network traffic, host-to-host
traffic, and network-to-host traffic.

Lab Equipment: Router 1 and Router 2 from the eRouters menu and PC 1, PC 2, PC 3, PC 4, and
PC 5 from the eStations menu

Background Reading: Lab Primer Lesson 10: Access Lists

1. Establish the configurations outlined in the tables below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Host Name</th>
<th>FA0/0</th>
<th>FA0/1</th>
<th>Serial 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Router1</td>
<td>192.168.3.1 /24</td>
<td>192.168.1.1 /25</td>
<td>192.168.2.1 /24</td>
</tr>
<tr>
<td></td>
<td>Router2</td>
<td></td>
<td></td>
<td>192.168.2.2 /24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Host</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC 1</td>
<td>192.168.3.2</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
</tr>
<tr>
<td>PC 2</td>
<td>192.168.1.130</td>
<td>255.255.255.128</td>
<td>192.168.1.129</td>
</tr>
<tr>
<td>PC 3</td>
<td>192.168.1.131</td>
<td>255.255.255.128</td>
<td>192.168.1.129</td>
</tr>
<tr>
<td>PC 4</td>
<td>192.168.1.2</td>
<td>255.255.255.128</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>PC 5</td>
<td>192.168.1.3</td>
<td>255.255.255.128</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>
2. Configure RIP on the two routers. Be sure to use the proper network statements.
   
   ```
   Router1#conf t
   Router1(config)#router rip
   Router1(config-router)#network 192.168.2.0
   Router1(config-router)#network 192.168.3.0
   ```
   
   ```
   Router2#conf t
   Router2(config)#router rip
   Router2(config-router)#network 192.168.1.0
   Router2(config-router)#network 192.168.2.0
   ```
   
3. Use the `show ip route` command on each router to make sure that the routes have been received.
   
   ```
   Router1#show ip route
   ```
   
   ```
   Router2#show ip route
   ```
   
4. Verify that you can ping PC 1 from PC 2.
   
   ```
   C:>ping 192.168.3.2
   ```
   
**Network-to-Network Access List**

5. Examine the network diagram below. The first access list you create should allow only traffic from the Administration network (PC 4 and PC 5) destined for PC 1 on the Corporate HQ network. To accomplish this, use an extended access list. Because you are allowing all traffic, you should use IP as the protocol. The access list should look something like the following:
   
   ```
   Router1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.127 192.168.3.0 0.0.0.255 log
   ```
   
   ```
   Router1(config)#access-list 100 permit ip 192.168.2.0 0.0.0.0 any
   ```
   
   This access list is very simple because you are only allowing two types of traffic and denying all other traffic. Because there is an implicit `deny` statement at the end of all access lists, you only need a `permit` statement for the pings and a `permit` statement for the RIP broadcasts.
6. Now you need to apply the access list to the interface. Because the traffic is coming from Router2 and going to Router1, you should place the access list on Router1’s serial 0 interface. The access list will check all inbound traffic.

```
Router1#conf t
Router1(config)#interface serial 0
Router1(config-if)#ip access-group 100 in
```

7. To test the access list, try to ping PC 1 from PC 2, PC 3, PC 4, and PC 5. PC 2 and PC 3 should not be able to ping PC 1, but PC 4 and PC 5 should be able to. If this access list works, continue on to the next step.

```
C:>ping 192.168.3.2
```

**Host-to-Host Access List**

8. In this portion of the lab, you will block an individual PC from accessing the central file server. PC 2 is being used by a new employee whom you do not want to have access to the file server (PC 5) for 30 days. To accomplish this, you decide to implement an access list on Router2 that will block access to PC 5 only from PC 2. In this instance, you are setting the access list manually. The list must be manually removed after 30 days.

For lab scenario purposes, you should use the `log` keyword. This will show logging output on the screen of Router2 when the access list is invoked. For this part of the lab, the log will show up on the screen only when you deny access from PC 2.
Router2(config)#access-list 101 deny ip host 192.168.1.130 192.168.1.3 0.0.0.0 log
Router2(config)#access-list 101 permit ip any any

9. Apply the access list to Router2’s Fast Ethernet 0/0 interface.
   
   Router2#conf t
   Router2(config)#interface FastEthernet 0/0
   Router2(config-if)#ip access-group 101 in

10. Connect to PC 2, and verify that you cannot ping PC 5. Connect to PC 3, and verify that you can ping PC 5.
   C:>ping 192.168.1.3

11. Finally, connect to Router2, and verify that the log statements displayed on the console match the corresponding pings sent from the PCs.

Network-to-Host Access List

12. Before you create this access list, remove the preceding access lists from Router1 and Router2.
   
   Router1(config)#interface serial 0
   Router1(config-if)#no ip access-group 100 in

   Router2(config)#interface FastEthernet 0/0
   Router2(config-if)#no ip access-group 101 in

13. Create an extended access list that blocks all traffic to PC 1 from the Network Users area in the topology. The access list should look something like the following:
   
   Router2(config)#access-list 102 deny ip 192.168.1.128 0.0.0.127 host 192.168.3.2 log
   Router2(config)#access-list 102 permit ip any any

14. Apply this access list to outbound traffic on the serial 0 interface of Router2.
   
   Router2(config)#interface serial 0
   Router2(config-if)#ip access-group 102 out

15. To test this access list, try to ping PC 1 from PC 2 or PC 3. The pings should fail. You can also view the log file on Router2.
   C:>ping 192.168.3.2

Lab 33: Telnet

Objective: Learn to establish a Telnet session between two routers.

Lab Equipment: Router 1 and Router 2 from the eRouters menu

Note: The Simulator has limited Telnet support beyond the commands shown within this lab.

   1. Connect to Router 1, and set the host name to Router1. Then access the Telnet lines. Each line in a router represents an active Telnet session that the router can support. Routers in the Simulator support five Telnet lines, so use the line vty 0 4 command.
Router>enable
Router#conf t
Router(config)#hostname Router1
Router1(config)#line vty 0 4
Router1(config-line)#

2. Configure the router to require the use of a login password.
   Router1(config-line)#login

3. Configure boson as the password that will be used to establish a Telnet session.
   Router1(config-line)#password boson

4. Now, assign the IP address of 34.25.67.18 255.255.255.224 to Router1’s Ethernet 0 interface, and enable the interface.
   Router1(config-line)#exit
   Router1(config)#interface Ethernet 0
   Router1(config-if)#ip address 34.25.67.18 255.255.255.224
   Router1(config-if)#no shut

5. Next, connect to Router 2, set its host name to Router2, and then access its Ethernet 0 interface.
   Router>en
   Router#conf t
   Router(config)#hostname Router2
   Router2(config)#interface Ethernet 0
   Router2(config-if)#

6. Assign the IP address 34.25.67.2 255.255.255.224 to Router2’s Ethernet 0 interface, and enable the interface.
   Router2(config-if)#ip address 34.25.67.2 255.255.255.224
   Router2(config-if)#no shutdown
   Router2(config-if)#end

7. From Router2, telnet into Router1’s Ethernet 0 interface.
   Router2#telnet 34.25.67.18

8. You will be prompted for a password. Type the boson password, and press ENTER. You will see a dialog box informing you that NetSim provides limited support for Telnet. Notice that the router host name changes from Router2 to Router1, which indicates that you have established a Telnet session to Router1. Now, press the CTRL+SHIFT+6 key combination, then immediately press the X key. Notice that the host name changes back to Router2.
   Password:
   Router1> Press CTRL+SHIFT+6, then press X
   Router2#

9. Type the show sessions command to view all active Telnet sessions. To resume a Telnet session, specify the number of the session you would like to resume. In this case, there is only one Telnet session, so type the resume 1 command.
Router2#show sessions
Router2#resume 1
Router1#

10. Because you have telneted into Router1 again, the host name has changed to Router1 again. Press the CTRL+SHIFT+6 key combination followed by the X key to return to Router2.

Router1# Press CTRL+SHIFT+6, followed by X
Router2#

11. To disconnect the session, type the disconnect 1 command.
Router2#disconnect 1

Lab 34: VLANs

Objective: Become familiar with the benefits of VLANs on a LAN while using a Cisco Catalyst 1900 series switch.

Lab Equipment: Router 1 from the eRouters menu, Switch 1 from the eSwitches menu, and PC 1 and PC 2 from the eStations menu

In this lab, you are going to configure a router and a switch to support VLANs. First, you will set up PC 1 and PC 2 so that they can ping each other through the switch. You will then change the VLANs on the switch and observe that the PCs can no longer ping each other or the router. Next, you will change the configuration on the switch so that the PCs are on the same VLAN; they will then be able to ping each other again. You will configure the network to the specifications shown in the diagram below.

![Diagram of network configuration]
1. Connect to Router 1, assign it a host name of **Router1**, and configure the IP address of 24.17.2.1 255.255.255.0 on the Fast Ethernet 0/0 interface.
   
   ```
   Router>enable
   Router#conf t
   Router(config)#hostname Router1
   Router1(config)#interface Fast0/0
   Router1(config-if)#ip add 24.17.2.1 255.255.255.0
   Router1(config-if)#no shut
   ```

2. Connect to PC 1, and set the IP address to 24.17.2.3 255.255.255.0 with a default gateway of 24.17.2.1.
   
   ```
   C:>winipcfg
   ```

3. Connect to PC 2, and set the IP address to 24.17.2.4 255.255.255.0 with a default gateway of 24.17.2.1.
   
   ```
   C:>winipcfg
   ```

4. You should now be able to ping Router1 and PC 1 from PC 2.
   
   ```
   C:>ping 24.17.2.1
   C:>ping 24.17.2.3
   ```

5. Now, connect to Switch 1 and set up the VLANs. The switch automatically has VLAN 1 set up on all ports. In this case, you need to set up a separate VLAN for the PCs. Start by creating VLAN 22.
   
   ```
   >enable
   #config t
   (config)#vlan 22 name pcs
   ```

6. Now you need to assign the ports to the new VLAN. Start by assigning port 1 for PC 1 to VLAN 22.
   
   ```
   (config)#int e0/1
   (config-if)#vlan-membership static 22
   ```

7. Connect to PC 2 again, and try to ping Router1 and PC 1.
   
   ```
   C:>ping 24.17.2.1
   C:>ping 24.17.2.3
   ```

   Consider the result. You were able to ping from PC 2 to Router1, but not from PC 2 to PC 1. Why? On the switch, you set VLAN 22 to only cover port 1. That means ports 2 through 12 and the two Fast Ethernet ports were still on VLAN 1. So, when the ping packets came into the switch from PC 2, they were tagged with VLAN 1 and could only travel out of ports tagged with VLAN 1. (Although there are exceptions to this rule, they will not be covered in this lab manual.) Consequently, the ping packets could not go out port 1 to PC 1.

8. Connect to the switch again and configure port 2, which is where PC 2 is connected, to be included in VLAN 22.
   
   ```
   (config-if)#exit
   (config)#int e0/2
   (config-if)#vlan-membership static 22
   ```
9. Connect to PC 2 once again, and repeat the pings to Router1 and PC 1.
   C:>ping 24.17.2.1
   C:>ping 24.17.2.3

   What did you notice that was different? You should have been able to ping PC 1 but not Router 1. When the ping packets came in, they were tagged with VLAN 22. Consequently, the packets could only travel out port 1 to PC 1. This is what you wanted to accomplish.

10. Connect to the switch again, and view the VLAN port assignments by using the `show vlan` and `show vlan-membership` commands.

   (config-if)#end
   #show vlan
   #show vlan-membership

11. On the switch, assign FastEthernet 0/26 to VLAN 22. This will allow you to ping all devices.

   #conf t
   (config)#interface FastEthernet 0/26
   (config-if)#vlan-membership static 22

12. Send test pings from Router1 to PC 1 and PC 2, and from PC 1 and PC 2 to Router1.

   Router1#ping 24.17.2.3
   Router1#ping 24.17.2.4

   C:>ping 24.17.2.1
   C:>ping 24.17.2.1

---

**Lab 35: VTP**

**Objective:** Configure VLANs on Cisco Catalyst 2950 switches.

**Lab Equipment:** Switch 3 and Switch 4 from the eSwitches menu

**Goals:**

- Assign VLANs to multiple ports.
- Configure VLAN Trunking Protocol (VTP) to establish a server and client connection.
- Create a trunk line between the two switches to carry the VLANs.
- Test the configuration.

1. Start by assigning host names and IP addresses to Switch 3 and Switch 4 according to the table below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Switch 3</th>
<th>Switch 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Switch3</td>
<td>Switch4</td>
</tr>
<tr>
<td>IP Address (VLAN1)</td>
<td>10.1.1.1</td>
<td>10.1.1.2</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
Switch>enable
Switch#conf t
Switch(config)#hostname Switch3
Switch3(config)#interface vlan1
Switch3(config-if)#ip address 10.1.1.1 255.255.255.0
Switch3(config-if)#no shutdown
Switch3(config-if)#end
Switch3#

Switch>enable
Switch#conf t
Switch(config)#hostname Switch4
Switch4(config)#interface vlan1
Switch4(config-if)#ip address 10.1.1.2 255.255.255.0
Switch4(config-if)#no shutdown
Switch4(config-if)#end
Switch4#

2. Verify that the switches are connected to each other by pinging Switch3 from Switch4.
   Switch4#ping 10.1.1.1

3. Add VLAN 8 and VLAN 14 to Switch3, assign ports 2 through 5 to VLAN 8, and assign
   ports 6 through 10 to VLAN 14.
   Switch3#vlan database
   Switch3(vlan)#vlan 8
   Switch3(vlan)#vlan 14
   Switch3(vlan)#exit
   Switch3#conf t
   Switch3(config)#interface range fast0/2 – 5
   Switch3(config-if-range)#switchport access vlan 8
   Switch3(config-if-range)#exit
   Switch3(config)#interface range fast 0/6 – 10
   Switch3(config-if-range)#switchport access vlan 14
   Switch3(config-if-range)#exit
   Switch3(config)#exit

4. Use the show vlan command on Switch3 to verify that your configurations are correct.
   Switch3#show vlan

5. By default, a Catalyst switch is configured as a VTP server. Configure Switch3 as a VTP
   server, and configure Switch4 as a VTP client. Also, change the VTP domain to Boson
   and add a VTP password of rules.
   Switch3#vlan database
   Switch3(vlan)#vtp server
   Switch3(vlan)#vtp domain Boson
Switch3(vlan)#vtp password rules
Switch3(vlan)#exit
Switch3#

Switch4(vlan)#vtp client
Switch4(vlan)#vtp domain Boson
Switch4(vlan)#vtp password rules
Switch4(vlan)#exit
Switch4#

6. Next, create the trunk link that will transport the VLAN configurations from Switch3 to Switch4. To accomplish this, enable trunking on the port that links between the two switches. The encapsulation method will be 802.1q because that is the only supported encapsulation for the 2950 switch.

```
Switch3# conf t
Switch3(config)#interface fast 0/12
Switch3(config-if)#switchport mode trunk
Switch3(config-if)#end
```

```
Switch4#conf t
Switch4(config)#interface fast 0/12
Switch4(config-if)#switchport mode trunk
Switch4(config-if)#end
```

7. After this configuration, you should be able to view the VLANs from Switch3 on Switch4. To verify the VLAN configurations, use the `show vlan` command on Switch4. Also, the `show vtp status` command will display some VTP-specific information.

```
Switch4# show vlan
Switch4# show vtp status
```

Lab 36: OSPF Single Area Configuration and Testing

Objective: Configure Routers 1, 2, and 4 with IP addresses and the Open Shortest Path First (OSPF) Routing Protocol.

Lab Equipment: Router 1, Router 2, and Router 4 from the eRouters menu

Background Reading: Lab Primer Lesson 7: Routing Protocols

Goals:
- Set the host name, and bring up the interfaces.
- Configure the OSPF routing protocol.
- Select the directly connected networks.
- Display the routing table.
- Display the OSPF protocol information.
1. Configure Routers 1, 2, and 4 to the specifications outlined in the table and diagram below.

<table>
<thead>
<tr>
<th>Device</th>
<th>Router 1</th>
<th>Router 2</th>
<th>Router 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Router1</td>
<td>Router2</td>
<td>Router4</td>
</tr>
<tr>
<td>Ethernet 0</td>
<td>10.1.1.1 /24</td>
<td>10.1.1.2 /24</td>
<td>10.1.1.2 /24</td>
</tr>
<tr>
<td>Serial 0</td>
<td>172.16.10.1 /16</td>
<td>172.16.10.2 /16</td>
<td>172.16.10.2 /16</td>
</tr>
</tbody>
</table>

2. Verify that each router can ping its directly connected neighbors.
   - Router1#ping 10.1.1.2
   - Router1#ping 172.16.10.2
   - Router2#ping 10.1.1.1
   - Router4#ping 172.16.10.1

3. Add OSPF to Router1; use the Process ID number 100.
   - Router1#config terminal
   - Router1(config)#router ospf 100
   - Router1(config-router)#

4. Add the network(s) to which Router1 is directly connected.
   - Router1(config-router)#network 10.1.1.0 0.0.0.255 area 0
   - Router1(config-router)#network 172.16.0.0 0.0.255.255 area 0

5. Now, add OSPF to Router2.
   - Router2#config terminal
   - Router2(config)#router ospf 100
   - Router2(config-router)#

6. Add the network(s) to which Router2 is directly connected.
   - Router2(config-router)#network 10.1.1.0 0.0.0.255 area 0
   `Router4#configure terminal
   Router4(config)#router ospf 100
   Router4(config-router)#`

8. Add the network(s) to which Router4 is directly connected.
   `Router4(config-router)#network 172.16.0.0 0.0.255.255 area 0`

9. OSPF should now be running on all three routers. Press CTRL+Z to exit to privileged mode, and see if you can ping non-directly connected routers. From Router2, you should now be able to ping Router4’s serial 0 interface.
   `Router2#ping 172.16.10.2`

10. Next, connect to Router4 and ping Router2’s Ethernet 0 interface.
    `Router4#ping 10.1.1.2`

If you can ping both devices, then you have correctly configured routing. If you were not successful, trace back through the lab steps.

11. Now, display the routing table on Router2.
    `Router2#show ip route`

12. Display the specific IP routing protocol information on Router2.
    `Router2#show ip protocols`

13. Type the command that will display the OSPF database.
    `Router2#show ip ospf database`

14. Type the command that will display all of the OSPF neighbors.
    `Router2#show ip ospf neighbor`

15. Finally, type the command that will display all router interfaces that are running OSPF.
    `Router2#show ip ospf interface`
Lab 37: Implementing Network Address Translation Part I

Objective
Configure a simulated network to translate private IP addresses on the local area network (LAN) to public IP addresses by using Network Address Translation (NAT). After you have successfully completed the tasks in this lab, you should be able to communicate with an Internet host, which is configured with a public IP address, by using a PC, which is configured with a private IP address and is on the LAN.

Lab Topology
The simulated network topology consists of a LAN that is connected to the Internet via RouterA. All hosts on the LAN are configured with private IP addresses from the 192.168.100.0/24 network. The two PC hosts on the LAN are connected to SwitchA. SwitchA is also connected to the FastEthernet interface of RouterA. Interface Serial0/0 on RouterA is connected to the ISP router, which in turn provides access to the Internet. The diagram below represents this topology.
Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list nnn permit x.x.x.x.y.y.y</td>
<td>defines access list; permits all IP addresses on network x.x.x.x with mask y.y.y</td>
</tr>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>interface fastethernet slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>interface serial slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>ip nat inside</td>
<td>sets an interface to be an inside interface</td>
</tr>
<tr>
<td>ip nat inside source list access_list pool name</td>
<td>translates anything that matches the access list to an address from the pool</td>
</tr>
<tr>
<td>ip nat outside</td>
<td>sets an interface to be an outside interface</td>
</tr>
<tr>
<td>ip nat pool name start_address end_address netmask subnet_mask</td>
<td>creates an address pool</td>
</tr>
<tr>
<td>ip route ip_address subnet_mask next_hop_ip</td>
<td>forwards all traffic destined to ip_address subnet_mask to next_hop_ip</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>sends an ICMP echo request to the specified address</td>
</tr>
<tr>
<td>pool {ip address pool}</td>
<td>names a NAT pool</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show ip route</td>
<td>displays the IP routing table</td>
</tr>
<tr>
<td>source list {access-list}</td>
<td>names an access list that must be matched before address translation can occur</td>
</tr>
</tbody>
</table>

Lab Tasks

Task 1: Load the Lab 37 Initial Network Configuration

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator. The initial configuration will assign the correct host names and IP addresses to each device. Your objective is to properly configure NAT to allow hosts on the private LAN to access Internet hosts.

Task 2: Examine the Initial Network Configuration

A. Verify IP address assignments
1. Do the IP addresses assigned to all devices match the values shown in the network topology diagram? _________________________________________________
2. What is a private IP address? ___________________________________________
3. Which devices in the simulated network topology have private IP addresses? _________

_______________________________________________________________
4. What is a public IP address? __________________________________________

5. Which devices in the simulated network topology have public IP addresses? ______

6. Why would you want to assign private IP addresses to the LAN in the simulated network?

B. Test network connectivity

1. From the console of PC1, are you able to ping the Internet Web server? Why or why not?

2. From the console of RouterA, are you able to ping the Internet Web server? Why or why not?

Task 3: Plan for NAT

A. Network requirements

1. You should allow for four hosts on the private LAN to use NAT to reach Internet hosts.

2. Only hosts in the 192.168.100.128/30 network should be allowed to use NAT. Given that the LAN uses the 192.168.100.0/24 network, what range of IP addresses should be allowed to use NAT? ________________________________________

What range of IP addresses should not be allowed to use NAT? ___________________

3. Given the address ranges that should and should not be allowed to use NAT, which PC host(s) on the network should be able to use NAT? ____________________________

Which PC host(s) on the network should not be able to use NAT? ________________

Task 4: Implement NAT

A. Identify devices for NAT

1. Which device in the simulated network should perform NAT? __________________________

Why? ____________________________________________

2. Which interfaces on this device will be involved in implementing NAT? ______________

3. Which interface connects to the private network? ____________________________

What type of NAT interface is this? ____________________________

4. What command should you use to properly configure this interface for NAT? __________

Enter this command into the running configuration of the appropriate device.

5. Which interface connects to the public network? ____________________________

What type of NAT interface is this? ____________________________

6. What IOS command should you use to properly configure this interface for NAT? ______

Enter this command into the running configuration of the appropriate device.
B. Allocate public IP addresses for use by hosts on the private LAN

1. The following IP address range is available for hosts on the private LAN to use when communicating with hosts on the public Internet: 200.152.100.65 through 200.152.100.70.

2. Given the IP address range above, what command should you use to properly configure NAT when translating private LAN addresses to public Internet addresses on RouterA? This command should allocate a pool of addresses that internal hosts with private IP addresses will use when communicating with Internet hosts. When you create this pool, name it small-pool.

   ________________________________________________________________
   Enter this command into the running configuration of the device that you selected to perform NAT.

C. Determine which hosts on the LAN can use NAT

1. The simulated private LAN uses the 192.168.100.0/24 network. However, only hosts with IP addresses in the range from 192.168.100.128 through 192.168.100.131 should be able to access the Internet by using NAT.

2. Based on the range requirement above, should PC1 be able to access the Internet by using NAT? Why or why not? ______________________________________

   ________________________________________________________________

3. Based on the range requirement above, should PC2 be able to access the Internet by using NAT? Why or why not? ______________________________________

   ________________________________________________________________

4. Write a standard access list that will cover the host range from 192.168.100.128 through 192.168.100.131 on RouterA. ______________________________________

   Enter this command into the running configuration of the device that you selected to perform NAT.

D. Configure a device to perform NAT

1. You have already entered a number of configuration commands on the selected device that are required in order for NAT to function correctly. However, while these commands support NAT, they do not cause the device to actually begin the address translation process.

2. The following command on RouterA actually begins the translation process.

   ip nat inside source list {access-list} pool {ip address pool}

   The individual parts of this command perform the following functions:

   - **ip nat** — begins the process of configuring NAT
   - **inside** — specifies that the traffic received on the inside interface should be address-translated when it passes out through the outside interface
   - **source list (access-list)** — names an access list that must be matched before address translation can occur; this determines which hosts on the private network will have their addresses translated and which will not
   - **pool {ip address pool}** — names a NAT pool, which in this case is a pool of public IP addresses that will be used by hosts on the private LAN when they communicate with hosts
What command should you use to actually begin the address translation process? Use your access-list number and pool name where appropriate. _____________________
Enter this command into the running configuration of the device that you selected to perform NAT.

Task 5: Verify NAT

A. Verify the routing process

1. Is it now possible for hosts on the private LAN to communicate with Internet hosts? Why or why not? ________________________________

2. How did you determine this? ________________________________

3. If hosts on the private LAN cannot communicate with Internet hosts, what command should you use to enable them to communicate? ________________________________
Enter this command into the running configuration of the appropriate device.

B. Verify NAT

1. If you have successfully completed all of the previous lab tasks, NAT should be completely configured and operational on the simulated network. You should now verify that NAT is functioning correctly.

2. Which host on the simulated LAN should be able to communicate with Internet hosts by using NAT? ________________________________
   Try to ping the Internet Web server from the console of this host. Is the ping successful? ________________________________
   If not, review and correct your configuration.

3. Which host on the simulated LAN should not be able to communicate with Internet hosts by using NAT? ________________________________
   Try to ping the Internet Web server from the console of this host. Is the ping successful? ________________________________
   If so, review and correct your configuration.

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Verify IP address assignments

1. Yes, the IP addresses assigned in the initial lab configuration match the values shown in the network topology diagram.

2. Private IP addresses, as defined by RFC 1918, are IP addresses that are used by networks
that are not directly connected to the public Internet. This RFC designates Class A, Class B, and Class C private address blocks that are available for organizations to assign to their internal networks. The simulated network in this lab uses the private 192.168.100.0/24 Class C network. To allow hosts on private networks to access the public Internet, NAT must be used. Private IP addresses are not routable on the public Internet and are usually filtered by Internet service providers (ISPs). It is also a good practice for operators of private networks that connect to the Internet to use filters at their network edge to prevent any privately addressed IP traffic from exiting their network.

