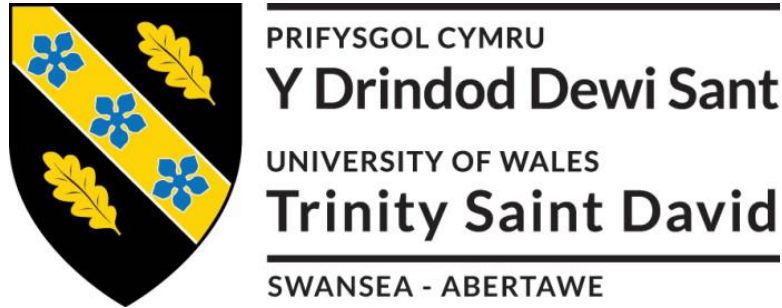




Network & Data Centre Management Lab Manual

B.Sc. (Hons) Computer Networks & Cybersecurity
School of Applied Computing
Faculty of Architecture, Computing and
Engineering
University of Wales Trinity St David
Swansea.



Module Leader: Dr Carlene Campbell

Table of Contents

Lab1 - Accessing Network Devices with SSH	4
Part 1: Configure Basic Device Settings	5
Part 2: Configure the Router for SSH Access	6
Part 3: Examine a Telnet Session with Wireshark	7
Part 4: Examine an SSH session with Wireshark	9
Part 5: Configure the Switch for SSH Access	12
Part 6: SSH From the CLI on the Switch	13
Lab2 – Managing Router Configuration Files with Terminal Emulation Software	15
Part 1: Configure Basic Device Settings	16
Part 2: Use Terminal Emulation Software to Create a Backup Configuration File	17
Part 3: Use a Backup Configuration File to Restore a Router	18
Lab3 - Testing Network Latency with Ping and Traceroute	21
Part 1: Use Ping to Document Network Latency	21
Part 2: Use Traceroute to Document Network Latency	24
Lab4 – Managing Router Configuration Files with Terminal Emulation Software	26
Part 1: Configure Basic Device Settings	27
Part 2: Use Terminal Emulation Software to Create a Backup Configuration File	28
Part 3: Use a Backup Configuration File to Restore a Router	29
Lab5 – Managing Device Configuration Files Using TFTP, Flash, and USB	32
Part 1: Build the Network and Configure Basic Device Settings	33
Part 2: (Optional) Download TFTP Server Software	33
Part 3: Use TFTP to Back Up and Restore the Switch Running Configuration	34
Part 4: Use TFTP to Back Up and Restore the Router Running Configuration	39
Part 5: Back Up and Restore Configurations Using Router Flash Memory	40
Part 6: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration	42
Lab6 – Building a Switched Network with Redundant Links	46
Part 1: Build the Network and Configure Basic Device Settings	47
Part 2: Determine the Root Bridge	47
Part 3: Observe STP Port Selection Based on Port Cost	50
Part 4: Observe STP Port Selection Based on Port Priority	52
Lab7 – Configuring Rapid PVST+, PortFast, and BPDU Guard	55
Part 1: Build the Network and Configure Basic Device Settings	56
Part 2: Configure VLANs, Native VLAN, and Trunks	57
Part 3: Configure the Root Bridge and Examine PVST+ Convergence	58
Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence	60
Lab8 – Configuring HSRP and GLBP	64
Part 1: Build the Network and Verify Connectivity	66
Part 2: Configure First Hop Redundancy Using HSRP	67
Part 3: Configure First Hop Redundancy Using GLBP	70
Lab9 – Configuring EtherChannel	73
Part 1: Configure Basic Switch Settings	74
Part 2: Configure PAgP	75
Part 3: Configure LACP	78
Lab10 – Troubleshooting EtherChannel	80
Part 1: Build the Network and Load Device Configurations	81
Part 2: Troubleshoot EtherChannel	84
Lab11 – Configuring Syslog and NTP	87
Part 1: Configure Basic Device Settings	88
Part 2: Configure NTP	89
Part 3: Configure Syslog	90
Lab12 – Configuring SNMP	95
Part 1: Build the Network and Configure Basic Device Settings	96
Part 2: Configure SNMP Manager and Agents	97
Part 3: Convert OID Codes with the Cisco SNMP Object Navigator	101

Lab13 – Collecting and Analyzing NetFlow Data	105
Part 1: Build the Network and Configure Basic Device Settings	106
Part 2: Configure NetFlow on a Router	107
Part 3: Analyze NetFlow Using the CLI	108
Part 4: Explore NetFlow Collector and Analyzer Software	110

Lab1 - Accessing Network Devices with SSH

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure the Router for SSH Access

Part 3: Examine a Telnet Session with Wireshark

Part 4: Examine a SSH Session with Wireshark

Part 5: Configure the Switch for SSH Access

Part 6: SSH from the CLI on the Switch

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. However, protocols such as Telnet do not authenticate or encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

For SSH to function, the network devices communicating must be configured to support it. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

In this lab, you will configure a router to accept SSH connectivity, and use Wireshark to capture and view Telnet and SSH sessions. This will demonstrate the importance of encryption with SSH. You will also be challenged to configure a switch for SSH connectivity on your own.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary.

from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

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

Required Resources

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

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Task 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- d. Assign **class** as the privileged EXEC encrypted password.
- e. Assign **cisco** as the console password and enable login.
- f. Assign **cisco** as the vty password and enable login.
- g. Encrypt the plain text passwords.
- h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- i. Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- j. Save the running configuration to the startup configuration file.

Task 4: Configure PC-A.

Step 1: Configure PC-A with an IP address and subnet mask.

Step 2: Configure a default gateway for PC-A.

Task 5: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Part 2: Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk, because all information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Task 1: Configure device authentication.

The device name and domain are used as part in the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

Step 1: Configure device name.

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

Step 2: Configure the domain for the device.

```
R1(config)# ip domain-name ccna-lab.com
```

Task 2: Configure the encryption key method.

```
R1(config)# crypto key generate rsa modulus 1024
```

```
The name for the keys will be: R1.ccna-lab.com
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 1 seconds)
```

```
R1(config)#
```

```
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Task 3: Configure a local database username.

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

```
R1(config)#
```

```
*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjTlHbmYxZigc
```

```
R1(config)#
```

Note: A privilege level of 15 gives the user administrator rights.

Task 4: Enable SSH on the VTY lines.

Step 1: Enable Telnet and SSH on the inbound VTY lines using the **transport input** command.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input telnet ssh
```

Step 2: Change the login method to use the local database for user verification.

```
R1(config-line)# login local
```

```
R1(config-line)# end
```

```
R1#
```

Task 5: Save the running configuration to the startup configuration file.

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

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

```
Building configuration...
[OK]
R1#
```

Part 3: Examine a Telnet Session with Wireshark

In Part 3, you will use Wireshark to capture and view the transmitted data of a Telnet session on the router. You will use Tera Term to telnet to R1, sign in, and then issue the show run command on the router.

Note: If a Telnet/SSH client software package is not installed on your PC, you must install one before continuing. Two popular freeware Telnet/SSH packages are Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) and PuTTY (www.putty.org).

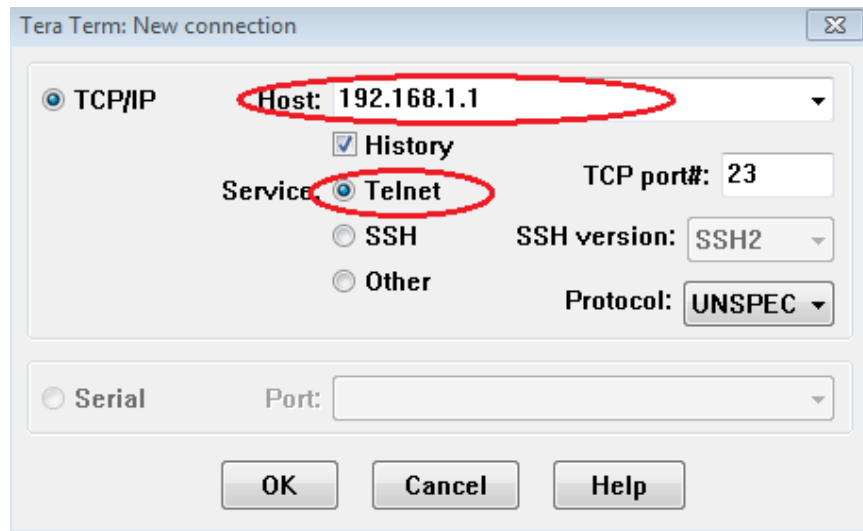
Note: Telnet is not available from the command prompt in Windows 7, by default. To enable Telnet for use in the command prompt window, click **Start > Control Panel > Programs > Programs and Features > Turn Windows features on or off**. Click the **Telnet Client** check box, and then click **OK**.

Task 1: Open Wireshark and start capturing data on the LAN interface.

Note: If you are unable to start the capture on the LAN interface, you may need to open Wireshark using the **Run as Administrator** option.

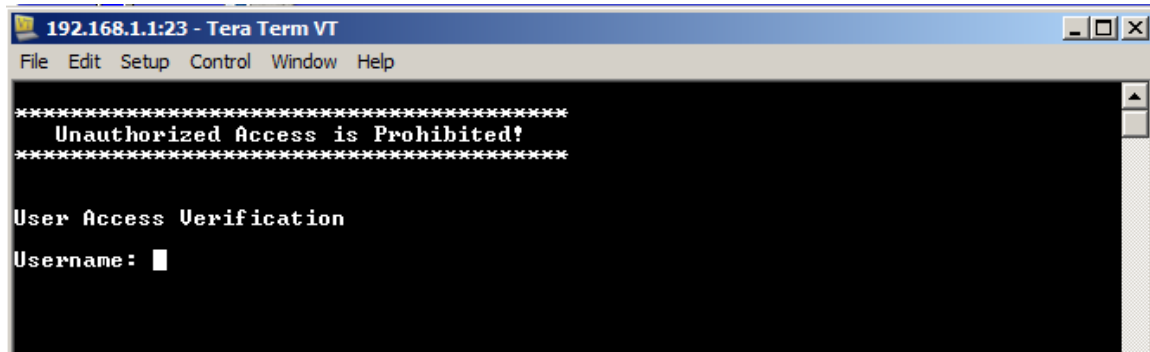
Task 2: Start a Telnet session to the router.

Step 1: Open Tera Term and select the **Telnet** Service radio button and in the Host field, enter **192.168.1.1**.



What is the default TCP port for Telnet sessions? _____

Step 2: At the Username: prompt, enter **admin** and at the Password: prompt, enter **adminpass**. These prompts are generated because you configured the VTY lines to use the local database with the **login local** command.



Step 3: Issue the **show run** command.

```
R1# show run
```

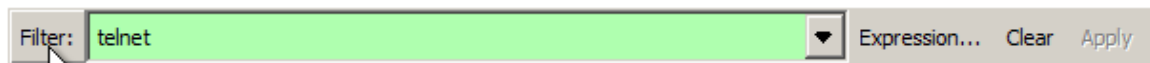
Step 4: Enter **exit** to exit the Telnet session and out of Tera Term.

```
R1# exit
```

Task 3: Stop the Wireshark capture.

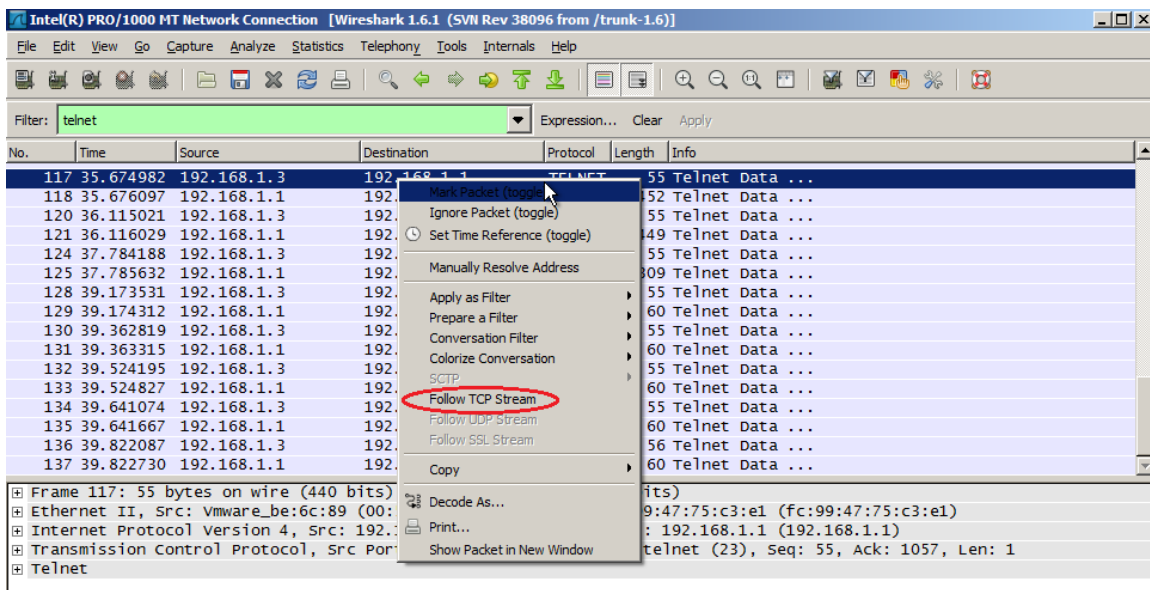


Task 4: Apply a Telnet filter on the Wireshark capture data.

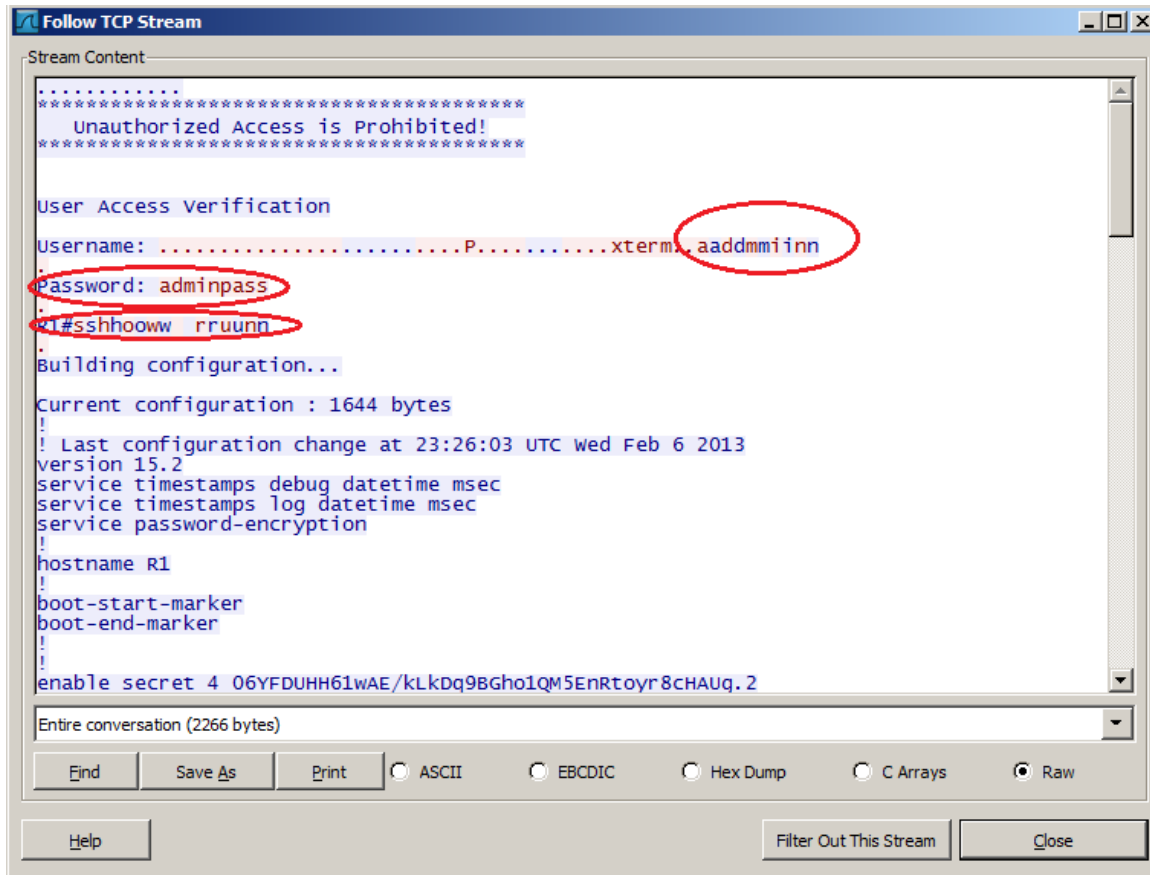


Task 5: Use the Follow TCP Stream feature in Wireshark to view the Telnet session.

Step 1: Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and in the drop-down list, select **Follow TCP Stream**.



Step 2: The Follow TCP Stream window displays the data for your Telnet session with the router. The entire session is displayed in clear text, including your password. Notice that the username and **show run** command that you entered are displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.



Step 3: After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**.

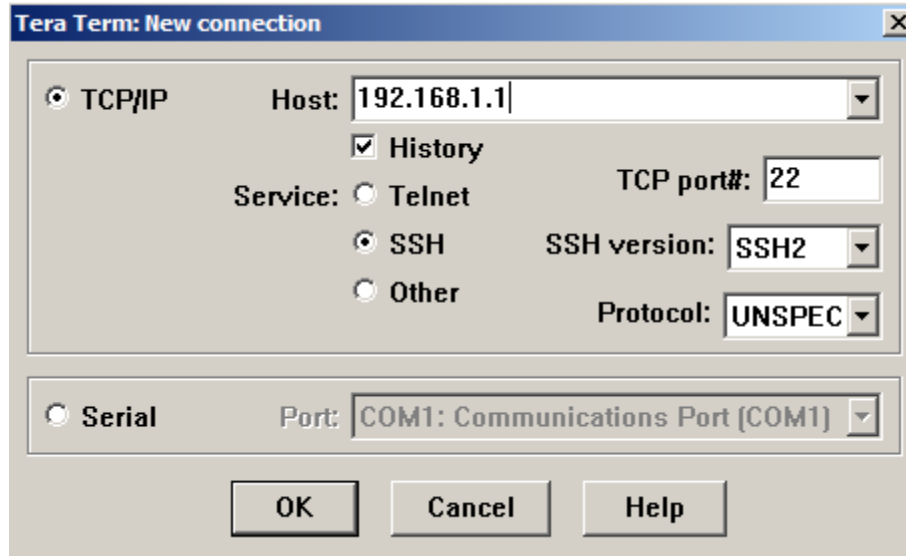
Part 4: Examine an SSH session with Wireshark

In Part 4, you will use the Tera Term software to establish an SSH session with the router. Wireshark will be used to capture and view the data of this SSH session.