3. PC1, PC2, and the FastEthernet0/0 interface of RouterA make up the simulated LAN and are all configured with private IP addresses from the 192.168.100.0/24 RFC 1918 Class C network. SwitchA is also part of the private LAN but is not configured for IP, so it acts only as a Layer-2 device and is transparent to IP.

4. A public IP address is routable across the public Internet. The Internet Assigned Numbers Authority (IANA) is the organization that is responsible for assigning IP addresses on the public Internet. IANA delegates this task to regional registries such as the American Registry for Internet Numbers (ARIN), which is responsible for the assignment of IP addresses in North America.

5. The Serial0/0 interface of RouterA, all interfaces of the ISP router, and the Internet Web server are configured with public IP addresses.

6. The primary benefit that results from the use of private IP addresses on privately operated networks is the conservation of the public IP address space. The public IP address space is finite and would have been exhausted long ago without the widespread adoption of private IP addressing of privately operated networks. In a typical private network, it is possible for hundreds of hosts with private IP addresses to access the public Internet using a few or even a single public IP address.

B. Test network connectivity

1. No, a ping from the console of PC1 to the Internet Web server is not successful. PC1 is configured with a private IP address and the Internet Web server is configured with a public IP address. In this network, there is presently no process in place to translate private IP addresses to public IP addresses.

2. No, a ping from the console of RouterA to the Internet Web server is not successful. RouterA has no knowledge of the 25.16.59.0 network; therefore, it cannot move traffic to the Internet Web server at 25.16.59.2.

Task 3: Plan for NAT

A. Network Requirements

1. No answer required.

2. Hosts in the range of 192.168.100.128 through 192.168.100.131 should be allowed to use NAT. No other hosts in the 192.168.100.0/24 network should be allowed to use NAT.

3. PC1, which has an IP address of 192.168.100.2, should not be allowed to use NAT. PC2, which has an IP address of 192.168.100.129, should be allowed to use NAT.
Task 4: Implement NAT

A. Identify devices for NAT
1. RouterA should perform the NAT function in the simulated network, because it has one interface connected to the private LAN and another interface connected to the ISP router. Since RouterA is at the boundary between the public and private networks, it is the device that should perform NAT.
2. Interfaces Serial0/0 and FastEthernet0/0 will be involved in implementing NAT.
3. FastEthernet0/0 on RouterA connects to the private LAN. In Cisco NAT terminology, this is known as the inside interface.
4. You should use the following commands to properly configure RouterA for NAT.
   ```
   config t
   interface FastEthernet0/0
   ip nat inside
   ```
5. Serial0/0 on RouterA connects to the public Internet via the ISP router. In Cisco NAT terminology, this is known as the outside interface.
6. You should use the following commands to properly configure RouterA for NAT.
   ```
   config t
   interface Serial0/0
   ip nat outside
   ```

B. Allocate public IP addresses for use by hosts on the private LAN
1. No answer required.
2. You should use the following commands to properly configure NAT when translating private LAN addresses to public Internet addresses.
   ```
   config t
   ip nat pool small-pool 200.152.100.65 200.152.100.70 netmask 255.255.255.252
   ```

C. Determine which hosts on the LAN can use NAT
1. No answer required.
2. No, PC1 should not be able to access the Internet by using NAT, because it is configured with an IP address of 192.168.100.2, which does not fall within the allowed IP address range (192.168.100.128 – 192.168.100.131) for NAT.
3. Yes, PC2 should be able to access the Internet by using NAT, because it is configured with an IP address of 192.168.100.129, which falls within the allowed IP address range (192.168.100.128 – 192.168.100.131) for NAT.
4. You should use the following access list to cover the host range of 192.168.100.128 through 192.168.100.131.
   ```
   config t
   access-list 1 permit 192.168.100.128 0.0.0.3
   ```
D. Configure a device to perform NAT
1. No answer required.
2. You should use the following command to begin the address translation process.
   ip nat inside source list 1 pool small-pool

Task 5: Verify NAT

A. Verify the routing process
1. No, it is not possible for hosts on the private LAN to communicate with Internet hosts, because RouterA is not configured with a default route to direct Internet traffic out Serial0/0 to the ISP router.
2. Issuing the `show ip route` command on RouterA reveals that RouterA knows only about its directly connected networks.
3. You should use the following command on RouterA to direct non-local traffic to the ISP router.
   ip route 0.0.0.0 0.0.0.0 200.152.200.1

B. Verify NAT
1. No answer required.
2. PC2 should be able to communicate with Internet hosts by using NAT. Yes, a ping to the Internet Web server from the console of PC2 is successful.
3. PC1 should not be able to communicate with Internet hosts by using NAT. No, a ping to the Internet Web server from the console of PC1 is not successful.
Sample Configuration Script

```
RouterA

! Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
enable secret cisco
!
ip subnet-zero
!
interface Serial0/0
ip address 200.152.200.2 255.255.255.252
no ip directed-broadcast
ip nat outside
!
interface FastEthernet0/0
ip address 192.168.100.1 255.255.255.0
no ip directed-broadcast
ip nat inside
!
interface FastEthernet0/1
no ip address
no ip directed-broadcast
shutdown
!
ip nat inside source list 1 pool small-pool
ip nat pool small-pool 200.152.100.65 200.152.100.70 netmask 255.255.255.252
!
ip classless
no ip http server
!
ip route 0.0.0.0 0.0.0.0 200.152.200.1
access-list 1 permit 192.168.100.128 0.0.0.3
!
line con 0
transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```
Lab 38: Implementing Network Address Translation Part II

Objective

Configure a simulated network to translate public IP addresses on the wide area network (WAN) to private IP addresses by using Network Address Translation (NAT). After you have successfully completed the tasks in this lab, Internet hosts should be able to communicate with the Web server in the demilitarized zone (DMZ). Users on the private, or inside, network should also be able to access the Internet. Your NAT implementation should minimize the number of public IP addresses used by hosts on the private network when accessing the Internet.

Lab Topology

The simulated network topology consists of a local area network (LAN) that is connected to RouterA. RouterA connects to RouterB. The network between RouterA and RouterB is used as a DMZ to which the Web server is connected. RouterB connects to the Internet via the ISP router. The diagram below represents this topology.
Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access list $nnn$ permit $x.x.x.y.y.y$</td>
<td>defines access list; permits all IP addresses on network $x.x.x$ with mask $y.y.y$</td>
</tr>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>interface fastethernet $slot/port$</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>interface serial $slot/port$</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>ip nat inside</td>
<td>sets an interface to be an inside interface</td>
</tr>
<tr>
<td>ip nat inside source list $nnn$ interface $interface_number$ overload</td>
<td>translates anything that matches the access list to the address of the specified interface</td>
</tr>
<tr>
<td>ip nat inside source static $x.x.x.y.y.y$</td>
<td>statically translates address $x.x.x$ to address $y.y.y$</td>
</tr>
<tr>
<td>ip nat outside</td>
<td>sets an interface to be an outside interface</td>
</tr>
<tr>
<td>ping $ip_address$</td>
<td>enters VLAN database configuration mode</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
</tbody>
</table>

Lab Tasks

Task 1: Load the Lab 38 Initial Network Configuration

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator. The initial configuration will assign the correct host names and IP addresses to each device. Your objective is to properly configure NAT to allow hosts on the Internet to access the Web server in the DMZ and to also allow private LAN hosts to use NAT to access the Internet.

Task 2: Examine the Initial Network Configuration

A. Verify IP address assignments

1. Do the IP addresses assigned to all devices match the values shown in the network topology diagram? __________________________________________

2. What is a DMZ, and what is its purpose when designing a network topology? __________

3. Which hosts and router interfaces in the simulated network have public IP addresses? __________________________________________

4. Which hosts and router interfaces in the simulated network have private IP addresses? __________________________________________

B. Test Network Connectivity

1. From the console of Int_host, are you able to ping SRV001? Why or why not? __________
2. From the console of PC2, are you able to ping Int_host? Why or why not? ________________

Task 3: Plan for NAT

A. Network requirements
1. All hosts on the private LAN should be able to use Dynamic NAT to reach Internet hosts.
2. SRV001 in the DMZ should be accessible to Int_host by using Static NAT. Internet hosts should be able to reach SRV001 by using the public IP address 200.5.22.21.

Task 4: Implement NAT

A. Implement Static NAT
1. Review the network topology diagram. Which device should be configured for Static NAT?

2. The router interface that connects to the private network is called the inside interface in NAT terminology. The router interface that connects to the public network is called the outside interface. What commands should you use to configure the interfaces for NAT?

Enter these commands into the running configuration of the device you selected to perform Static NAT.

3. Static NAT is most often used when you want to make a host on a privately addressed internal network appear as if it is connected directly to the Internet with a public IP address. SRV001 is configured with the private IP address 192.168.101.3 in the simulated network. What command should you use to allow SRV001 to be accessed by using the public IP address 200.5.22.21?

Enter this command into the running configuration of the device you selected to perform Static NAT.

B. Implement Dynamic NAT
1. Review the network topology diagram. Which device should be configured for Dynamic NAT?

2. Which hosts on the private LAN should use NAT? ______________________

3. What command should you use to create an access list that matches the IP addresses of all the hosts that should be able to use Dynamic NAT?

Enter this command into the running configuration of the device you selected to perform Dynamic NAT.

4. To allow hosts on the private LAN to access the Internet, you will need to configure NAT to reference the access list you previously created. Your implementation of Dynamic NAT should use a single public IP address and share it among all hosts on the private LAN. What command should you use to enable NAT?

Enter this command into the running configuration of the device you selected to perform Dynamic NAT.
Task 5: Verify NAT

A. Verify Static NAT
1. Log on to the console of Int_host, and attempt to ping the public IP address that you assigned to SRV001 by using Static NAT. What ping command did you use? __________
   Was this ping successful? Why or why not? _________________________________
   If not, review and correct your configuration.
2. Briefly explain how Static NAT is able to allow a privately addressed host on the inside network to be reachable via a public IP address on the outside network. ________________

B. Verify Dynamic NAT
1. Log on to the consoles of PC1 and PC2, and attempt to ping the public IP address assigned to Int_host. What ping command did you use? ________________
   Was this ping successful? Why or why not? _________________________________
   If not, review and correct your configuration.
2. Briefly explain how Dynamic NAT allows multiple hosts on the private network to communicate with the Internet by using a single public IP address. ________________

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Verify IP address assignments
1. Yes, all assigned IP addresses match the values shown in the network topology diagram.
2. A network demilitarized zone (DMZ) is a network located between the private network, which is called the inside network in NAT terminology, and the external network. The external network is usually the Internet and is called the outside network in NAT terminology. The DMZ boundaries are created by connecting two routers or firewalls to the DMZ, one facing the private network and the other facing the external network. The DMZ is most often used to contain hosts that will provide externally accessible services such as Web servers and e-mail servers. The DMZ serves two primary purposes: to protect hosts connected to the DMZ from external attacks launched from the Internet, and to protect hosts on the internal network from servers in the DMZ in the event that the servers in the DMZ are compromised.
3. The following hosts and router interfaces are configured with public IP addresses:
   - Int_host
   - Serial0 on the ISP Router
   - FastEthernet0/0 on the ISP Router
   - Serial0 on RouterB
4. The following hosts and router interfaces are configured with private IP addresses:
   - FastEthernet0/0 on RouterB
   - SRV001
   - FastEthernet0/0 on RouterA
   - FastEthernet0/1 on RouterA
   - PC1
   - PC2

B. Test network connectivity
1. No, a ping to SRV001 from the console of Int_host is not successful. In the initial configuration, SRV001 is only reachable via its private IP address of 192.168.101.3, because Static NAT has not yet been configured. When a ping to 192.168.101.3 is issued from the console of Int_host, Int_host forwards this traffic to its default gateway, the ISP router. The ISP router does not have a route to the 192.168.101.0 private network; consequently, it drops the packet.

2. No, a ping to Int_host from the console of PC2 is not successful. When the ping command to 200.2.2.2, the IP address of Int_host, is issued from the console of PC2, PC2 forwards this traffic per its default route to RouterA. RouterA does not have a route to the 200.2.2.0 network; therefore, it forwards the traffic per its default route to RouterB. RouterB does not have a route to 200.2.2.0, so it forwards the traffic per its default route to the ISP router. The ISP router has 200.2.2.0 as one of its directly connected networks and can therefore deliver the packet to its destination, which is Int_host.

Upon receiving the ping packet from PC2, Int_host prepares to reply to the ping by examining the source IP address in the ping packet that it received from PC2. Int_host determines that the ping reply should be sent to 192.168.100.3, which is the IP address of PC2. Int_host forwards this traffic to its default gateway, which is the ISP router. The ISP router does not have a route to the 192.168.100.0 private network; consequently, it drops the packet and the ping fails.

Task 4: Implement NAT
A. Implement Static NAT
1. You should configure RouterB for Static NAT. To support NAT, the router must have one interface connected to the private, or inside, network and another interface connected to the public, or outside, network. RouterB is the only router in the simulated network topology that meets this requirement.

2. You should use the following commands on RouterB to configure the interface for NAT.
   ```
   config t
   interface FastEthernet0/0
   ip nat inside
   interface Serial0
   ip nat outside
   ```

3. You should use the following command on RouterB to allow SRV001 to be accessed by using the public IP address.
   ```
   ip nat inside source static 192.168.101.3 200.5.22.21
   ```
B. Implement Dynamic NAT

1. You should configure RouterB for Dynamic NAT. NAT must always be configured on a router that has one interface connected to the inside network and another interface connected to the outside network.

2. RouterB on the private LAN should use NAT.

3. You should use the following access list to match the IP addresses of all the hosts that should be able to use NAT.

   \texttt{access-list 1 permit 192.168.100.0 0.0.0.255}

4. You should use the following command to enable NAT.

   \texttt{ip nat inside source list 1 interface serial0 overload}

Task 5: Verify NAT

A. Verify Static NAT

1. You should use the following command on Int_host.

   \texttt{ping 200.5.22.21}

   Yes, the ping to SRV001 at 200.5.22.21 is successful, because Static NAT is translating the public IP address 200.5.22.21 to the private IP address assigned to SRV001.

2. Network Address Translation (NAT) is used to perform address translation between two networks, which are identified as the \texttt{inside} network and the \texttt{outside} network in NAT terminology. NAT is configured on a router that has one interface, which connects to the inside network, and another interface, which connects to the outside network.

   Static NAT is used to allow a host that is connected to a private network and configured with a private IP address to be reachable from an external network such as the Internet. NAT associates a public IP address with the internal host’s private IP address and sends inbound packets addressed to the public IP address to the host’s private IP address.

   In this lab exercise, the FastEthernet0/0 interface on RouterB is configured as the inside interface, because it connects to the privately addressed internal LAN. Serial0 is configured as the outside interface, because it connects to the Internet via the ISP router. The \texttt{ip nat inside source static 192.168.101.3 200.5.22.21} command causes any traffic addressed to 200.5.22.21 to be delivered to 192.168.101.3 instead.

B. Verify Dynamic NAT

1. You should use the following command on PC1 and PC2.

   \texttt{ping 200.2.2.2}

   Yes, the ping to Int_host at 200.2.2.2 is successful, because Dynamic NAT translates the source address of the packets addressed to 200.2.2.2 to 52.2.2.2, the public IP address assigned to Serial0. The \texttt{overload} keyword causes traffic from all hosts on the private network to carry the source IP address of Serial0. When Int_host (200.2.2.2) replies to the ping, it sends its reply to 52.2.2.2, which is a public IP address that can be routed across the Internet. When the reply traffic arrives at Serial0 on RouterB, NAT translates the destination IP address to the private IP address of the PC that initiated the ping.
2. Dynamic NAT is most often used to allow privately addressed hosts on an internal network to access hosts on an external network such as the Internet. In this lab exercise, FastEthernet0/0 on RouterB is configured as the inside interface, because it connects to the private LAN. Serial0 on RouterB is configured as the outside interface, because it connects to the external network, which is the Internet in this scenario.

When hosts on the private LAN send packets addressed to Internet hosts, these packets are sent to the default gateway, which is RouterA, and then on to RouterB for routing to the Internet. The `ip nat inside source list 1 interface serial0 overload` configuration command on RouterB causes packets that match the access-list to have their source address in the IP header to be rewritten with the public IP address assigned to Serial0. Routers configured with Dynamic NAT maintain a dynamic translation table to keep track of which internal hosts have sent traffic to which external hosts. This table is used to ensure that return traffic from the external hosts can be delivered to the internal host that initiated the connection.
Sample Configuration Script

```plaintext
! Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
enable secret cisco
!
ip subnet-zero
!
interface Serial0
ip address 52.2.2.2 255.255.255.252
no ip directed-broadcast
ip nat outside
!
interface FastEthernet0/0
ip address 192.168.101.2 255.255.255.0
no ip directed-broadcast
ip nat inside
!
interface FastEthernet0/1
no ip address
no ip directed-broadcast
shutdown
!
routing rip
   network 192.168.101.0
!
ip nat inside source static 192.168.101.3 200.5.22.21
ip nat inside source list 1 interface serial0 overload
ip classless
no ip http server
!
ip route 0.0.0.0 0.0.0.0 52.2.2.1
access-list 1 permit 192.168.100.0 0.0.0.255
!
line con 0
   transport input none
line aux 0
line vty 0 4
!
o no scheduler allocate
end
```
Lab 39: Basic Switch Configuration

Objective
A new switch has been added to the local area network (LAN). In addition to the default management virtual LAN (VLAN), two other VLANs, EVEN and ODD, are in use. First you must configure the IP address and default gateway on Switch2. Next you will determine the VLAN Trunk Protocol (VTP) domain in use, and join Switch2 as a client to that VTP domain. Finally you will configure the port connected to PC3 so that it is in VLAN ODD, and configure the port connected to PC4 so that it is in VLAN EVEN. Only Switch2 needs to be configured. All other devices in the simulated network topology have been configured correctly. All configuration passwords have been set to “cisco”.

Lab Topology
The simulated network topology consists of two switches, Switch1 and Switch2. Each switch has two PC hosts connected. Switch1 is connected to Router1. You will not be configuring Router1 in this lab. The diagram below represents this topology.
# Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp neighbor detail [detail]</td>
<td>displays the cdp neighbor entries</td>
</tr>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>interface fastethernet slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>interface vlan vlan_id</td>
<td>enters interface configuration mode, and enters the VLAN to which the IP information is assigned</td>
</tr>
<tr>
<td>ip address ip_address</td>
<td>assigns an IP address to an interface</td>
</tr>
<tr>
<td>ip default-gateway ip_address</td>
<td>configures a default gateway IP address to which traffic destined to remote networks will be forwarded</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>sends an ICMP echo request to the specified address</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show running-configuration</td>
<td>displays the active configuration</td>
</tr>
<tr>
<td>show vlan</td>
<td>displays VLAN information</td>
</tr>
<tr>
<td>show vtp status</td>
<td>displays VTP configuration</td>
</tr>
<tr>
<td>switchport access vlan vlan_id</td>
<td>assigns the default VLAN for a port</td>
</tr>
<tr>
<td>switchport mode access</td>
<td>configures a switchport as an access port, which is used to connect to an end node such as a computer or printer</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>configures a switchport as a trunk port which should only be connected to a trunk port on another router or switch in order to carry traffic from multiple VLANs</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>starts the terminal emulation program from a PC, router, or switch that permits you to access devices remotely over the network</td>
</tr>
<tr>
<td>vtp domain domain_name</td>
<td>assigns the domain name for VTP</td>
</tr>
<tr>
<td>vtp mode {client</td>
<td>server</td>
</tr>
<tr>
<td>vtp password password</td>
<td>assigns the VTP password; switches must be configured with the same VTP domain and VTP password in order for VTP to propagate VLAN information between the switches</td>
</tr>
</tbody>
</table>

# Lab Tasks

**Task 1: Load the Lab 39 Initial Network Configuration**

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator.
Task 2: Examine the Initial Network Configuration

A. Examine the current VTP configuration on Switch2

1. The VLAN Trunk Protocol (VTP) allows switches to exchange information about VLANs. This reduces administrative effort, because VLANs created on one switch can be automatically learned by other switches in the VTP domain.

2. From the console of Switch2, what command should you use to determine the VLANs that exist on Switch2?

3. What VLANs currently exist on Switch2?

4. Do VLAN ODD and VLAN EVEN exist on Switch2?
   If these VLANs do not exist on Switch2, briefly explain why this is the case.

5. What command should you use to determine the VTP domain and VTP mode currently configured on Switch2?
   Enter this command into the running configuration of Switch2.
   What VTP domain and VTP mode are currently configured on Switch2?

B. Test for network connectivity between Switch1 and Switch2

1. Later in this lab, you will examine the VTP configuration on Switch1. Currently, your only access to this simulated network is from the console of Switch2. In other words, you do not have direct access to the console of Switch1. If you want to interact with Switch1, what should you do?

2. You should test basic connectivity between two devices before attempting to use any commands that require network connectivity. The `ping` command is useful for this purpose. In order to attempt a ping to Switch1 from Switch2, you must first know the IP address assigned to Switch1. What command should you use to determine the IP address of Switch1 given that your only access is to the console of Switch2?

3. What is the IP address assigned to Switch1?

4. Try to ping Switch1 from the console of Switch2. Is the ping successful? If not, why did the ping fail?

Task 3: Configure VTP to Propagate VLAN Configuration

A. Configure the management VLAN on Switch2

1. Before a switch can successfully execute commands that require Layer 3 connectivity, such as `ping` and `telnet`, the switch must have at least one interface configured with an IP address. What command should you use to determine if any interfaces on Switch2 are configured with IP addresses?
   Does Switch2 currently have any interfaces configured with IP addresses?

2. By default, all switchports are placed in VLAN 1. What commands should you use to create an interface for the default VLAN on Switch1 and assign the IP address 192.168.100.3 to this interface? You should use a 24-bit mask.
   Enter these commands into the running configuration of Switch2.
3. Switch2 now has an interface configured for IP. Try to ping the IP address of Switch1 again. Is the ping successful? __________________________________________
   Why is the ping successful now when it failed earlier? ________________________

4. Now that you have configured a VLAN interface on Switch2, Switch2 can function as a Layer 3 network node. You can now issue commands on Switch2 that require IP connectivity, such as the ping and telnet commands. In order for Switch2 to communicate with networks that are not directly connected, Switch2, similar to any other Layer 3 network node such as a desktop PC, should be configured with a default gateway.

5. Refer to the command summary; what command should you use to configure a default gateway on Switch2? Configure Switch2 with a default gateway IP address of 192.168.100.1. __________________________________________________________
   Enter this command into the running configuration of Switch2.

6. Switch2 will now be able to forward any non-local IP traffic to the default gateway; the traffic will then be routed to the appropriate remote network.

B. Examine the current VTP configuration on Switch1

1. Examine the VTP configuration on Switch1. Your only access to the network is from the console of Switch2. The console password on Switch1 is “Oldsmar” and the enable secret on Switch1 is “cisco”. What command should you use to access the console of Switch1 from the console of Switch2? ______________________________________

2. Now that you have access to the console of Switch1, what command should you use to determine the VTP domain and VTP mode for Switch1? _________________________
   What is the VTP domain that is currently configured on Switch1? ________________
   What is the VTP mode that is currently configured on Switch1? _________________

C. Configure VTP on Switch2

1. Switch1 is currently configured as a VTP server. What command should you use to configure Switch2 as a VTP client?
   Enter this command into the running configuration of Switch2.

2. In order for VTP to propagate the VLAN configuration on Switch1 to Switch2, Switch1 and Switch2 must be part of the same VTP domain. Examine Switch1; are Switch1 and Switch2 currently in the same VTP domain? ______________________________________

3. What command should you use to configure Switch2 for membership in the same VTP domain as Switch1? ________________________________
   Enter this command into the running configuration of Switch2.

4. What command should you use to check for a VTP password on Switch1? ________________
   Verify that a VTP password has been configured on Switch1. The same VTP password should also be configured on Switch2.

5. Was a VTP password configured on Switch1? If so, what command should you use to configure this same VTP password on Switch2? ________________________________
   Enter this command into the running configuration of Switch2.
Task 4: Verify VTP

A. Verify the proper operation of VTP
1. What commands should you use to list the VLANs that currently exist on Switch2? __________
   Enter these commands at the console of Switch2.
2. Do the ODD and EVEN VLANs appear on Switch2? __________________________
   If so, why do they appear now when they were missing earlier? ___________________

Task 5: Configure VLAN Trunking

A. Test for connectivity between the switches
1. What commands should you use to examine the running configuration of Switch1?
   Remember that your only access to the network is from the console of Switch2. __________

2. Examine the running configuration of Switch1; to which VLAN does the switchport that
   connects to PC1 belong? ____________________________
   To which VLAN does the switchport that connects to PC2 belong? _______________________
3. Review the objectives at the beginning of this lab. You have been instructed to configure
   the VLAN membership for the switchports to which PC3 and PC4 connect. What statement
   can you make about the VLAN membership of the switchports for PC1 and PC3? _________
   What statement can you make about the VLAN membership of the switchports for PC2 and
   PC4? __________________________
4. Log on to the console of PC1, and attempt to ping PC3. Is the ping successful? Why or why
   not? ______________________________________
5. Log on to the console of PC2, and attempt to ping PC4. Is the ping successful? Why or why
   not? ______________________________________

B. Configure VLANs on Switch1 and Switch2
1. VLANs are virtual LANs that exist on the same switch. When VLANs are configured on a
   switch, each VLAN behaves as a separate, isolated LAN. Often in larger switched networks
   consisting of multiple switches, you may want the VLANs to span multiple switches. In
   other words, you may want to configure several VLANs on two switches (SwitchA and
   SwitchB, for example) and ensure that the hosts, which are connected to the same VLANs,
   can communicate with each other even though they are connected to different physical
   switches. In order to accomplish this, you should configure a VLAN trunk between the
   switches. In order to do this, you should connect an unused switchport on SwitchA to an
   unused switchport on SwitchB and configure the two ports; thus they will be connected as
   trunk ports.
2. Examine the network topology diagram. To which switchport is PC3 on Switch2 connected?
   To which switchport is PC4 on Switch2 connected? ____________________________
3. Refer to the objectives at the beginning of this lab. Which VLAN should the switchport to which PC3 connects be made a member of? ________________________________  
Which VLAN should the switchport to which PC4 connects be made a member of? ______

4. What commands should you use to place the switchports to which PC3 and PC4 connect into the appropriate VLANs? Make sure that you configure both of these ports as access ports. An access port is used to connect an end-station node such as a PC host or a printer. _________________________________________________________

Enter these commands into the running configuration of Switch2.

5. PC1 on Switch1 and PC3 on Switch2 are now in the same VLAN. Log on to the console of PC1, and attempt to ping PC3. Is the ping successful? Why or why not? ________________

C. Configure VLAN trunking between Switch1 and Switch2

1. Even though VLANs with the same VLAN ID exist on both Switch1 and Switch2, hosts in the same VLANs on different switches cannot yet communicate with each other, because a VLAN trunk between Switch1 and Switch2 has not yet been configured.

2. Examine the network topology diagram. Which switchport on Switch1 should be configured as a trunk port? ________________________________  
Which switchport on Switch2 should be configured as a trunk port? ________________

3. The appropriate switchport on Switch1 is already configured as a trunk port. What commands should you use to examine the running configuration of Switch1 to verify this? Remember that your only access to the network is from the console of Switch2. ________

4. What command should you use to configure the appropriate switchport on Switch2 for trunking? _________________________________________________________

Enter this command into the running configuration of Switch2.

D. Verify VLAN Trunking

1. Log on to the console of PC1, and attempt to ping PC3. Is the ping successful? If so, why is it successful now when it failed earlier? ________________________________

2. Log on to the console of PC2, and attempt to ping PC4. Is the ping successful? If so, why is it successful now when it failed earlier? ________________________________

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Examine the current VTP configuration on Switch2

1. No answer required.

2. You should use the `show vlan` command to determine the VLANs that exist on Switch2.
3. The following VLAN IDs exist on Switch2:
   1, 1002, 1003, 1004, and 1005

   These VLANs are created by default and do not include any VLANs specific to this lab.

4. No, VLAN ODD (VLAN 11) and VLAN EVEN (VLAN 22) do not currently exist on Switch2. They have not been created manually, nor have they been automatically learned via VTP, because VTP has not yet been configured on Switch2.

5. You should use the `show vtp status` command to determine the VTP domain and VTP mode currently configured on Switch2.

B. Test for network connectivity between Switch1 and Switch2

1. You should use the `telnet` command to open a virtual console session on Switch1 from the console of Switch2.

2. You should use the `show cdp neighbors detail` command on the console of Switch2 to receive a list of directly connected devices and the IP address of each device.

3. The IP address assigned to Switch1 is 192.168.100.2.

4. No, the `ping 192.168.100.2` command entered from the console of Switch2 fails, because Switch2 does not have an interface configured for IP.

Task 3: Configure VTP to Propagate VLAN Configuration

A. Configure the management VLAN on Switch2

1. You should use the `show ip interface brief` command to determine if any interfaces on Switch2 are configured for IP.

   No, Switch2 does not currently have any interfaces configured for IP.

2. You should use the following commands on Switch2 to create an interface for the default VLAN.

   ```
   config t
   interface vlan1
   ip address 192.168.100.3 255.255.255.0
   ```

3. Yes, the `ping 192.168.100.2` command entered from the console of Switch2 is successful, because Switch2 now has an interface configured for IP. A switch cannot perform any functions that require IP connectivity until at least one interface is configured for IP and an IP address and mask are assigned to the interface.

4. No answer required.

5. You should use the following commands to configure a default gateway on Switch2.

   ```
   config t
   ip default-gateway 192.168.100.1
   ```

6. No answer required.
B. Examine the current VTP configuration on Switch1

1. You should use the `telnet 192.168.100.2` command from the console of Switch2 to access the console of Switch1.

2. You should use the `show vtp status` command on the virtual console of Switch1 to determine the VTP domain and VTP mode for Switch1.

   The VTP domain on Switch1 is tampa.
   The VTP mode on Switch1 is server.

C. Configure VTP on Switch2

1. You should use the following commands on Switch2 to configure Switch2 as a VTP client.
   ```
   config t
   vtp mode client
   ```

2. No, Switch1 and Switch2 are currently not in the same VTP domain.

3. You should use the following commands on Switch2 to configure Switch2 for membership in the same VTP domain as Switch1.
   ```
   config t
   vtp domain tampa
   ```

4. You should use the `show running-config` command on the virtual console of Switch1 to check for a VTP password.

5. Yes, a VTP password is configured on Switch1. You should use the following commands on Switch2 to configure the same password on Switch2.
   ```
   config t
   vtp password Orlando
   ```

Task 4: Verify VTP

A. Verify the proper operation of VTP

1. You should use the `show vlan` command on Switch2 to list the VLANs that currently exist.

2. Yes, the ODD and EVEN VLANs exist on Switch2.

   Switches will only exchange VLAN information if the VTP domain and VTP password match. Note that VLANs can only be configured on a switch that is in VTP server mode. VLAN configuration cannot be changed on a switch that is in VTP client mode.

   Switches that are in VTP client mode will receive the VLAN configuration from a switch that is configured as a VTP server. In this case, Switch1 was already configured as a VTP server; however, the VTP domain and VTP password on Switch2 did not match the VTP domain and VTP password on Switch1. After you configured the VTP domain and VTP password on Switch2 to match Switch1, VTP propagated the VLANs configured on Switch1 to Switch2.
Task 5: Configure VLAN Trunking

A. Test for connectivity between the switches

1. You should use the `telnet 192.168.100.2` command on Switch2.

   You should then use the `show running-config` command on the virtual console of Switch1 to examine the running configuration of Switch1.

2. The switchport that connects to PC1 belongs to VLAN 11.

   The switchport that connects to PC2 belongs to VLAN 22.

3. The switchport to which PC1 connects belongs to VLAN 11, and the switchport to which PC3 connects belongs to the default VLAN 1.

   The switchport to which PC2 connects belongs to VLAN 22, and the switchport to which PC4 connects belongs to the default VLAN 1.

4. No, the ping from PC1 to PC3 fails, because the switchports to which each PC connects are in different VLANs.

5. No, the ping from PC2 to PC4 fails, because the switchports to which each PC connects are in different VLANs.

B. Configure VLANs on Switch1 and Switch2

1. No answer required.

2. PC3 is connected to interface FastEthernet0/3 on Switch2.

   PC4 is connected to interface FastEthernet0/4 on Switch2.

3. The switchport to which PC3 connects should be made a member of VLAN 11.

   The switchport to which PC4 connects should be made a member of VLAN 22.

4. You should use the following commands on Switch2 to place the switchports to which PC3 and PC4 connect in the appropriate VLANs.

   ```
   config t
   interface fastethernet0/3
   switchport mode access
   switchport access vlan 11
   interface fastethernet0/4
   switchport mode access
   switchport access vlan 22
   ```

5. No, the ping from PC1 to PC3 still fails; although PC1 and PC3 are now in the same VLAN, the switchports to which these PC hosts connect are on different switches.

C. Configure VLAN trunking between Switch1 and Switch2

1. No answer required.
2. Switchport FastEthernet0/2 on Switch1 should be configured as a trunk port.

Switchport FastEthernet0/1 on Switch2 should be configured as a trunk port.

3. You should use the telnet 192.168.100.2 command on Switch2.

You should then use the `show running-config` command on the virtual console of Switch1 to examine the running configuration of Switch1.

4. You should use the following commands on Switch2 to configure the appropriate switchport for trunking.

```
config t
interface fastethernet0/1
switchport mode trunk
```

D. Verify VLAN Trunking

1. Yes, the ping from PC1 to PC3 is successful, because the VLAN trunk between Switch1 and Switch2 has now been configured. Traffic on the trunk link is tagged with the appropriate VLAN ID so that the switch on the other end of the link can direct the traffic to the appropriate VLAN.

2. Yes, the ping from PC2 to PC4 is successful, because the VLAN trunk between Switch1 and Switch2 has now been configured and is operating properly. Traffic on the trunk link is tagged with the appropriate VLAN ID so that the switch on the other end of the link can direct the traffic to the appropriate VLAN.
Sample Configuration Script

```
Switch2

!  
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch2
enable secret cisco
!
ip subnet-zero
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport mode access
switchport access vlan 11
!
interface FastEthernet0/4
switchport mode access
switchport access vlan 22
!
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
!
vtp mode Client
vtp domain tampa
vtp password orlando
!
interface Vlan 1
ip address 192.168.100.3 255.255.255.0
no ip route-cache
no shutdown
!
vlan 11 name odd
vlan 22 name even
!
ip classless
no ip http server
!
line con 0
transport input none
line aux 0
line vty 0 15
!
no scheduler allocate
end
```
Lab 40: Basic Router Configuration

Objective
This lab will give you hands-on experience with tasks you encounter when configuring a router. You would typically perform these types of tasks when setting up the local area network (LAN) for a new office. You will complete a variety of tasks, including setting the router's host name, configuring basic security, configuring basic IP addressing, and saving and backing up the router configuration.

Lab Topology
The simulated network topology consists of a router and two switches. Each switch has two PC hosts connected. You will only be configuring Router1 in this lab. The diagram below represents this topology.
**Command Summary**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>copy running-configuration startup-configuration</td>
<td>copies the running configuration to NVRAM</td>
</tr>
<tr>
<td>copy running-configuration tftp</td>
<td>copies the running configuration to the TFTP server</td>
</tr>
<tr>
<td>description description</td>
<td>applies the specified description to an interface</td>
</tr>
<tr>
<td>disable</td>
<td>returns to user EXEC mode</td>
</tr>
<tr>
<td>enable</td>
<td>enters privileged EXEC mode</td>
</tr>
<tr>
<td>enable password password</td>
<td>sets the enable password</td>
</tr>
<tr>
<td>enable secret password</td>
<td>sets the enable secret password</td>
</tr>
<tr>
<td>exit</td>
<td>exits one level in the menu structure</td>
</tr>
<tr>
<td>hostname host_name</td>
<td>sets the host name</td>
</tr>
<tr>
<td>interface fastethernet slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>ip address ip_address subnet_mask</td>
<td>assigns an IP address to an interface</td>
</tr>
<tr>
<td>ip host host_name ip_address</td>
<td>maps host_name to ip_address</td>
</tr>
<tr>
<td>line console 0</td>
<td>accesses console line configuration mode</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>accesses virtual console line configuration mode for all five virtual consoles</td>
</tr>
<tr>
<td>login</td>
<td>configures the device to require the use of a login password</td>
</tr>
<tr>
<td>no shutdown</td>
<td>brings up an administratively down interface</td>
</tr>
<tr>
<td>password password</td>
<td>sets a login password</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces as the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show running-configuration</td>
<td>displays the active configuration file</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>starts the terminal emulation program from a PC, router, or switch that permits you to access devices remotely over the network</td>
</tr>
</tbody>
</table>

**Lab Tasks**

**Task 1: Load the Lab 40 Initial Network Configuration**

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator.

**Task 2: Establish a Console Session with Router1**

**A. Connect to the device**

1. When configuring a real router, you will gain access to a console session by connecting the router’s console port to a serial port on your computer using a Cisco console cable. These
cables are sometimes called “rollover” cables. Once the cable is connected, you then launch a terminal emulation program to connect to a console session on the router.

2. To connect to a device in the simulated network, launch the NetMap Viewer, right-click the device that you want to configure, and select **Configure**.

3. You will be configuring Router1 in this lab. Launch the NetMap Viewer by clicking the **NetMap** button on the NetSim button bar. When the NetMap Viewer launches, you will see a network topology map, which displays all the devices in the simulated network.

4. Locate Router1 on the topology map, right-click the Router1 icon, and select **Configure**. A console window will launch and the IOS command prompt will appear. Describe the command prompt. What does it look like? What characters are displayed?

B. Understand EXEC modes

1. When you connect to a Cisco router, you are presented with an EXEC prompt. You can interact with the router’s command line interface at this prompt. Initially, the command line interface is in user EXEC mode. In user EXEC mode, no configuration changes are permitted. Only commands that display system information and commands that temporarily modify the terminal settings are permitted.

2. Before proceeding with the configuration tasks in this lab, you will need to enter privileged EXEC mode. In privileged EXEC mode, you have access to any and all configuration commands. At the command prompt, use the **enable** command to enter privileged EXEC mode. What change did you observe in the appearance of the command prompt?

Task 3: Perform Basic Router Configuration Tasks

A. Configure the host name

1. Assigning a host name to the router makes it easier to identify the device during a console session. Refer to the command summary at the beginning of this lab; what commands should you use to set the host name of the router?

2. Before you are able to enter commands that will change the router’s current configuration, you will need to enter configuration mode. Enter the **configure terminal** command at the console prompt. What changes to the prompt did you notice after you entered this command?

3. You should now be in configuration mode as indicated by the change in the appearance of the command prompt. Refer to the command summary; what commands should you use to change the host name to **Router1**?

Enter these commands at the console prompt.

4. What change did you notice to the command prompt after you entered this command?

5. Type the **exit** command at the command prompt. What change in the appearance of the prompt did you notice?
B. Configure a router interface

1. A router interface is the point at which the router connects to a network. Routers have different types of interfaces; each is intended to connect to a specific type of network. You will configure an Ethernet interface in this lab. An Ethernet interface is used to connect to an Ethernet network, which is the network type used on most office LANs.

2. In order to configure an interface, you should begin by making sure that you are at a privileged EXEC mode prompt. If you find that you are not at a privileged EXEC mode prompt, what command should you use? If necessary, use this command to access the privileged EXEC mode prompt. _______________________________________

3. In order to enter configuration commands at the privileged EXEC mode prompt, it is necessary to enter configuration mode by using the `configure terminal` command. Note that when you enter any IOS command at the command prompt, it is only necessary to enter enough of each keyword so that the command parser can uniquely identify the command that you want to execute. In the case of this command, you could enter `conf t` to achieve the same result. What did you type to enter configuration mode? __________________

4. Once you have entered configuration mode, you must next enter interface configuration mode, specifying which interface you want to configure. In this task, you will be configuring the first FastEthernet interface on the router, which is identified as fastethernet0/0. To configure this interface, you should use the `interface fastethernet0/0` command. You could also use the command shortcut, `int fa0/0`. What change in the appearance of the prompt did you notice after you entered this command? ________________________

5. You will now assign an IP address to the FastEthernet 0/0 interface. Refer to the command summary; what commands should you use to assign the IP address 192.168.100.1 with a mask of 255.255.255.0 to the FastEthernet 0/0 interface on Router1? __________________

Enter these commands at the interface configuration prompt.
After configuring the IP address on the FastEthernet 0/0 interface on Router1, you should enter the `no shutdown` command while you are still in interface configuration mode; router interfaces are shut down by default until you activate them by entering the `no shutdown` command into the running configuration.

6. It is useful to enter a description to identify the purpose of the interface or to identify the network to which it connects. Refer to the command summary; what command should you use to add the description “BranchLAN” to FastEthernet 0/0 on Router1? ______________

Enter this command at the interface configuration prompt.

7. Now that you have added a description to interface FastEthernet 0/0 on Router1, use the `exit` command to exit interface configuration mode. Use the `exit` command again to exit the global configuration mode. Note that you can use the CTRL+Z key combination to exit all configuration modes and return immediately to the privileged EXEC mode prompt. Refer to the command summary; use the appropriate command to display the currently executing configuration on Router1. Do you see the interface description that you applied to FastEthernet 0/0? Where does it appear? Note that when you issue the command to display the running configuration, the output is paginated; the running configuration will run to the bottom of the page and stop. When you see “—More—” displayed at the bottom of the
screen, this indicates there is more text to display but the output is paused so that it does not scroll off the screen. Press the spacebar to view the next page of text.

C. Configuring EXEC mode security

1. Previously, you entered a command that elevated your privilege level from user EXEC to privileged EXEC. Were you prompted for any type of credentials before your privilege level was elevated? 

2. What impact does this have on security? 

3. The `enable password` command is used to password-protect access to the router's privileged EXEC mode. First, make sure that you are in privileged EXEC mode. How can you tell if you are in privileged EXEC mode? If you are not in privileged EXEC mode and want to enter privileged EXEC mode, what should you do? 

4. At the privileged EXEC mode prompt, use the `configure terminal` command to enter configuration mode. Next, use the `enable password` command to set the enable password to “Boson”. Then use the `exit` command to exit configuration mode and return to the privileged EXEC mode prompt. 

5. Use the `show running-config` command to display the currently executing configuration commands. Can you see the enable password? What impact does this have on security? 

6. At the privileged EXEC mode prompt, enter the `disable` command. What change did you notice in the appearance of the command prompt? Now attempt to enter configuration mode by using the `configure terminal` command. What happens? Why? 

7. Return to privileged EXEC mode by using the `enable` command. Do you notice a different behavior? Briefly explain the behavior you observe and why it occurs. 

8. At the privileged EXEC mode prompt, use the `enable secret` command to set the enable secret to “Cisco”. What additional commands did you use? 

9. Use the `show running-config` command to view the currently executing router configuration. Can you see the enable secret? 

10. Which is the most secure, the enable password or the enable secret? Why? 

11. When the enable password and the enable secret are both configured, which one controls access to privileged EXEC mode? Briefly explain this.
D. Configure console security

1. When you right-click a router or switch icon in the NetMap Viewer and select Configure, you are simulating the process of connecting to the router’s console port with a console cable connected to a notebook or desktop computer that is equipped with terminal emulation software. When you did this earlier, what was the next thing that happened?

What are the security implications of this?

2. It is a good security practice to secure the console so that a password is required before any access to the console is granted. Refer to the command summary; what commands should you use to ensure that you are prompted for a password before console access is granted? The password should be “Orlando”.

Enter these commands at the privileged EXEC mode prompt on Router1.

3. Use the exit command to exit line configuration mode. Use the exit command again to exit global configuration mode. Use the exit command again to terminate the console session.

4. Right-click Router1 in the NetMap Viewer and click Configure. Do you notice a different behavior this time? What has changed?

How do you explain this behavior?

E. Configure virtual console security

1. You have learned how to access an EXEC session on a router by directly connecting a console cable from your PC to the router’s console port. This requires that you have physical access to the router or switch that you are configuring. There are many situations where it would be useful to be able to access a router’s EXEC session from the network. By using this technique, you could access the EXEC session on a router or switch without regard to your physical location or the physical location of the router or switch being configured as long as you have network connectivity to the device being configured.

2. Cisco routers and switches have five virtual consoles (some have more than five) that are numbered zero through four. A user on the network can use a terminal emulation program that supports the Telnet protocol to remotely connect to one of these virtual consoles. Because there are five virtual consoles, up to five concurrent remote user sessions can exist simultaneously.

3. Unlike a directly-connected console port session, a router will not accept an incoming virtual console session request until virtual console password security has been configured.

4. Log on to the console of PC1 and use the telnet command to request a virtual console session with Router1. What happens? Can you explain why?

5. Refer to the command summary; what commands should you use to configure the five virtual consoles with the password “Tampa”? Note that it is possible to configure the five virtual consoles individually and assign different passwords to each; however, this is not
a good practice, because users have no way of knowing to which virtual console they will connect when they issue the `telnet` command to initiate a virtual console session with a router or a switch. Enter these commands at the privileged EXEC mode prompt on Router1.

6. Log on to the console of PC1, and use the `telnet` command to request a virtual console session with Router1 just as you did before. What happens differently this time? Can you explain why?

Task 4: Save and Back up the Router Configuration

A. Save the configuration to NVRAM

1. When configuration commands are entered at an EXEC mode prompt, they are executed immediately and become part of the running configuration. The running configuration is stored in RAM, which is volatile storage. This means that the configuration will be lost if the router loses power or is restarted for any reason.

Saving the running configuration to non-volatile random access memory (NVRAM) allows the configuration to be saved so that when the router is shut down or rebooted, the saved configuration, including any new commands entered prior to the last save, will be applied when the router restarts.

2. To save the running configuration to NVRAM, you should use the `copy` command. Refer to the command summary; what `copy` command should you use to save the running configuration to non-volatile memory? Enter this command on Router1. Note that the `copy` command is not entered in configuration mode. Use the `exit` command to return to the privileged EXEC mode prompt if necessary.

B. Back up the router configuration

1. In addition to copying the running configuration to NVRAM, it is also important to copy the configuration to a location other than on the router itself. Configurations stored in NVRAM may not survive a router hardware failure or other severe error condition. For this reason, it is important to back up the configuration to a different location. The Trivial File Transfer Protocol (TFTP) can be used for this purpose.

2. You will be copying the configuration to a TFTP server located at IP address 192.168.100.2. Refer to the command summary; what command should you use to map this IP address to the host name “TFTPServer”? Enter this command at the privileged EXEC mode prompt on Router1. After using this command, you can use the friendly name “TFTPServer” rather than the IP address when you are referring to the TFTP server.

3. Just as the `copy` command was used to copy the configuration from the running configuration to NVRAM, the `copy` command can also be used to copy the configuration
to a TFTP server. When you use the **copy** command to back up the configuration to a TFTP server, you will be prompted for the name of the file that you want to save the configuration to. Refer to the command summary; what **copy** command should you use to copy the running configuration to a TFTP server? Be sure to refer to the TFTP server using the host name TFTPServer. Enter this command at the privileged EXEC mode prompt on Router1.

### Lab Solutions

**Task 2: Establish a Console Session with Router1**

**A. Connect to the device**

1. No answer required.
2. No answer required.
3. No answer required.
4. The command prompt displayed is **Router>**. Since the host name has not yet been set, the default host name “Router” is displayed as part of the prompt. When the EXEC session begins, the initial privilege level is user, as indicated by the “>” symbol at the end of the prompt.

**B. Understand EXEC modes**

1. No answer required.
2. When the **enable** command is used to enter privileged EXEC mode, the “#” symbol will appear at the end of the prompt. To leave privileged EXEC mode and return to user EXEC mode, use the **disable** command.

**Task 3: Perform Basic Router Configuration Tasks**

**A. Configure the host name**

1. You should use the **hostname Router1** command to set the host name.
2. After you enter the **configure terminal** command at the privileged EXEC mode prompt, the prompt changes to **Router(config)#**. The “#” symbol indicates privileged EXEC mode and “(config)” indicates global configuration mode. In global configuration mode, you can enter configuration commands that affect the entire router. This is in contrast to interface configuration mode, where you can enter only commands that affect a specified interface.
3. You should enter the following commands on Router1 to change the host name to Router1.  
   ```
   config
   hostname Router1
   ```
4. The command prompt changed to **Router1#** after you entered the **hostname** command to change the host name to **Router1**.
5. The command prompt changes from `Router1(config)#` to `Router1#`. This indicates that the router is no longer in global configuration mode.

B. Configure a router interface

1. No answer required.

2. The `enable` command will change the device from user EXEC mode to privileged EXEC mode. If the `enable password` or `enable secret` command has been used to configure a password for privileged EXEC mode, a password prompt will be presented and the correct password must be entered before the privileged EXEC mode prompt will appear.

3. You could type any identifiable abbreviation of `configure terminal`.

4. After entering the interface `fastethernet0/0` command, the interface configuration prompt appears. The interface configuration prompt on Router1 is `Router1(config-if)#`.

5. You should enter the following commands on Router1 to configure the FastEthernet interface.
   
   ```
   ip address 192.168.100.1 255.255.255.0
   no shutdown
   ```

6. You should enter the `description BranchLAN` command to add a description to the FastEthernet interface.

7. Yes, the interface description is visible in the running configuration that is displayed as a result of entering the `show running-configuration` command.

C. Configure EXEC mode security

1. There was no prompt for credentials. You needed only to enter the `enable` command to enter privileged EXEC mode.

2. This is not secure. Anyone who has physical access to the router can open a console session, enter privileged EXEC mode, and execute any IOS command.

3. Privileged EXEC mode is indicated by the “#” symbol at the end of the command prompt. If the router is not in privileged EXEC mode, the “>” symbol will appear at the end of the command prompt. Use the `enable` command to enter privileged EXEC mode. Use the `disable` command to exit privileged EXEC mode and return to user EXEC mode.

4. No answer required.

5. Yes, the enable password is shown in clear text when the running configuration is displayed as a result of entering the `show running-config` command.

   This has a negative impact on security, because anyone who sees the output of the `show running-config` command can easily see the privileged EXEC mode password.

6. When you enter the `disable` command, the prompt changes from `Router#` to `Router>`, indicating that the console session has returned to user EXEC mode.

The `configure terminal` command is rejected, because configuration commands are not allowed in user EXEC mode.
7. Yes, the behavior is different now. A password is now required when the `enable` command is used to enter privileged EXEC mode.

This new behavior occurs because the `enable password` command has been used to secure access to privileged EXEC mode.

8. You should use the following commands on Router1 to set the enable secret.

   ```
   enable
cfg t
   enable secret Cisco
   ```

9. No, the enable secret is not visible when the output of `show running-config` is viewed. The enable secret is encrypted and appears as an indecipherable string of random characters in the running configuration.

10. The enable secret is more secure than the enable password. The enable password is stored in clear text and can be viewed by anyone who can see the output of the `show running-config` command. The enable secret is encrypted and is not visible in the output of the `show running-config` command.

11. When both an enable password and an enable secret have been configured, the enable secret will be used to control access to privileged EXEC mode, because the enable secret takes priority over the enable password when both are configured.

D. Configure console security

1. Upon connecting to the console port, the user EXEC mode prompt appeared immediately. This is a security risk, because anyone with physical access to the router can connect to the console port and access the user EXEC mode prompt without entering a password.

2. You should enter the following commands on Router1 to ensure that all users are prompted for a password.

   ```
   configure terminal
   line console 0
   login
   password Orlando
   ```

3. No answer required.

4. Yes, the behavior is different. A password prompt is presented and you must enter the correct password before you can access the user EXEC mode prompt.

This behavior is the result of entering global configuration mode, using the `line console 0` command to access line configuration mode, entering the `login` command, and then entering the `password` command.

E. Configure virtual console security

1. No answer required.

2. No answer required.
3. No answer required.

4. The telnet connection request is rejected. Unlike the console port, the virtual consoles will not accept a connection until security has been configured. The **login** and **password** commands must be applied to the virtual console lines before a telnet request will be accepted.

5. You should use the following commands on Router1 to configure the virtual consoles with a password.

   ```
   configure terminal
   line vty 0 4
   password Tampa
   login
   exit
   ```

6. The virtual console password prompt for Router1 appears.

   Now that the virtual consoles have been configured with the **login** and **password** commands, Router1 will accept a telnet connection request and will present a password prompt. After the correct virtual console password is entered, the user EXEC mode prompt for Router1 will appear.

**Task 4: Save and Back up the Router Configuration**

**A. Save the configuration to NVRAM**

1. No answer required.

2. You should use the **copy running-configuration startup-configuration** command to save the running configuration to NVRAM.

**B. Back up the router configuration**

1. No answer required.

2. You should use the following commands on Router1 to map the IP address to the host name TFTPServer.

   ```
   configure terminal
   ip host tftpsrv 192.168.100.2
   exit
   ```

3. You should use the **copy running-configuration tftp** command to copy the running configuration to a TFTP server.
Sample Configuration Script