Task 1: Open Wireshark and start capturing data on the LAN interface.

Task 2: Start an SSH session on the router.

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



Tera Term: New connection

☒ **TCP/IP** Host: 192.168.1.1

☒ History

Service: ☐ Telnet TCP port#: 22

☒ SSH SSH version: SSH2

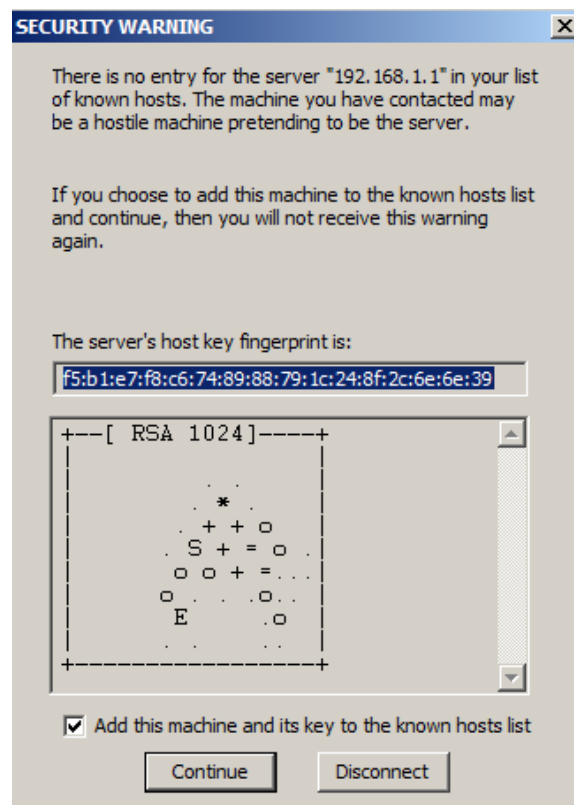
☐ Other Protocol: UNSPEC

☐ **Serial** Port: COM1: Communications Port (COM1)

OK Cancel Help

What is the default TCP port used for SSH sessions? _____

Step 2: The first time you establish a SSH session to a device, a **SECURITY WARNING** is generated to let you know that you have not connected to this device before. This message is part of the authentication process. Read the security warning and then click **Continue**.



SECURITY WARNING

There is no entry for the server "192.168.1.1" in your list of known hosts. The machine you have contacted may be a hostile machine pretending to be the server.

If you choose to add this machine to the known hosts list and continue, then you will not receive this warning again.

The server's host key fingerprint is:

f5:b1:e7:f8:c6:74:89:88:79:1c:24:8f:2c:6e:6e:39

+-[RSA 1024]-+-

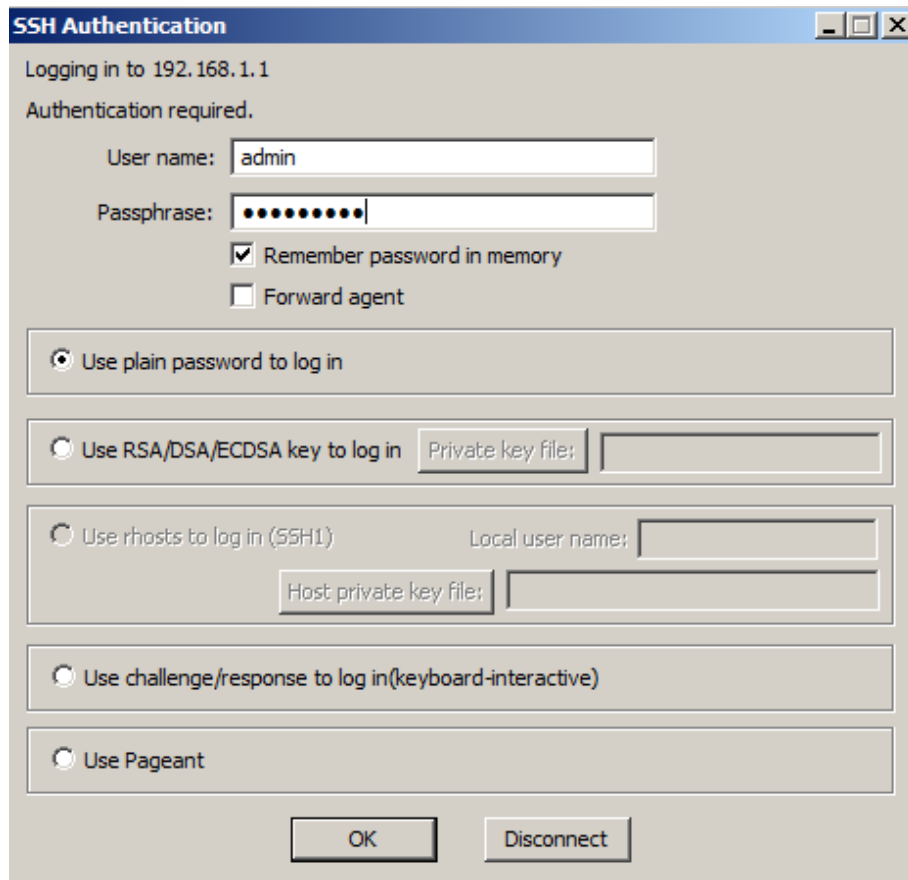
```

      *
    . + + .
  . S + = .
 . o o + = .
 o . . . o .
  E   . o
    . . .
  
```

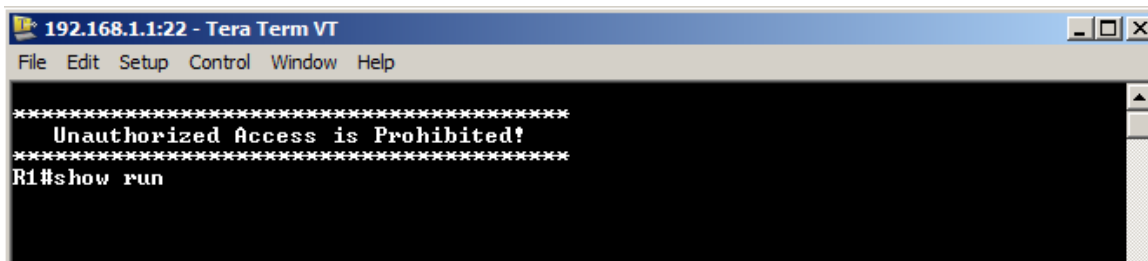
☒ Add this machine and its key to the known hosts list

Continue Disconnect

Step 3: In the SSH Authentication window, enter **admin** for the username and **adminpass** for the passphrase. Click **OK** to sign into the router.



Step 4: You have established a SSH session on the router. The Tera Term software looks very similar to a command window. At the command prompt, issue the **show run** command.



Step 5: Exit the SSH session and out of Tera Term by issuing the **exit** command.

R1# **exit**

Task 3: Stop the Wireshark capture.



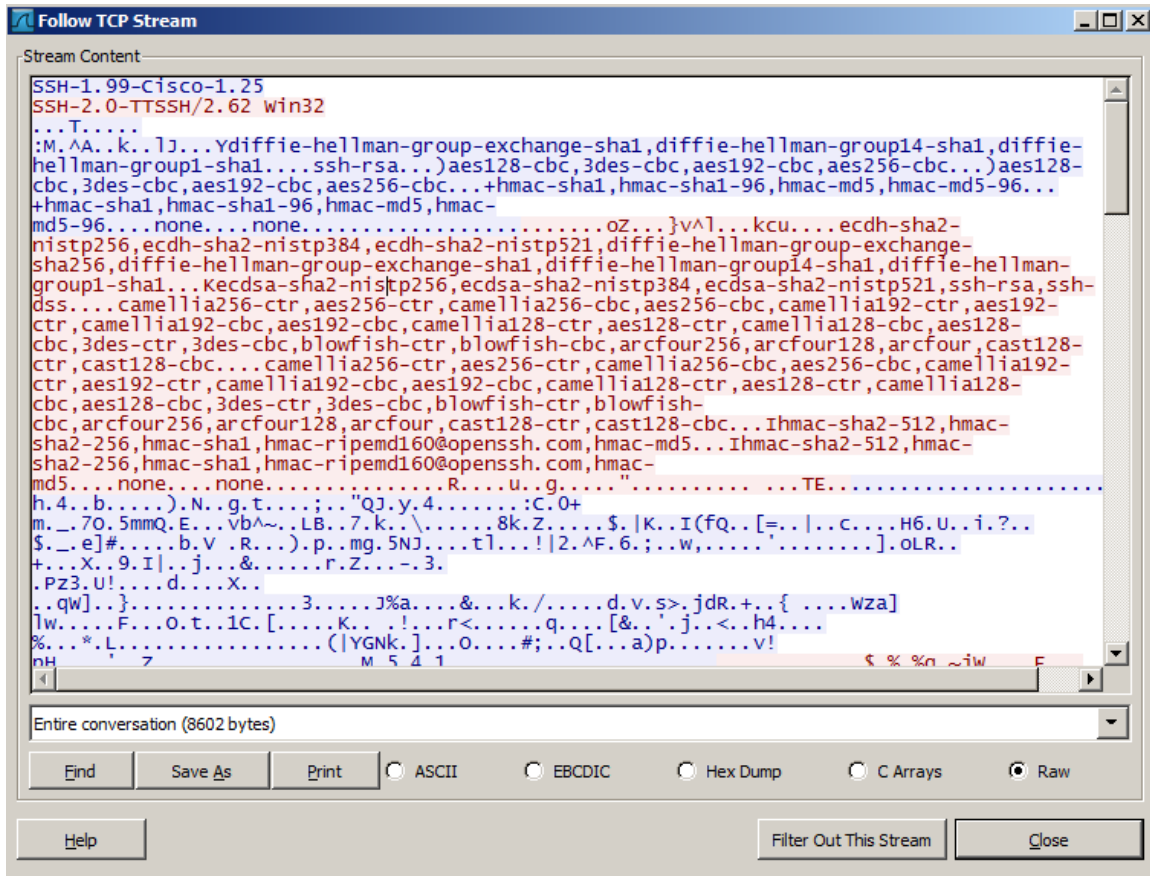
Task 4: Apply an SSH filter on the Wireshark Capture data.



Task 5: Use the Follow TCP Stream feature in Wireshark to view the Telnet session.

Step 1: Right-click one of the **SSHv2** lines in the **Packet list** section of Wireshark, and in the drop-down list, select the **Follow TCP Stream** option.

Step 2: Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.



Why is SSH preferred over Telnet for remote connections?

Step 3: After examining your SSH session, click **Close**.

Step 4: Close Wireshark.

Part 5: Configure the Switch for SSH Access

In Part 5, you are to configure the switch in the topology to accept SSH connections. Once the switch has been configured, establish a SSH session on it using Tera Term.

Task 1: Configure the basic settings on the switch.

Task 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

Task 3: Establish a SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on the S1.

Task 4: Troubleshoot as necessary.

Are you able to establish a SSH session with the switch?

Part 6: SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 6, you will SSH to the router from the CLI on the switch.

Task 1: View the parameters available for the Cisco IOS SSH client.

Use the question mark (?) to display the parameter options available with the **ssh** command.

```
S1# ssh ?
  -c      Select encryption algorithm
  -l      Log in using this user name
  -m      Select HMAC algorithm
  -o      Specify options
  -p      Connect to this port
  -v      Specify SSH Protocol Version
  -vrf    Specify vrf name
  WORD    IP address or hostname of a remote system
```

Task 2: SSH to router R1 from S1.

Step 1: You must use the **-l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **adminpass** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
*****
Warning: Unauthorized Access is Prohibited!
*****
```

```
R1#
```

Step 2: You can return to S1 without closing your SSH session to R1 by pressing **Ctrl+Shift+6**. Release the **Ctrl+Shift+6** keys and press **x**. You should see the switch privilege EXEC prompt display.

```
R1#
S1#
```

Step 3: To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1#
```

Step 4: To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

What versions of SSH are supported from the CLI?

Reflection

How would you provide multiple users, each with their own username, access to a network device?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab2 – Managing Router Configuration Files with Terminal Emulation Software

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

Part 3: Use a Backup Configuration File to Restore a Router

Background / Scenario

It is a recommended best practice to maintain backup configuration files for routers and switches in the event that they need to be restored to a previous configuration. Terminal emulation software can be used to easily back up or restore a router or switch configuration file.

In this lab, you will use Tera Term to back up a router running configuration file, erase the router startup configuration file, reload the router, and then restore the missing router configuration from the backup configuration file.

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

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

Required Resources

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

- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Task 2: Cable the network as shown in the topology.

Attach the devices as shown in the topology and cable as necessary.

Task 3: Configure the PC-A network settings according to the Addressing Table.

Task 4: Initialize and reload the router and switch.

Task 5: Configure the router.

Step 1: Console into the router and enter global configuration mode.

Step 2: Set the router name to R1.

Step 3: Disable DNS lookup.

Step 4: Assign **class** as the privileged EXEC encrypted password.

Step 5: Assign **cisco** as the console password and enable login.

Step 6: Assign **cisco** as the vty password and enable login.

Step 7: Encrypt the plain text passwords.

Step 8: Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

Step 9: Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.

Step 10: Save the running configuration to the startup configuration file.

Task 6: Configure the switch.

Step 1: Console into the switch and enter into global configuration mode.

Step 2: Set the switch name to S1.

Step 3: Disable DNS lookup.

Step 4: Assign **class** as the privileged EXEC encrypted password.

Step 5: Assign **cisco** as the console password and enable login.

Step 6: Assign **cisco** as the vty password and enable login.

Step 7: Encrypt the plain text passwords.

Step 8: Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

Step 9: Configure the default SVI management interface with the IP address information contained in the Addressing Table.

Step 10: Configure the switch default gateway.

Step 11: Save the running configuration to the startup configuration file.

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

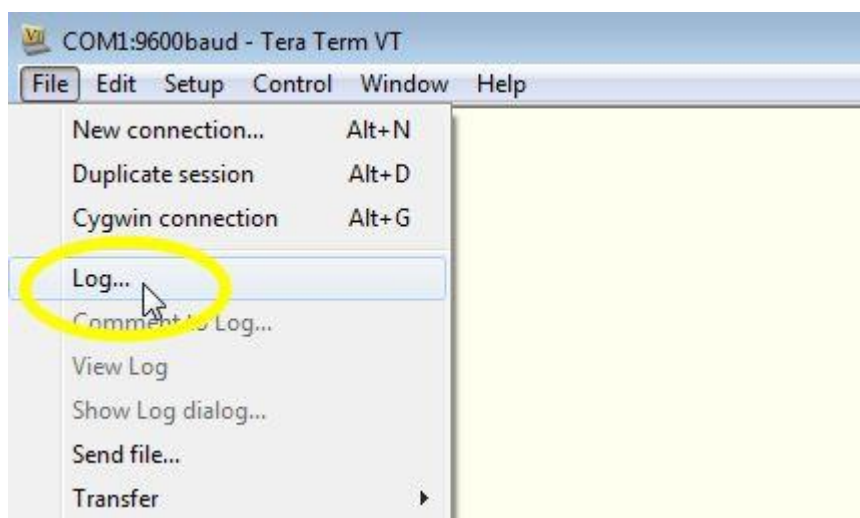
Task 2: Establish a Tera Term console session to the router.

Launch the Tera Term Program, and in the New Connection window, select the **Serial** radio button and the appropriate communications port for your PC (i.e., COM1).

Note: If Tera Term is not installed, you can download the latest version from a number of Internet sites. Simply search for a Tera Term download.

Step 1: In Tera Term, press Enter to connect to the router.

Step 2: From the **File** menu, choose **Log...**, and save the **teraterm.log** file to the Desktop. Ensure that the **Append** and **Plain text** check boxes are enabled (checked).



Step 3: The Tera Term log file will create a record of every command issued and every output displayed.

Note: You can use this feature to capture the output from several commands in sequence and use it for network documentation purposes. For example, you could issue the **show version**, **show ip interface brief**, and **show running-config** commands to capture information about the router.

Task 3: Display the router running-configuration.

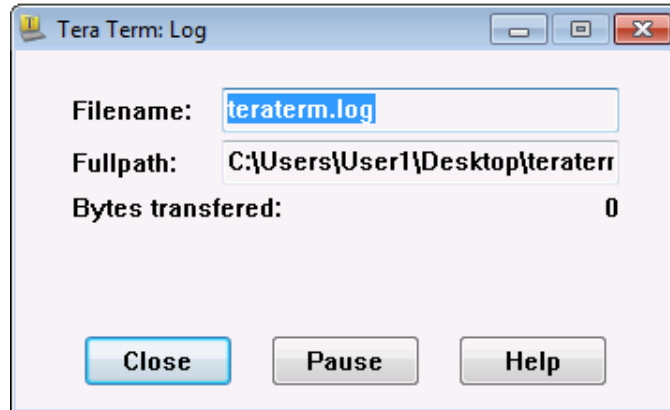
Step 1: Use the console password to log in to the router.

Step 2: Enter privileged EXEC mode.

Step 3: Enter the **show running-config** command.

Step 4: Continue pressing the space bar when **--More--** is displayed until you see the router R1# prompt return.

Step 5: Click the **Tera Term: Log** icon on the Task bar. Click **Close** to end log session.



Note: You can also copy and paste the text from the Tera Term window directly into a text editor.

Part 3: Use a Backup Configuration File to Restore a Router

Task 2: Erase the router startup-configuration and reload.

Step 1: From privileged EXEC mode erase the startup configuration.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
```

Step 2: Reload the router.