```
Router1

! Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
enable secret Cisco
enable password Boson
!
ip subnet-zero
ip host tftpsrv 192.168.100.2
!
interface Serial0/0
no ip address
no ip directed-broadcast
shutdown
!
interface FastEthernet0/0
description BranchLAN
ip address 192.168.100.1 255.255.255.0
no ip directed-broadcast
bandwidth 100000
!
interface FastEthernet0/1
no ip address
no ip directed-broadcast
bandwidth 100000
shutdown
!
ip classless
no ip http server
!
line con 0
login
transport input none
password Orlando
line aux 0
line vty 0 4
login
password Tampa
!
no scheduler allocate
end
```
Lab 41: Access Lists

Objective

In this simulated network, two virtual local area networks (VLANs) exist, VLAN 11 and VLAN 22. PC1 and PC3 are members of VLAN 11. PC2 and PC4 are members of VLAN 22. VLAN 11 uses the 192.168.101.0/24 network, and VLAN 22 uses the 192.168.102.0/24 network.

A trunk link between Switch1 and Switch2 allows the VLANs to span both switches. Router1 is also configured with a trunk link to Router1. Router1 is configured to provide inter-VLAN routing.

In the initial configuration, PC1, PC2, PC3, and PC4 can all communicate with each other.

The objective of this lab is to isolate the two VLANs by using access lists on Router1 to prevent hosts in the 192.168.101.0 network from communicating with hosts in the 192.168.102.0 network. After the access lists have been configured, PC1 should still be able to use ping and telnet to communicate with all other hosts. All configuration passwords have been set to “admin” unless otherwise noted.

Lab Topology

The simulated network topology for this lab consists of a LAN that has two switches connected by a trunk link. Each switch has two PC hosts connected. VLANs have been implemented on both switches. The VLANs are used to create separate networks with two PC hosts in each VLAN. A router connected to one of the switches handles inter-VLAN routing. The diagram below represents this topology.
Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>access list</strong> nnn permit x.x.x.x mask y.y.y.y mask</td>
<td>defines access list; permits all IP addresses on network x.x.x.x with mask y.y.y.y</td>
</tr>
<tr>
<td><strong>access-list</strong> access_list_number {deny</td>
<td>permit} {icmp</td>
</tr>
<tr>
<td><strong>access-list</strong> access_list_number {deny</td>
<td>permit} {icmp</td>
</tr>
<tr>
<td><strong>access-list</strong> access_list_number {deny</td>
<td>permit} {icmp</td>
</tr>
<tr>
<td><strong>access-list</strong> access_list_number {deny</td>
<td>permit} {icmp</td>
</tr>
<tr>
<td><strong>access-list</strong> access_list_number {deny</td>
<td>permit} {icmp</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td><strong>enable</strong> password</td>
<td>enters privileged EXEC mode</td>
</tr>
<tr>
<td><strong>exit</strong></td>
<td>exits one level in the menu structure</td>
</tr>
<tr>
<td><strong>interface fastethernet</strong> slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td><strong>ip access-group</strong> access_list_number {in</td>
<td>out}</td>
</tr>
<tr>
<td><strong>ping</strong> ip_address</td>
<td>verifies uplinkfast configuration</td>
</tr>
<tr>
<td><strong>show ip interface brief</strong></td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td><strong>show vlan</strong></td>
<td>displays VLAN information</td>
</tr>
<tr>
<td><strong>telnet</strong> ip_address</td>
<td>starts the terminal emulation program from a PC, router, or switch that permits you to access devices remotely over the network</td>
</tr>
</tbody>
</table>

Lab Tasks

Task 1: Load the Lab 41 Initial Network Configuration

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator.
Task 2: Examine the Initial Network Configuration

A. Examine the current VLAN configuration in the simulated network
1. Two VLANs are configured in the simulated network. What are the VLAN IDs? __________
   What are the VLAN names? ____________________________________________
   How did you determine this? ___________________________________________

2. To which VLAN does each PC host belong?
   PC1 ____________ PC2 ____________
   PC3 ____________ PC4 ____________
   How did you determine this? ___________________________________________

B. Examine network connectivity in the simulated network
1. Log on to the console of PC1, and attempt to ping PC2. Is the ping successful? ________
   Are PC1 and PC2 in the same VLAN? _____________________________________
   If the ping is successful, explain how the ping succeeds even though PC1 and PC2 are in
   different VLANs. ___________________________________________________
   _________________________________________________________________

2. From the console of PC1, attempt to ping PC3. Is the ping successful? Why or why not?
   _________________________________________________________________

Task 3: Configure Access Lists

A. Understand the purpose of access lists
1. Access lists can be used to permit or deny traffic passing through a router. Standard
   access lists can filter traffic based only on the source IP address. Extended access lists
   can filter traffic based on source or destination IP addresses. In addition, extended access
   lists can filter traffic based on the type of traffic.

   Standard access lists are identified by a numeric ID from 1 to 99. Extended access lists
   are identified by a numeric ID from 100 to 199. You will use extended access lists in this
   lab.

B. Prepare for access lists
1. To what network do PC1 and PC3 connect? _________________________________
2. To what network do PC2 and PC4 connect? _________________________________
3. When PC1 sends traffic to PC2, which device in the network is responsible for moving this
   traffic between networks? _________________________________
4. When PC2 sends traffic to PC4, which device in the network is responsible for moving this
   traffic between networks? _________________________________
5. What transport layer protocol is used by telnet? _______________________________
6. What network layer protocol is used by ping? _______________________________
C. Implement access lists for traffic flowing from VLAN 11 to VLAN 22

1. The objective for this lab is to use access lists to prevent any traffic from flowing between the two VLANs, with the exception that PC1 should be able to communicate with any of the hosts in VLAN 22 by using only ping and telnet. Hosts in both VLANs should be able to communicate with any other networks except the network for the other VLAN.

2. When constructing access lists, it is important to note that an access list can be made up of multiple access list statements. These statements are evaluated from top to bottom, so the sequence in which the statements are entered is very important. As soon as a packet matches an access list statement, it is either forwarded or dropped, depending upon whether the access list statement allows or denies matched packets.

Note that there is an implied “deny” at the end of every access list. This means that if a packet has not already been allowed or denied by one of the statements in the access list, it is automatically denied.

3. Examine the network. Which device is responsible for moving traffic between VLANs?

4. When access lists are used to control traffic flow between networks, they must be implemented at the point at which traffic flows between the networks. This is the device that you previously identified as responsible for moving traffic between VLANs. You should now log on to the console of this device, access the console command prompt, and enter global configuration mode. What commands did you use to accomplish this? The password should be “cisco”. __________________________________________________________

5. In order to accomplish the goal, you will need to create two access lists. One access list will control the flow of traffic from VLAN 11 to VLAN 22 and the other will control the flow of traffic from VLAN 22 to VLAN 11.

6. First, you will create the access list that allows ping and telnet traffic from VLAN 11 to VLAN 22, denies all other traffic from VLAN 11 to VLAN 22, and allows any other traffic from VLAN 11 to any destination. You should assign the access list number 111 to this access list. Refer to the command summary at the beginning of this lab. What access list command will allow ping traffic from PC1 to reach any host on VLAN 22? ____________

Enter this command into the running configuration of Router1.

7. What access list command will allow telnet traffic from PC1 to reach any host on VLAN 22?

Enter this command into the running configuration of Router1.

8. What access list command will deny any traffic other than telnet and ping traffic from VLAN 11 to VLAN 22? ________________________________

Enter this command into the running configuration of Router1.

9. Keep in mind that there is an implied “deny” at the end of every access list. What access list command will permit any other traffic from VLAN 11 to reach any destination other than VLAN 22? ________________________________

Enter this command into the running configuration of Router1.
10. Access list 111 has now been created, but it will not affect the traffic flow until it is assigned to an interface. Keep in mind that access list 111 will be used to filter traffic flowing from the PC hosts in VLAN 11. Which interface will receive traffic from the PC hosts in VLAN 11? ____________________________________________________

11. From the perspective of the router, which direction will the traffic be flowing through this interface as it moves from the PC hosts in VLAN 11 to VLAN 22: in or out? ___________
Refer to the command summary; what command should you use to assign access list 111 to the appropriate interface in the appropriate direction? _______________________

D. Implement access lists for traffic flowing from VLAN 22 to VLAN 11

1. You will now create the access list that allows ping and telnet traffic from VLAN 22 back to VLAN 11. This access list should deny all other traffic from VLAN 22 to VLAN 11 and allow any other traffic from VLAN 22 to any destination. You should assign the access list number 122 to this access list. Refer to the command summary; what access list command will allow ping reply traffic from any host on VLAN 22 to flow back to PC1? ___________

Enter this command into the running configuration of Router1.

2. What access list command will allow telnet traffic from any host on VLAN 22 to reach PC1? ___________________________________________________________

Enter this command into the running configuration of Router1.

3. What access list command will deny any traffic other than telnet and ping traffic from VLAN 22 to VLAN 11? ___________

Enter this command into the running configuration of Router1.

4. Keep in mind that there is an implied “deny” at the end of every access list. What access list command will permit any other traffic from VLAN 22 to reach any destination other than VLAN 11? ___________

Enter this command into the running configuration of Router1.

5. Access list 122 has now been created, but it will not affect the traffic flow until it is assigned to an interface. Keep in mind that access list 122 will be used to filter traffic flowing from the PC hosts in VLAN 22. Which interface will receive traffic from the PC hosts in VLAN 22? ___________

6. From the perspective of the router, which direction will the traffic flow through this interface as it moves from the PC hosts in VLAN 22 to VLAN 11: in or out? ___________
Refer to the command summary; what command should you use to assign access list 122 to the appropriate interface in the appropriate direction? _______________________

Task 4: Verify Access Lists

A. Verify ping

1. Log on to the console of PC1, and attempt to ping PC3. Is the ping successful? ________
How do the access lists affect the flow of traffic from PC1 to PC3? _______________________
2. From the console of PC1, attempt to ping PC2 and PC4. Are the pings successful? _____
   How do the access lists affect the flow of traffic from PC1 to PC4? ________________
   _________________________________________________________________

3. Log on to the console of PC3, and attempt to ping PC2 and PC4. Are the pings successful?
   _________________________________________________________________

   Briefly explain why the behavior you observe when you initiate pings from the console of
   PC3 may differ from the behavior you observe when you initiate pings from the console of
   PC1. ___________________________________________________________
   _________________________________________________________________

B. Verify Telnet

1. Log on to the console of PC1, and attempt to telnet to 192.168.102.1. Can you successfully
   connect to this IP address using telnet? ___________________________________
   How do the access lists affect the telnet session? ____________________________

2. Log on to the console of PC3, and attempt to telnet to 192.168.102.1. Can you successfully
   connect to this IP address using telnet? ___________________________________
   How do the access lists affect the telnet session? ____________________________

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Examine the current VLAN configuration in the simulated network

1. The two VLAN IDs are VLAN 11 and VLAN 22. VLAN 11 is named ODD and VLAN 22 is named
   EVEN. You can view this information by using the `show vlan` command.

2. PC1 belongs to VLAN 11.
   PC2 belongs to VLAN 22.
   PC3 belongs to VLAN 11.
   PC4 belongs to VLAN 22.

   You can determine the VLANs to which each PC belongs by reading the objective at the
   beginning of this lab.

B. Examine network connectivity in the simulated network

1. Yes, the ping from PC1 to PC2 is successful.

   No, PC1 and PC2 are in different VLANs. PC1 is in VLAN 11 and PC2 is in VLAN 22. The two
   VLANs are configured with different IP network addresses.

   The ping is successful, because PC1 determines that the destination IP address for PC2
   is in a different network and therefore forwards the traffic to its default gateway, Router1,
   for delivery. Router1 has subinterfaces in each VLAN, connected by a trunk link to Switch1.
   Router1 handles inter-VLAN routing for the simulated network.
2. Yes, the ping from PC1 to PC3 is successful, because both PC1 and PC3 belong to the same VLAN and are configured with the same network address. PC1 determines that PC3 is in the same network and sends its traffic to PC3 directly.

Task 3: Configure Access Lists

A. Understand the purpose of access lists
1. No answer required.

B. Prepare for access lists
1. PC1 and PC3 connect to the 192.168.101.0/24 network.
2. PC2 and PC4 connect to the 192.168.102.0/24 network.
3. When PC1 sends traffic to PC2, it must first forward this traffic to its default gateway, 192.168.101.1, which is the IP address of subinterface fa0/0.11 on Router1.
4. When PC2 sends traffic to PC4, it must first forward this traffic to its default gateway, 192.168.102.1, which is the IP address of subinterface fa0/0.22 on Router1.
5. Telnet uses TCP as its transport layer protocol.
6. Ping uses ICMP as its transport layer protocol.

C. Implement access lists for traffic flowing from VLAN 11 to VLAN 22
1. No answer required.
2. No answer required.
3. Router1 is responsible for moving traffic between the two VLANs in this simulated network.
4. You should use the `config t` command on Router1 to enter global configuration mode.
5. No answer required.
6. You should use the following commands on Router1 to allow ping traffic from PC1 to reach any host on VLAN 22.
   ```
   config t
   access-list 111 permit icmp host 192.168.101.11 192.168.102.0 0.0.0.255
   echo
   ```
7. You should use the following commands on Router1 to allow telnet traffic from PC1 to reach any host on VLAN 22.
   ```
   config t
   access-list 111 permit tcp host 192.168.101.11 192.168.102.0 0.0.0.255 eq telnet
   ```
8. You should use the following commands on Router1 to deny any traffic other than telnet and ping traffic from VLAN 11 to VLAN 22.
   ```
   config t
   access-list 111 deny ip 192.168.101.0 0.0.0.255 192.168.102.0 0.0.0.255
   ```
9. You should use the following commands on Router1 to permit any other traffic from VLAN 11 to reach any destination other than VLAN 22.
   ```
   config t
   access-list 111 permit ip 192.168.101.0 0.0.0.255 any
   ```
10. The subinterface FastEthernet0/0.11 on Router1, which has the IP address 192.168.101.1, is configured as the default gateway for the PC hosts in VLAN 11; this interface will receive traffic from the PC hosts in VLAN 11.

11. From the perspective of the router, traffic will be flowing in, toward FastEthernet0/0.11, on Router1.

You should use the following commands on Router1 to assign access list 111 to the interface:

```
config t
int fa0/0.11
ip access-group 111 in
exit
exit
```

D. Implement access lists for traffic flowing from VLAN 22 to VLAN 11

1. You should use the following commands on Router1 to allow ping traffic from any host on VLAN 22 to flow back to PC1.

```
config t
access-list 122 permit icmp 192.168.102.0 0.0.0.255 host 192.168.101.11 echo-reply
```

2. You should use the following commands on Router1 to allow telnet traffic from any host on VLAN 22 to reach PC1.

```
config t
access-list 122 permit tcp 192.168.102.0 0.0.0.255 host 192.168.101.11 eq telnet
```

3. You should use the following commands on Router1 to deny any traffic other than telnet and ping traffic from VLAN 22 to VLAN 11.

```
config t
access-list 122 deny ip 192.168.102.0 0.0.0.255 192.168.101.0 0.0.0.255
```

4. You should use the following commands on Router1 to permit any other traffic from VLAN 22 to reach any destination other than VLAN 11.

```
config t
access-list 122 permit ip 192.168.102.0 0.0.0.255 any
```

5. The subinterface FastEthernet0/0.22 on Router1, which has the IP address 192.168.102.1, is configured as the default gateway for the PC hosts in VLAN 22; this interface will receive traffic from the PC hosts in VLAN 22.

6. From the perspective of the router, traffic will be flowing in, toward FastEthernet0/0.22, on Router1.
You should use the following commands on Router1 to assign access list 122 to the interface.

```
config t
int fa0/0.22
ip access-group 122 in
exit
exit
```

Task 4: Verify Access Lists

A. Verify ping

1. Yes, the ping from PC1 to PC3 is successful.

The flow of traffic from PC1 to PC3 is not affected by the access lists on Router1. This is because PC1 and PC3 are in the same VLAN and are configured with IP addresses in the same network; therefore, this traffic never passes through Router1.

2. Yes, the pings from PC1 to PC2 and PC4 are successful.

Access list 111 is configured to allow ping traffic (icmp echo) from PC1 (192.168.101.11) to the 192.168.102.0/24 network. PC2 and PC4 are configured with IP addresses that fall within the 192.168.102.0/24 network; therefore, the ping traffic is permitted by the access list.

3. No, the pings from PC3 to PC2 and PC4 fail.

Ping traffic sent from PC3 to PC2 and PC4 is forwarded to Router1, the default gateway for PC3, because PC2 and PC4 are configured with IP addresses that are not in the same network as PC3. Access list 111 is configured to allow ping traffic (icmp echo) only from host PC1, not from the entire 192.168.101.0/24 network; therefore, these packets are dropped when the ping is initiated from PC3 but are forwarded when the ping is initiated from PC1.

B. Verify Telnet

1. Yes, a telnet connection from PC1 to 192.168.102.1 is successful.

Access list 111 is configured to allow telnet traffic flowing in to interface fa0/0.11 as long as this traffic is coming from PC1 and is addressed to a host in the 192.168.102.0/24 network.

2. No, a telnet connection from PC3 to 192.168.102.1 fails.

Access list 111 is configured to allow telnet traffic flowing in to interface fa0/0.11 only if the traffic is coming from PC1 and is addressed to a host in the 192.168.102.0/24 network. In this case, the traffic is not coming from PC1, but is instead coming from PC3; therefore, the traffic is dropped and the telnet connection fails.
Sample Configuration Script

```
Router1

! Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
enable secret cisco
!
ip subnet-zero
!
interface Serial0/0
no ip address
no ip directed-broadcast
!
interface FastEthernet0/0
encapsulation dot1q 1
ip address 192.168.100.1 255.255.255.0
no ip directed-broadcast
!
interface FastEthernet0/0.11
encapsulation dot1q 11
ip address 192.168.101.1 255.255.255.0
ip access-group 111 in
!
interface FastEthernet0/0.22
encapsulation dot1q 22
ip address 192.168.102.1 255.255.255.0
ip access-group 122 in
!
interface FastEthernet0/1
no ip address
no ip directed-broadcast
shutdown
!
ip classless
no ip http server
!
access-list 111 permit icmp host 192.168.101.11 192.168.101.11 192.168.102.0 0.0.0.255 echo
access-list 111 permit tcp host 192.168.101.11 192.168.101.11 192.168.102.0 0.0.0.255 eq telnet
access-list 111 deny ip 192.168.101.0 0.0.0.255 0.0.0.255 192.168.101.0 0.0.0.255
access-list 122 permit ip 192.168.101.0 0.0.0.255 0.0.0.255 any
access-list 122 permit icmp 192.168.102.0 0.0.0.255 0.0.0.255 host 192.168.101.11 echo-reply
access-list 122 permit tcp 192.168.102.0 0.0.0.255 0.0.0.255 host 192.168.101.11 eq telnet
access-list 122 deny ip 192.168.102.0 0.0.0.255 0.0.0.255 192.168.101.0 0.0.0.255
access-list 122 permit ip 192.168.102.0 0.0.0.255 0.0.0.255 any
!
line con 0
transport input none
line aux 0
line vty 0 4
login
password cisco
!
no scheduler allocate
end
```
Lab 42: Troubleshooting EIGRP

Objective
Troubleshoot a simulated network configured with Enhanced Interior Gateway Routing Protocol (EIGRP). The network has already been configured, but you will need to locate and correct some configuration errors. All passwords have been set to “cisco”.

Lab Topology
The simulated network topology for this lab consists of five routers connected by point-to-point serial wide area network (WAN) links. Each router also has a local area network (LAN) connected to its Ethernet interface. Each LAN has one host PC connected. This simulated topology is comparable to an actual network connecting five geographically separate offices, each with a LAN to which desktop PCs and servers are connected. The diagram below represents this topology.
Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth nnn</td>
<td>sets the specified interface bandwidth</td>
</tr>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>exit</td>
<td>exits from the current mode</td>
</tr>
<tr>
<td>interface serial slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>network ip_address</td>
<td>activates EIGRP on the specified network</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>sends an ICMP echo request to the specified address</td>
</tr>
<tr>
<td>router eigrp autonomous_system_number</td>
<td>enters EIGRP configuration mode</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show ip route</td>
<td>displays the IP routing table</td>
</tr>
<tr>
<td>show running-configuration</td>
<td>displays the active configuration file</td>
</tr>
<tr>
<td>telnet ip_address</td>
<td>starts the terminal emulation program from a PC, router, or switch that permits you to access devices remotely over the network</td>
</tr>
<tr>
<td>tracert ip_address</td>
<td>displays the network path to a given destination; used on Windows workstations</td>
</tr>
<tr>
<td>traceroute ip_address</td>
<td>displays the network path to a given destination; used on Cisco routers and switches</td>
</tr>
</tbody>
</table>

Lab Tasks

Task 1: Load the Lab 42 Initial Network Configuration
Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator. The initial configuration will assign the correct host names and IP addresses to each device.

Task 2: Examine the Initial Network Configuration
A. Verify IP address assignments
1. Do the IP addresses assigned to all devices match the values shown in the network topology diagram? ____________________________________________
   Be sure to examine the configuration of all four routers and PC hosts in order to become familiar with the simulated network topology and configuration.
2. What type of addressing is used for all routers and PC hosts in this lab? _______________
3. What impact will this have on connectivity to the Internet? ____________________________
B. Test network connectivity
1. Log on to the console of HostE, and attempt to ping each of the other hosts on all of the other LANs: HostA, HostB, HostC, and HostD. Are all of these pings successful? ________
   If not, which of the hosts fail to respond to a ping? ___________________________
2. If any of the hosts fail to respond to a ping, to which network do they connect? ________
3. Attempt to ping the IP addresses of each router interface from the console of HostE. Are all of these pings successful? __________________________________________
   If not, which router interfaces fail to respond to a ping? ________________________

C. Analyze routing tables
1. To troubleshoot the connectivity problems you have observed, you will need to gather information about the routes to all the other networks. Begin by observing the routes to other networks that are known by the default gateway for HostE. Which router serves as the default gateway for HostE? ____________________________________________
2. Display the routing table on the Key West router. What command did you use to do this? _________________________________________________________________
3. Compare the routes in the Key West routing table to the topology diagram. Are there any networks shown on the topology diagram that are not represented in the Key West routing table? __________________________________________________________
   If so, which routes are missing? __________________________________________

Task 3: Correct Connectivity Problems
A. Analyze missing routes
1. Refer to the missing routes that you previously identified and compare them to the hosts and router interfaces that did not respond to the pings from the console of HostE. Can you identify a relationship between the missing routes and the failed pings? ________
   _________________________________________________________________
2. Refer to the network topology diagram, and identify the network that is missing from the routing table on the Key West router. Which router in the simulated network is responsible for informing the other routers about the existence of this network? ________________

B. Analyze the router configuration
1. Refer to the command summary at the beginning of this lab; what command should you use to view the running configuration of the device that you have determined is responsible for informing the other routers of the existence of the missing route? ________________________
   Enter this command in the appropriate device.
2. What two methods do routers use to determine the best path to reach other networks to which they are not directly connected? ____________________________________
   Which of these two methods is used in the routers in the simulated network? ________
   How did you determine this? ___________________________________________
3. Review the running configuration. Can you identify which configuration commands are responsible for communicating information about directly connected networks to the other routers in the network? __________________________________________

   Does anything appear to be missing? ____________________________________

C. Correct the router configuration

1. You should now be able to determine which device is responsible for announcing the missing network to the rest of the routers. By examining its running configuration, you should be able to determine how this router is configured to announce these networks and which network is missing. Refer to the command summary; what commands should you use to configure this router to begin announcing the missing network to the other routers?

   Enter these commands into the running configuration of the appropriate router.

D. Verify connectivity

1. Return to the console of HostE, and attempt to ping the PC host and router interface that previously failed the ping test. Are these pings successful? Why or why not? ______________

2. Log on to the router that serves as the default gateway for HostE. Which router is this? _________________________________________________________________

3. Refer to the command summary; what command should you use to examine the entries in this router’s routing table? __________________________________________

4. Use the previous command to examine the routing table on the router that serves as the default gateway for HostE. Do you see a network listed now that was not there before? ______________
   Briefly explain why this route was missing before and why it is present now. ______________

Task 4: Investigate and Correct Network Performance Issues

A. Examine the WAN components of the network topology

1. Examine the network topology diagram. What type of connectivity exists between the routers? ______________
   What is the Data Link layer protocol used on these links? ______________

2. Describe the unique aspects of IP addressing used on this type of link. ______________

3. Are all five links equal in terms of the amount of data they are able to transport within a given period of time? ______________
   Briefly explain how you are able to determine this. ______________

4. If a ping is sent from the console of HostE to HostB, what path should this traffic follow through the network? ______________
   How is this path determined? ______________
B. Examine WAN performance issues
1. You are a network administrator of a network similar to the simulated network used in this lab. Some users complain of slow response times when accessing network resources across the WAN. Examine the connectivity between the routers; what do you think could cause this? ____________________________________________________________
   ____________________________________________________________
2. Log on to the console of HostE, and use the ping command to send traffic to HostB. Can you determine the path that the traffic follows? _______________________________
   If not, refer to the command summary; what command will enable you to determine the path taken by traffic sent from HostE to HostB? _______________________________
3. Log on to HostE, and enter the previous command; what path does traffic addressed to HostB follow? _______________________________________________________
4. What impact could this path have on network performance? ______________________
   ____________________________________________________________

C. Correct WAN performance problems
1. What is the difference between a routed protocol and a routing protocol? ____________
   ____________________________________________________________
   Give an example of each. __________________________________________
2. What routed protocol is used in the simulated network? _______________________
3. What routing protocol is used in the simulated network? _____________________
4. Which protocol is used to determine the path taken by traffic as it moves through the network? _______________________________________________________
5. On what basis does this routing protocol select the path that traffic will follow? ______
   ____________________________________________________________
6. You will need to examine the configuration of all five routers in the network. To connect to a device in the simulated network, launch the NetMap Viewer, right-click the device that you want to configure, and select Configure.
7. Examine the running configuration of the Tampa router. Do you see any missing or incorrect information on the Tampa router that could cause the routing protocol to select a suboptimal path? ____________________________________________
8. Examine the running configuration of the remaining four routers. Do you see any missing or incorrect information on any of these routers that could cause the routing protocol to select a suboptimal path? ____________________________________________
9. Based on your previous examination of the network, what commands should you use to correct any configuration errors that you found? ________________________________
   Enter these commands into the running configuration of the appropriate routers.
Task 5: Verify WAN Performance

A. Review path selection
1. How did the incorrect or missing configuration affect the path selection process used by the routing protocol? ___________________________________________________
2. Consider the configuration errors you found and corrected in the previous steps. Under what conditions might these configuration errors not affect network performance? ____________

B. Verify path selection
1. What command did you previously use to determine the path taken by traffic flowing from HostE to HostB? ___________________________________________________
2. Use this command again to determine the path taken by traffic flowing from HostE to HostB. Does this traffic take a different path now, since you have changed the configuration of some of the routers? ___________________________________________
3. What impact will this new path have on WAN performance? Briefly explain. ____________

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Verify IP address assignments
1. Yes, the IP addresses assigned to all devices match the values shown in the network topology diagram.
2. All router interfaces and PC hosts are configured with private IP addresses. Private IP addresses are nonunique and are intended to be used on internal networks. Private IP addresses cannot be used on networks that directly connect to the Internet.
3. Because of the private IP addresses used on this network, Network Address Translation (NAT) must be used if this private network requires access to the Internet.

B. Test network connectivity
1. No, not all of the pings are successful.
   A ping to HostA fails.
2. The host that fails to respond to a ping connects to the 192.168.2.0/24 network.
3. No, not all of the pings are successful.
   A ping to the Ethernet0 interface on the Tampa router at 192.168.2.1 fails.

C. Analyze routing tables
1. The Key West router serves as the default gateway for HostE.
2. On the Key West router, you should use the `show ip route` command to display the routing table.

3. Yes, there is a network on the topology diagram that does not appear in the Key West routing table.

   The route to the 192.168.2.0/24 network is missing.

**Task 3: Correct Connectivity Problems**

**A. Analyze missing routes**

1. HostA and the Ethernet0 interface on the Tampa router failed to respond to a ping from HostE. Both HostA and the Ethernet0 interface on the Tampa router are configured with IP addresses that belong to the network that is missing from the routes in the routing table on the Key West router.

2. Network 192.168.2.0/24 is missing from the routing table on the Key West router. The Tampa router is responsible for informing other routers about the existence of this network, because this network is directly connected to the Tampa router.

**B. Analyze the router configuration**

1. On the Tampa router, you should use the `show running-config` command to view the running configuration.

2. Routers can use either static routing or dynamic routing to select the best path to reach a destination. Static routing requires that a network administrator manually maintain the routing table on each router. Dynamic routing relies on a dynamic routing protocol that allows routers to automatically inform other routers about their directly connected networks.

   The simulated network uses the Cisco-proprietary EIGRP dynamic routing protocol. Routers automatically inform the other routers in the network about their directly connected networks.

   You can determine this by using the `show running-config` command to examine the router’s configuration and look for commands that enable and configure the dynamic routing protocol.

3. On the Tampa router, the following commands configure the EIGRP dynamic routing protocol.

   ```
   router eigrp 100
   network 192.168.100.0
   ```

   When dynamic routing protocols are configured, only networks that are directly connected to the router should be a part of the configuration. The configuration for the Tampa router is missing the `network 192.168.2.0` command, which configures EIGRP to announce information about the Tampa LAN to the other routers in the simulated network.
C. Correct the router configuration

1. You should use the following commands on the Tampa router to configure the router to begin announcing the missing network.

   ```
   config t
   router eigrp 100
   network 192.168.2.0
   ```

D. Verify connectivity

1. Yes, the pings to HostA and the Ethernet0 interface on the Tampa router from HostE are successful, because you have modified the configuration of the Tampa router to share information about the 192.168.2.0 network; this is the network to which HostA and the Tampa router belong. The other routers in the network can now find a path to the 192.168.2.0/24 network when they attempt to communicate with HostA.

2. The Key West router serves as the default gateway for HostE.

3. You should use the `show ip route` command on the Key West router to examine the entries in the routing table.

4. Yes, the route to network 192.168.2.0/24 is visible in the Key West router’s routing table now that the configuration on the Tampa router has been corrected. The Tampa router is directly connected to the 192.168.2.0/24 network and has been correctly configured to announce the existence of this network to the other routers in the topology.

Task 4: Investigate and Correct Network Performance Issues

A. Examine the WAN components of the network topology

1. The routers in the simulated network are connected by point-to-point serial links.

   A Data Link layer protocol is not specified in the configuration for the serial interfaces; therefore, the default High Level Data Link Control (HDL) protocol will be used by default.

2. The router interfaces that make up each point-to-point link must be configured with IP addresses in the same subnetwork. Each of these subnetworks will have only two IP addresses. In order to conserve IP addresses, the router interfaces that make up a point-to-point link are usually configured with a 30-bit prefix, which leaves only two bits for host addressing. With two host bits, only four, or $2^2=4$, addresses are possible. The first address is the network address, the next two addresses are host addresses, and the last address is the network broadcast address.

3. No, all five links are not equal in terms of the amount of data that they are able to transport within a given period of time.

   The ability of a link to transport data within a given period of time is called bandwidth. The network topology diagram shows that all WAN links are capable of moving data at 512 kilobits per second (Kbps) except the Orlando–Daytona link, which is capable of moving data at only 64 Kbps.
4. A ping from HostE would generate traffic that first goes to the default gateway of HostE, the Key West router. The traffic should then travel from the Key West router to the Miami router, then to the Tampa router, and finally to the Orlando router, which will deliver the traffic to its destination, HostB. This path is preferable, because all traversed links are 512-Kbps links.

B. Examine WAN performance issues
1. Performance could suffer if traffic travels across the Orlando–Daytona link. This link is capable of moving traffic at the rate of 64 Kbps, while all the other WAN links are capable of moving traffic at 512 Kbps. It is likely that the performance problems are occurring because traffic is inadvertently traveling across the Orlando–Daytona link, which should only be used in the event that one of the other links fails.

2. No, output from the `ping` command indicates only whether a specified host responds to an ICMP echo request or not. The `traceroute` command (`tracert` on the Microsoft Windows platform) indicates the path taken to reach a specified destination.

3. The output of the `tracert` command shows that traffic from HostE to HostB travels from HostE to the Key West router, then to the Miami router, then to the Daytona router, and finally to the Orlando router, which delivers the traffic to its destination.

4. This could have a negative impact on performance, because the Daytona–Orlando link is capable of moving traffic at only 64 Kbps, whereas all the other links are capable of moving traffic at 512 Kbps.

C. Correct WAN performance problems
1. A routed protocol is a protocol that configures each node and network with a logical address. A gateway device is used to route traffic from one logical network to the next.

   A routing protocol is used by gateway devices to inform each other of the networks that they know how to reach. Routing protocols allow for dynamic changes to the network topology.

   Examples of routed protocols are Internet Protocol (IP) and Internetwork Packet Exchange (IPX). Examples of routing protocols are EIGRP and Open Shortest Path First (OSPF).

2. The simulated network uses the IP routed protocol.

3. The simulated network uses the EIGRP routing protocol.

4. The routing protocol EIGRP determines the path taken by traffic as it moves through the network.

5. EIGRP prefers higher bandwidth links with low delay when determining a path. EIGRP can use additional metrics for path determination but uses only these two by default.

6. No answer required.

7. No, the Tampa router is configured correctly.

8. Yes, there is a configuration problem on the Orlando router and the Daytona router. Both of these routers are missing the `bandwidth` command on their serial interfaces that connect to each other.
9. You should use the following commands on the Daytona router to correct the configuration error.

```config
config t
interface s0/0
bandwidth 64
```

You should use the following commands on the Orlando router to correct the configuration error.

```config
config t
interface S1/0
bandwidth 64
```

**Task 5: Verify WAN Performance**

**A. Review path selection**

1. The missing `bandwidth` command caused EIGRP to incorrectly use the default bandwidth of 1544 Kbps when making its path selection. The actual bandwidth of this link is 64 Kbps.

2. If all WAN links had the same bandwidth, the missing `bandwidth` commands would not have been as noticeable but could still have caused traffic to be routed in an unexpected way. It is important to always configure each interface with the `bandwidth` command that appropriately describes the bandwidth of the link that is connected to the interface.

**B. Verify path selection**

1. The `tracert` command was used to determine the path taken by traffic flowing from HostE to HostB.

2. Yes, the traffic now takes a different path; it travels from Miami to Tampa and then to Orlando, thus avoiding the slower 64-Kbps link.

3. This will improve WAN performance, because only the 512-Kbps links will be used.
## Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Tampa Router</th>
<th>Orlando Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>! Version 12.1</td>
<td>! Version 12.1</td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
<td>no service password-encryption</td>
</tr>
<tr>
<td>! hostname Tampa</td>
<td>! hostname Orlando</td>
</tr>
<tr>
<td>enable secret cisco</td>
<td>enable secret cisco</td>
</tr>
<tr>
<td>! ip subnet-zero</td>
<td>! ip subnet-zero</td>
</tr>
<tr>
<td>interface Serial0/0</td>
<td>interface Serial0/0</td>
</tr>
<tr>
<td>description ToOrlando</td>
<td>description ToOrlando</td>
</tr>
<tr>
<td>ip address 192.168.100.2 255.255.255.252</td>
<td>ip address 192.168.100.1 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>! interface Serial1/0</td>
<td>! interface Serial1/0</td>
</tr>
<tr>
<td>description ToMiami</td>
<td>description ToTampa</td>
</tr>
<tr>
<td>ip address 192.168.100.9 255.255.255.252</td>
<td>ip address 192.168.100.5 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 64</td>
</tr>
<tr>
<td>! interface Ethernet0</td>
<td>! interface Ethernet0</td>
</tr>
<tr>
<td>description TampaLAN</td>
<td>description OrlandoLAN</td>
</tr>
<tr>
<td>ip address 192.168.2.1 255.255.255.0</td>
<td>ip address 192.168.1.1 255.255.255.0</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>! router eigrp 100</td>
<td>! router eigrp 100</td>
</tr>
<tr>
<td>network 192.168.100.0</td>
<td>network 192.168.100.0</td>
</tr>
<tr>
<td>network 192.168.2.0</td>
<td>network 192.168.1.0</td>
</tr>
<tr>
<td>! ip classless</td>
<td>! ip classless</td>
</tr>
<tr>
<td>no ip http server</td>
<td>no ip http server</td>
</tr>
<tr>
<td>! line con 0</td>
<td>! line con 0</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
</tr>
<tr>
<td>transport input none</td>
<td>transport input none</td>
</tr>
<tr>
<td>password admin</td>
<td>password admin</td>
</tr>
<tr>
<td>line aux 0</td>
<td>line aux 0</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>password sanfran</td>
<td>password sanfran</td>
</tr>
<tr>
<td>! no scheduler allocate</td>
<td>! no scheduler allocate</td>
</tr>
<tr>
<td>end</td>
<td>end</td>
</tr>
</tbody>
</table>
## Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Daytona Router</th>
<th>Key West Router</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>! Version 12.1</code></td>
<td><code>! Version 12.1</code></td>
</tr>
<tr>
<td><code>service timestamps debug uptime</code></td>
<td><code>service timestamps debug uptime</code></td>
</tr>
<tr>
<td><code>service timestamps log uptime</code></td>
<td><code>service timestamps log uptime</code></td>
</tr>
<tr>
<td><code>no service password-encryption</code></td>
<td><code>no service password-encryption</code></td>
</tr>
<tr>
<td><code>! hostname Daytona</code></td>
<td><code>! hostname KeyWest</code></td>
</tr>
<tr>
<td><code>enable secret cisco</code></td>
<td><code>enable secret cisco</code></td>
</tr>
<tr>
<td><code>! ip subnet-zero</code></td>
<td><code>! ip subnet-zero</code></td>
</tr>
<tr>
<td><code>! interface Serial0/0</code></td>
<td><code>! interface Serial0/0</code></td>
</tr>
<tr>
<td><code>description ToOrlando</code></td>
<td><code>description ToMiami</code></td>
</tr>
<tr>
<td><code>ip address 192.168.100.6 255.255.255.252</code></td>
<td><code>ip address 192.168.100.18 255.255.255.252</code></td>
</tr>
<tr>
<td><code>no ip directed-broadcast</code></td>
<td><code>no ip directed-broadcast</code></td>
</tr>
<tr>
<td><code>bandwidth 64</code></td>
<td><code>bandwidth 512</code></td>
</tr>
<tr>
<td><code>! interface Serial1/0</code></td>
<td><code>! interface Serial1/0</code></td>
</tr>
<tr>
<td><code>description ToMiami</code></td>
<td><code>description ToMiami</code></td>
</tr>
<tr>
<td><code>ip address 192.168.100.13 255.255.255.252</code></td>
<td><code>ip address 192.168.100.18 255.255.255.252</code></td>
</tr>
<tr>
<td><code>no ip directed-broadcast</code></td>
<td><code>no ip directed-broadcast</code></td>
</tr>
<tr>
<td><code>bandwidth 512</code></td>
<td><code>shutdown</code></td>
</tr>
<tr>
<td><code>! interface Ethernet0</code></td>
<td><code>! interface Ethernet0</code></td>
</tr>
<tr>
<td><code>description DaytonaLAN</code></td>
<td><code>description DaytonaLAN</code></td>
</tr>
<tr>
<td><code>ip address 192.168.4.1 255.255.255.0</code></td>
<td><code>ip address 192.168.5.1 255.255.255.0</code></td>
</tr>
<tr>
<td><code>no ip directed-broadcast</code></td>
<td><code>no ip directed-broadcast</code></td>
</tr>
<tr>
<td><code>! router eigrp 100</code></td>
<td><code>! router eigrp 100</code></td>
</tr>
<tr>
<td><code>network 192.168.100.0</code></td>
<td><code>network 192.168.100.0</code></td>
</tr>
<tr>
<td><code>network 192.168.4.0</code></td>
<td><code>network 192.168.5.0</code></td>
</tr>
<tr>
<td><code>! ip classless</code></td>
<td><code>! ip classless</code></td>
</tr>
<tr>
<td><code>no ip http server</code></td>
<td><code>no ip http server</code></td>
</tr>
<tr>
<td><code>! line con 0</code></td>
<td><code>! line con 0</code></td>
</tr>
<tr>
<td><code>login</code></td>
<td><code>login</code></td>
</tr>
<tr>
<td><code>transport input none</code></td>
<td><code>transport input none</code></td>
</tr>
<tr>
<td><code>password admin</code></td>
<td><code>password admin</code></td>
</tr>
<tr>
<td><code>line aux 0</code></td>
<td><code>line aux 0</code></td>
</tr>
<tr>
<td><code>line vty 0 4</code></td>
<td><code>line vty 0 4</code></td>
</tr>
<tr>
<td><code>login</code></td>
<td><code>login</code></td>
</tr>
<tr>
<td><code>password sanfran</code></td>
<td><code>password sanfran</code></td>
</tr>
<tr>
<td><code>! no scheduler allocate</code></td>
<td><code>! no scheduler allocate</code></td>
</tr>
<tr>
<td><code>end</code></td>
<td><code>end</code></td>
</tr>
</tbody>
</table>


Lab 43: Variable Length Subnet Masks

Objective
The simulated network for this lab consists of routers and PC hosts. Each router connects to another to form a wide area network (WAN) that connects each office to the others.

Various connectivity problems exist; some hosts cannot communicate with other hosts. You must examine the IP addressing that is already in place and correct the errors that are causing the connectivity problems. All Telnet passwords have been set to “sanfran”. All other passwords have been set to “cisco”.

Lab Topology
Each of the four routers has an Ethernet interface connected to the local area network (LAN) and two serial interfaces that connect the routers to the WAN in such a way that each router is connected to two other routers. A single PC host computer is connected to each LAN.

A fifth router with a single serial WAN interface is also connected to the network. The connectivity problems were observed soon after this router was connected to the network. The network topology diagram displays this topology in more detail.

Your only access to the network is from the console of the Miami router or the console of HostD. The diagram below represents this topology.
Lab Tasks

Task 1: Load the Lab 43 Initial Network Configuration
Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator.

Task 2: Examine the Initial Network Configuration

A. Examine the initial network addressing plan

1. All IP addresses in the network topology fall within the 200.120.45.0/24 network. What is significant about the /24 notation used to define this network? ____________________________

2. Examine the topology diagram; how many networks exist? Your count should include both LANs and WANs. ____________________________

3. How is it possible to address all these networks, given that you are only allocated the 200.120.45.0/24 network? Briefly explain. ____________________________

4. Examine the IP addresses assigned to each router interface and each PC host. Later, you will use this information to calculate the maximum number of host addresses that are available on each network. What additional information do you need in order to perform these calculations? ____________________________

Refer to the command summary at the beginning of this lab; what command should you use to find this information? ____________________________

5. Calculate the maximum number of hosts, first valid host IP addresses, last valid host IP addresses, network address, and broadcast address for each network in the simulated topology. Write this information on the lab topology diagram for later reference.
B. Examine the initial network connectivity

1. Log on to the console of the Miami router and attempt to ping the following devices.
   Indicate whether the pings were successful or not.
   - Daytona Ethernet0
   - Key West Serial0/0
   - HostE
   - Orlando Serial0/0
   - Daytona Serial1/0
   - HostC
   - Daytona Serial0/0
   - Orlando Serial1/0
   - HostB

2. Refer to the command summary for the appropriate commands that will enable you to perform some basic troubleshooting for the hosts and router interfaces that fail the ping test. Do you see anything obvious, such as interfaces that are administratively down or incorrectly configured clocking on the serial interfaces?

Task 3: Correct configuration issues

A. Examine the specific points of failure

1. Refer to your network examination. Were you able to ping HostC from the console of the Miami router?

2. Use the telnet command at the console of the Miami router to open a virtual console session on the Daytona router. Attempt to ping HostC from the console of the Daytona router. Is this ping successful?

   Why would a ping to a directly connected host fail if all interfaces are up and operating properly?

   You may want to examine the routing table on the Daytona router for clues to why this is happening.

3. From the console of the Miami router, attempt to ping the Ethernet0 interface on the Daytona router. Is this ping successful?

   If this ping is successful and the ping to the PC host connected to this interface fails, what conclusion can you draw?

4. From the console of the Miami router, attempt to ping the Ethernet0 interface on the Key West router. Is this ping successful?

5. From the console of the Miami router, attempt to ping HostE. Is this ping successful?

6. Based on the information you have gathered so far, briefly explain what you think is the root cause of the connectivity problems that you have observed.

7. Are all IP addresses configured correctly?

B. Correct the configuration

1. On which device does the configuration error exist?

2. How is this configuration error causing the connectivity problems that you have observed?

3. Refer to the command summary; what command should you use to correct the configuration error that you have discovered?

Enter this command into the running configuration of the device on which the error exists.
Task 4: Verify Configuration

A. Verify connectivity
1. Log on to the console of the Miami router and retry the pings that failed earlier. Are the pings successful now? ________________________________________
2. Are there any remaining devices on the network that fail to respond to a ping? ________
3. From the console of the Miami router, use the ping command to verify that you have connectivity to all hosts and router interfaces.

B. Verify routing
1. Log on to the console of the Miami router and examine the contents of the IP routing table. Refer to the command summary; what command should you use to do this? __________
2. How have the contents of the IP routing table changed? ________________________
3. What affect does this have on network connectivity? __________________________

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Examine the initial network addressing plan
1. The 200.120.45.0/24 network is written in Classless Interdomain Routing (CIDR) format. The /24 indicates the prefix length. A 24-bit prefix indicates that the first 24 bits of the 32-bit IP address represent the network portion of the address. The remaining 8 bits represent the host address. A /24 prefix is equivalent to a Class C mask of 255.255.255.0. The CIDR notation differs from classful addresses; in CIDR notation, the prefix can be of any length and does not necessarily fall on an octet boundary. Prefix lengths of 8, 16, and 24 bits correspond to classful masks of 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.
2. The topology for this lab includes 5 LANs and 5 WANs, for a total of 10 networks in the topology.
3. It is possible to take the 200.120.45.0/24 network and subdivide it further by using Variable Length Subnet Masking (VLSM). VLSM is the process of “borrowing” bits from the host portion of the assigned address space to create subnetworks of varying sizes.
4. In addition to the IP addresses assigned to each router interface and each PC host, you also need to know the value of the subnet mask assigned to each.

You can find the value of the subnet mask by using the show running-config command on the routers and the ipconfig command on the PC hosts.
5.  

<table>
<thead>
<tr>
<th>Network</th>
<th>First Host</th>
<th>Last Host</th>
<th>Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orlando–Daytona WAN</td>
<td>200.120.45.240</td>
<td>200.120.45.241</td>
<td>200.120.45.242</td>
</tr>
<tr>
<td></td>
<td>200.120.45.242</td>
<td></td>
<td>200.120.45.243</td>
</tr>
<tr>
<td>Orlando–Tampa WAN</td>
<td>200.120.45.236</td>
<td>200.120.45.237</td>
<td>200.120.45.238</td>
</tr>
<tr>
<td></td>
<td>200.120.45.239</td>
<td></td>
<td>200.120.45.239</td>
</tr>
<tr>
<td>Tampa–Miami WAN</td>
<td>200.120.45.244</td>
<td>200.120.45.245</td>
<td>200.120.45.246</td>
</tr>
<tr>
<td></td>
<td>200.120.45.247</td>
<td></td>
<td>200.120.45.247</td>
</tr>
<tr>
<td>Miami–Key West WAN</td>
<td>200.120.45.252</td>
<td>200.120.45.253</td>
<td>200.120.45.254</td>
</tr>
<tr>
<td></td>
<td>200.120.45.255</td>
<td></td>
<td>200.120.45.255</td>
</tr>
<tr>
<td>Miami–Daytona WAN</td>
<td>200.120.45.248</td>
<td>200.120.45.249</td>
<td>200.120.45.250</td>
</tr>
<tr>
<td></td>
<td>200.120.45.251</td>
<td></td>
<td>200.120.45.251</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>First Host</th>
<th>Last Host</th>
<th>Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orlando LAN</td>
<td>200.120.45.0</td>
<td>200.120.45.1</td>
<td>200.120.45.62</td>
</tr>
<tr>
<td></td>
<td>200.120.45.63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daytona LAN</td>
<td>200.120.45.160</td>
<td>200.120.45.161</td>
<td>200.120.45.190</td>
</tr>
<tr>
<td></td>
<td>200.120.45.191</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tampa LAN</td>
<td>200.120.45.64</td>
<td>200.120.45.65</td>
<td>200.120.45.126</td>
</tr>
<tr>
<td></td>
<td>200.120.45.127</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Miami LAN</td>
<td>200.120.45.128</td>
<td>200.120.45.129</td>
<td>200.120.45.158</td>
</tr>
<tr>
<td></td>
<td>200.120.45.159</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key West LAN</td>
<td>200.120.45.176</td>
<td>200.120.45.177</td>
<td>200.120.45.190</td>
</tr>
<tr>
<td></td>
<td>200.120.45.191</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B. Examine the initial network connectivity

1. Daytona Ethernet0: YES, Key West Serial0/0: YES, HostE: NO
   Orlando Serial0/0: YES, Daytona Serial1/0: YES, HostC: NO
   Daytona Serial0/0: YES, Orlando Serial1/0: YES, HostB: YES

2. All interfaces are up/up and clocking is correctly configured on all serial links. All interfaces are configured with an IP address. There are no obvious configuration problems.

Task 3: Correct Configuration Issues

A. Examine the specific points of failure

1. No, a ping to HostC from the console of the Miami router failed.
2. No, a ping to HostC from the virtual console of the Daytona router fails.

A ping to a directly connected host could fail if an erroneous route in the routing table diverts the traffic to an invalid destination, where the traffic is ultimately dropped.
3. Yes, a ping to the Ethernet0 interface of the Daytona router is successful.
4. Yes, a ping to the Ethernet0 interface on the Key West router is successful.
5. No, a ping to HostE fails.
6. The output of the `show ip route` command shows that all routes to the 200.120.45.176/28 network point toward the Key West router. This causes a problem with traffic addressed to HostC, which is connected to the Daytona router. Further examination reveals that the IP addresses of the Key West Ethernet0 interface and HostE fall into different networks; therefore, traffic addressed to HostE can never be delivered.
7. No, all IP addresses are not assigned correctly. The Ethernet0 interface on the Key West router is configured with an incorrect IP address.

B. Correct the configuration
1. The configuration error exists on the Key West router.
2. The Ethernet0 interface on the Key West router is configured with an incorrect IP address. This interface is configured with an IP address of 200.120.45.177 with a mask of 255.255.255.240.

This causes two problems: First, this IP address and the IP address of HostE, which is connected to Ethernet0, are in different networks and therefore cannot communicate. This prevents the rest of the network from reaching HostE.

The second problem is that the IP address that is currently assigned to Ethernet0 on the Key West router overlaps the network assigned to the Daytona LAN. The Daytona LAN is configured with a 27-bit prefix (mask 255.255.255.224) and has an address range from 200.120.45.160 through 200.120.45.191. The Ethernet0 interface on the Key West router is configured with an IP address of 200.120.45.177 with a 28-bit prefix (mask 255.255.255.240).

This causes the Key West router to announce a network via Enhanced Interior Gateway Routing Protocol (EIGRP) that overlaps half of the Daytona LAN network. The network that the Key West router announces has a 28-bit prefix and is preferred over the overlapping network with the shorter prefix, which the Daytona router advertises. The result is that half of the Daytona LAN’s network addresses are unreachable.

3. You should use the following commands on the Key West router to correct the configuration error.