```
R1# reload
Proceed with reload? [confirm]
```

Step 3: At the System Configuration Dialog prompt, type **no**; a router prompt displays, indicating an unconfigured router.

```
--- System Configuration Dialog ---

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

Press RETURN to get started!
<output omitted>
Router>
```

Step 4: Enter privileged EXEC mode and enter a **show running-config** command to verify that all of the previous configurations were erased.

Task 3: Edit the saved configuration backup file to prepare it for restoring the router configuration.

To restore the router configuration from a saved running configuration backup file, you must edit the text.

Step 1: Open the **teraterm.log** text file.

Step 2: Remove each instance of **--More--** in the text file.

Note: The **--More--** was generated by pressing the Spacebar when displaying the running configuration.

Step 3: Delete the initial lines of the backup configuration file, so that the first line starts with the first configuration command as shown below.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

Step 4: Replace the encrypted secret password.

```
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
```

Change to:

```
enable secret class
```

Step 5: In the lines for interface GigabitEthernet0/1, insert a new line to enable the interface.

```
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
```

Change to:

```
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
no shutdown
```

Step 6: Change the message-of-the-day (MOTD) banner configuration to insert the delimiting characters as if you were entering the command at the command line.

```
banner motd ^C Unauthorized Access is Prohibited! ^C
```

Change to:

```
banner motd `` Unauthorized Access is Prohibited! ``
```

Step 7: In line con 0 and vty 0 4 sections, replace the encrypted password.

```
line con 0
password 7 104D000A0618
line vty 0 4
password 7 104D000A0618
```

Change to:

```
line con 0
password cisco
line vty 0 4
password cisco
```

Step 8: After you have made all of the edits to the backup configuration file, save your changes to filename, **R1-config-backup**.

Note: When saving the file, an extension, such as **.txt**, may be added to the filename automatically.

Task 4: Restore the router configuration.

You can restore the edited running configuration directly to the console terminal in router global configuration mode, and the configurations are entered as if they were commands entered individually at the command prompt.

Step 1: From the Tera Term console connection to the router, enter global configuration mode.

Step 2: From the **File** menu, select **Send file....**

Step 3: Locate **R1-config-backup** and select **Open**.

Step 4: Save the running configuration to the startup configuration file.

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

Step 5: Verify the new running configuration.

Task 5: Back up and restore the switch.

Go back to the beginning of Part 2 and follow the same steps to backup and restore the switch configuration.

Reflection

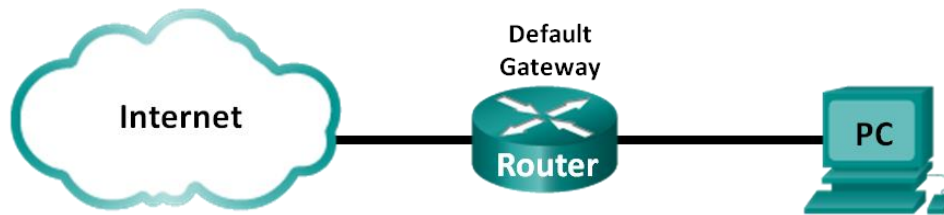
Why do you think it is important to use a text editor instead of a word processor to copy and save your command configurations?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab3 - Testing Network Latency with Ping and Traceroute

Topology



Objectives

Part 1: Use Ping to Document Network Latency

Part 2: Use Traceroute to Document Network Latency

Background / Scenario

To obtain realistic network latency statistics, this activity must be performed on a live network. Be sure to check with your instructor for any local security restrictions against using the **ping** command on the network.

The purpose of this lab is to measure and evaluate network latency over time, and during different periods of the day to capture a representative sample of typical network activity. This will be accomplished by analyzing the return delay from a distant computer with the **ping** command. Return delay times, measured in milliseconds, will be summarized by computing the average latency (mean) and the range (maximum and minimum) of the delay times.

Required Resources

- 1 PC (Windows 7, Vista, or XP with Internet access)

Part 1: Use Ping to Document Network Latency

In Part 1, you will examine network latency to several websites in different parts of the globe. This process can be used in an enterprise production network to create a performance baseline.

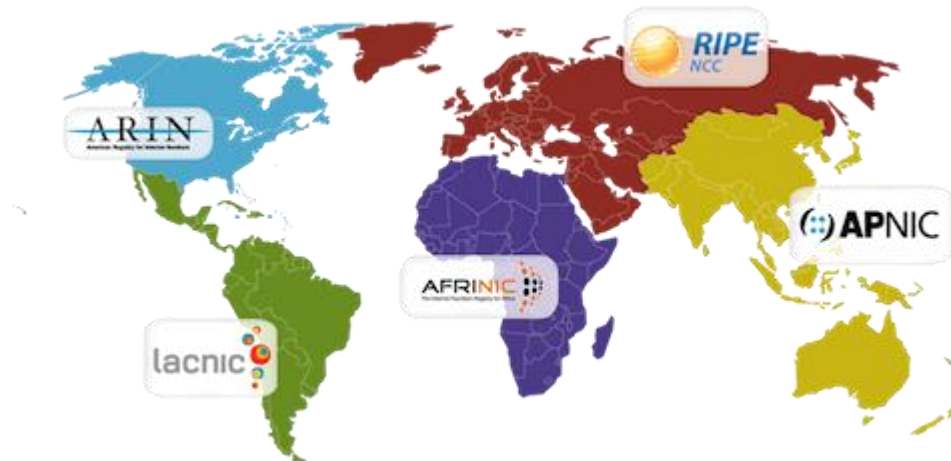
Task 1: Verify connectivity.

Ping the following Regional Internet Registry (RIR) websites to verify connectivity:

```

C:\Users\User1> ping www.arin.net
C:\Users\User1> ping www.lacnic.net
C:\Users\User1> ping www.afrinic.net
C:\Users\User1> ping www.apnic.net
  
```

Note: Because www.ripe.net does not reply to ICMP requests, it cannot be used for this lab.



Task 2: Collect network data.

You will collect a sufficient amount of data to compute statistics on the **ping** output by sending out 25 echo requests to each address listed in Step 1. Record the results for each website to text files.

Step 1: At the command prompt, type **ping** to list the available options.

```
C:\Users\User1> ping
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

Options:

```
-t          Ping the specified host until stopped.
            To see statistics and continue - type Control-Break;
            To stop - type Control-C.
-a          Resolve addresses to hostnames.
-n count    Number of echo requests to send.
-l size     Send buffer size.
-f          Set Don't Fragment flag in packet (IPv4-only).
-i TTL      Time To Live.
-v TOS      Type Of Service (IPv4-only. This setting has been deprecated
```

<output omitted>

Step 2: Using the **ping** command with the count option, you can send 25 echo requests to the destination as illustrated below. Furthermore, it will create a text file with filename of **arin.txt** in the current directory. This text file will contain the results of the echo requests.

```
C:\Users\User1> ping -n 25 www.arin.net > arin.txt
```

Note: The terminal remains blank until the command has finished, because the output has been redirected to a text file, **arin.txt**, in this example. The **>** symbol is used to redirect the screen output to the file and overwrite the file if it already exists. If appending more results to the file is desired, replace **>** with **>>** in the command.

Step 3: Repeat the **ping** command for the other websites.

```
C:\Users\User1> ping -n 25 www.afrinic.net > afrinic.txt
```

```
C:\Users\User1> ping -n 25 www.apnic.net > apnic.txt
```

```
C:\Users\User1> ping -n 25 www.lacnic.net > lacnic.txt
```

Task 3: Verify data collection.

To see the results in the file created, use the **more** command at the command prompt.

```
C:\Users\User1> more arin.txt

Pinging www.arin.net [192.149.252.76] with 32 bytes of data:
Reply from 192.149.252.76: bytes=32 time=108ms TTL=45
Reply from 192.149.252.76: bytes=32 time=114ms TTL=45
Reply from 192.149.252.76: bytes=32 time=112ms TTL=45
<output omitted>
Reply from 192.149.252.75: bytes=32 time=111ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45

Ping statistics for 192.149.252.75:
    Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 107ms, Maximum = 121ms, Average = 111ms
```

Note: Press the Spacebar to display the rest of the file or press **q** to exit.

To verify that the files have been created, use the **dir** command to list the files in the directory. Also the wildcard ***** can be used to filter only the text files.

```
C:\Users\User1> dir *.txt

Volume in drive C is OS
Volume Serial Number is 0A97-D265

Directory of C:\Users\User1

02/07/2013  12:59 PM                1,642 afrinic.txt
02/07/2013  01:00 PM                1,615 apnic.txt
02/07/2013  12:40 PM                1,641 arin.txt
02/07/2013  12:58 PM                1,589 lacnic.txt
               4 File(s)              6,487 bytes
               0 Dir(s)  34,391,453,696 bytes free
```

Record your results in the following table.

	Minimum	Maximum	Average
www.afrinic.net			
www.apnic.net			
www.arin.net			
www.lacnic.net			

Compare the delay results. How is delay affected by geographical location?

Part 2: Use Traceroute to Document Network Latency

The routes traced may go through many hops and a number of different ISPs depending on the size of the ISPs and the location of the source and destination hosts. The **traceroute** commands can also be used to observe network latency. In Part 2, the **tracert** command is used to trace the path to the same destinations in Part 1.

The **tracert** command uses ICMP TTL Exceed packets and ICMP echo replies to trace the path.

Task 1: Use the tracert command and record the output to text files.

Copy the following commands to create the traceroute files:

```
C:\Users\User1> tracert www.arin.net > traceroute_arin.txt
C:\Users\User1> tracert www.lacnic.net > traceroute_lacnic.txt
C:\Users\User1> tracert www.afrinic.net > traceroute_afrinic.txt
C:\Users\User1> tracert www.apnic.net > traceroute_apnic.txt
```

Task 2: Use the more command to examine the traced path.

Step 1: Use the **more** command to access the content of these files:

```
C:\Users\User1> more traceroute_arin.txt
```

```
Tracing route to www.arin.net [192.149.252.75]
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	11 ms	12 ms	11 ms	10.39.0.1
3	10 ms	15 ms	11 ms	172.21.0.116
4	19 ms	10 ms	11 ms	70.169.73.90
5	13 ms	10 ms	11 ms	chnddsrj01-ae2.0.rd.ph.cox.net [70.169.76.229]
6	72 ms	71 ms	70 ms	mrfddsrj02-ae0.0.rd.dc.cox.net [68.1.1.7]
7	72 ms	71 ms	72 ms	68.100.0.146
8	74 ms	83 ms	73 ms	172.22.66.29
9	75 ms	71 ms	73 ms	172.22.66.29
10	74 ms	75 ms	73 ms	wsip-98-172-152-14.dc.dc.cox.net [98.172.152.14]
11	71 ms	71 ms	71 ms	host-252-131.arin.net [192.149.252.131]
12	73 ms	71 ms	71 ms	www.arin.net [192.149.252.75]

```
Trace complete.
```

In this example, it took less than 1 ms to receive a reply from the default gateway (192.168.1.1). In hop count 6, the round trip to 68.1.1.7 took an average of 71 ms. For the round trip to the final destination at www.arin.net took an average of 72 ms.

Between lines 5 and 6, there is more network delay as indicated by the round trip time increase from an average of 11 ms to 71 ms

Step 2: Perform the same analysis with the rest of the tracert results.

What can you conclude regarding the relationship between the roundtrip time and geographical location?

Reflection

1. The **tracert** and **ping** results can provide important network latency information. What do you need to do if you want an accurate baseline picture regarding network latency for your network?

2. How can you use the baseline information?

Lab4 – Managing Router Configuration Files with Terminal Emulation Software

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

Part 3: Use a Backup Configuration File to Restore a Router

Background / Scenario

It is a recommended best practice to maintain backup configuration files for routers and switches in the event that they need to be restored to a previous configuration. Terminal emulation software can be used to easily back up or restore a router or switch configuration file.

In this lab, you will use Tera Term to back up a router running configuration file, erase the router startup configuration file, reload the router, and then restore the missing router configuration from the backup configuration file.

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

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

Required Resources

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

- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Task 2: Cable the network as shown in the topology.

Attach the devices as shown in the topology and cable as necessary.

Task 3: Configure the PC-A network settings according to the Addressing Table.

Task 4: Initialize and reload the router and switch.

Task 5: Configure the router.

Step 1: Console into the router and enter global configuration mode.

Step 2: Set the router name to R1.

Step 3: Disable DNS lookup.

Step 4: Assign **class** as the privileged EXEC encrypted password.

Step 5: Assign **cisco** as the console password and enable login.

Step 6: Assign **cisco** as the vty password and enable login.

Step 7: Encrypt the plain text passwords.

Step 8: Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

Step 9: Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.

Step 10: Save the running configuration to the startup configuration file.

Task 6: Configure the switch.

Step 1: Console into the switch and enter into global configuration mode.

Step 2: Set the switch name to S1.

Step 3: Disable DNS lookup.

Step 4: Assign **class** as the privileged EXEC encrypted password.

Step 5: Assign **cisco** as the console password and enable login.

Step 6: Assign **cisco** as the vty password and enable login.

Step 7: Encrypt the plain text passwords.

Step 8: Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

Step 9: Configure the default SVI management interface with the IP address information contained in the Addressing Table.

Step 10: Configure the switch default gateway.

Step 11: Save the running configuration to the startup configuration file.

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

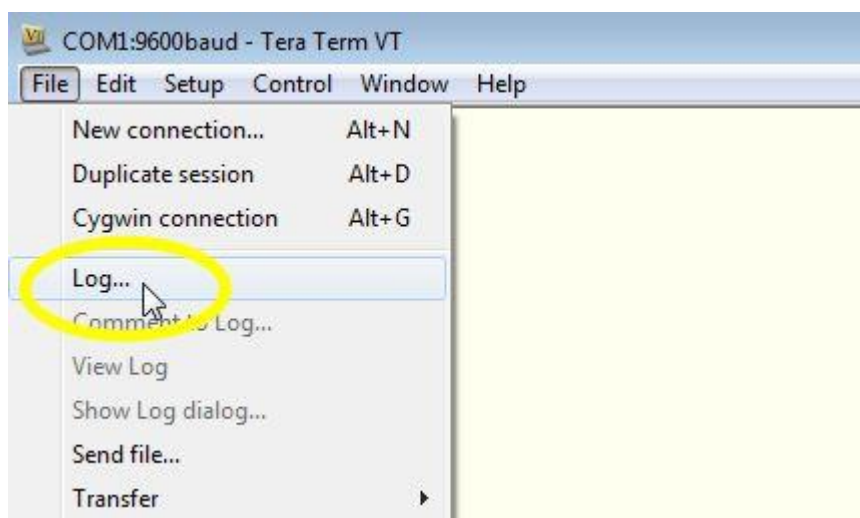
Task 2: Establish a Tera Term console session to the router.

Launch the Tera Term Program, and in the New Connection window, select the **Serial** radio button and the appropriate communications port for your PC (i.e., COM1).

Note: If Tera Term is not installed, you can download the latest version from a number of Internet sites. Simply search for a Tera Term download.

Step 1: In Tera Term, press Enter to connect to the router.

Step 2: From the **File** menu, choose **Log...**, and save the **teraterm.log** file to the Desktop. Ensure that the **Append** and **Plain text** check boxes are enabled (checked).



Step 3: The Tera Term log file will create a record of every command issued and every output displayed.

Note: You can use this feature to capture the output from several commands in sequence and use it for network documentation purposes. For example, you could issue the **show version**, **show ip interface brief**, and **show running-config** commands to capture information about the router.

Task 3: Display the router running-configuration.

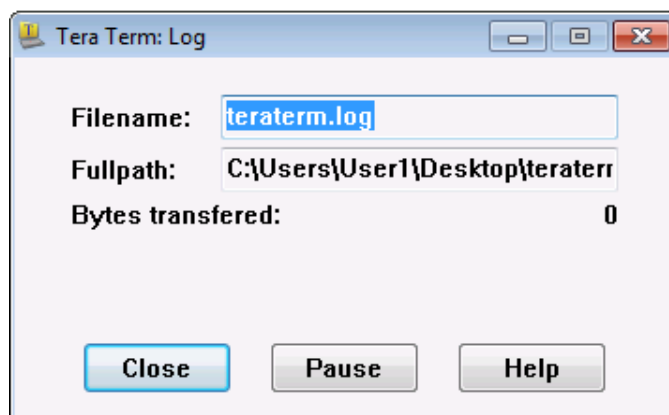
Step 1: Use the console password to log in to the router.

Step 2: Enter privileged EXEC mode.

Step 3: Enter the **show running-config** command.

Step 4: Continue pressing the space bar when **--More--** is displayed until you see the router R1# prompt return.

Step 5: Click the **Tera Term: Log** icon on the Task bar. Click **Close** to end log session.



Note: You can also copy and paste the text from the Tera Term window directly into a text editor.

Part 3: Use a Backup Configuration File to Restore a Router

Task 2: Erase the router startup-configuration and reload.

Step 1: From privileged EXEC mode erase the startup configuration.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
```

Step 2: Reload the router.

```
R1# reload
Proceed with reload? [confirm]
```

Step 3: At the System Configuration Dialog prompt, type **no**; a router prompt displays, indicating an unconfigured router.

```
--- System Configuration Dialog ---

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

Press RETURN to get started!
<output omitted>
Router>
```

Step 4: Enter privileged EXEC mode and enter a **show running-config** command to verify that all of the previous configurations were erased.

Task 3: Edit the saved configuration backup file to prepare it for restoring the router configuration.

To restore the router configuration from a saved running configuration backup file, you must edit the text.

Step 1: Open the **teraterm.log** text file.

Step 2: Remove each instance of **--More--** in the text file.

Note: The **--More--** was generated by pressing the Spacebar when displaying the running configuration.