```
config t
interface Ethernet0
ip address 200.120.45.193 255.255.255.240
```

Task 4: Verify Configuration
A. Verify connectivity
1. Yes, all the pings are successful. The pings to HostC and HostE, which failed before, are now successful.
2. No, there are no devices that fail to respond to a ping. All the pings are now successful.

B. Verify routing
1. You should use the `show ip route` on the Miami router to examine the contents of the IP routing table.
2. The route to the 200.120.45.176/28 network, which points toward the Key West router, is gone and has been replaced by the correct route to the 200.120.45.160/27 network, which points toward the Daytona router.
3. The rest of the network can now reach HostC and HostE.
### Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Miami Router</th>
<th>Key West Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>! Version 12.1</td>
<td>! Version 12.1</td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
<td>no service password-encryption</td>
</tr>
<tr>
<td>! hostname Miami</td>
<td>! hostname KeyWest</td>
</tr>
<tr>
<td>enable secret cisco</td>
<td>enable secret cisco</td>
</tr>
<tr>
<td>! ip subnet-zero</td>
<td>! ip subnet-zero</td>
</tr>
<tr>
<td>! interface Serial0/0</td>
<td>! interface Serial0/0</td>
</tr>
<tr>
<td>description ToTampa</td>
<td>description ToDaytona</td>
</tr>
<tr>
<td>ip address 200.120.45.246 255.255.255.252</td>
<td>ip address 200.120.45.254 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>! interface Serial1/0</td>
<td>! interface Serial1/0</td>
</tr>
<tr>
<td>description toDaytona</td>
<td>description toKeyWest</td>
</tr>
<tr>
<td>ip address 200.120.45.250 255.255.255.252</td>
<td>ip address 200.120.45.254 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>! interface Serial1/1</td>
<td>! interface Serial1/1</td>
</tr>
<tr>
<td>description toKeyWest</td>
<td>description toKeyWest</td>
</tr>
<tr>
<td>ip address 200.120.45.253 255.255.255.252</td>
<td>ip address 200.120.45.254 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>! interface Ethernet0</td>
<td>! interface Ethernet0</td>
</tr>
<tr>
<td>description MiamiLAN</td>
<td>description KeyWestLAN</td>
</tr>
<tr>
<td>ip address 200.120.45.129 255.255.255.224</td>
<td>ip address 200.120.45.193 255.255.255.240</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>! router eigrp 100</td>
<td>! router eigrp 100</td>
</tr>
<tr>
<td>network 200.120.45.0</td>
<td>network 200.120.45.0</td>
</tr>
<tr>
<td>! ip classless</td>
<td>! ip classless</td>
</tr>
<tr>
<td>no ip http server</td>
<td>no ip http server</td>
</tr>
<tr>
<td>! line con 0</td>
<td>! line con 0</td>
</tr>
<tr>
<td>transport input none</td>
<td>transport input none</td>
</tr>
<tr>
<td>line aux 0</td>
<td>line aux 0</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
</tr>
<tr>
<td>password sanfran</td>
<td>password sanfran</td>
</tr>
<tr>
<td>! no scheduler allocate</td>
<td>! no scheduler allocate</td>
</tr>
<tr>
<td>end</td>
<td>end</td>
</tr>
</tbody>
</table>
Lab 44: Configuring OSPF

Objective
This lab will give you hands-on experience working with the Open Shortest Path First (OSPF) routing protocol. The simulated network is partially configured with OSPF. A new router, which connects the Key West location to the rest of the network, has recently been added and has not yet been configured for OSPF. In addition, at least one configuration error exists that is preventing OSPF from functioning correctly in other parts of the network. You must configure the new Key West router for OSPF and identify and correct any remaining configuration errors in the simulated network. Some passwords have been set to “cisco”.

Lab Topology
The simulated network topology for this lab consists of five routers connected by a series of wide area network (WAN) links. These WAN links are capable of moving traffic at the rate of 512 kilobits per second (Kbps) with the exception of the Orlando—Daytona link, which is a 64-Kbps link. Each router is connected to two neighboring routers with the exception of the Key West router, which is connected by a single 512-Kbps WAN link to the Miami router.

Each router also has an Ethernet interface connected to the local area network (LAN) at each location. Each LAN has one PC host connected. All router interfaces are configured with IP addresses from the 200.120.45.0/24 network.

Variable Length Subnet Masking (VLSM) is used to divide this network into appropriately sized subnetworks for each WAN and LAN in the topology. The OSPF routing protocol is used to allow each router to dynamically update its routing table with routes to reach all networks in the topology. This is a single-area OSPF topology. The diagram below represents this topology.
Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>network network wildcard_mask area_id</td>
<td>activates OSPF on the specified network</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>sends an ICMP echo request</td>
</tr>
<tr>
<td>router ospf area_id</td>
<td>enters router configuration mode for an OSPF process</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show ip ospf neighbor</td>
<td>displays OSPF neighbor information</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>displays routing protocols enabled for a device</td>
</tr>
<tr>
<td>show ip route</td>
<td>displays the IP routing table</td>
</tr>
<tr>
<td>show running-configuration</td>
<td>displays the active configuration file</td>
</tr>
</tbody>
</table>

Lab Tasks

Task 1: Load the Lab 44 Initial Network Configuration

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator.

Task 2: Examine the Initial Network Configuration

A. Examine the routing topology

1. Log on to the console of the Key West router. Refer to the command summary at the beginning of this lab; what command should you use to display the routing table on the Key West router? __________________________________________________________________________

   Examine the output of this command. What conclusion can you draw regarding the operation of the OSPF routing protocol on the Key West router? __________________________________________________________________________

B. Examine the configuration

1. Refer to the command summary; what command should you use to display the currently executing configuration on the Key West router? __________________________________________________________________________

   Use this command to examine the currently executing configuration on the Key West router. What other commands could you use to view more information regarding the operation of OSPF on the Key West router? __________________________________________________________________________

2. Review the information you have gathered so far. Is the OSPF routing protocol running on the Key West router? __________________________________________________________________________

   How did you determine this? __________________________________________________________________________

3. If OSPF is running on the Key West router, what would prevent OSPF from learning about the
other networks in the topology? __________________________________________________

4. In order for OSPF to send and receive updates from its neighbors, the appropriate router interfaces must be configured for OSPF. Examine the configuration of the Key West router and determine if this has been done. What command is missing or misconfigured?

C. Correct the configuration
1. Examine the information that you have gathered so far, and briefly explain how you plan to correct the configuration error you have found. ____________________________________________________________

Refer to the command summary; what command should you use to correct this error? ____________________________________________________________

2. Enter these commands into the running configuration of the Key West router.

D. Verify OSPF behavior
1. After you correct the configuration error you have discovered, use the appropriate commands to reexamine the routing table on the Key West router. What change do you observe? ____________________________________________________________

Task 3: Examine the Remainder of the Topology
A. Evaluate the current routing topology
1. Log on to the console of the Key West router. Refer to the network topology diagram; which interfaces and hosts are you able to ping successfully? ____________________________________________________________

2. Examine the routing table on the Key West router. Are routes to any of the networks in the topology missing? ____________________________________________________________
   If so, which network routes are missing? ____________________________________________________________

3. From the console of the Key West router, attempt to ping some of the devices that are configured with IP addresses that fall within networks listed in the routing table of the Key West router. Do any of these pings fail? ____________________________________________________________
   If so, briefly explain why this is the case. ____________________________________________________________

B. Examine the remaining routers in the topology
1. From the console of the Key West router, attempt to ping the Ethernet0 interface on the Daytona router. Is this ping successful? ____________________________________________________________

2. From the console of the Key West router, attempt to ping HostC. Is this ping successful? ____________________________________________________________

3. If these pings are not successful, examine the configuration of the Daytona router and briefly explain why these pings may not be successful. ____________________________________________________________
4. Refer to the command summary; what commands should you use to correct the problems that you observe? __________________________________________________
Enter these commands into the running configuration of the Daytona router. In the following steps, you will enter similar commands into the running configuration of the Orlando router and the Tampa router.

5. What changes in the routing tables on the Key West router do you observe after you make these changes? __________________________________________________

6. From the console of the Key West router, attempt to ping the Ethernet0 interface on the Daytona router and HostC. Are these pings successful now? Briefly explain. __________

7. Examine the running configuration of the Orlando router. From the console of the Key West router, attempt to ping the Ethernet0 interface on the Orlando router and HostB. Are these pings successful? ____________________________
   If not, what configuration errors do you observe on the Orlando router that would cause these pings to fail? ____________________________

8. Enter the appropriate commands into the running configuration of the Orlando router to correct the problems. From the console of the Key West router, attempt to ping the Ethernet0 interface on the Orlando router and HostB. Are these pings successful now?

9. If these pings are successful, briefly explain why they are successful now when they failed earlier. ____________________________

10. Examine the running configuration of the Tampa router. From the console of the Key West router, attempt to ping the Ethernet0 interface on the Tampa router and HostA. Are these pings successful? ____________________________
    If not, what configuration errors do you observe on the Tampa router that would cause these pings to fail? ____________________________

11. Enter the appropriate commands into the running configuration of the Tampa router to correct the problems. From the console of the Key West router, attempt to ping the Ethernet0 interface on the Tampa router and HostA. Are these pings successful now? __________

12. If these pings are successful, briefly explain why they are successful now when they failed earlier. ____________________________

Task 4: Verify Network Connectivity

A. Verify Routes

1. Examine the network topology diagram and identify all existing networks. Log on to the console of each router and ensure that all networks are either directly connected or listed as OSPF routes in the routing table. Are any routes missing? ____________________________
   If so, review and correct your configuration.
B. Verify connectivity
1. Log on to the console of HostE and attempt to ping each router interface and each PC host. Are these pings successful? ________________________________
   If not, review and correct your configuration.

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Examine the routing topology
1. You should use the `show ip route` command on the Key West router to display the routing table.

   There are no OSPF routes in the Key West routing table. This indicates that OSPF on the Key West router is misconfigured or is not receiving updates from an OSPF neighbor.

B. Examine the configuration
1. You should use the `show running-config` command on the Key West router to display the currently executing configuration.

   Other commands that would provide information about the operation of OSPF on the Key West router include `show ip ospf neighbor` and `show ip protocols`.

2. Yes, the OSPF routing protocol is running on the Key West router. The output of the `show ip protocols` command clearly indicates this. Also, you can examine the running configuration on the Key West router by issuing the `show running-config` command. This shows that the `router ospf 1` command has been used to create an OSPF process.

3. Once the OSPF process has been created by using the `router ospf area_id` command, the interfaces that should attempt to create OSPF neighbor relationships must be configured with the appropriate `network` commands in router configuration mode. Entering the `router ospf area_id` command places the router in router configuration mode.

   The `network` command configures a network address, a wildcard mask, and an area ID. OSPF will attempt to create OSPF neighbor relationships by sending OSPF Hello packets out all interfaces that match the network address and wildcard mask used in the `network` command. If the network and mask specified in the `network` commands on the Key West router do not match the IP address assigned to any of the router’s interfaces, none of the router interfaces will establish relationships with OSPF neighbors and the router will not be able to learn about the other networks in the topology.

   For example, `network 200.120.45.0 0.0.0.255 area 0` will include all interfaces addressed in the range 200.120.45.0 through 200.120.45.254 and will attempt to put these interfaces into OSPF area 0. Alternatively, a wildcard mask with all zeros could be used to identify a specific interface. The `network 200.120.45.193 0.0.0.0 area 0` command will match only the interface configured with IP address 200.120.45.193.
4. The appropriate interfaces are configured for OSPF. However, the network command on the Key West router is misconfigured and will not match any interfaces; therefore, no Hello packets will be sent in an attempt to locate OSPF neighbors.

C. Correct the configuration
1. The network 200.120.45.0 0.0.0.0 area 0 command in the OSPF configuration on the Key West router will not match any interfaces, because a wildcard mask with all zeros tells the router to match the exact address given, which is a network address, not an IP address assigned to an interface. When a wildcard mask with all zeros is used, a specific IP address must be given, not a network address.

To correct the configuration, you should first remove the incorrect network statement and then add the correct one on the Key West router by using the following commands.

```
config t
router ospf 1
no network 200.120.45.0 0.0.0.0 area 0
network 200.120.45.0 0.0.0.255 area 0
```

These commands remove the incorrect wildcard mask and replace it with the correct one. The network 200.120.45.0 0.0.0.255 area 0 command tells OSPF to use any interface configured with an IP address that falls within the 200.120.45.0/24 network.

2. No answer required.

D. Verify OSPF behavior
1. Before you corrected the OSPF configuration on the Key West router, the only networks listed in the routing table were the networks directly connected to the Key West router. After you have corrected the OSPF configuration on the Key West router, the Key West router forms an OSPF neighbor relationship with the Miami router and begins to receive routing table updates via OSPF.

Task 3: Examine the Remainder of the Topology

A. Evaluate the current routing topology
1. From the console of the Key West router, it is now possible to successfully ping all the interfaces of the Miami router and HostD, which connects to the Miami router. It is not possible to ping any of the interfaces on the distant interfaces of the Daytona and Tampa routers.

2. Yes, there are networks in the topology that are missing from the routing table of the Key West router in the current configuration. The following networks are missing:

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.120.45.64</td>
<td>Tampa LAN</td>
</tr>
<tr>
<td>200.120.45.160</td>
<td>Daytona LAN</td>
</tr>
<tr>
<td>200.120.45.0</td>
<td>Orlando LAN</td>
</tr>
<tr>
<td>200.120.45.236</td>
<td>Orlando–Tampa WAN</td>
</tr>
<tr>
<td>200.120.45.240</td>
<td>Orlando–Daytona WAN</td>
</tr>
</tbody>
</table>
3. Pings are successful to all of the devices that fall within the networks listed in the Key
West router’s routing table.

B. Examine the remaining routers in the topology
1. No, a ping to the Ethernet0 interface at 200.120.45.161 from the console of the Key West
router fails.
2. No, a ping to HostC at 200.120.45.180, on the Daytona LAN, fails.
3. The wildcard mask on the network command in the OSPF configuration on the Daytona
router is incorrect. A mask of 0.0.0.63 is too restrictive and matches the Ethernet0
interface but does not match either of the serial interfaces. This prevents the Orlando–
Daytona and Daytona–Miami WAN networks from being announced to the other routers in
the topology.
4. You should use the following commands on the Daytona router to correct the problems.

```
config t
router ospf 1
no network 200.120.45.0 0.0.0.63 area 0
network 200.120.45.0 0.0.0.255 area 0
```
5. Routes to the Orlando–Daytona WAN and the Daytona–Miami WAN now appear in the
routing table on the Key West router.
6. Yes, pings from the console of the Key West router to the Ethernet0 interface on the
Daytona router and HostC on the Daytona LAN are successful, because the Key West router
now has a route to the Daytona LAN in its routing table.
7. No, pings to the Ethernet0 interface on the Orlando router and to HostB on the Orlando
LAN fail.

The output of the show ip protocols command shows that the Orlando router appears
to have an OSPF process configured. However, there are no network commands in the OSPF
configuration; therefore, no interfaces on the Orlando router are exchanging OSPF routing
table updates with OSPF neighbors.
8. You should use the following commands on the Orlando router to correct the problems.

```
config t
router ospf 1
network 200.120.45.0 0.0.0.255 area 0
```
Yes, pings to the Ethernet0 interface on the Orlando router and HostB on the Orlando LAN
are now successful.
9. The pings are successful because the Key West router can now locate a path to the
Orlando LAN in its routing table.
10. No, pings from the console of the Key West router to Ethernet0 on the Tampa router and to
HostA on the Tampa LAN fail.

The output of the show ip protocols command shows that the Tampa router is not currently
running OSPF.
11. You should use the following command on the Tampa router to correct the problems.
   ```
   config t
   router ospf 1
   network 200.120.45.0 0.0.0.255 area 0
   ```
   Yes, pings from the console of the Key West router to the Ethernet0 interface on the Tampa router and to HostA on the Tampa LAN are now successful.

12. These pings are successful because the Key West router can now identify a path to the Tampa LAN by looking in its routing table.

**Task 4: Verify Network Connectivity**

**A. Verify routes**

1. No, there are no missing routes. All networks in the topology are present in the routing tables of all routers. These routes are either directly connected or learned by OSPF.

**B. Verify connectivity**

1. Yes, pings from the console of HostE to each router interface and to each PC host are successful.
### Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Key West</th>
<th>Tampa</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hostname KeyWest</code></td>
<td><code>hostname Tampa</code></td>
</tr>
<tr>
<td><code>enable secret cisco</code></td>
<td><code>enable secret admin</code></td>
</tr>
<tr>
<td><code>ip subnet-zero</code></td>
<td><code>ip subnet-zero</code></td>
</tr>
<tr>
<td><code>interface Serial0/0</code></td>
<td><code>interface Serial0/0</code></td>
</tr>
<tr>
<td><code>description toMiami</code></td>
<td><code>description ToOrlando</code></td>
</tr>
<tr>
<td><code>ip address 200.120.45.254 255.255.255.252</code></td>
<td><code>ip address 200.120.45.238 255.255.255.252</code></td>
</tr>
<tr>
<td><code>no ip directed-broadcast</code></td>
<td><code>no ip directed-broadcast</code></td>
</tr>
<tr>
<td><code>bandwidth 512</code></td>
<td><code>bandwidth 512</code></td>
</tr>
<tr>
<td><code>interface Serial1/0</code></td>
<td><code>interface Serial1/0</code></td>
</tr>
<tr>
<td><code>description ToMiami</code></td>
<td><code>description ToMiami</code></td>
</tr>
<tr>
<td><code>ip address 200.120.45.193 255.255.255.240</code></td>
<td><code>ip address 200.120.45.245 255.255.255.252</code></td>
</tr>
<tr>
<td><code>no ip directed-broadcast</code></td>
<td><code>no ip directed-broadcast</code></td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td><code>bandwidth 512</code></td>
</tr>
<tr>
<td><code>interface Ethernet0</code></td>
<td><code>interface Ethernet0</code></td>
</tr>
<tr>
<td><code>description KeyWestLAN</code></td>
<td><code>description TampaLAN</code></td>
</tr>
<tr>
<td><code>ip address 200.120.45.0.0.0.0.255 area 0</code></td>
<td><code>ip address 200.120.45.0.0.0.0.255 area 0</code></td>
</tr>
<tr>
<td><code>ip classless</code></td>
<td><code>ip classless</code></td>
</tr>
<tr>
<td><code>no ip http server</code></td>
<td><code>no ip http server</code></td>
</tr>
<tr>
<td><code>line con 0</code></td>
<td><code>login</code></td>
</tr>
<tr>
<td><code>transport input none</code></td>
<td><code>password admin</code></td>
</tr>
<tr>
<td><code>line aux 0</code></td>
<td><code>line aux 0</code></td>
</tr>
<tr>
<td><code>line vty 0-4</code></td>
<td><code>line vty 0-4</code></td>
</tr>
<tr>
<td><code>login</code></td>
<td><code>login</code></td>
</tr>
<tr>
<td><code>password sanfran</code></td>
<td><code>password cisco</code></td>
</tr>
<tr>
<td><code>no scheduler allocate</code></td>
<td><code>no scheduler allocate</code></td>
</tr>
<tr>
<td><code>end</code></td>
<td><code>end</code></td>
</tr>
</tbody>
</table>
Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Daytona</th>
<th>Orlando</th>
</tr>
</thead>
<tbody>
<tr>
<td>! Version 12.1</td>
<td>! Version 12.1</td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
<td>no service password-encryption</td>
</tr>
<tr>
<td>! hostname Daytona</td>
<td>! hostname Orlando</td>
</tr>
<tr>
<td>enable secret admin</td>
<td>enable secret admin</td>
</tr>
<tr>
<td>! ip subnet-zero</td>
<td>! ip subnet-zero</td>
</tr>
<tr>
<td>! interface Serial0/0</td>
<td>! interface Serial0/0</td>
</tr>
<tr>
<td>description ToOrlando</td>
<td>description ToOrlando</td>
</tr>
<tr>
<td>ip address 200.120.45.242 255.255.255.252</td>
<td>ip address 200.120.45.237 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>! interface Serial1/0</td>
<td>! interface Serial1/0</td>
</tr>
<tr>
<td>description ToMiami</td>
<td>description ToMiami</td>
</tr>
<tr>
<td>ip address 200.120.45.249 255.255.255.252</td>
<td>ip address 200.120.45.241 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>! interface Ethernet0</td>
<td>! interface Ethernet0</td>
</tr>
<tr>
<td>description DaytonaLAN</td>
<td>description OrlandoLAN</td>
</tr>
<tr>
<td>ip address 200.120.45.161 255.255.255.224</td>
<td>ip address 200.120.45.1 255.255.255.192</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>! router ospf 1</td>
<td>! router ospf 1</td>
</tr>
<tr>
<td>network 200.120.45.128 0.0.0.63 area 0</td>
<td>network 200.120.45.0 0.0.0.255 area 0</td>
</tr>
<tr>
<td>network 200.120.45.0 0.0.0.255 area 0</td>
<td>! ip classless</td>
</tr>
<tr>
<td>! ip classless</td>
<td>! no ip http server</td>
</tr>
<tr>
<td>no ip http server</td>
<td>! line con 0</td>
</tr>
<tr>
<td>! line con 0</td>
<td>login</td>
</tr>
<tr>
<td>login</td>
<td>transport input none</td>
</tr>
<tr>
<td>transport input none</td>
<td>password admin</td>
</tr>
<tr>
<td>password admin</td>
<td>line aux 0</td>
</tr>
<tr>
<td>line aux 0</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>login</td>
</tr>
<tr>
<td>login</td>
<td>password cisco</td>
</tr>
<tr>
<td>password cisco</td>
<td>! no scheduler allocate</td>
</tr>
<tr>
<td>! no scheduler allocate</td>
<td>end</td>
</tr>
</tbody>
</table>
Lab 45: EIGRP Authentication

Objective
Understand the Enhanced Interior Gateway Routing Protocol (EIGRP) authentication process, and configure the routers in the simulated network to require EIGRP authentication before they advertise routes to or accept routing table updates from EIGRP neighbors.

Lab Topology
The simulated network topology for this lab consists of five routers connected by point-to-point serial wide area network (WAN) links. Each router also has a local area network (LAN) connected to its Ethernet interface. Each LAN has one host PC connected. This simulated topology is comparable to an actual network connecting five geographically separate offices, each with a LAN to which desktop PCs and servers are connected.

In the initial configuration, the serial WAN links and the Ethernet LANs are connected and all interfaces are up. IP addresses have been assigned to each interface and EIGRP has been configured so that each router is advertising its directly connected networks. The network is fully functional. You can log on to the console of any device and successfully ping any of the other devices in the network. The diagram below represents this topology.
## Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip route *</td>
<td>deletes routes from the IP routing table</td>
</tr>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>interface serial slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>ip authentication key-chain eigrp as_number key-chain</td>
<td>enables authentication of EIGRP packets</td>
</tr>
<tr>
<td>ip authentication mode as_number md5</td>
<td>specifies the type of authentication used in EIGRP packets</td>
</tr>
<tr>
<td>key chain key_chain_name</td>
<td>creates or modifies a key chain</td>
</tr>
<tr>
<td>key key_id</td>
<td>creates or modifies a key chain key</td>
</tr>
<tr>
<td>key-string key_string_text</td>
<td>specifies the text string for the key</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>sends an ICMP echo request</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>displays routing protocols enabled for a device</td>
</tr>
<tr>
<td>show ip route</td>
<td>displays the IP routing table</td>
</tr>
<tr>
<td>tracert ip_address</td>
<td>displays the network path to a given destination</td>
</tr>
</tbody>
</table>

## Lab Tasks

### Task 1: Load the Lab 45 Initial Network Configuration

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator.

### Task 2: Examine the Initial Network Configuration

#### A. Verify routing

1. Log on to the console of the Key West router. Examine the routes in the Key West routing table. Compare these routes to the networks shown on the network topology diagram. Are routes to all networks present? _______________________________________

2. How many possible paths could be taken by traffic between HostE and HostB? ________

3. What path does traffic from HostE follow as it moves through the network to HostB? _____

   How did you determine this? _____________________________________________

4. Why do the routers in this network choose this particular path? ____________________________
5. What is the EIGRP autonomous system number in the simulated network? ___________
What purpose does this number serve? ________________________________________
_______________________________________________________________

B. Verify connectivity
1. Log on to the console of HostE, and attempt to ping HostA, HostB, HostC, and HostD. Are
these pings successful? _____________________________________________
2. Log on to the console of HostB, and attempt to ping interface Ethernet0 on the Key West
router. Is this ping successful? _______________________________________

Task 3: Understand EIGRP Authentication
A. Understand unauthenticated EIGRP
1. Full connectivity is established by the initial configuration for this lab. EIGRP is properly
configured and routes are being advertised between neighbors. Briefly explain the
requirements for routers that are using EIGRP to exchange routing table updates. ________
_______________________________________________________________
_______________________________________________________________
2. What security risks related to EIGRP exist when a network is configured in this manner?
_______________________________________________________________
_______________________________________________________________

B. Understand authenticated EIGRP
1. How might implementing EIGRP authentication mitigate the security risks that you
previously described? Briefly explain. ____________________________________
_______________________________________________________________
2. What are some potential disadvantages of EIGRP authentication? How might they be
mitigated? _______________________________________________________
_______________________________________________________________

Task 4: Implement EIGRP Authentication
A. Configure the authentication credentials
1. Create a key chain named MyKeyChain1 and add a key with the key string “sanjose”.
Create this key as key 1. Refer to the command summary at the beginning of this lab;
what commands should you use to create this key chain? ______________________
_______________________________________________________________
Enter these commands into the running configuration of the Key West and Miami routers.
2. You should begin by setting up EIGRP authentication between the Key West and Miami
routers. Which interfaces on these routers are responsible for sending routing table
updates between the Key West and the Miami routers? _______________________
3. Now you will configure the authentication mode on these interfaces. The EIGRP
authentication mode is configured on a per-interface basis. You should configure the
EIGRP authentication mode on the router interfaces that are responsible for sending
routing table updates between the Key West and the Miami routers. Refer to the command summary; what commands should you use on each of these interfaces? 

Enter these commands into the running configuration of the Key West and Miami routers.

4. Now that you have configured the EIGRP authentication mode on the appropriate interfaces, you should enter an additional command to identify the authentication key that will be used for EIGRP authentication. This command will reference the key chain that you created earlier. Refer to the command summary; what commands should you use to identify the key chain that should be used for each interface? 

Enter these commands into the running configuration of the Key West and Miami routers.

5. Note that the names of the key chains do not have to be identical on each router. The key strings however, must be identical. The key strings are used to create an MD5 hash, which is included in each EIGRP packet sent from the selected interface. The router receiving the EIGRP packet will generate its own MD5 hash from its key chain. If the hashes match, the EIGRP packet will be accepted and processed. Remember that you should configure the EIGRP authentication mode on both routers and the key strings must match on both routers.

6. The Miami and Key West routers are the only routers connected to their respective LANs; therefore, neither router is currently sending EIGRP updates from or receiving EIGRP updates on their Ethernet interfaces. Why might it still be a good idea to configure EIGRP authentication on the Ethernet interfaces of the Key West and Miami routers? 

Task 5: Verify EIGRP Authentication

A. Verify routing tables
1. After you have configured EIGRP authentication, display the routing table on the Key West router. Compare the current contents of the routing table with the routes you previously observed. Do you see any changes after implementing EIGRP authentication? Briefly explain.

B. Verify connectivity
1. Log on to the console of HostE, and attempt to ping HostA, HostB, HostC, and HostD. Are these pings successful? If not, review and correct your configuration.

2. Log on to the console of HostB, and attempt to ping interface Ethernet0 on the Key West router. Is this ping successful? If not, review and correct your configuration.

C. Verify authentication
1. Log on to the console of the Key West router. Use the no form of the key chain command to remove the key chain from the Key West router. What command should you use to accomplish this? 


2. Use the `clear ip route *` command to delete all routes from the Key West routing table. Wait at least 30 seconds, and then display the Key West routing table. What do you observe? ______________________________________________________

3. How are the changes that you observed in the routing table related to the removal of the key chain? Briefly explain. ___________________________________________________________

4. On the Key West router, re-create the key chain that you previously deleted. Wait approximately 30 seconds, and examine the Key West routing table again. What do you observe? Briefly explain. _______________________________________________________

5. Based on the behavior you observed in the previous four steps, what conclusion can you draw regarding the operation of EIGRP authentication between the Key West and Miami routers? ________________________________________________________

6. For more experience with EIGRP authentication, configure EIGRP authentication on the Tampa–Orlando, Tampa–Miami, Miami–Daytona, and Daytona–Orlando serial links.

**Lab Solutions**

**Task 2: Examine the Initial Network Configuration**

**A. Verify routing**

1. Yes, routes to all networks are present in the Key West routing table. You can use the `show ip route` command to determine this.

2. There are two possible paths from HostE to HostB: Key West to Miami to Daytona to Orlando, or Key West to Miami to Tampa to Orlando.

3. You can use the `traceroute` command (tracert on the Microsoft Windows platform) to determine the path that traffic takes from HostE to HostB. Traffic first goes to the default gateway of HostE, the Key West router. The traffic then travels from the Key West router to the Miami router, then to the Tampa router, and finally to the Orlando router, which will deliver the traffic to its destination, HostB.

4. The EIGRP routing protocol chooses the Key West to Miami to Tampa to Orlando path, because all the links in this path are 512-kilobits per second (Kbps) links. The Daytona to Orlando link is 64-Kbps and is therefore avoided if better paths are available.

5. You can use the `show ip protocols` command to determine that the EIGRP autonomous system number (ASN) in the simulated network is 100. This number uniquely identifies an EIGRP process. It is possible to run multiple EIGRP processes on the same router by giving each instance of EIGRP its own ASN. The `network` commands, which are a part of the EIGRP configuration, determine which interfaces are associated with which EIGRP process.
B. Verify connectivity
1. Yes, pings from the console of HostE to HostA, HostB, HostC, and HostD are successful.
2. Yes, a ping from the console of HostB to the Ethernet0 interface on the Key West router is successful.

Task 3: Understand EIGRP Authentication

A. Understand unauthenticated EIGRP
1. For two routers to form an EIGRP relationship and exchange routing table updates, the following conditions must be met:
   A. The routers must be configured with EIGRP.
   B. The routers must have interfaces that are either directly connected or connected to a common multi-access media such as Ethernet.
   C. The routers must be configured with common ASNs.
   D. The routers must have the appropriate network commands, which are used to configure EIGRP to use the interfaces that form the link between the two routers.
2. The major security risk associated with unauthenticated EIGRP is that any router added to the network can be configured with EIGRP and will automatically be included in the EIGRP topology as long as the ASN and network requirements are met. It is possible that an unknown or unauthorized router could be accidentally or maliciously connected to the network. This router could then be configured to negatively impact the routing topology of the entire network.

B. Understand authenticated EIGRP
1. Routers configured with EIGRP authentication will only accept updates from EIGRP neighbors that have been configured with the same authentication key. This ensures that routing table updates are received only from trusted sources; however, if the key becomes compromised as a result of poor administrative practices, updates may come from untrusted sources.
2. A potential disadvantage of using EIGRP authentication is the additional administrative overhead. Good key management practices, such as securely storing configuration backups and writing good network documentation, will reduce the administrative effort.

Task 4: Implement EIGRP Authentication

A. Configure the authentication credentials
1. You should use the following commands on the Key West router to create a key chain.
   ```
   config t
   key chain MyKeyChain1
   key 1
   key-string sanjose
   ```
You should use the following commands on the Miami router to create a key chain.