Step 3: Delete the initial lines of the backup configuration file, so that the first line starts with the first configuration command as shown below.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

Step 4: Replace the encrypted secret password.

```
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
```

Change to:

```
enable secret class
```

Step 5: In the lines for interface GigabitEthernet0/1, insert a new line to enable the interface.

```
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
```

Change to:

```
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
no shutdown
```

Step 6: Change the message-of-the-day (MOTD) banner configuration to insert the delimiting characters as if you were entering the command at the command line.

```
banner motd ^C Unauthorized Access is Prohibited! ^C
```

Change to:

```
banner motd `` Unauthorized Access is Prohibited! ``
```

Step 7: In line con 0 and vty 0 4 sections, replace the encrypted password.

```
line con 0
password 7 104D000A0618
line vty 0 4
password 7 104D000A0618
```

Change to:

```
line con 0
password cisco
line vty 0 4
password cisco
```

Step 8: After you have made all of the edits to the backup configuration file, save your changes to filename, **R1-config-backup**.

Note: When saving the file, an extension, such as **.txt**, may be added to the filename automatically.

Task 4: Restore the router configuration.

You can restore the edited running configuration directly to the console terminal in router global configuration mode, and the configurations are entered as if they were commands entered individually at the command prompt.

Step 1: From the Tera Term console connection to the router, enter global configuration mode.

Step 2: From the **File** menu, select **Send file....**

Step 3: Locate **R1-config-backup** and select **Open**.

Step 4: Save the running configuration to the startup configuration file.

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

Step 5: Verify the new running configuration.

Task 5: Back up and restore the switch.

Go back to the beginning of Part 2 and follow the same steps to backup and restore the switch configuration.

Reflection

Why do you think it is important to use a text editor instead of a word processor to copy and save your command configurations?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab5 – Managing Device Configuration Files Using TFTP, Flash, and USB

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: (Optional) Download TFTP Server Software

Part 3: Use TFTP to Back Up and Restore the Switch Running Configuration

Part 4: Use TFTP to Back Up and Restore the Router Running Configuration

Part 5: Back Up and Restore Running Configurations Using Router Flash Memory

Part 6: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

Background / Scenario

Cisco networking devices are often upgraded or swapped out for a number of reasons. It is important to maintain backups of the latest device configurations, as well as a history of configuration changes. A TFTP server is often used to backup configuration files and IOS images in production networks. A TFTP server is a centralized and secure method used to store the backup copies of the files and restore them as necessary. Using a centralized TFTP server, you can back up files from many different Cisco devices.

In addition to a TFTP server, most of the current Cisco routers can back up and restore files locally from CompactFlash (CF) memory or a USB flash drive. The CF is a removable memory module that has replaced the limited internal flash memory of earlier router models. The IOS image for the router resides in the CF memory, and the router uses this IOS Image for the boot process. With the larger size of the CF memory, additional files can be stored for backup purposes. A removable USB flash drive can also be used for backup purposes.

In this lab, you will use TFTP server software to back up the Cisco device running configuration to the TFTP server or flash memory. You can edit the file using a text editor and copy the new configuration back to a Cisco device.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary

from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

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

Required Resources

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

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses for router R1, switch S1 and PC-A.

Task 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Task 2: Initialize and reload the router and switch.

Task 3: Configure basic settings for each device.

Step 1: Configure basic device parameters as shown in the Addressing Table.

Step 2: To prevent the router and switch from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.

Step 3: Assign **class** as the privileged EXEC encrypted password.

Step 4: Configure the passwords and allow login for console and vty lines using the **cisco** as the password.

Step 5: Configure the default gateway for the switch.

Step 6: Encrypt the clear text passwords.

Step 7: Configure the IP address, subnet mask, and default gateway for PC-A.

Task 4: Verify connectivity from PC-A.

Step 1: Ping from PC-A to S1.

Step 2: Ping from PC-A to R1.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: (Optional) Download TFTP Server Software

A number of free TFTP servers are available on the Internet for download. The Tftpd32 server is used with this lab.

Note: Downloading a TFTP server from a website requires Internet access.

Task 1: Verify availability of a TFTP server on PC-A.

Step 1: Click the **Start** menu and select **All Programs**.

Step 2: Search for a TFTP server on PC-A.

Step 3: If a TFTP server is not found, a TFTP server can be downloaded from the Internet.

Task 2: Download a TFTP server.

Step 1: Tftpd32 is used in this lab. This server can be downloaded from the following link:

http://tftpd32.jounin.net/tftpd32_download.html

Step 2: Choose the appropriate version for your system and install the server.

Part 3: Use TFTP to Back Up and Restore the Switch Running Configuration**Task 1: Verify connectivity to switch S1 from PC-A.**

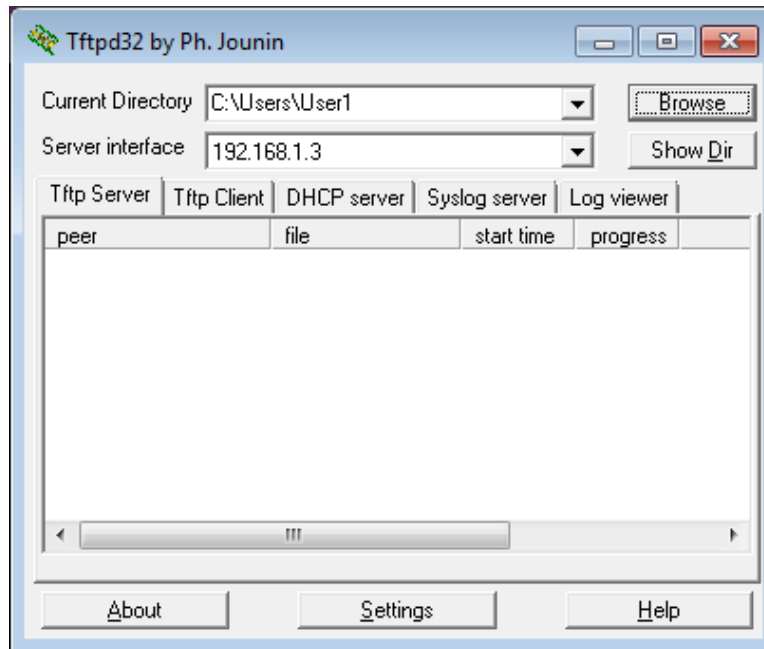
The TFTP application uses the UDP Layer 4 transport protocol, which is encapsulated in an IP packet. For TFTP file transfers to function, there must be Layer 1 and 2 (Ethernet, in this case) and Layer 3 (IP) connectivity between the TFTP client and the TFTP server. The LAN topology in this lab uses only Ethernet at Layers 1 and 2. However, TFTP transfers can also be accomplished over WAN links that use other Layer 1 physical links and Layer 2 protocols. As long as there is IP connectivity between the client and server, as demonstrated by ping, the TFTP transfer can take place. If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: A common misconception is that you can TFTP a file over the console connection. This is not the case because the console connection does not use IP. The TFTP transfer can be initiated from the client device (router or switch) using the console connection, but there must be IP connectivity between the client and server for the file transfer to take place.

Task 2: Start the TFTP server.

Step 1: Click the **Start** menu and select **All Programs**.

Step 2: Find and select **Tftpd32** or **Tftpd64**. The following window displays that the TFTP server is ready.



Step 3: Click **Browse** to choose a directory where you have write permission, such as C:\Users\User1, or the Desktop.

Task 3: Explore the copy command on a Cisco device.

Step 1: Console into switch S1 and, from the privileged EXEC mode prompt, enter **copy ?** to display the options for source or “from” location and other available copy options. You can specify **flash:** or **flash0:** as the source, however, if you simply provide a filename as the source, **flash0:** is assumed and is the default. Note that **running-config** is also an option for the source location.

```
S1# copy ?
/erase          Erase destination file system.
/error          Allow to copy error file.
/noverify       Don't verify image signature before reload.
/verify         Verify image signature before reload.
archive:        Copy from archive: file system
cns:            Copy from cns: file system
flash0:         Copy from flash0: file system
flash1:         Copy from flash1: file system
flash:          Copy from flash: file system
ftp:            Copy from ftp: file system
http:           Copy from http: file system
https:          Copy from https: file system
null:           Copy from null: file system
nvram:          Copy from nvram: file system
rcp:            Copy from rcp: file system
running-config  Copy from current system configuration
scp:            Copy from scp: file system
startup-config  Copy from startup configuration
system:         Copy from system: file system
tar:            Copy from tar: file system
```

```
tftp:          Copy from tftp: file system
tmpsys:       Copy from tmpsys: file system
xmodem:       Copy from xmodem: file system
ymodem:       Copy from ymodem: file system
```

Step 2: Use the ? to display the destination options after a source file location is chosen. The **flash:** file system for S1 is the source file system in this example.

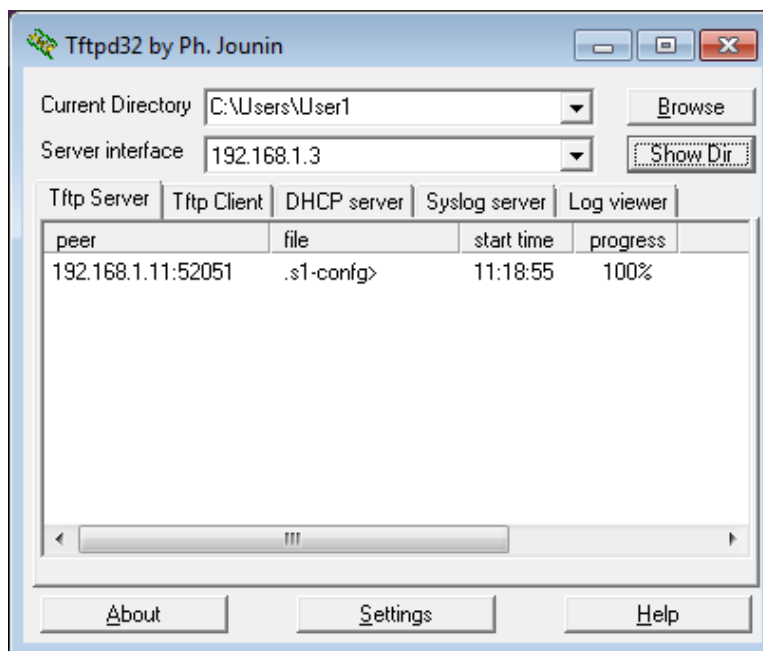
```
S1# copy flash: ?
archive:      Copy to archive: file system
flash0:       Copy to flash0: file system
flash1:       Copy to flash1: file system
flash:        Copy to flash: file system
ftp:          Copy to ftp: file system
http:         Copy to http: file system
https:        Copy to https: file system
idconf        Load an IDConf configuration file
null:         Copy to null: file system
nvram:        Copy to nvram: file system
rcp:          Copy to rcp: file system
running-config Update (merge with) current system configuration
scp:          Copy to scp: file system
startup-config Copy to startup configuration
syslog:       Copy to syslog: file system
system:       Copy to system: file system
tftp:         Copy to tftp: file system
tmpsys:       Copy to tmpsys: file system
xmodem:       Copy to xmodem: file system
ymodem:       Copy to ymodem: file system
```

Task 4: Transfer the running-config file from switch S1 to TFTP server on PC-A.

Step 1: From the privileged EXEC mode on the switch, enter the **copy running-config tftp:** command. Provide the remote host address of the TFTP server (PC-A), 192.168.1.3. Press Enter to accept default destination filename (**s1-confg**) or provide your own filename. The exclamation marks (!!) indicate the transfer process is in progress and is successful.

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [s1-confg]?
!!
1465 bytes copied in 0.663 secs (2210 bytes/sec)
S1#
```

The TFTP server also displays the progress during the transfer.



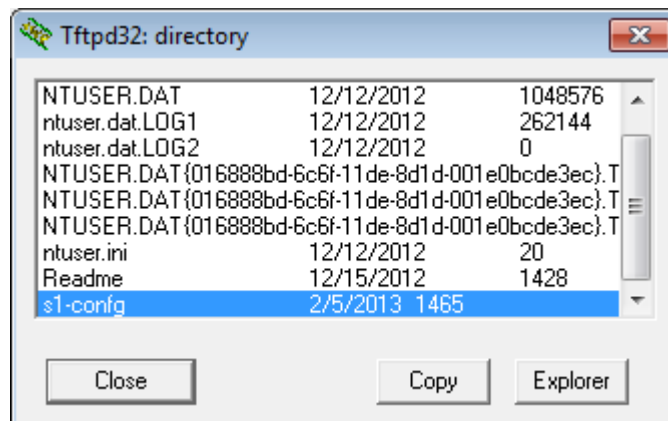
Note: If you do not have permission to write to the current directory that is used by the TFTP server, the following error message displays:

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [s1-config]?
%Error opening tftp://192.168.1.3/s1-config (Permission denied)
```

You can change the current directory in TFTP server by clicking **Browse** and choosing a different folder.

Note: Other issues, such as a firewall blocking TFTP traffic, can prevent the TFTP transfer. Please check with your instructor for further assistance.

Step 2: In the Tftpd32 server window, click **Show Dir** to verify that the **s1-config** file has been transferred to your current directory. Click **Close** when finished.



Task 5: Create a modified switch running configuration file.

The saved running configuration file, **s1-config**, can also be restored to the switch by using the **copy** command from the switch. The original or a modified version of the file can be copied to the flash file system of the switch.

Step 1: Navigate to the TFTP directory on PC-A by using the file system of PC-A, and then locate the **s1-config** file. Open this file using a text editor program, such as WordPad.

Step 2: With the file open, locate the **hostname S1** line. Replace **S1** with **Switch1**. Delete all the self-generated crypto keys, as necessary. A sample of the keys is displayed below. These keys are not exportable and can cause errors while updating the running configuration.

```
crypto pki trustpoint TP-self-signed-1566151040
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1566151040
  revocation-check none
  rsakeypair TP-self-signed-1566151040
!
!
crypto pki certificate chain TP-self-signed-1566151040
certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
<output omitted>
  E99574A6 D945014F B6FE22F3 642EE29A 767EABF7 403930CA D2C59E23 102EC12E
  02F9C933 B3296D9E 095EBDAF 343D17F6 AF2831C7 6DA6DFE3 35B38D90 E6F07CD4
  40D96970 A0D12080 07A1C169 30B9D889 A6E2189C 75B988B9 0AF27EDC 6D6FA0E5
  CCFA6B29 729C1E0B 9DADACD0 3D7381
quit
```

Step 3: Save this file as a plain text file with a new filename, **Switch1-config.txt**, in this example.

Note: When saving the file, an extension, such as **.txt**, may be added to the filename automatically.

Step 4: In the Tftpd32 server window, click **Show Dir** to verify that the **Switch1-config.txt** file is located in the current directory.

Task 6: Upload running configuration file from TFTP server to switch S1.

Step 1: From the privileged EXEC mode on the switch, enter the **copy tftp running-config** command. Provide the remote host address of the TFTP server, 192.168.1.3. Enter the new filename, **Switch1-config.txt**. The exclamation mark (!) indicates the transfer process is in progress and is successful.

```
S1# copy tftp: running-config
Address or name of remote host []? 192.168.1.3
Source filename []? Switch1-config.txt
Destination filename [running-config]?
Accessing tftp://192.168.1.3/Switch1-config.txt...
Loading Switch1-config.txt from 192.168.1.3 (via Vlan1): !
[OK - 1580 bytes]
[OK]
1580 bytes copied in 9.118 secs (173 bytes/sec)
*Mar  1 00:21:16.242: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new certificate
```

```
*Mar  1 00:21:16.251: %SYS-5-CONFIG_I: Configured from tftp://192.168.1.3/Switch1-
confg.txt by console
```

```
Switch1#
```

After the transfer has completed, the prompt has changed from S1 to Switch1, because the running configuration is updated with the **hostname Switch1** command in the modified running configuration.

Step 2: Enter the **show running-config** command to examine running configuration file.

```
Switch1# show running-config
```

```
Building configuration...
```

```
Current configuration : 3062 bytes
```

```
!
```

```
! Last configuration change at 00:09:34 UTC Mon Mar 1 1993
```

```
!
```

```
version 15.0
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname Switch1
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
<output omitted>
```

Note: This procedure merges the running-config from the TFTP server with the current running-config in the switch or router. If changes were made to the current running-config, the commands in the TFTP copy are added. Alternatively, if the same command is issued, it updates the corresponding command in the switch or router current running-config.

If you want to completely replace the current running-config with the one from the TFTP server, you must erase the switch startup-config and reload the device. You will then need to configure the VLAN 1 management address, so there is IP connectivity between the TFTP server and the switch.

Part 4: Use TFTP to Back Up and Restore the Router Running Configuration

The backup and restore procedure from Part 3 can also be performed with a router. In Part 4, the running configuration file will be backed up and restored using a TFTP server.

Task 1: Verify connectivity to router R1 from PC-A.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Task 2: Transfer the running configuration from router R1 to TFTP server on PC-A.

Step 1: From the privileged EXEC mode on R1, enter the **copy running-config tftp** command. Provide the remote host address of the TFTP server, 192.168.1.3, and accept the default filename.

Step 2: Verify that the file has been transferred to the TFTP server.

Task 3: Restore the running configuration file to the router.

Step 1: Erase the startup-config file on the router.

Step 2: Reload the router.

Step 3: Configure the G0/1 interface on the router with an IP address 192.168.1.1.

Step 4: Verify connectivity between the router and PC-A.

Step 5: Use the **copy** command to transfer the running-config file from the TFTP server to the router. Use **running-config** as the destination.

Step 6: Verify the router has updated the running-config.

Part 5: Back Up and Restore Configurations Using Router Flash Memory

For the 1941 and other newer Cisco routers, there is no internal flash memory. The flash memory for these routers uses CompactFlash (CF) memory. The use of CF memory allows for more available flash memory and easier upgrades without the need to open the router case. Besides storing the necessary files, such as IOS images, the CF memory can store other files, such as a copy of the running configuration. In Part 5, you will create a backup copy of the running configuration file and save it on the CF memory on the router.

Note: If the router does not use CF, the router may not have enough flash memory for storing the backup copy of running configuration file. You should still read through the instructions and become familiar with the commands.

Task 1: Display the router file systems.

The **show file systems** command displays the available file systems on the router. The **flash0:** file system is the default file system on this router as indicated by the asterisk (*) symbol (at the beginning of the line). The hash (#) sign (at the end of the highlighted line) indicates that it is a bootable disk. The **flash0:** file system can also be referenced using the name **flash:**. The total size of the **flash0:** is 256 MB with 62 MB available. Currently the **flash1:** slot is empty as indicated by the — under the headings, Size (b) and Free (b). Currently **flash0:** and **nvr:** are the only available file systems.

```
R1# show file systems
```

```
File Systems:
```

Size (b)	Free (b)	Type	Flags	Prefixes
-	-	opaque	rw	archive:
-	-	opaque	rw	system:
-	-	opaque	rw	tmpsys:
-	-	opaque	rw	null:
-	-	network	rw	tftp:
* 260153344	64499712	disk	rw	flash0: flash:#
-	-	disk	rw	flash1:
262136	242776	nvr:	rw	nvr:
-	-	opaque	wo	syslog:
-	-	opaque	rw	xmodem:
-	-	opaque	rw	ymodem:
-	-	network	rw	rcp:
-	-	network	rw	http:
-	-	network	rw	ftp:
-	-	network	rw	scp:
-	-	opaque	ro	tar:

```
-          -   network   rw   https:
-          -   opaque    ro   cns:
```

Where is the startup-config file located? _____

Note: Verify there is at least 1 MB (1,048,576 bytes) of free space. If there is not enough space in the flash memory, please contact your instructor for further instructions. You can determine the size of flash memory and space available using the **show flash** or **dir flash:** command at the privileged EXEC prompt.

Task 2: Copy the router running configuration to flash.

A file can be copied to flash by using the **copy** command at the privileged EXEC prompt. In this example, the file is copied into **flash0:**, because there is only one flash drive available as displayed in the previous step, and it is also the default file system. The **R1-running-config-backup** file is used as the filename for the backup running configuration file.

Note: Remember that filenames are case-sensitive in the IOS file system.

Step 1: Copy the running configuration to flash memory.

```
R1# copy running-config flash:
Destination filename [running-config]? R1-running-config-backup
2169 bytes copied in 0.968 secs (2241 bytes/sec)
```

Step 2: Use **dir** command to verify the running-config has been copied to flash.

```
R1# dir flash:
Directory of flash0:/

   1  drw-                0  Nov 15 2011 14:59:04 +00:00  ipsdir
<output omitted>
   20  -rw-             67998028  Aug 7 2012 17:39:16 +00:00  c1900-universalk9-mz.SPA.152-
4.M3.bin
   22  -rw-              2169    Feb 4 2013 23:57:54 +00:00  R1-running-config-backup
   24  -rw-              5865    Jul 10 2012 14:46:22 +00:00  lpnat
   25  -rw-              6458    Jul 17 2012 00:12:40 +00:00  lpIPSec

260153344 bytes total (64503808 bytes free)
```

Step 3: Use the **more** command to view the running-config file in flash memory. Examine the file output and scroll to the Interface section. Notice the **no shutdown** command is not included with the GigabitEthernet0/1. The interface is shut down when this file is used to update the running configuration on the router.

```
R1# more flash:R1-running-config-backup
<output omitted>
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
<output omitted>
```

Task 3: Erase the startup configuration and reload the router.

Task 4: Restore the running configuration from flash.

Step 1: Verify the router has the default initial configuration.

Step 2: Copy the saved running-config file from flash to update the running-config.

```
Router# copy flash:R1-running-config-backup running-config
```

Step 3: Use the **show ip interface brief** command to view the status of the interfaces. The interface GigabitEthernet0/1 was not enabled when the running configuration was updated, because it is administratively down.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	TFTP	administratively down	down
Serial10/0/0	unassigned	YES	unset	administratively down	down
Serial10/0/1	unassigned	YES	unset	administratively down	down

The interface can be enabled using the **no shutdown** command in the interface configuration mode on the router.

Another option is to add the **no shutdown** command for the GigabitEthernet0/1 interface to the saved file before updating the router running configuration file. This will be done in Part 6 using a saved file on a USB flash drive.

Note: Because the IP address was configured by using a file transfer, TFTP is listed under the Method heading in the **show ip interface brief** output.

Part 6: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

A USB flash drive can be used to backup and restore files on a router with an available USB port. Two USB ports are available on the 1941 routers.

Note: USB ports are not available on all routers, but you should still become familiar with the commands.

Note: Because some ISR G1 routers (1841, 2801, or 2811) use File Allocation Table (FAT) file systems, there is a maximum size limit for the USB flash drives that can be used in this part of the lab. The recommended maximum size for an ISR G1 is 4 GB. If you receive the following message, the file system on the USB flash drive may be incompatible with the router or the capacity of the USB flash drive may have exceed maximum size of the FAT file system on the router.

```
*Feb  8 13:51:34.831: %USBFLASH-4-FORMAT: usbflash0 contains unexpected values in
partition table or boot sector. Device needs formatting before use!
```

Task 1: Insert a USB flash drive into a USB port on the router.

Notice the message on the terminal when inserting the USB flash drive.

```
R1#
```

```
* *Feb  5 20:38:04.678: %USBFLASH-5-CHANGE: usbflash0 has been inserted!
```

Task 2: Verify that the USB flash file system is available.

```
R1# show file systems
```

```
File Systems:
```

Size (b)	Free (b)	Type	Flags	Prefixes
-	-	opaque	rw	archive:
-	-	opaque	rw	system:
-	-	opaque	rw	tmpsys:

```

-          -   opaque      rw   null:
-          -   network     rw   tftp:
* 260153344 64512000 disk     rw   flash0: flash:#
-          -   disk       rw   flash1:
262136     244676 nvram     rw   nvram:
-          -   opaque     wo   syslog:
-          -   opaque     rw   xmodem:
-          -   opaque     rw   ymodem:
-          -   network     rw   rcp:
-          -   network     rw   http:
-          -   network     rw   ftp:
-          -   network     rw   scp:
-          -   opaque     ro   tar:
-          -   network     rw   https:
-          -   opaque     ro   cns:
7728881664 7703973888 usbflash rw   usbflash0:

```

Task 3: Copy the running configuration file to the USB flash drive.

Use the **copy** command to copy the running configuration file to the USB flash drive.

```

R1# copy running-config usbflash0:
Destination filename [running-config]? R1-running-config-backup.txt
2198 bytes copied in 0.708 secs (3105 bytes/sec)

```

Task 4: List the file on the USB flash drive.

Use the **dir** command (or **show** command) on the router to list the files on the USB flash drive. In this sample, a flash drive was inserted into USB port 0 on the router.

```

R1# dir usbflash0:
Directory of usbflash0:/

 1  -rw-          16216  Nov 15 2006 09:34:04 +00:00  ConditionsFR.txt
 2  -rw-           2462  May 26 2006 21:33:40 +00:00  Nlm.ico
 3  -rw-       24810439  Apr 16 2010 10:28:00 +00:00  Twice.exe
 4  -rw-           71   Jun 4 2010 11:23:06 +00:00  AUTORUN.INF
 5  -rw-        65327   Mar 11 2008 10:54:26 +00:00  ConditionsEN.txt
 6  -rw-          2198   Feb 5 2013 21:36:40 +00:00  R1-running-config-backup.txt

```

```

7728881664 bytes total (7703973888 bytes free)

```

Task 5: Erase the startup-config and reload the router.

Task 6: Modify the saved file.

Step 1: Remove the USB drive from the router.

```

Router#
*Feb  5 21:41:51.134: %USBFLASH-5-CHANGE: usbflash0 has been removed!

```

Step 2: Insert the USB drive into the USB port of a PC.

Step 3: Modify the file using a text editor. The **no shutdown** command is added to the GigabitEthernet0/1 interface. Save the file as a plain text file on to the USB flash drive.

```
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
no shutdown
duplex auto
speed auto
!
```

Step 4: Remove the USB flash drive from the PC safely.

Task 7: Restore the running configuration file to the router.

Step 1: Insert the USB flash drive into a USB port on the router. Notice the port number where the USB drive has been inserted if there is more than one USB port available on the router.

```
*Feb  5 21:52:00.214: %USBFLASH-5-CHANGE: usbflash1 has been inserted!
```

Step 2: List the files on the USB flash drive.

```
Router# dir usbflash1:
Directory of usbflash1:/

 1  -rw-          16216  Nov 15 2006 09:34:04 +00:00  ConditionsFR.txt
 2  -rw-           2462  May 26 2006 21:33:40 +00:00  Nlm.ico
 3  -rw-       24810439  Apr 16 2010 10:28:00 +00:00  Twice.exe
 4  -rw-           71   Jun 4 2010 11:23:06 +00:00  AUTORUN.INF
 5  -rw-        65327   Mar 11 2008 10:54:26 +00:00  ConditionsEN.txt
 6  -rw-         2344   Feb 6 2013 14:42:30 +00:00  R1-running-config-backup.txt

7728881664 bytes total (7703965696 bytes free)
```

Step 3: Copy the running configuration file to the router.

```
Router# copy usbflash1:R1-running-config-backup.txt running-config
Destination filename [running-config]?
2344 bytes copied in 0.184 secs (12739 bytes/sec)
R1#
```

Step 4: Verify that the GigabitEthernet0/1 interface is enabled.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	TFTP	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

The G0/1 interface is enabled because the modified running configuration included the **no shutdown** command.

Reflection

1. What command do you use to copy a file from the flash to a USB drive?

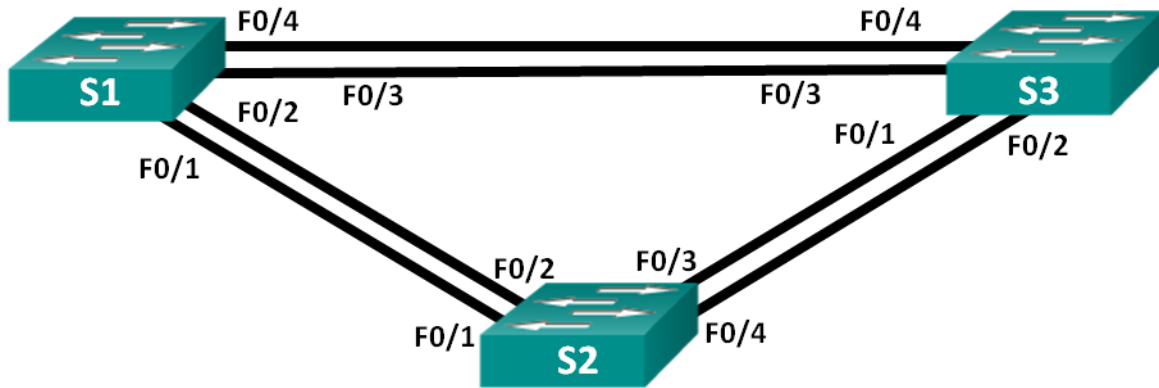
2. What command do you use to copy a file from the USB flash drive to a TFTP server?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab6 – Building a Switched Network with Redundant Links

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
S3	VLAN 1	192.168.1.3	255.255.255.0

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Determine the Root Bridge

Part 3: Observe STP Port Selection Based on Port Cost

Part 4: Observe STP Port Selection Based on Port Priority

Background / Scenario

Redundancy increases the availability of devices in the network topology by protecting the network from a single point of failure. Redundancy in a switched network is accomplished through the use of multiple switches or multiple links between switches. When physical redundancy is introduced into a network design, loops and duplicate frames can occur.

The Spanning Tree Protocol (STP) was developed as a Layer 2 loop-avoidance mechanism for redundant links in a switched network. STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.

In this lab, you will use the **show spanning-tree** command to observe the STP election process of the root bridge. You will also observe the port selection process based on cost and priority.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

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

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the switches.

Task 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Task 2: Initialize and reload the switches as necessary.

Task 3: Configure basic settings for each switch.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as shown in the topology.

Step 3: Assign **class** as the encrypted privileged EXEC mode password.

Step 4: Assign **cisco** as the console and vty passwords and enable login for console and vty lines.

Step 5: Configure logging synchronous for the console line.

Step 6: Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.

Step 7: Configure the IP address listed in the Addressing Table for VLAN 1 on all switches.

Step 8: Copy the running configuration to the startup configuration.

Task 4: Test connectivity.

Verify that the switches can ping one another.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

Troubleshoot until you are able to answer yes to all questions.

Part 2: Determine the Root Bridge

Every spanning-tree instance (switched LAN or broadcast domain) has a switch designated as the root bridge. The root bridge serves as a reference point for all spanning-tree calculations to determine which redundant paths to block.

An election process determines which switch becomes the root bridge. The switch with the lowest bridge identifier (BID) becomes the root bridge. The BID is made up of a bridge priority value, an extended system ID, and the MAC address of the switch. The priority value can range from 0 to 65,535, in increments of 4,096, with a default value of 32,768.

Task 1: Deactivate all ports on the switches.

Task 2: Configure connected ports as trunks.

Task 3: Activate ports F0/2 and F0/4 on all switches.

Task 4: Display spanning tree information.

Issue the **show spanning-tree** command on all three switches. The Bridge ID Priority is calculated by adding the priority value and the extended system ID. The extended system ID is always the VLAN number. In the example below, all three switches have equal Bridge ID Priority values ($32769 = 32768 + 1$, where default priority = 32768, VLAN number = 1); therefore, the switch with the lowest MAC address becomes the root bridge (S2 in the example).

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
      Address      0cd9.96d2.4000
      Cost          19
      Port          2 (FastEthernet0/2)
      Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID Priority      32769 (priority 32768 sys-id-ext 1)
      Address      0cd9.96e8.8a00
      Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
      Aging Time    300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

S2# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
      Address      0cd9.96d2.4000
      This bridge is the root
      Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID Priority      32769 (priority 32768 sys-id-ext 1)
      Address      0cd9.96d2.4000
      Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
      Aging Time    300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID    Priority    32769
  Address    0cd9.96d2.4000
    Cost      19
    Port      2 (FastEthernet0/2)
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  
```

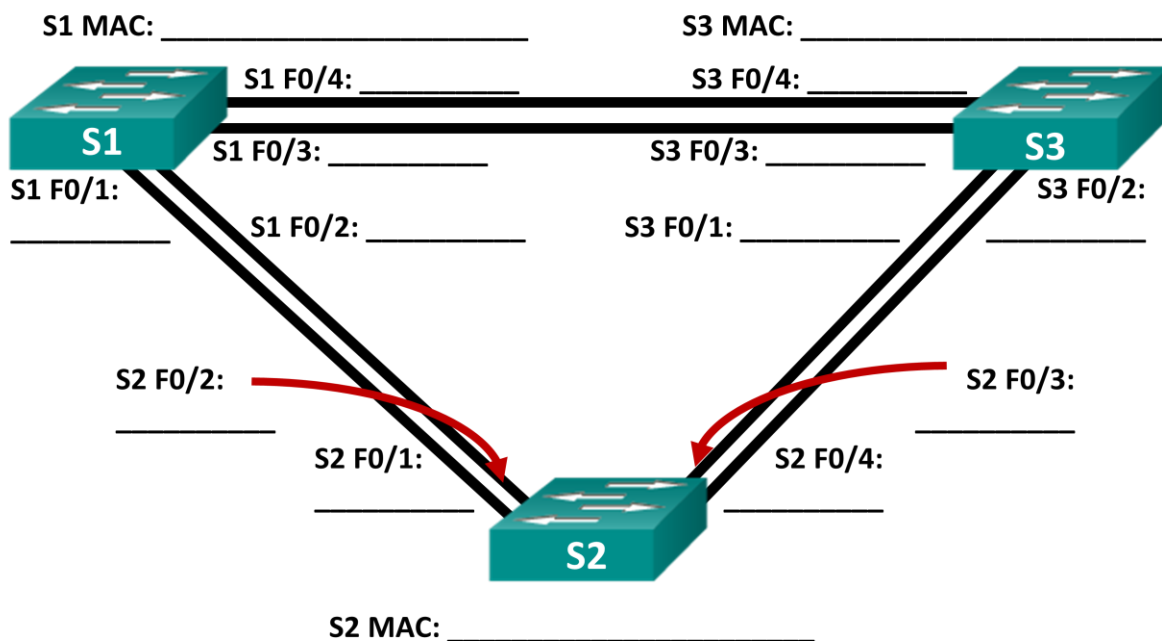
```

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
  Address    0cd9.96e8.7400
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
    Aging Time 300 sec
  
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

Note: The default STP mode on the 2960 switch is Per VLAN Spanning Tree (PVST).

In the diagram below, record the Role and Status (Sts) of the active ports on each switch in the Topology.



Based on the output from your switches, answer the following questions.

Which switch is the root bridge? _____

Why did spanning tree select this switch as the root bridge?

Which ports are the root ports on the switches? _____

Which ports are the designated ports on the switches? _____

What port is showing as an alternate port and is currently being blocked? _____

Why did spanning tree select this port as the non-designated (blocked) port?

Part 3: Observe STP Port Selection Based on Port Cost

The spanning tree algorithm (STA) uses the root bridge as the reference point and then determines which ports to block, based on path cost. The port with the lower path cost is preferred. If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. Lower values are always preferred. In Part 3, you will change the port cost to control which port is blocked by spanning tree.

Task 1: Locate the switch with the blocked port.

With the current configuration, only one switch should have a port that is blocked by STP. Issue the **show spanning-tree** command on both non-root switches. In the example below, spanning tree is blocking port F0/4 on the switch with the highest BID (S1).

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID    Priority    32769
           Address    0cd9.96d2.4000
           Cost      19
           Port      2 (FastEthernet0/2)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0cd9.96e8.8a00
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

```
S3# show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
```

```
Root ID    Priority    32769
           Address    0cd9.96d2.4000
           Cost      19
           Port      2 (FastEthernet0/2)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0cd9.96e8.7400
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

Note: Root bridge and port selection may differ in your topology.

Task 2: Change port cost.

In addition to the blocked port, the only other active port on this switch is the port designated as the root port. Lower the cost of this root port to 18 by issuing the **spanning-tree cost 18** interface configuration mode command.

```
S1(config)# interface f0/2
S1(config-if)# spanning-tree cost 18
```

Task 3: Observe spanning tree changes.

Re-issue the **show spanning-tree** command on both non-root switches. Observe that the previously blocked port (S1 - F0/4) is now a designated port and spanning tree is now blocking a port on the other non-root switch (S3 - F0/4).