```
config t
key chain MyKeyChain2
key 1
key-string sanjose
```

2. The Serial0/0 interface on the Key West router and the Serial1/1 interface on the Miami router are directly connected to each other and are therefore responsible for sending EIGRP updates between these two routers.

3. You should use the following commands on the Key West router to configure the EIGRP authentication mode.

```
config t
interface Serial0/0
ip authentication mode eigrp 100 md5
```

You should use the following commands on the Miami router to configure the EIGRP authentication mode.

```
config t
interface serial1/1
ip authentication mode eigrp 100 md5
```

4. You should use the following commands on the Key West router to identify the authentication key that will be used for EIGRP authentication.

```
config t
interface serial0/0
ip authentication key-chain eigrp 100 MyKeyChain1
```

You should use the following commands on the Miami router to identify the authentication key that will be used for EIGRP authentication.

```
config t
interface serial1/1
ip authentication key-chain eigrp 100 MyKeyChain2
```

5. No answer required.

6. It would be a good practice to configure EIGRP authentication on the Ethernet0 interfaces of the Miami and Key West routers to protect the routing topology in the event that an unknown or unauthorized router is connected to the Miami or Key West LANs.

**Task 5: Verify EIGRP Authentication**

A. Verify routing tables

1. There should be no changes to the routing table as a result of EIGRP authentication. If routes are missing after you configure EIGRP authentication, you should investigate and correct any authentication problems.
B. Verify connectivity
1. Yes, pings from the console of HostE to HostA, HostB, HostC, and HostD are successful.
2. Yes, pings from the console of HostB to Ethernet0 on the Key West router are successful.

C. Verify authentication
1. You should use the `no key chain MyKeyChain1` command on the Key West router to remove the key.
2. After removing the key chain from the Key West router and clearing the routing table, all the EIGRP routes are absent.
3. Removing the key chain from the Key West router prevents the Key West router from authenticating to the Miami router; therefore, the Miami router no longer accepts EIGRP packets from the Key West router, thereby ending the EIGRP neighbor relationship between the Miami and Key West routers. As a result, the EIGRP routes are dropped from the Key West routing table.
4. After you re-create the key chain on the Key West router, the router can once again authenticate with the EIGRP process on the Miami router, thus restoring the EIGRP neighbor relationship between the Key West and Miami routers. The Key West and Miami routers once again begin to exchange EIGRP packets. The EIGRP routes are put back into the Key West routing table.
5. Based on the behavior observed in the previous steps, EIGRP authentication will only allow routes to be advertised between routers that are configured with a valid key.
6. No answer required.
Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Miami</th>
<th>Key West</th>
</tr>
</thead>
</table>
| ! Version 12.1  
 service timestamps debug uptime  
 service timestamps log uptime  
 no service password-encryption  
 ! hostname Miami  
 enable secret cisco  
 !  
 key chain mykeychain2  
 key 1  
 key-string sanjose  
 !  
 ip subnet-zero  
 !  
 interface Serial0/0  
 description ToTampa  
 ip address 192.168.100.10 255.255.255.252  
 no ip directed-broadcast  
 bandwidth 512  
 !  
 interface Serial1/0  
 description toDaytona  
 ip address 192.168.100.14 255.255.255.252  
 no ip directed-broadcast  
 !  
 interface Serial1/1  
 description toKeyWest  
 ip address 192.168.100.17 255.255.255.252  
 ip authentication mode eigrp 100 md5  
 ip authentication key-chain eigrp 100 mykeychain2  
 no ip directed-broadcast  
 bandwidth 512  
 !  
 interface Ethernet0  
 description MiamiLAN  
 ip address 192.168.3.1 255.255.255.0  
 no ip directed-broadcast  
 !  
 router eigrp 100  
 network 192.168.3.0  
 network 192.168.100.0  
 !  
 ip classless  
 no ip http server  
 !  
 line con 0  
 login  
 transport input none  
 password admin  
 line aux 0  
 line vty 0 4  
 login  
 password san fran  
 no scheduler allocate  
 end | ! Version 12.1  
 service timestamps debug uptime  
 service timestamps log uptime  
 no service password-encryption  
 ! hostname KeyWest  
 enable secret cisco  
 !  
 key chain mykeychain1  
 key 1  
 key-string sanjose  
 !  
 ip subnet-zero  
 !  
 interface Serial0/0  
 description toMiami  
 ip address 192.168.100.18 255.255.255.252  
 no ip directed-broadcast  
 !  
 interface Serial1/0  
 no ip address  
 no ip directed-broadcast  
 shutdown  
 !  
 interface Serial1/1  
 description toKeyWest  
 ip address 192.168.100.17 255.255.255.252  
 ip authentication mode eigrp 100 md5  
 ip authentication key-chain eigrp 100 mykeychain1  
 no ip directed-broadcast  
 bandwidth 512  
 !  
 interface Ethernet0  
 description KeyWestLAN  
 ip address 192.168.5.1 255.255.255.0  
 no ip directed-broadcast  
 !  
 router eigrp 100  
 network 192.168.100.0  
 network 192.168.5.0  
 !  
 ip classless  
 no ip http server  
 !  
 line con 0  
 login  
 transport input none  
 password admin  
 line aux 0  
 line vty 0 4  
 login  
 password san fran  
 !  
 no scheduler allocate  
 end |
Lab 46: OSPF Authentication

Objective
Understand the Open Shortest Path First (OSPF) authentication process, and configure the routers in the simulated network to require OSPF authentication before they advertise routes to or accept routing table updates from OSPF neighbors. This lab covers OSPF basic authentication as well as OSPF encrypted authentication. All passwords have been set to “cisco”.

Lab Topology
The simulated network topology for this lab consists of five routers connected by point-to-point serial wide area network (WAN) links. Each router also has a local area network (LAN) connected to its Ethernet interface. Each LAN has one host PC connected. This simulated topology is comparable to an actual network connecting five geographically separate offices, each with a LAN to which desktop PCs and servers are connected.

In the initial configuration, the serial WAN links and the Ethernet LANs are connected and all interfaces are up. IP addresses have been assigned to each interface and OSPF has been configured so that each router is advertising its directly connected networks. The network is fully functional. You can log on to the console of any device and successfully ping any of the other devices in the network. The diagram below represents this topology.
# Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td><code>interface serial slot/port</code></td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>`ip ospf authentication [message-digest</td>
<td>null]`</td>
</tr>
<tr>
<td><code>ip ospf authentication-key password</code></td>
<td>assigns a password to be used by neighboring routers that are using OSPF MD5 authentication</td>
</tr>
<tr>
<td><code>ip ospf message-digest-key key_id encryption_type md5 key</code></td>
<td>enables OSPF MD5 authentication</td>
</tr>
<tr>
<td><code>no ip ospf authentication</code></td>
<td>removes the authentication type for an interface</td>
</tr>
<tr>
<td><code>ping ip_address</code></td>
<td>sends an ICMP echo request</td>
</tr>
<tr>
<td><code>show ip interface brief</code></td>
<td>summarizes all interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td><code>show ip ospf interface interface slot/port</code></td>
<td>displays OSPF interface information</td>
</tr>
<tr>
<td><code>show ip ospf neighbor</code></td>
<td>displays OSPF neighbor information</td>
</tr>
<tr>
<td><code>show ip route</code></td>
<td>displays the IP routing table</td>
</tr>
</tbody>
</table>

# Lab Tasks

**Task 1: Load the Lab 46 Initial Network Configuration**

Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator.

**Task 2: Examine the Initial Network Configuration**

**A. Verify routing**

1. Log on to the console of the Key West router. Examine the routes in the Key West routing table. Compare these routes to the networks shown on the network topology diagram. Are routes to all networks present? _______________________________________

**B. Verify connectivity**

1. Log on to the console of HostE, and attempt to ping HostA, HostB, HostC, and HostD. Are these pings successful? _______________________________________

2. Log on to the console of HostB, and attempt to ping interface Ethernet0 on the Key West router. Is this ping successful? _______________________________________

---

Boson NetSim for CCNA Lab Manual 239
Task 3: Understand OSPF Authentication

A. Understand unauthenticated OSPF
1. Full connectivity is established by the initial configuration for this lab. OSPF is properly configured and routes are being advertised between neighbors. Briefly explain the requirements for routers that are using OSPF to exchange routing table updates when using OSPF.

2. What security risks related to OSPF exist when a network is configured in this manner?

B. Understand authenticated OSPF
1. How might implementing OSPF authentication mitigate the security risks that you previously outlined? Briefly explain.

Task 4: Implement OSPF Basic Authentication

A. Configure the authentication credentials
1. In this lab, you will begin by configuring OSPF authentication between the Key West and Miami routers. Which interfaces are used to connect the Key West and Miami routers to the Key West–Miami WAN serial link?

2. Refer to the command summary at the beginning of this lab; what commands should you use to enable OSPF authentication on the interfaces you previously identified?

Enter these commands into the running configuration of the Key West and Miami routers.

3. Next, you will configure an OSPF authentication key on each interface. You will use the text string “sanjose” as the authentication key on both routers. Note that the same key must be used on each pair of interfaces in order for authentication to succeed. If the keys do not match, authentication will fail and OSPF updates will not be exchanged between the two routers.

4. Refer to the command summary; what commands should you use to configure an OSPF authentication key on the interfaces that you previously identified?

Enter these commands into the running configuration of the Key West and Miami routers.

Task 5: Verify OSPF Authentication

A. Verify routing tables
1. After you have configured OSPF authentication, display the routing table on the Key West router. Compare the current contents of the routing table with the routes you previously observed. Do you see any changes after implementing OSPF authentication? Briefly explain.
B. Verify connectivity
1. Log on to the console of HostE, and attempt to ping HostA, HostB, HostC, and HostD. Are these pings successful? __________________________________________________________
   If not, review and correct your configuration.
2. Log on to the console of HostB, and attempt to ping the Ethernet0 interface on the Key West router. Is this ping successful? __________________________________________
   If not, review and correct your configuration.
3. Based on the behavior you observed in the previous two steps, what conclusion can you draw regarding the operation of OSPF authentication between the Key West and Miami routers? _________________________________________________________
   ________________________________________________________________
4. Refer to the command summary; what commands should you use to view additional information about the operation of OSPF? ________________________________________________________________
   ________________________________________________________________

Task 6: Implement OSPF Encrypted Authentication
A. Implement OSPF encrypted authentication
1. You have now implemented basic OSPF authentication. Briefly explain the potential security risks associated with OSPF basic authentication. ________________________________________________________________
   2. Review the commands you used to enable basic OSPF authentication between the Miami and Key West routers. You now need to remove these commands from the configuration of the Miami and Key West routers. What commands should you use to accomplish this?
   Enter these commands into the running configuration of the Miami and Key West routers.
3. You will now reconfigure these same interfaces to use message digest authentication. Routers configured with message digest authentication use the authentication key to compute an MD5 hash, which is included in the OSPF packets. The neighbor also computes an MD5 hash from its authentication key and compares the two hash values. The OSPF packet is accepted only if the two hashes match. Refer to the command summary; what commands should you use to enable message digest authentication on the interfaces that connect the Miami and Key West routers?
   Enter these commands into the running configuration of the Miami and Key West routers.
B. Verify OSPF encrypted authentication
1. Repeat Task 5 to verify the correct configuration of OSPF encrypted authentication.
Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Verify routing
1. Yes, routes to all networks are present in the Key West routing table. You can use the `show ip route` command to determine this.

B. Verify connectivity
1. Yes, pings from the console of HostE to HostA, HostB, HostC, and HostD are successful.
2. Yes, a ping from the console of HostB to the Ethernet0 interface on the Key West router is successful.

Task 3: Understand OSPF Authentication

A. Understand unauthenticated OSPF
1. In order for two routers configured with OSPF to form a neighbor relationship, they must have interfaces that are either directly connected or connected to a multi-access network media such as Ethernet. In addition, the IP addresses and masks must be in the same network and the OSPF Hello and Dead timers must be set to the same value. Routers configured with OSPF will form neighbor relationships with any other router that meets these requirements.
2. The major security risk associated with unauthenticated OSPF is that any router that meets the previous requirements will automatically form a neighbor relationship with a new OSPF router that is brought online. It is possible that an unknown or unauthorized router could be added to the network and could be configured to alter the routing topology of the entire network.

B. Understand authenticated OSPF
1. Routers configured with OSPF authentication will only accept updates from OSPF neighbors that have been configured with the same authentication credentials. This will prevent unknown or unauthorized routers from causing unintentional or malicious alterations to the network routing topology.

Task 4: Implement OSPF Basic Authentication

A. Configure the authentication credentials
1. The Serial0/0 interface on the Key West router and the Serial1/1 interface on the Miami router are directly connected to each other and are therefore responsible for sending OSPF updates between the two routers.
2. You should use the following commands on the Key West router to enable OSPF authentication.
   ```
   config t
   interface serial0/0
   ip ospf authentication
   ```
You should use the following commands on the Miami router to enable OSPF authentication.

```
config t
interface serial1/1
ip ospf authentication
```

3. No answer required.

4. You should use the following commands on the Key West router to configure an OSPF authentication key.

```
config t
interface serial0/0
ip ospf authentication-key sanjose
```

You should use the following commands on the Miami router to configure an OSPF authentication key.

```
config t
interface serial1/1
ip ospf authentication-key sanjose
```

Task 5: Verify OSPF Basic Authentication

A. Verify routing tables

1. There should be no changes to the routing table as a result of OSPF authentication. If routes are missing after you configure OSPF authentication, you should investigate and correct any authentication problems.

B. Verify connectivity

1. Yes, pings from the console of HostE to HostA, HostB, HostC, and HostD are successful.
2. Yes, pings from the console of HostB to Ethernet0 on the Key West router are successful.
3. No changes have occurred to the routing table, and pings in the previous steps were successful; these indicate that OSPF authentication is functioning.
4. You should use the `show ip ospf neighbor` command on the Key West and Miami routers to view additional information.

    You should use the `show ip ospf interface serial0/0` command on the Key West router to view additional information.

    You should use the `show ip ospf interface serial1/1` command on the Miami router to view additional information.

Task 6: Implement OSPF Encrypted Authentication

A. Implement OSPF encrypted authentication

1. Basic OSPF authentication sends the authentication key across the network in clear text. If the packets traveling across the network media were to be captured with a network analyzer, the authentication key would be easily compromised.
2. You should use the following commands on the Key West router to remove basic OSPF authentication.

```config
config t
interface serial0/0
no ip ospf authentication
no ip ospf authentication-key sanjose
```

You should use the following commands on the Miami router to remove basic OSPF authentication.

```config
config t
interface serial1/1
no ip ospf authentication
no ip ospf authentication-key sanjose
```

3. You should use the following commands on the Key West router to enable message digest authentication.

```config
config t
interface serial0/0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 sanjose
```

You should use the following commands on the Miami router to enable message digest authentication.

```config
config t
interface serial1/1
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 sanjose
```

**B. Verify OSPF Encrypted Authentication**

1. See solutions in Task 5.
Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Miami</th>
<th>Key West</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>Version 12.1</td>
<td>Version 12.1</td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
<td>no service password-encryption</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>hostname Miami</td>
<td>hostname KeyWest</td>
</tr>
<tr>
<td>enable secret cisco</td>
<td>enable secret cisco</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>ip subnet-zero</td>
<td>ip subnet-zero</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface Serial0/0</td>
<td>interface Serial0/0</td>
</tr>
<tr>
<td>description ToTampa</td>
<td>description ToTampa</td>
</tr>
<tr>
<td>ip address 200.120.45.246 255.255.255.252</td>
<td>ip address 200.120.45.254 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface Serial1/0</td>
<td>interface Serial1/0</td>
</tr>
<tr>
<td>description ToDaytona</td>
<td>description ToDaytona</td>
</tr>
<tr>
<td>ip address 200.120.45.250 255.255.255.252</td>
<td>ip address 200.120.45.250 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface Serial1/1</td>
<td>interface Serial1/1</td>
</tr>
<tr>
<td>description toKeyWest</td>
<td>description toKeyWest</td>
</tr>
<tr>
<td>ip address 200.120.45.253 255.255.255.252</td>
<td>ip address 200.120.45.253 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>ip ospf message-digest-key 1 md5 sanjose</td>
<td>ip ospf message-digest-key 1 md5 sanjose</td>
</tr>
<tr>
<td>ip ospf authentication message-digest</td>
<td>ip ospf authentication message-digest</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface Ethernet0</td>
<td>interface Ethernet0</td>
</tr>
<tr>
<td>description MiamiLAN</td>
<td>description MiamiLAN</td>
</tr>
<tr>
<td>ip address 200.120.45.129 255.255.255.224</td>
<td>ip address 200.120.45.129 255.255.255.224</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>router ospf 1</td>
<td>router ospf 1</td>
</tr>
<tr>
<td>network 200.120.45.0 0.0.0.255 area 0</td>
<td>network 200.120.45.193 255.255.255.240</td>
</tr>
<tr>
<td>!</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>ip classless</td>
<td>ip classless</td>
</tr>
<tr>
<td>no ip http server</td>
<td>no ip http server</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>line con 0</td>
<td>line con 0</td>
</tr>
<tr>
<td>transport input none</td>
<td>transport input none</td>
</tr>
<tr>
<td>line aux 0</td>
<td>line aux 0</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
</tr>
<tr>
<td>password sanfran</td>
<td>password sanfran</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>no scheduler allocate</td>
<td>no scheduler allocate</td>
</tr>
<tr>
<td>end</td>
<td>end</td>
</tr>
</tbody>
</table>


Lab 47: EIGRP and Wildcard Masks

Objective
Understand wildcard masks and use wildcard masks to specify which interfaces Enhanced Interior Gateway Routing Protocol (EIGRP) should use.

Lab Topology
The simulated network topology for this lab consists of five routers connected by point-to-point serial wide area network (WAN) links. Each router also has a local area network (LAN) connected to its Ethernet interface. Each LAN has one host PC connected. This simulated topology is comparable to an actual network connecting five geographically separate offices, each with a LAN to which desktop PCs and servers are connected. The diagram below represents this topology.
Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>interface serial slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>network network [wildcard]</td>
<td>specifies a list of networks for the EIGRP routing process</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>sends an ICMP echo request</td>
</tr>
<tr>
<td>show ip eigrp interfaces</td>
<td>displays information about interfaces configured for EIGRP</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>summarizes all interfaces and the IP address assigned to each as well as</td>
</tr>
<tr>
<td></td>
<td>the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show ip route</td>
<td>displays the IP routing table</td>
</tr>
<tr>
<td>show running-configuration</td>
<td>displays the active configuration file</td>
</tr>
</tbody>
</table>

Lab Tasks

Task 1: Load the Lab 47 Initial Network Configuration
Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator. The initial configuration will assign the correct host names and IP addresses to each device.

Task 2: Examine the Initial Network Configuration

A. Verify routing
1. Log on to the console of the Key West router, and display the contents of the Key West routing table. Refer to the command summary at the beginning of this lab; what command should you use to do this? ___________________________________
2. Refer to the network topology diagram and the contents of the Key West routing table. Are all networks shown in the topology diagram listed as either directly connected routes or EIGRP routes? ___________________________________

B. Verify connectivity
1. Log on to the console of HostE, and attempt to ping HostA, HostB, HostC, and HostD. Are these pings successful? ___________________________________

Task 3: Implement EIGRP Wildcard Masks

A. Examine the current EIGRP configuration
1. Examine the current EIGRP configuration on all five routers. How many EIGRP autonomous systems are present in the network? ___________________________________
2. How did you determine this? ___________________________________
3. What commands should you use to identify the interfaces that should attempt to form EIGRP neighbor relationships? _________________________________________

B. Understand wildcard masks
1. The network commands in the router eigrp configuration of each router identify the router interfaces that will participate in the EIGRP routing topology. In the initial configuration for this lab, the network commands include only the classful network address. This limits the flexibility of assigning interfaces to the EIGRP process. Briefly explain why this is so.
_______________________________________________________________
_______________________________________________________________

2. A wildcard mask is the inverse of a subnet mask. The mask 0.0.0.255 is an example of a classful wildcard mask. In the binary address, the bits that are zeros must match exactly and the bits that are ones will match any address. A wildcard mask of 0.0.0.255 would require exact matches in the first three octets and would match anything in the fourth octet.

3. Given the explanation of a wildcard mask, explain how EIGRP would select interfaces if it were configured with the network 192.168.100.0 0.0.0.255 command. _____________
_______________________________________________________________

C. Implement EIGRP wildcard masks
1. Examine the configuration of each of the five routers in the topology. How many network commands do you see listed in the EIGRP configuration of each router? _____________

2. Why are multiple network commands required? Briefly explain. ___________________
_______________________________________________________________

3. Reconfigure EIGRP on each router so that a single network command can be used to identify all interfaces that will run EIGRP. What commands should you use? _____________
_______________________________________________________________

Task 4: Verify EIGRP Wildcard Masks
A. Verify routing
1. Log on to the console of the Key West router, and display the contents of the Key West routing table. What command should you use to do this? _______________________

2. Refer to the network topology diagram and the output of the Key West routing table. Are all networks shown in the topology diagram either directly connected routes or EIGRP routes?
_______________________________________________________________

3. Compare this output to the results you previously received. Do you observe any changes after implementing EIGRP wildcard masks? ________________________________

B. Verify connectivity
1. Log on to the console of HostE, and attempt to ping HostA, HostB, HostC, and HostD. Are these pings successful? ____________________________
   If any of the pings fail, review and correct your configuration.
Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Verify routing
   1. You should use the `show ip route` command on the Key West router to display the contents of the routing table.
   2. Yes, all networks in the simulated topology are either directly connected or EIGRP routes in the Key West routing table.

B. Verify connectivity
   1. Yes, pings from the console of HostE to HostA, HostB, HostC, and HostD are successful.

Task 3: Implement EIGRP Wildcard Masks

A. Examine the current EIGRP configuration
   1. There is one EIGRP autonomous system in the simulated network.
   2. An examination of all five routers shows that they are all configured with the `router eigrp 100` command. The number 100 indicates the autonomous system number (ASN) with which the EIGRP routing process will associate.
   3. The `network` command is used to identify the router interfaces that will take part in the EIGRP routing process and attempt to form relationships with their EIGRP neighbors. Each router in the simulated network is configured with `network` commands that EIGRP uses to determine which interfaces to use.

B. Understand wildcard masks
   1. When the `network` command is configured with only a network address, EIGRP will include all interfaces whose IP address falls within the classful network boundary identified by the `network` command. For example, the `network 192.168.1.0` command will cause EIGRP to use all interfaces that are configured with IP addresses that fall within the 192.168.1.0/24 Class C network.
   2. No answer required.
   3. The `network 192.168.100.0 0.0.0.255` command indicates that EIGRP will use all interfaces with an IP address that falls between 192.168.100.1 and 192.168.100.254. This particular example uses a wildcard mask that falls on a classful network boundary.

The benefit of using wildcard masks is that they can designate a range of addresses that does not necessarily fall on a network boundary.

To calculate the wildcard mask, begin by calculating a subnet mask that, when combined with the network address, covers the range of IP addresses desired. Then, subtract the subnet mask you calculated from 255.255.255.255.
If you wanted to include all interfaces configured with IP addresses that fall in the range 192.168.100.1 through 192.168.100.30, you can use regular subnetting techniques to determine that the network 192.168.100.0 and the subnet mask 255.255.255.224 will define this range. You could then subtract 255.255.255.224 from 255.255.255.255 to find the wildcard mask 0.0.0.31. You would then use the network 192.168.100.0 0.0.0.31 command to configure EIGRP to use interfaces configured with IP addresses that fall between 192.168.100.1 and 192.168.100.30.

C. Implement EIGRP wildcard masks
1. Each router is configured with two network commands.
2. All five routers are configured with 192.168.0.0 private Class C addresses. Each router has interfaces that are configured with IP addresses that fall in different Class C networks in the 192.168.0.0 address space. It is therefore necessary to identify each Class C network with a separate network command in the EIGRP configuration.
3. You should use the following commands on all routers in the topology to reconfigure EIGRP so that a single network command can be used.