```
S1# show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol ieee
```

```
Root ID    Priority    32769
           Address    0cd9.96d2.4000
           Cost      18
           Port      2 (FastEthernet0/2)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0cd9.96e8.8a00
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 300 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/2	Root	FWD	18	128.2	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
  Address     0cd9.96d2.4000
   Cost       19
   Port       2 (FastEthernet0/2)
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID    Priority      32769 (priority 32768 sys-id-ext 1)
  Address     0cd9.96e8.7400
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time    300 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

Why did spanning tree change the previously blocked port to a designated port, and block the port that was a designated port on the other switch?

Task 4: Remove port cost changes.

Step 1: Issue the **no spanning-tree cost 18** interface configuration mode command to remove the cost statement that you created earlier.

```

S1(config)# interface f0/2
S1(config-if)# no spanning-tree cost 18

```

Step 2: Re-issue the **show spanning-tree** command to verify that STP has reset the port on the non-root switches back to the original port settings. It takes approximately 30 seconds for STP to complete the port transition process.

Part 4: Observe STP Port Selection Based on Port Priority

If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. The default port priority value is 128. STP aggregates the port priority with the port number to break ties. Lower values are always preferred. In Part 4, you will activate redundant paths to each switch to observe how STP selects a port using the port priority.

Step 1: Activate ports F0/1 and F0/3 on all switches.

Step 2: Wait 30 seconds for STP to complete the port transition process, and then issue the **show spanning-tree** command on the non-root switches. Observe that the root port has moved to the lower numbered port linked to the root switch, and blocked the previous root port.

S1# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
             Address      0cd9.96d2.4000
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID    Priority      32769 (priority 32768 sys-id-ext 1)
             Address      0cd9.96e8.8a00
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Altn	BLK	19	128.2	P2p
Fa0/3	Altn	BLK	19	128.3	P2p
Fa0/4	Altn	BLK	19	128.4	P2p

S3# **show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
             Address      0cd9.96d2.4000
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID    Priority      32769 (priority 32768 sys-id-ext 1)
             Address      0cd9.96e8.7400
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15 sec

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Altn	BLK	19	128.2	P2p
Fa0/3	Desg	FWD	19	128.3	P2p
Fa0/4	Desg	FWD	19	128.4	P2p

What port did STP select as the root port on each non-root switch? _____

Why did STP select these ports as the root port on these switches?

Reflection

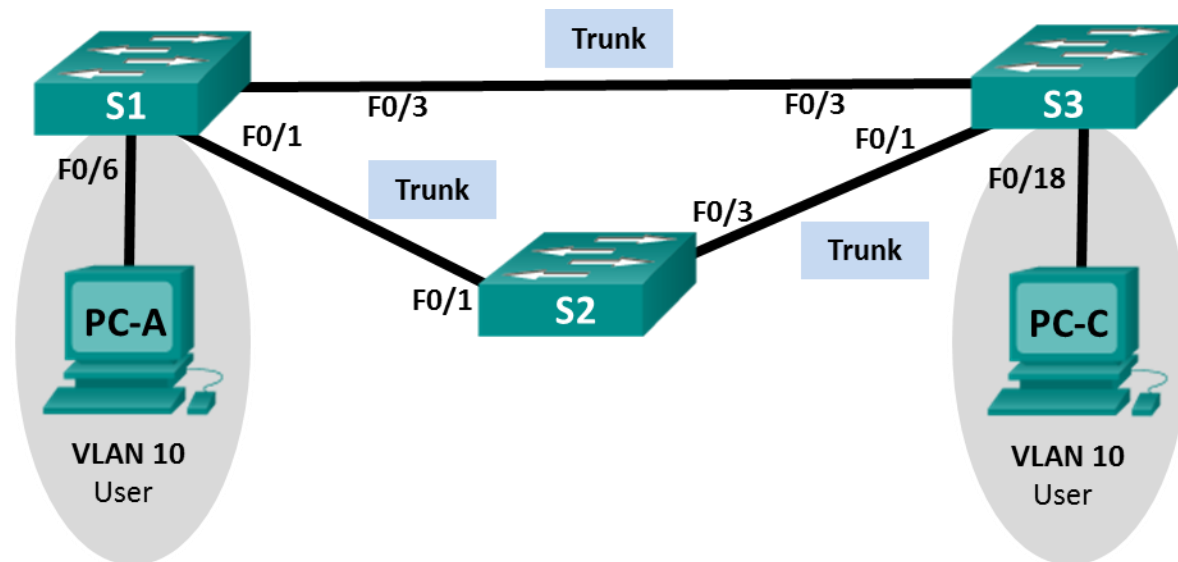
1. After a root bridge has been selected, what is the first value STP uses to determine port selection?

2. If the first value is equal on the two ports, what is the next value that STP uses to determine port selection?

3. If both values are equal on the two ports, what is the next value that STP uses to determine port selection?

Lab7 – Configuring Rapid PVST+, PortFast, and BPDU Guard

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

VLAN Assignments

VLAN	Name
10	User
99	Management

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure VLANs, Native VLAN, and Trunks

Part 3: Configure the Root Bridge and Examine PVST+ Convergence

Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

Background / Scenario

The Per-VLAN Spanning Tree (PVST) protocol is Cisco proprietary. Cisco switches default to PVST. Rapid PVST+ (IEEE 802.1w) is an enhanced version of PVST+ and allows for faster spanning-tree calculations and convergence in response to Layer 2 topology changes. Rapid PVST+ defines three port states: discarding, learning, and forwarding, and provides multiple enhancements to optimize network performance.

In this lab, you will configure the primary and secondary root bridge, examine PVST+ convergence, configure Rapid PVST+ and compare its convergence to PVST+. In addition, you will configure edge ports to transition immediately to a forwarding state using PortFast and prevent the edge ports from forwarding BDPUs using BDPU guard.

Note: This lab provides minimal assistance with the actual commands necessary for configuration. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

Note: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

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

Required Resources

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

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

Task 1: Cable the network as shown in the topology.

Task 2: Configure PC hosts.

Task 3: Initialize and reload the switches as necessary.

Task 4: Configure basic settings for each switch.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as shown in the Topology.

Step 3: Assign **cisco** as the console and vty passwords and enable login.

Step 4: Assign **class** as the encrypted privileged EXEC mode password.

Step 5: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 6: Shut down all switch ports.

Step 7: Copy the running configuration to startup configuration.

Part 2: Configure VLANs, Native VLAN, and Trunks

In Part 2, you will create VLANs, assign switch ports to VLANs, configure trunk ports, and change the native VLAN for all switches.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure the VLANs, native VLAN, and trunks without referring to the appendix.

Task 1: Create VLANs.

Use the appropriate commands to create VLANs 10 and 99 on all of the switches. Name VLAN 10 as **User** and VLAN 99 as **Management**.

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
```

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
```

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
```

Task 2: Enable user ports in access mode and assign VLANs.

For S1 F0/6 and S3 F0/18, enable the ports, configure them as access ports, and assign them to VLAN 10.

Task 3: Configure trunk ports and assign to native VLAN 99.

For ports F0/1 and F0/3 on all switches, enable the ports, configure them as trunk ports, and assign them to native VLAN 99.

Task 4: Configure the management interface on all switches.

Using the Addressing Table, configure the management interface on all switches with the appropriate IP address.

Task 5: Verify configurations and connectivity.

Use the **show vlan brief** command on all switches to verify that all VLANs are registered in the VLAN table and that the correct ports are assigned.

Use the **show interfaces trunk** command on all switches to verify trunk interfaces.

Use the **show running-config** command on all switches to verify all other configurations.

What is the default setting for spanning-tree mode on Cisco switches?

Verify connectivity between PC-A and PC-C. Was your ping successful? _____

If your ping was unsuccessful, troubleshoot the configurations until the issue is resolved.

Note: It may be necessary to disable the PC firewall to successfully ping between PCs.

Part 3: Configure the Root Bridge and Examine PVST+ Convergence

In Part 3, you will determine the default root in the network, assign the primary and secondary root, and use the **debug** command to examine convergence of PVST+.

Note: The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure the root bridge without referring to the appendix.

Task 1: Determine the current root bridge.

Which command allows a user to determine the spanning-tree status of a Cisco Catalyst switch for all VLANs? Write the command in the space provided.

Use the command on all three switches to determine the answers to the following questions:

Note: There are three instances of the spanning tree on each switch. The default STP configuration on Cisco switches is PVST+, which creates a separate spanning tree instance for each VLAN (VLAN 1 and any user-configured VLANs).

What is the bridge priority of switch S1 for VLAN 1? _____

What is the bridge priority of switch S2 for VLAN 1? _____

What is the bridge priority of switch S3 for VLAN 1? _____

Which switch is the root bridge? _____

Why was this switch elected as the root bridge?

Task 2: Configure a primary and secondary root bridge for all existing VLANs.

Having a root bridge (switch) elected by MAC address may lead to a suboptimal configuration. In this lab, you will configure switch S2 as the root bridge and S1 as the secondary root bridge.

Step 1: Configure switch S2 to be the primary root bridge for all existing VLANs. Write the command in the space provided.

Step 2: Configure switch S1 to be the secondary root bridge for all existing VLANs. Write the command in the space provided.

Use the **show spanning-tree** command to answer the following questions:

What is the bridge priority of S1 for VLAN 1? _____

What is the bridge priority of S2 for VLAN 1? _____

Which interface in the network is in a blocking state? _____

Task 3: Change the Layer 2 topology and examine convergence.

To examine PVST+ convergence, you will create a Layer 2 topology change while using the **debug** command to monitor spanning-tree events.

Step 1: Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

```
S3# debug spanning-tree events
```

Spanning Tree event debugging is on

Step 2: Create a topology change by disabling interface F0/1 on S3.

```
S3(config)# interface f0/1
```

```
S3(config-if)# shutdown
```

```
*Mar 1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to down
*Mar 1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
*Mar 1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar 1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning
*Mar 1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

Note: Before proceeding, use the **debug** output to verify that all VLANs on F0/3 have reached a forwarding state then use the command **no debug spanning-tree events** to stop the **debug** output.

Through which port states do each VLAN on F0/3 proceed during network convergence?

Using the time stamp from the first and last STP debug message, calculate the time (to the nearest second) that it took for the network to converge. **Hint:** The debug timestamp format is date hh.mm.ss:msec.

Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

In Part 4, you will configure Rapid PVST+ on all switches. You will configure PortFast and BPDU guard on all access ports, and then use the **debug** command to examine Rapid PVST+ convergence.

Note: The required commands for Part 4 are provided in Appendix A. Test your knowledge by trying to configure the Rapid PVST+, PortFast, and BPDU guard without referring to the appendix.

Task 1: Configure Rapid PVST+.

Step 1: Configure S1 for Rapid PVST+. Write the command in the space provided.

Step 2: Configure S2 and S3 for Rapid PVST+.

Step 3: Verify configurations with the **show running-config | include spanning-tree mode** command.

```
S1# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S2# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S3# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

Task 2: Configure PortFast and BPDU Guard on access ports.

PortFast is a feature of spanning tree that transitions a port immediately to a forwarding state as soon as it is turned on. This is useful in connecting hosts so that they can start communicating on the VLAN instantly, rather than waiting on spanning tree. To prevent ports that are configured with PortFast from forwarding BPDUs, which could change the spanning tree topology, BPDU guard can be enabled. At the receipt of a BPDU, BPDU guard disables a port configured with PortFast.

Step 1: Configure interface F0/6 on S1 with PortFast. Write the command in the space provided.

Step 2: Configure interface F0/6 on S1 with BPDU guard. Write the command in the space provided.

Step 3: Globally configure all non-trunking ports on switch S3 with PortFast. Write the command in the space provided.

Step 4: Globally configure all non-trunking PortFast ports on switch S3 with BPDU guard. Write the command in the space provided.

Task 3: Examine Rapid PVST+ convergence.

Step 1: Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

Step 2: Create a topology change by enabling interface F0/1 on switch S3.

```
S3(config)# interface f0/1
S3(config-if)# no shutdown
*Mar 1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 01:28:37.588: RSTP(1): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(1): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(10): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(10): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(99): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(99): Fa0/1 is now designated
*Mar 1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(1): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(10): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.605: RSTP(99): Fa0/1 is now root port
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root
*Mar 1 01:28:37.605: RSTP(99): synced Fa0/1
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 is now alternate
*Mar 1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a proposal
*Mar 1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Using the time stamp from the first and last RSTP debug message, calculate the time that it took for the network to converge.

Reflection

1. What is the main benefit of using Rapid PVST+?

2. How does configuring a port with PortFast allow for faster convergence?

3. What protection does BPDU guard provide?

Appendix A – Switch Configuration Commands

Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/1
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface f0/3
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# exit
S1(config)# spanning-tree vlan 1,10,99 root secondary
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
```

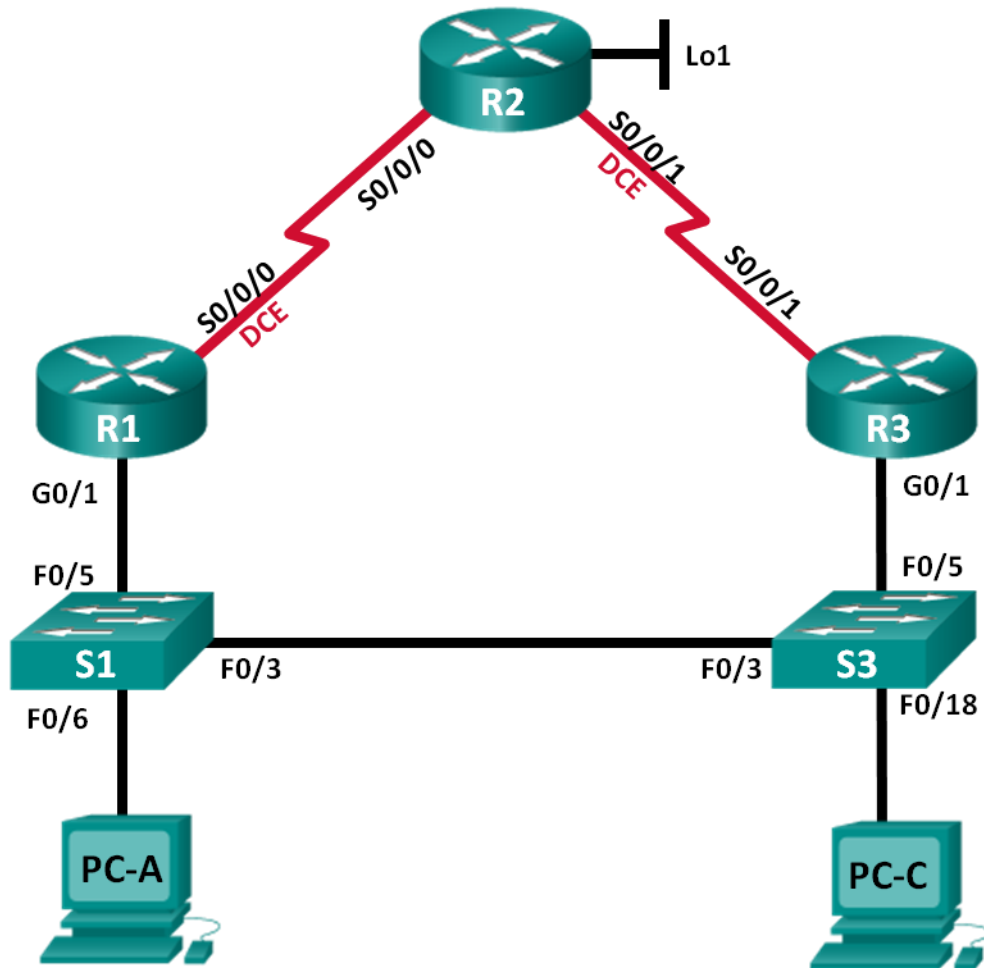
```
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface f0/3
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0
S2(config-if)# exit
S2(config)# spanning-tree vlan 1,10,99 root primary
S2(config)# spanning-tree mode rapid-pvst
```

Switch S3

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
S3(config-vlan)# exit
S3(config)# interface f0/18
S3(config-if)# no shutdown
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 10
S3(config-if)# spanning-tree portfast
S3(config-if)# spanning-tree bpduguard enable
S3(config-if)# interface f0/1
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface f0/3
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface vlan 99
S3(config-if)# ip address 192.168.1.13 255.255.255.0
S3(config-if)# exit
S3(config)# spanning-tree mode rapid-pvst
```

Lab8 – Configuring HSRP and GLBP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo1	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.1.3	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure First Hop Redundancy using HSRP

Part 3: Configure First Hop Redundancy using GLBP

Background / Scenario

Spanning tree provides loop-free redundancy between switches within your LAN. However, it does not provide redundant default gateways for end-user devices within your network if one of your routers fails. First Hop Redundancy Protocols (FHRPs) provide redundant default gateways for end devices with no end-user configuration necessary.

In this lab, you will configure two FHRPs. In Part 2, you will configure Cisco's Hot Standby Routing Protocol (HSRP), and in Part 3 you will configure Cisco's Gateway Load Balancing Protocol (GLBP).

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

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

Required Resources

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

- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Task 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Task 2: Configure PC hosts.

Task 3: Initialize and reload the routers and switches as necessary.

Task 4: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as shown in the topology.

Step 3: Configure IP addresses for the routers as listed in the Addressing Table.

Step 4: Set clock rate to **128000** for all DCE serial interfaces.

Step 5: Assign **class** as the encrypted privileged EXEC mode password.

Step 6: Assign **cisco** for the console and vty password and enable login.

Step 7: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 8: Copy the running configuration to the startup configuration.

Task 5: Configure basic settings for each switch.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as shown in the topology.

Step 3: Assign **class** as the encrypted privileged EXEC mode password.

Step 4: Configure IP addresses for the switches as listed in the Addressing Table.

Step 5: Configure the default gateway on each switch.

Step 6: Assign **cisco** for the console and vty password and enable login.

Step 7: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 8: Copy the running configuration to the startup configuration.

Task 6: Verify connectivity between PC-A and PC-C.

Ping from PC-A to PC-C. Were the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: It may be necessary to disable the PC firewall to successfully ping between PCs.

Task 7: Configure routing.

Step 1: Configure EIGRP on the routers and use AS of 1. Add all the networks, except 209.165.200.224/27 into the EIGRP process.