```
config t
no router eigrp 100
router eigrp 100
network 192.168.0.0 0.0.255.255
```

Note that removing the entire EIGRP configuration using the no router eigrp 100 command saves time, because it is not necessary to remove each network command individually. Removing the EIGRP configuration removes all of the associated network commands.

Task 4: Verify EIGRP Wildcard Masks
A. Verify routing
1. You should use the show ip route command on the Key West router to display the contents of the routing table.
2. Yes, all networks in the topology diagram are either directly connected or EIGRP routes.
3. There are no changes in the EIGRP routing table on the Key West router as a result of implementing EIGRP wildcard masks.

B. Verify connectivity
1. Yes, pings from the console of HostE to HostA, HostB, HostC, and HostD are successful.
Sample Configuration Scripts

Key West

! Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname KeyWest
enable secret cisco
!
ip subnet-zero
!
interface Serial0/0
description toMiami
ip address 192.168.100.18 255.255.255.252
no ip directed-broadcast
bandwidth 512
!
interface Serial1/0
no ip address
no ip directed-broadcast
shutdown
!
interface Ethernet0
description KeyWestLAN
ip address 192.168.5.1 255.255.255.0
no ip directed-broadcast
!
router eigrp 100
network 192.168.0.0 0.0.255.255
!
ip classless
no ip http server
!
line con 0
login
transport input none
password admin
line aux 0
line vty 0 4
login
password sanfran
!
no scheduler allocate
end
Lab 48: Configuring IPv6

Objective
Understand and implement Internet Protocol version 6 (IPv6) addressing in the simulated network topology, and implement Routing Information Protocol next generation (RIPng) to implement dynamic IPv6 routing.

Lab Topology
The simulated network topology for this lab consists of five routers connected by point-to-point serial wide area network (WAN) links. Each router also has a local area network (LAN) connected to its Ethernet interface. Each LAN has one host PC connected. This simulated topology is comparable to an actual network connecting five geographically separate offices, each with a LAN to which desktop PCs and servers are connected. The diagram below represents this topology.
Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>enters global configuration mode</td>
</tr>
<tr>
<td>interface serial slot/port</td>
<td>enters interface configuration mode</td>
</tr>
<tr>
<td>ip address</td>
<td>assigns an IPv4 address to an interface</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>assigns an IPv6 address to an interface</td>
</tr>
<tr>
<td>ipv6 router rip process_name</td>
<td>configures a router for RIPng</td>
</tr>
<tr>
<td>ipv6 rip process_name enable</td>
<td>configures an interface for RIPng</td>
</tr>
<tr>
<td>ping ip_address</td>
<td>sends an ICMP echo request</td>
</tr>
<tr>
<td>ping ipv6 ip_address</td>
<td>sends an ICMP echo request to an IPv6 address</td>
</tr>
<tr>
<td>show ip route</td>
<td>displays the IP routing table</td>
</tr>
<tr>
<td>show ipv6 interface brief</td>
<td>summarizes all IPv6 interfaces and the IP address assigned to each as well as the interface status: up, down, or administratively down</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>displays the contents of the IPv6 routing table</td>
</tr>
<tr>
<td>show running-configuration</td>
<td>displays the currently running configuration file</td>
</tr>
</tbody>
</table>

Lab Tasks

Task 1: Load the Lab 48 Initial Network Configuration
Make sure that the correct topology and configuration files for this lab are loaded. This will occur automatically when you select this lab from the Lab Navigator. The initial configuration will assign the correct host names and IP addresses to each device.

Task 2: Examine the Initial Network Configuration

A. Verify IP addressing
1. Examine the running configuration of the five routers, and compare the IP addresses on the WAN interfaces to the IP addresses on the network topology diagram. Are the IP addresses assigned to the device correct? ____________________________
   The IP address assigned to each router interface should match the IP address on the network topology diagram.

2. What types of IP addresses are currently assigned to the Key West, Miami, Tampa, Orlando, and Daytona routers? ____________________________

3. What is the theoretical maximum number of unique IP addresses of this type that can be assigned? ____________________________

4. Why is there a need to change this method of IP addressing? ____________________________
Task 3: Explore IPv6

A. Understand IPv6 addresses
1. Internet Protocol version 6 (IPv6) addresses will eventually replace the IP addresses currently in use today. What are the expected benefits of this new type of IP addressing?

________________________________________________________________________

2. What are some of the major differences between current IP addressing and IPv6? ______

________________________________________________________________________

3. What is the theoretical maximum number of IPv6 addresses that can be assigned? ______

4. The transition to IPv6 will not happen immediately. The transition from current IP addressing to IPv6 will occur over time. Briefly describe some of the techniques that will allow current IP addressing to coexist with IPv6 addressing. _____________________

________________________________________________________________________

Task 4: Implement IPv6

A. Implement IPv6 addresses
1. You will implement IPv6 addresses on the WAN links that connect the Miami, Tampa, Daytona, and Orlando routers. You will not implement IPv6 addresses on the WAN link that connects the Miami and Key West routers or on the LANs.

2. The diagram below shows the IPv6 addresses that should be assigned to each end of the WAN links:

![Diagram showing IPv6 addresses for Miami, Tampa, Daytona, and Orlando routers]
3. Refer to the command summary, and review the commands used to assign an IPv6 address to an interface. Compare these commands to the commands you currently use to assign IP addresses to an interface. What are the differences? ________________________________________________________________

4. Log on to the console of each router, and assign the IPv6 addresses shown in the table above. What commands should you use? ________________________________________________________________
   Enter these commands into the running configuration of each of the four routers shown in the diagram.

B. Implement IPv6 routing

1. Updated routing protocols capable of working with IPv6 network addresses must be used in order for IPv6 routes to be exchanged with other routers. You will implement Routing Information Protocol next generation (RIPng) in this lab. RIPng is capable of working with IPv6 addresses.

2. Refer to the command summary, and identify the commands you will use to enable IPv6 dynamic routing with RIPng. How do these commands differ from the commands you would use to enable RIP prior to IPv6? ________________________________________________________________

3. What commands should you use to configure RIPng on each of the routers shown in the previous diagram? ________________________________________________________________
   Enter these commands into the running configuration of each of the four routers shown in the diagram.

Task 5: Verify IPv6

A. Verify IPv6 addresses

1. Examine each of the four routers that you have configured with IPv6 addresses. What commands can you use to verify that the IPv6 addresses have been assigned correctly?
   ________________________________________________________________
   Enter these commands at the privileged EXEC mode prompt on each of the four routers, and verify that you have assigned the IPv6 addresses correctly.

2. Correct any configuration errors that you find before you continue.

3. Now that you have configured IPv6 addressing, what has happened with the other IP addresses that were previously configured on the Tampa, Orlando, Daytona, and Miami routers? ________________________________________________________________

B. Verify IPv6 routing

1. Refer to the command summary; what command should you use to display the contents of the IPv6 routing table on each of the four routers that you have configured? ________________
   Enter this command at the privileged EXEC mode prompt on each of the four routers.
2. Do you see the IPv6 networks that represent the WAN links, which are connected to each of the four routers? ___________________________________________________
Are there any missing networks? _______________________________________
If so, correct your configuration before you continue.

3. Now that you have configured IPv6 routing, what has happened to the contents of the existing routing tables on the Tampa, Orlando, Daytona, and Miami routers? __________
_______________________________________________________________
How did you determine this? ________________________________________

C. Verify IPv6 connectivity
1. Log on to the console of the Tampa router. Identify the interface that connects the Tampa router to the Orlando router. How did you determine which interface this is? __________
_______________________________________________________________

2. What is the IPv6 address of the interface on the Orlando router that connects the Orlando router to Tampa? ___________________________________________________

3. From the console of the Tampa router, attempt to ping the IPv6 address of the Orlando router that you previously identified. What must you do differently when you ping an IPv6 address? __________
Was the ping successful? __________________________________________
If not, review and correct your configuration.

4. Refer to the network topology diagram shown at the beginning of this lab. Identify the legacy IP address assigned to the interface of the Orlando router that connects to Tampa. From the console of the Tampa router, attempt to ping this IP address. Is this ping successful? __________

5. Based on the result of the previous ping, what conclusions can you draw regarding the coexistence of IPv6 address and legacy IP addresses on the same device? __________
_______________________________________________________________

Lab Solutions

Task 2: Examine the Initial Network Configuration

A. Verify IP addressing
1. Yes, the IP addresses assigned to each router interface match the IP addresses on the network topology diagram.

2. The Key West, Miami, Tampa, Orlando, and Daytona routers are currently configured with IPv4 addresses.

3. The theoretical maximum number of unique IP addresses that can be assigned in the IPv4 address space is $2^{32}$, which equals 4,294,467,295 IP addresses. Due to inefficiencies in the allocation of addresses, it is estimated that there are approximately 1.3 billion useable IPv4 addresses available.
4. A new method of IP addressing is needed because the IPv4 address space is being rapidly exhausted. Address conservation technologies such as Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Masking (VLSM) and private IP addressing combined with Network Address Translation (NAT) and Port Address Translation (PAT) have extended the life of IPv4 addressing long beyond initial predictions. Even so, the rapidly growing number of traditional Internet users is rapidly exhausting the remaining available IPv4 addresses. A new IP addressing technique that allows for a much larger number of IP addresses is needed to meet the increasing demand of traditional Internet users and the explosive growth of new Internet-enabled devices such as wireless phones and other handheld devices.

Task 3: Exploring IPv6

A. Understand IPv6 addresses

1. The primary benefit of IPv6 is the dramatically larger number of IP addresses that can be assigned. Other benefits include built-in security, automatic address configuration, a simpler header structure, and better support for mobile devices.

2. A major difference between IPv4 and IPv6 addresses is the length of the address. An IPv4 address is 32 bits in length and is usually represented in dotted decimal notation as four decimal octets. An IPv6 address is 128 bits in length and is usually represented as eight 16-bit hexadecimal values. IPv4 addresses are usually assigned with a dotted decimal subnet mask such as 255.255.255.248. IPv6 addresses are usually assigned with a prefix length in CIDR notation.

3. The theoretical maximum number of IPv6 addresses that can be assigned is $3.4 \times 10^{38}$ IP addresses.

4. The transition to IPv6 is supported by several technologies: Dual-stacking is a technique that allows a device to be configured with both IPv4 and IPv6 addresses and participate in IPv4 and IPv6 networks simultaneously. Additionally, 6to4 tunneling allows an IPv6 network to encapsulate and transport IPv4 traffic, while 4to6 tunneling allows an IPv4 network to encapsulate and transport IPv4 traffic.

Task 4: Implement IPv6

A. Implement IPv6 addresses

1. No answer required.

2. No answer required.

3. The `ip address` command is used in interface configuration mode to assign an IPv4 address in dotted-decimal notation with a dotted decimal mask. The `ipv6 address` command is used in interface configuration mode to assign an IPv6 address in dotted hexadecimal notation with a CIDR prefix length.
4. You should use the following commands on the Orlando router to assign IPv6 addresses to the appropriate interfaces.
   ```
   config t
   ipv6 unicast-routing
   int s0/0
   ipv6 address 2001:0:1:1::2/64
   int s1/0
   ipv6 address 2001:0:1:0::1/64
   ```

   You should use the following commands on the Tampa router to assign IPv6 addresses to the appropriate interfaces.
   ```
   config t
   ipv6 unicast-routing
   int s0/0
   ipv6 address 2001:0:1:1::1/64
   int s1/0
   ipv6 address 2001:0:1:3::1/64
   ```

   You should use the following commands on the Daytona router to assign IPv6 addresses to the appropriate interfaces.
   ```
   config t
   ipv6 unicast-routing
   int s0/0
   ipv6 address 2001:0:1:0::2/64
   int s1/0
   ipv6 address 2001:0:1:2::2/64
   ```

   You should use the following commands on the Miami router to assign IPv6 addresses to the appropriate interfaces.
   ```
   config t
   ipv6 unicast-routing
   int s0/0
   ipv6 address 2001:0:1:3::2/64
   int s1/0
   ipv6 address 2001:0:1:2::1/64
   ```

B. Implement IPv6 routing

1. No answer required.

2. The major difference with RIPng is that you no longer configure interfaces for RIP with the `network` command, which you would enter in router configuration mode. You can configure interfaces for RIPng by using the `ipv6 rip process_name enable` command, which you enter in interface configuration mode.
3. You should use the following commands on the Orlando router to configure RIPng on the appropriate interfaces.
   ```
   config t
   ipv6 router rip boson
   int s0/0
   ipv6 rip boson enable
   int s1/0
   ipv6 rip boson enable
   ```
   You should use the following commands on the Tampa router to configure RIPng on the appropriate interfaces.
   ```
   config t
   ipv6 router rip boson
   int s0/0
   ipv6 rip boson enable
   int s1/0
   ipv6 rip boson enable
   ```
   You should use the following commands on the Daytona router to configure RIPng on the appropriate interfaces.
   ```
   config t
   ipv6 router rip boson
   int s0/0
   ipv6 rip boson enable
   int s1/0
   ipv6 rip boson enable
   ```
   You should use the following commands on the Miami router to configure RIPng on the appropriate interfaces.
   ```
   config t
   ipv6 router rip boson
   int s0/0
   ipv6 rip boson enable
   int s1/0
   ipv6 rip boson enable
   ```

**Task 5: Verify IPv6**

A. Verify IPv6 addresses

1. You can use the following commands on the Tampa, Orlando, Miami, and Daytona routers to verify that the IPv6 addresses have been assigned correctly.
   ```
   show ipv6 interface brief
   show running-config
   ```
2. No answer required.

3. The IPv4 addresses that were previously assigned to the interfaces on the Tampa, Orlando, Miami, and Daytona routers are still assigned. An examination of the output of the `show running-config` command shows that the IPv4 and IPv6 addresses can coexist.

**B. Verify IPv6 routing**

1. The `show ipv6 route` command displays the contents of the IPv6 routing table. Routers loaded with IOS version 12.3 or later have the ability to maintain IPv4 and IPv6 addresses on the same interfaces. When IPv4 and IPv6 addresses are configured on the same router, this is called “dual stacking.” This allows a router to simultaneously communicate with IPv4 and IPv6 networks.

2. Yes, IPv6 networks that represent the WAN links between the Daytona, Orlando, Tampa, and Miami routers are present in the IPv6 routing table of all four routers.

3. When routers are configured with both IPv4 and IPv6 addresses, separate IPv4 and IPv6 routing tables are maintained. The contents of the Orlando, Tampa, Daytona, and Miami IPv4 routing tables are unaffected by the configuration of IPv6.

   The `show ip route` and `show ipv6 route` commands can be used on all four routers to display the IPv4 and IPv6 routing tables, respectively.

**C. Verify IPv6 connectivity**

1. The output of the `show running-config` command on the Tampa router shows that the `interface description` command has been used to identify that serial0/0 on the Tampa router connects to the Orlando router.

2. The IPv6 address of the Orlando router interface that connects to Tampa is 2001:0:1:1::2/64.

3. You must use the `ping ipv6` command when you ping an IPv6 address.

   Yes, the ping to 2001:0:1:1::2/64 from the console of the Tampa router is successful.

4. Yes, the ping to 192.168.100.1 from the console of the Tampa router is successful.

5. It can be concluded that IPv4 and IPv6 addressing can coexist on the same router. This will allow for an orderly transition from IPv4 addressing to IPv6 addressing.
Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Orlando</th>
<th>Tampa</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>Version 12.1</td>
<td>Version 12.1</td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
<td>no service password-encryption</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>hostname Orlando</td>
<td>hostname Tampa</td>
</tr>
<tr>
<td>enable secret cisco</td>
<td>enable secret cisco</td>
</tr>
<tr>
<td>!ip subnet-zero</td>
<td>!ip subnet-zero</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>ipv6 unicast-routing</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface Serial0/0</td>
<td>interface Serial0/0</td>
</tr>
<tr>
<td>description ToTampa</td>
<td>description ToTampa</td>
</tr>
<tr>
<td>ip address 192.168.100.1 255.255.255.252</td>
<td>ip address 192.168.100.2 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>ipv6 address 2001:0:1:1::2/64</td>
<td>ipv6 address 2001:0:1:1::1/64</td>
</tr>
<tr>
<td>ipv6 rip boson enable</td>
<td>ipv6 rip boson enable</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface Serial1/0</td>
<td>interface Serial1/0</td>
</tr>
<tr>
<td>description ToDaytona</td>
<td>description ToDaytona</td>
</tr>
<tr>
<td>ip address 192.168.100.5 255.255.255.252</td>
<td>ip address 192.168.100.9 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 64</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>ipv6 address 2001:0:1::1/64</td>
<td>ipv6 address 2001:0:1:3::1/64</td>
</tr>
<tr>
<td>ipv6 rip boson enable</td>
<td>ipv6 rip boson enable</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface Ethernet0</td>
<td>interface Ethernet0</td>
</tr>
<tr>
<td>description OrlandoLAN</td>
<td>description TampaLAN</td>
</tr>
<tr>
<td>ip address 192.168.1.1 255.255.255.0</td>
<td>ip address 192.168.2.1 255.255.255.0</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>ipv6 router rip boson</td>
<td>ipv6 router rip boson</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>router eigrp 100</td>
<td>router eigrp 100</td>
</tr>
<tr>
<td>network 192.168.1.0</td>
<td>network 192.168.100.0</td>
</tr>
<tr>
<td>network 192.168.100.0</td>
<td>network 192.168.2.0</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>ip classless</td>
<td>ip classless</td>
</tr>
<tr>
<td>no ip http server</td>
<td>no ip http server</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>line con 0</td>
<td>line con 0</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
</tr>
<tr>
<td>transport input none</td>
<td>transport input none</td>
</tr>
<tr>
<td>password admin</td>
<td>password admin</td>
</tr>
<tr>
<td>line aux 0</td>
<td>line aux 0</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
</tr>
<tr>
<td>password sanfran</td>
<td>password sanfran</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>no scheduler allocate</td>
<td>no scheduler allocate</td>
</tr>
<tr>
<td>end</td>
<td>end</td>
</tr>
</tbody>
</table>
## Sample Configuration Scripts

<table>
<thead>
<tr>
<th>Daytona</th>
<th>Miami</th>
</tr>
</thead>
<tbody>
<tr>
<td>! Version 12.1</td>
<td>! Version 12.1</td>
</tr>
<tr>
<td>service timestamps debug uptime</td>
<td>service timestamps debug uptime</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
<td>service timestamps log uptime</td>
</tr>
<tr>
<td>no service password-encryption</td>
<td>no service password-encryption</td>
</tr>
<tr>
<td>! hostname Daytona</td>
<td>! hostname Miami</td>
</tr>
<tr>
<td>enable secret cisco</td>
<td>enable secret cisco</td>
</tr>
<tr>
<td>!ip subnet-zero</td>
<td>!ip subnet-zero</td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>ipv6 unicast-routing</td>
</tr>
<tr>
<td>! interface Serial0/0</td>
<td>! interface Serial0/0</td>
</tr>
<tr>
<td>description ToOrlando</td>
<td>description ToOrlando</td>
</tr>
<tr>
<td>ip address 192.168.100.6 255.255.255.252</td>
<td>ip address 192.168.100.10 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 64</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>ipv6 address 2001:0:1::2/64</td>
<td>ipv6 address 2001:0:1:3::2/64</td>
</tr>
<tr>
<td>ipv6 rip boson enable</td>
<td>ipv6 rip boson enable</td>
</tr>
<tr>
<td>! interface Serial1/0</td>
<td>! interface Serial1/0</td>
</tr>
<tr>
<td>description ToMiami</td>
<td>description toDaytonia</td>
</tr>
<tr>
<td>ip address 192.168.100.13 255.255.255.252</td>
<td>ip address 192.168.100.14 255.255.255.252</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>bandwidth 512</td>
<td>bandwidth 512</td>
</tr>
<tr>
<td>ipv6 address 2001:0:1:2::2/64</td>
<td>ipv6 address 2001:0:1:2:64/0</td>
</tr>
<tr>
<td>ipv6 rip boson enable</td>
<td>ipv6 rip boson enable</td>
</tr>
<tr>
<td>! interface Ethernet0</td>
<td>! interface Ethernet0</td>
</tr>
<tr>
<td>description DaytonaLAN</td>
<td>description MiamiLAN</td>
</tr>
<tr>
<td>ip address 192.168.4.1 255.255.255.0</td>
<td>ip address 192.168.3.1 255.255.255.0</td>
</tr>
<tr>
<td>no ip directed-broadcast</td>
<td>no ip directed-broadcast</td>
</tr>
<tr>
<td>! ipv6 router rip boson</td>
<td>! ipv6 router rip boson</td>
</tr>
<tr>
<td>! router eigrp 100</td>
<td>! router eigrp 100</td>
</tr>
<tr>
<td>network 192.168.100.0</td>
<td>network 192.168.3.0</td>
</tr>
<tr>
<td>network 192.168.4.0</td>
<td>network 192.168.100.0</td>
</tr>
<tr>
<td>! ip classless</td>
<td>! ip classless</td>
</tr>
<tr>
<td>no ip http server</td>
<td>no ip http server</td>
</tr>
<tr>
<td>! line con 0</td>
<td>! line con 0</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
</tr>
<tr>
<td>transport input none</td>
<td>transport input none</td>
</tr>
<tr>
<td>password admin</td>
<td>password admin</td>
</tr>
<tr>
<td>line aux 0</td>
<td>line aux 0</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>line vty 0 4</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
</tr>
<tr>
<td>password sanfran</td>
<td>password sanfran</td>
</tr>
<tr>
<td>! no scheduler allocate</td>
<td>! no scheduler allocate</td>
</tr>
<tr>
<td>end</td>
<td>end</td>
</tr>
</tbody>
</table>