Step 2: Configure a default route on R2 using Lo1 as the exit interface to 209.165.200.224/27 network and redistribute this route into the EIGRP process.

Task 8: Verify connectivity.

Step 1: From PC-A, you should be able to ping every interface on R1, R2, R3, and PC-C. Were all pings successful? _____

Step 2: From PC-C, you should be able to ping every interface on R1, R2, R3, and PC-A. Were all pings successful? _____

Part 2: Configure First Hop Redundancy Using HSRP

Even though the topology has been designed with some redundancy (two routers and two switches on the same LAN network), both PC-A and PC-C are configured with only one gateway address. PC-A is using R1 and PC-C is using R3. If either of these routers or the interfaces on the routers went down, the PC could lose its connection to the Internet.

In Part 2, you will test how the network behaves both before and after configuring HSRP. To do this, you will determine the path that packets take to the loopback address on R2.

Task 1: Determine the path for Internet traffic for PC-A and PC-C.

Step 1: From a command prompt on PC-A, issue a **tracert** command to the 209.165.200.225 loopback address of R2.

```
C:\ tracert 209.165.200.225
Tracing route to 209.165.200.225 over a maximum of 30 hops

  1      1 ms      1 ms      1 ms  192.168.1.1
  2     13 ms     13 ms     13 ms  209.165.200.225
```

Trace complete.

What path did the packets take from PC-A to 209.165.200.225? _____

Step 2: From a command prompt on PC-C, issue a **tracert** command to the 209.165.200.225 loopback address of R2.

What path did the packets take from PC-C to 209.165.200.225? _____

Task 2: Start a ping session on PC-A, and break the connection between S1 and R1.

Step 1: From a command prompt on PC-A, issue a **ping -t** command to the **209.165.200.225** address on R2. Make sure you leave the command prompt window open.

Note: The pings continue until you press **Ctrl+C**, or until you close the command prompt window.

```
C:\ ping -t 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
```

```

Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
<output omitted>

```

Step 2: As the ping continues, disconnect the Ethernet cable from F0/5 on S1. You can also shut down the S1 F0/5 interface, which creates the same result.

What happened to the ping traffic?

Step 3: Repeat Steps 2a and 2b on PC-C and S3. Disconnect cable from F0/5 on S3.

What were your results?

Step 4: Reconnect the Ethernet cables to F0/5 or enable the F0/5 interface on both S1 and S3, respectively. Re-issue pings to 209.165.200.225 from both PC-A and PC-C to make sure connectivity is re-established.

Task 3: Configure HSRP on R1 and R3.

In this step, you will configure HSRP and change the default gateway address on PC-A, PC-C, S1, and S2 to the virtual IP address for HSRP. R1 becomes the active router via configuration of the HSRP priority command.

Step 1: Configure HSRP on R1.

```

R1(config)# interface g0/1
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt

```

Step 2: Configure HSRP on R3.

```

R3(config)# interface g0/1
R3(config-if)# standby 1 ip 192.168.1.254

```

Step 3: Verify HSRP by issuing the **show standby** command on R1 and R3.

```

R1# show standby
GigabitEthernet0/1 - Group 1
  State is Active
    1 state change, last state change 00:02:11
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.784 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3, priority 100 (expires in 9.568 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)

```

```
R3# show standby
GigabitEthernet0/1 - Group 1
  State is Standby
    4 state changes, last state change 00:02:20
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.128 secs
  Preemption disabled
  Active router is 192.168.1.1, priority 150 (expires in 10.592 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Gi0/1-1" (default)
```

Using the output shown above, answer the following questions:

Which router is the active router? _____

What is the MAC address for the virtual IP address? _____

What is the IP address and priority of the standby router?

Step 4: Use the **show standby brief** command on R1 and R3 to view an HSRP status summary. Sample output is shown below.

```
R1# show standby brief
                P indicates configured to preempt.
                |
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Gi0/1      1    150 P Active  local          192.168.1.3     192.168.1.254
```

```
R3# show standby brief
                P indicates configured to preempt.
                |
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Gi0/1      1    100 Standby 192.168.1.1    local          192.168.1.254
```

Step 5: Change the default gateway address for PC-A, PC-C, S1, and S3. Which address should you use?

Verify the new settings. Issue a ping from both PC-A and PC-C to the loopback address of R2. Are the pings successful? _____

Task 4: Start a ping session on PC-A and break the connection between the switch that is connected to the Active HSRP router (R1).

Step 1: From a command prompt on PC-A, issue a **ping -t** command to the 209.165.200.225 address on R2. Ensure that you leave the command prompt window open.

Step 2: As the ping continues, disconnect the Ethernet cable from F0/5 on S1 or shut down the F0/5 interface.

What happened to the ping traffic?

Task 5: Verify HSRP settings on R1 and R3.

Step 1: Issue the **show standby brief** command on R1 and R3.

Which router is the active router? _____

Step 2: Reconnect the cable between the switch and the router or enable interface F0/5.

Step 3: Disable the HSRP configuration commands on R1 and R3.

```
R1(config)# interface g0/1
R1(config-if)# no standby 1
```

```
R3(config)# interface g0/1
R3(config-if)# no standby 1
```

Part 3: Configure First Hop Redundancy Using GLBP

By default, HSRP does NOT do load balancing. The active router always handles all of the traffic, while the standby router sits unused, unless there is a link failure. This is not an efficient use of resources. GLBP provides nonstop path redundancy for IP by sharing protocol and MAC addresses between redundant gateways. GLBP also allows a group of routers to share the load of the default gateway on a LAN. Configuring GLBP is very similar to HSRP. Load balancing can be done in a variety of ways using GLBP. In this lab, you will use the round-robin method.

Task 1: Configure GLBP on R1 and R3.

Step 1: Configure GLBP on R1.

```
R1(config)# interface g0/1
R1(config-if)# glbp 1 ip 192.168.1.254
R1(config-if)# glbp 1 preempt
R1(config-if)# glbp 1 priority 150
R1(config-if)# glbp 1 load-balancing round-robin
```

Step 2: Configure GLBP on R3.

```
R3(config)# interface g0/1
R3(config-if)# glbp 1 ip 192.168.1.254
R3(config-if)# glbp 1 load-balancing round-robin
```

Task 2: Verify GLBP on R1 and R3.

Step 1: Issue the **show glbp brief** command on R1 and R3.

```
R1# show glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Gi0/1	1	-	150	Active	192.168.1.254	local	192.168.1.3
Gi0/1	1	1	-	Active	0007.b400.0101	local	-
Gi0/1	1	2	-	Listen	0007.b400.0102	192.168.1.3	-

```
R3# show glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Gi0/1	1	-	100	Standby	192.168.1.254	192.168.1.1	local
Gi0/1	1	1	-	Listen	0007.b400.0101	192.168.1.1	-
Gi0/1	1	2	-	Active	0007.b400.0102	local	-

Task 3: Generate traffic from PC-A and PC-C to the R2 loopback interface.

Step 1: From a command prompt on PC-A, ping the 209.165.200.225 address of R2.

```
C:\> ping 209.165.200.225
```

Step 2: Issue an **arp -a** command on PC-A. Which MAC address is used for the 192.168.1.254 address?

Step 3: Generate more traffic to the loopback interface of R2. Issue another **arp -a** command. Did the MAC address change for the default gateway address of 192.168.1.254?

As you can see, both R1 and R3 play a role in forwarding traffic to the loopback interface of R2. Neither router remains idle.

Task 4: Start a ping session on PC-A, and break the connection between the switch that is connected to R1.

Step 1: From a command prompt on PC-A, issue a **ping -t** command to the 209.165.200.225 address on R2. Make sure you leave the command prompt window open.

Step 2: As the ping continues, disconnect the Ethernet cable from F0/5 on S1 or shut down the F0/5 interface.

What happened to the ping traffic?

Reflection

1. Why would there be a need for redundancy in a LAN?

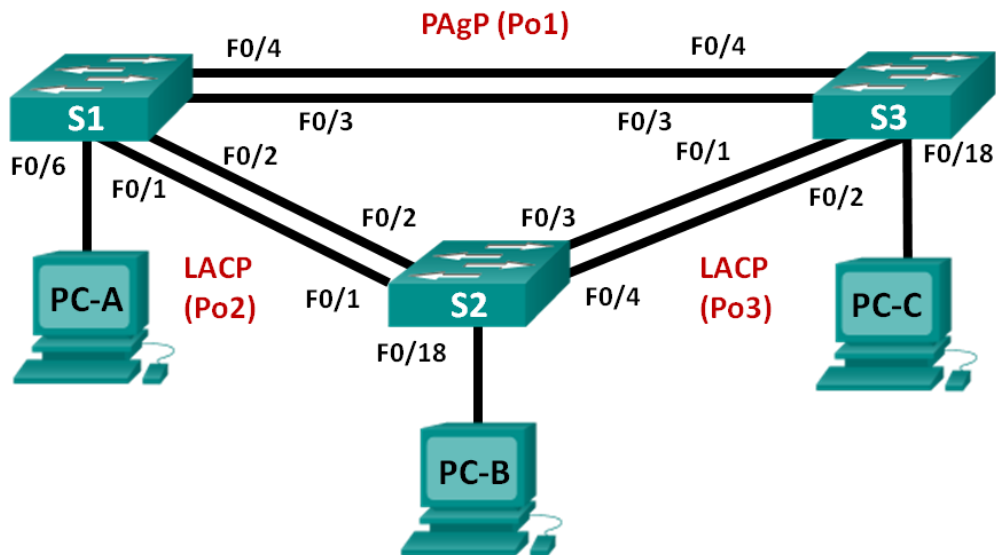
2. If you had a choice, which protocol would you implement in your network, HSRP or GLBP? Explain your choice.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab9 – Configuring EtherChannel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

Objectives

Part 1: Configure Basic Switch Settings

Part 2: Configure PAgP

Part 3: Configure LACP

Background / Scenario

Link aggregation allows the creation of logical links that are comprised of two or more physical links. This provides increased throughput beyond using only one physical link. Link aggregation also provides redundancy if one of the links fails.

In this lab, you will configure EtherChannel, a form of link aggregation used in switched networks. You will configure EtherChannel using Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP).

Note: PAgP is a Cisco-proprietary protocol that you can only run on Cisco switches and on switches that are licensed vendors to support PAgP. LACP is a link aggregation protocol that is defined by IEEE 802.3ad, and it is not associated with any specific vendor.

LACP allows Cisco switches to manage Ethernet channels between switches that conform to the 802.3ad protocol. You can configure up to 16 ports to form a channel. Eight of the ports are in active mode and the other eight are in standby mode. When any of the active ports fail, a standby port becomes active. Standby mode works only for LACP, not for PAgP.

Note: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

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

Required Resources

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

Part 1: Configure Basic Switch Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

Task 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Task 2: Initialize and reload the switches.

Task 3: Configure basic settings for each switch.

Step 1: Disable DNS lookup.

Step 2: Configure the device name as displayed in the topology.

Step 3: Encrypt plain text passwords.

Step 4: Create a MOTD banner warning users that unauthorized access is prohibited.

Step 5: Assign **class** as the encrypted privileged EXEC mode password.

Step 6: Assign **cisco** as the console and vty password and enable login.

Step 7: Configure logging synchronous to prevent console message from interrupting command entry.

Step 8: Shut down all switchports except the ports connected to PCs.

Step 9: Configure VLAN 99 and name it **Management**.

Step 10: Configure VLAN 10 and name it **Staff**.

Step 11: Configure the switch ports with attached hosts as access ports in VLAN 10.

Step 12: Assign the IP addresses according to the Addressing Table.

Step 13: Copy the running configuration to startup configuration.

Task 4: Configure the PCs.

Assign IP addresses to the PCs according to the Addressing Table.

Part 2: Configure PAgP

PAgP is a Cisco proprietary protocol for link aggregation. In Part 2, a link between S1 and S3 will be configured using PAgP.

Task 1: Configure PAgP on S1 and S3.

For a link between S1 and S3, configure the ports on S1 with PAgP desirable mode and the ports on S3 with PAgP auto mode. Enable the ports after PAgP modes have been configured.

```
S1(config)# interface range f0/3-4
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)# no shutdown

S3(config)# interface range f0/3-4
S3(config-if-range)# channel-group 1 mode auto
Creating a port-channel interface Port-channel 1

S3(config-if-range)# no shutdown
*Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar 1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
S3(config-if-range)#
*Mar 1 00:09:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
*Mar 1 00:09:16.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to up
S3(config-if-range)#
*Mar 1 00:09:16.357: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Mar 1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
*Mar 1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

Task 2: Examine the configuration on the ports.

Currently the F0/3, F0/4, and Po1 (Port-channel1) interfaces on both S1 and S3 are in access operational mode with the administrative mode in dynamic auto. Verify the configuration using the **show run interface interface-id** and **show interfaces interface-id switchport** commands, respectively. The example configuration outputs for F0/3 on S1 are as follows:

```
S1# show run interface f0/3
Building configuration...

Current configuration : 103 bytes
!
interface FastEthernet0/3
channel-group 1 mode desirable
```

```
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Task 3: Verify that the ports have been aggregated.

```
S1# show etherchannel summary

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1
```

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)

S3# **show etherchannel summary**

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

```

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	PAgP	Fa0/3 (P) Fa0/4 (P)

What do the flags, SU and P, indicate in the Ethernet summary?

Task 4: Configure trunk ports.

After the ports have been aggregated, commands applied at the port channel interface affect all the links that were bundled together. Manually configure the Po1 ports on S1 and S3 as trunk ports and assign them to native VLAN 99.

```

S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99

```

```

S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99

```

Task 5: Verify that the ports are configured as trunk ports.

Step 1: Issue the **show run interface interface-id** commands on S1 and S3. What commands are listed for F0/3 and F0/4 on both switches? Compare the results to the running configuration for the Po1 interface? Record your observation.

Step 2: Issue the **show interfaces trunk** and **show spanning-tree** commands on S1 and S3. What trunk port is listed? What is the native VLAN? What is concluding result from the output?

From the **show spanning-tree** output, what is port cost and port priority for the aggregated link?

Part 3: Configure LACP

LACP is an open source protocol for link aggregation developed by the IEEE. In Part 3, the link between S1 and S2, and the link between S2 and S3 will be configured using LACP. Also, the individual links will be configured as trunks before they are bundled together as EtherChannels.

Task 1: Configure LACP between S1 and S2.

```
S1(config)# interface range f0/1-2
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99
S1(config-if-range)# channel-group 2 mode active
Creating a port-channel interface Port-channel 2
```

```
S1(config-if-range)# no shutdown
```

```
S2(config)# interface range f0/1-2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 2 mode passive
Creating a port-channel interface Port-channel 2
```

```
S2(config-if-range)# no shutdown
```

Task 2: Verify that the ports have been aggregated.

What protocol is Po2 using for link aggregation? Which ports are aggregated to form Po2? Record the command used to verify.

Task 3: Configure LACP between S2 and S3.

Step 1: Configure the link between S2 and S3 as Po3 and use LACP as the link aggregation protocol.

```
S2(config)# interface range f0/3-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 3 mode active
Creating a port-channel interface Port-channel 3
S2(config-if-range)# no shutdown
```

```
S3(config)# interface range f0/1-2
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
S3(config-if-range)# channel-group 3 mode passive
Creating a port-channel interface Port-channel 3
```

```
S3(config-if-range)# no shutdown
```

Step 2: Verify that the EtherChannel has formed.

Task 4: Verify end-to-end connectivity.

Verify that all devices can ping each other within the same VLAN. If not, troubleshoot until there is end-to-end connectivity.

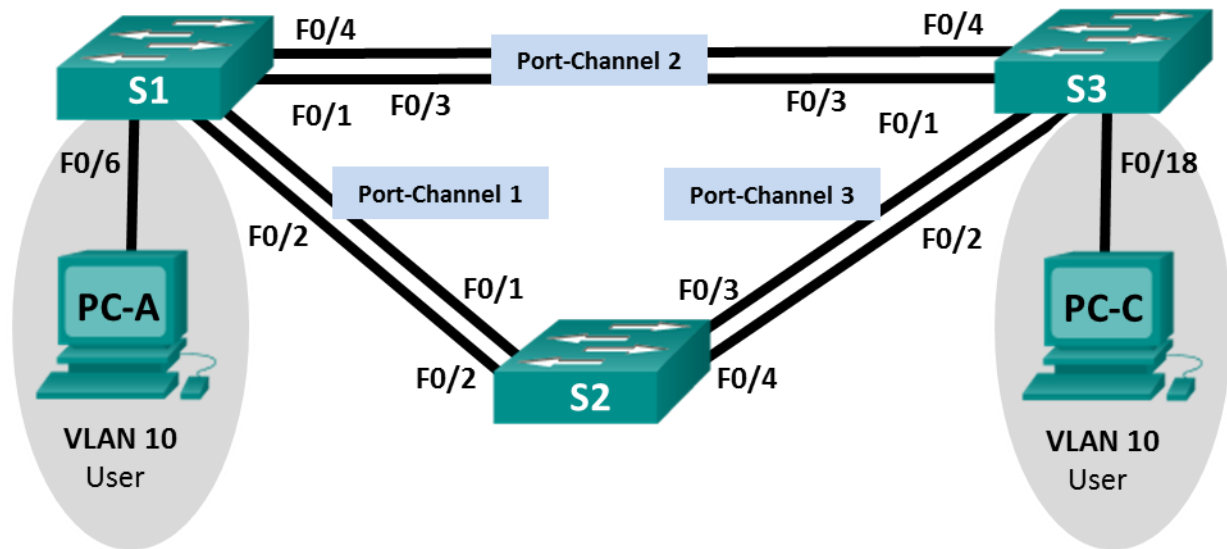
Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

What could prevent EtherChannels from forming?

Lab10 - Troubleshooting EtherChannel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

VLAN Assignments

VLAN	Name
10	User
99	Management

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot EtherChannel

Background / Scenario

The switches at your company were configured by an inexperienced network administrator. Several errors in the configuration have resulted in speed and connectivity issues. Your manager has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of

EtherChannel and standard testing methods, find and correct the errors. Ensure that all of the EtherChannels use Port Aggregation Protocol (PAgP), and that all hosts are reachable.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

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

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

In Part 1, you will set up the network topology, configure basic settings on the PC hosts, and load configurations on the switches.

Task 1: Cable the network as shown in the topology.

Task 2: Configure the PC hosts.

Task 3: Erase the startup and VLAN configurations and reload the switches.

Task 4: Load switch configurations.

Load the following configurations into the appropriate switch. All switches have the same passwords. The privileged EXEC password is **class**. The password for console and vty access is **cisco**. As all switches are Cisco devices, the network administrator decided to use Cisco's PAgP on all port channels configured with EtherChannel. Switch S2 is the root bridge for all VLANs in the topology.

Switch S1 Configuration:

```
hostname S1
interface range f0/1-24, g0/1-2
shutdown
exit
enable secret class
no ip domain lookup
line vty 0 15
password cisco
login
line con 0
password cisco
logging synchronous
login
exit
vlan 10
```

```

name User
vlan 99
  Name Management
interface range f0/1-2
  switchport mode trunk
  channel-group 1 mode active
  switchport trunk native vlan 99
  no shutdown
interface range f0/3-4
  channel-group 2 mode desirable
  switchport trunk native vlan 99
  no shutdown
interface f0/6
  switchport mode access
  switchport access vlan 10
  no shutdown
interface vlan 99
  ip address 192.168.1.11 255.255.255.0
interface port-channel 1
  switchport trunk native vlan 99
  switchport mode trunk
interface port-channel 2
  switchport trunk native vlan 99
  switchport mode access

```

Switch S2 Configuration:

```

hostname S2
interface range f0/1-24, g0/1-2
  shutdown
  exit
enable secret class
no ip domain lookup
line vty 0 15
  password cisco
  login
line con 0
  password cisco
  logging synchronous
  login
  exit
vlan 10
  name User
vlan 99
  name Management
spanning-tree vlan 1,10,99 root primary
interface range f0/1-2

```

```

switchport mode trunk
channel-group 1 mode desirable
switchport trunk native vlan 99
no shutdown
interface range f0/3-4
switchport mode trunk
channel-group 3 mode desirable
switchport trunk native vlan 99
interface vlan 99
ip address 192.168.1.12 255.255.255.0
interface port-channel 1
switchport trunk native vlan 99
switchport trunk allowed vlan 1,99
interface port-channel 3
switchport trunk native vlan 99
switchport trunk allowed vlan 1,10,99
switchport mode trunk

```

Switch S3 Configuration:

```

hostname S3
interface range f0/1-24, g0/1-2
shutdown
exit
enable secret class
no ip domain lookup
line vty 0 15
password cisco
login
line con 0
password cisco
logging synchronous
login
exit
vlan 10
name User
vlan 99
name Management
interface range f0/1-2
interface range f0/3-4
switchport mode trunk
channel-group 3 mode desirable
switchport trunk native vlan 99
no shutdown
interface f0/18
switchport mode access
switchport access vlan 10

```

```
no shutdown
interface vlan 99
ip address 192.168.1.13 255.255.255.0
interface port-channel 3
switchport trunk native vlan 99
switchport mode trunk
```

Task 5: Save your configuration.

Part 2: Troubleshoot EtherChannel

In Part 2, you must examine the configurations on all switches, make corrections if needed, and verify full functionality.

Task 1: Troubleshoot S1.

Step 1: Use the **show interfaces trunk** command to verify that the port channels are functioning as trunk ports.

Do port channels 1 and 2 appear as trunked ports? _____

Step 2: Use the **show etherchannel summary** command to verify that interfaces are configured in the correct port channel, the proper protocol is configured, and the interfaces are in use.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

Step 3: Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.

Step 4: Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configurations.

Step 5: Use the **show interfaces trunk** command to verify trunk settings.

Step 6: Use the **show etherchannel summary** command to verify that the port channels are up and in use.

Task 2: Troubleshoot S2.

Step 1: Issue the command to verify that the port channels are functioning as trunk ports. Record the command used in the space provided below.

Based on the output, are there any issues with the configurations? If issues are found, record them in the space provided below.

Step 2: Issue the command to verify that interfaces are configured in the correct port channel and the proper protocol is configured.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

Step 3: Use the command **show run | begin interface Port-channel** to view the running configuration beginning with the first port-channel interface.

Step 4: Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configuration.

Step 5: Issue the command to verify trunk settings.

Step 6: Issue the command to verify that the port channels are functioning. Remember that port channel issues can be caused by either end of the link.

Task 3: Troubleshoot S3.

Step 1: Issue the command to verify that the port channels are functioning as trunk ports.

Based on the output, are there any issues with the configurations? If issues are found, record them in the space provided below.

Step 2: Issue the command to verify that the interfaces are configured in the correct port channel and that the proper protocol is configured.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

Step 3: Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.

Step 4: Resolve all problems found. Record the commands used to correct the configuration.

Step 5: Issue the command to verify trunk settings. Record the command used in the space provided below.

Step 6: Issue the command to verify that the port channels are functioning. Record the command used in the space provided below.

Task 4: Verify EtherChannel and Connectivity.

Step 1: Use the **show interfaces etherchannel** command to verify full functionality of the port channels.

Step 2: Verify connectivity of the management VLAN.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

Step 3: Verify connectivity of PCs.

Can PC-A ping PC-C? _____

If EtherChannels are not fully functional, connectivity between switches does not exist, or connectivity between hosts does not exist. Troubleshoot to resolve any remaining issues.

Note: It may be necessary to disable the PC firewall for pings between the PCs to succeed.

Lab11 – Configuring Syslog and NTP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	G0/0	172.16.2.1	255.255.255.0	N/A
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure NTP

Part 3: Configure Syslog

Background / Scenario

Syslog messages that are generated by the network devices can be collected and archived on a syslog server. The information can be used for monitoring, debugging, and troubleshooting purposes. The administrator can control where the messages are stored and displayed. Syslog messages can be time-stamped for analysis of the sequence of network events; therefore, it is important to synchronize the clock across the network devices with a Network Time Protocol (NTP) server.

In this lab, you will configure R1 as the NTP server and R2 as a Syslog and NTP client. The syslog server application, such as Tftp32d or other similar program, will be running on PC-B. Furthermore, you will control the severity level of log messages that are collected and archived on the syslog server.

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

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

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and Syslog software, such as tftpd32)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, routing, device access, and passwords.

Task 1: Cable the network as shown in the topology.

Task 2: Initialize and reload the routers as necessary.

Task 3: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure the device name.

Step 3: Encrypt plain text passwords.

Step 4: Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.

Step 5: Assign **class** as the encrypted privileged EXEC mode password.

Step 6: Assign **cisco** as the console and vty password and enable login.

Step 7: Set console logging to synchronous mode.

Step 8: Apply the IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces.

Step 9: Set the clock rate to **128000** for the DCE serial interface.

Task 4: Configure routing.

Enable single-area OSPF on the routers with process ID 1. Add all the networks into the OSPF process for area 0.

Task 5: Configure PC-B.

Configure the IP address and default gateway for PC-B according to the Addressing Table.

Task 6: Verify end-to-end connectivity.

Verify that each device is able to ping every other device in the network successfully. If not, troubleshoot until there is end-to-end connectivity.

Task 7: Save the running configuration to the startup configuration.

Part 2: Configure NTP

In Part 2, you will configure R1 as the NTP server and R2 as the NTP client of R1. Synchronized time is important for syslog and debug functions. If the time is not synchronized, it is difficult to determine what network event caused the message.

Task 1: Display the current time.

Issue the **show clock** command to display the current time on R1.

```
R1# show clock
*12:30:06.147 UTC Tue May 14 2013
```

Record the information regarding the current time displayed in the following table.

Date	
Time	
Time Zone	

Task 2: Set the time.

Use the **clock set** command to set the time on R1. The following is an example of setting the date and time.

```
R1# clock set 9:39:00 05 july 2013
R1#
*Jul  5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54
UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by
console.
```

Note: The time can also be set using the **clock timezone** command in the global configuration mode. For more information regarding this command, research the **clock timezone** command at www.cisco.com to determine the zone for your region.

Task 3: Configure the NTP master.

Configure R1 as the NTP master by using the **ntp master stratum-number** command in global configuration mode. The stratum number indicates the number of NTP hops away from an authoritative time source. In this lab, the number 5 is the stratum level of this NTP server.

```
R1(config)# ntp master 5
```

Task 4: Configure the NTP client.

Step 1: Issue **show clock** command on R2. Record the current time displayed on R2 in the following table.

Date	
Time	
Time Zone	

Step 2: Configure R2 as the NTP client. Use the **ntp server** command to point to the IP address or hostname of the NTP server. The **ntp update-calendar** command periodically updates the calendar with NTP time.

```
R2(config)# ntp server 10.1.1.1
R2(config)# ntp update-calendar
```

Task 5: Verify NTP configuration.

Step 1: Use the **show ntp associations** command to verify that R2 has an NTP association with R1.

```
R2# show ntp associations
```

```

address          ref clock      st   when   poll reach  delay  offset  disp
*~10.1.1.1       127.127.1.1    5    11     64   177 11.312 -0.018  4.298
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

```

Step 2: Issue **show clock** on R1 and R2 to compare the timestamp.

Note: It could take a few minutes before the timestamp on R2 is synchronized with R1.

```
R1# show clock
```

```
09:43:32.799 UTC Fri Jul 5 2013
```

```
R2# show clock
```

```
09:43:37.122 UTC Fri Jul 5 2013
```

Part 3: Configure Syslog

Syslog messages from network devices can be collected and archived on a syslog server. In this lab, Tftpd32 will be used as the syslog server software. The network administrator can control the types of messages that can be sent to the syslog server.

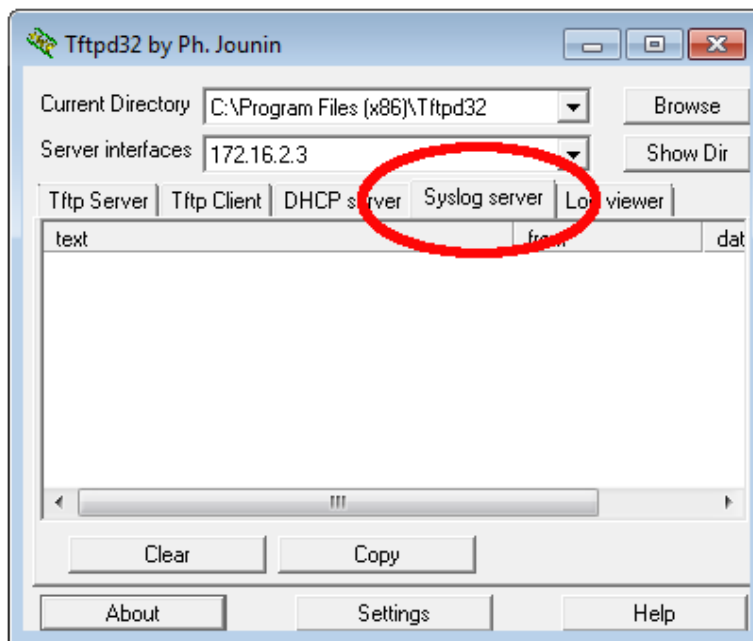
Task 1: (Optional) Install syslog server.

If a syslog server is not already installed on the PC, download and install the latest version of a syslog server, such as Tftpd32, on the PC. The latest version of Tftpd32 can be found at the following link:

<http://tftpd32.jounin.net/>

Task 2: Start the syslog server on PC-B.

After starting the Tftpd32 application, click the **syslog server** tab.



Task 3: Verify that the timestamp service is enabled on R2.

Use the **show run** command to verify that the timestamp service is enabled for logging on R2.

```
R2# show run | include timestamp
service timestamps debug datetime msec
service timestamps log datetime msec
```

If the timestamp service is not enabled, use the following command to enable it.

```
R2(config)# service timestamps log datetime msec
```

Task 4: Configure R2 to log messages to the syslog server.

Configure R2 to send Syslog messages to the syslog server, PC-B. The IP address of the PC-B syslog server is 172.16.2.3.

```
R2(config)# logging host 172.16.2.3
```

Task 5: Display the default logging settings.

Use the **show logging** command to display the default logging settings.

```
R2# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
```

```
No Active Message Discriminator.
```

```
No Inactive Message Discriminator.
```

```
Console logging: level debugging, 47 messages logged, xml disabled,
filtering disabled
```

```
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
```

```
Buffer logging: level debugging, 47 messages logged, xml disabled,
filtering disabled
```

```
Exception Logging: size (4096 bytes)
```

```
Count and timestamp logging messages: disabled
```

```
Persistent logging: disabled
```

```
No active filter modules.
```

```
Trap logging: level informational, 49 message lines logged
```

```
Logging to 172.16.2.3 (udp port 514, audit disabled,
link up),
```

```
6 message lines logged,
```

```
0 message lines rate-limited,
```

```
0 message lines dropped-by-MD,
```

```
xml disabled, sequence number disabled
```

```
filtering disabled
```

```
Logging Source-Interface: VRF Name:
```

What is the IP address of the syslog server? _____

What protocol and port is syslog using? _____

At what level is trap logging enabled? _____

Task 6: Configure and observe the effect of logging severity levels on R2.

Step 1: Use the **logging trap ?** command to determine the various trap levels availability. When configuring a level, the messages sent to the syslog server are the trap level configured and any lower levels.

```
R2(config)# logging trap ?
<0-7>          Logging severity level
alerts         Immediate action needed          (severity=1)
critical       Critical conditions              (severity=2)
debugging      Debugging messages              (severity=7)
emergencies    System is unusable              (severity=0)
errors         Error conditions                 (severity=3)
informational  Informational messages          (severity=6)
notifications  Normal but significant conditions (severity=5)
warnings       Warning conditions              (severity=4)
<cr>
```

If the **logging trap warnings** command was issued, which severity levels of messages are logged?

Step 2: Change the logging severity level to 4.

```
R2(config)# logging trap warnings
```

or

```
R2(config)# logging trap 4
```

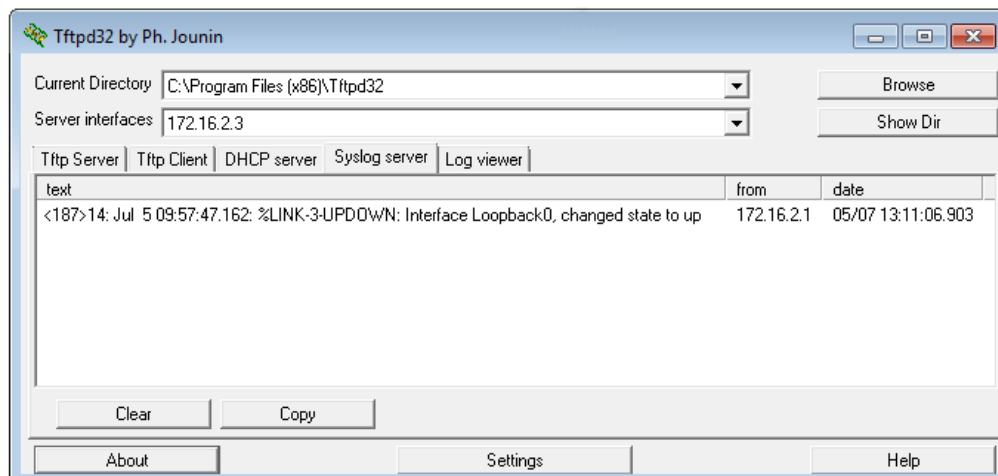
Step 3: Create interface Loopback0 on R2 and observe the log messages on both the terminal window and the syslog server window on PC-B.

```
R2(config)# interface lo 0
```

```
R2(config-if)#
```

```
Jul  5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
```

```
Jul  5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
```



Step 4: Remove the Loopback 0 interface on R2 and observe the log messages.

```
R2(config-if)# no interface lo 0
R2(config)#
Jul  5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
Jul  5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
```

At severity level 4, are there any log messages on the syslog server? If any log messages appeared, explain what appeared and why.

Step 5: Change the logging severity level to 6.

```
R2(config)# logging trap informational

or

R2(config)# logging trap 6
```

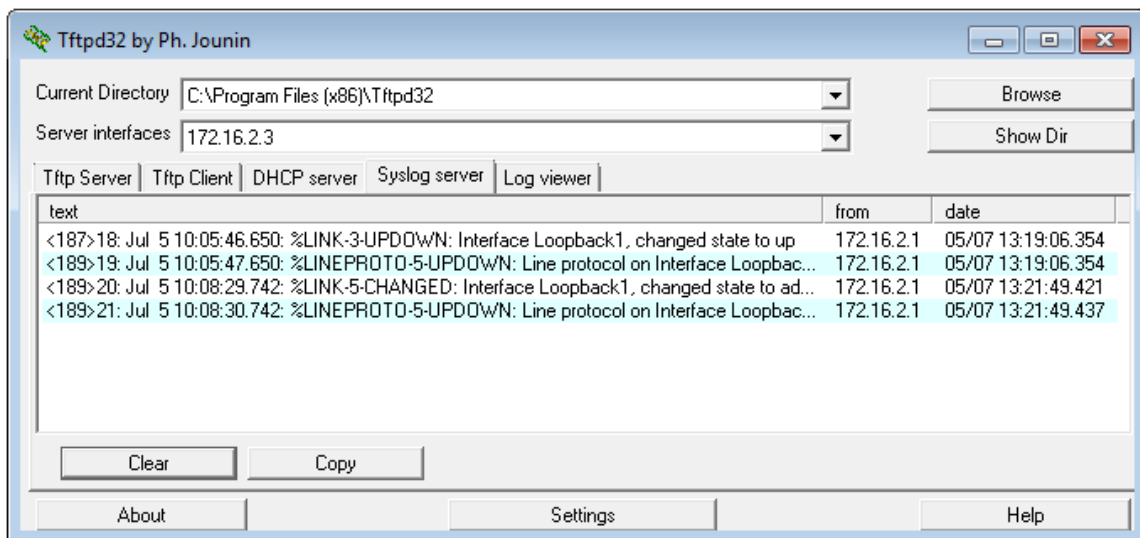
Step 6: Clear the syslog entries on PC-B. Click **Clear** in the Tftpd32 dialog box.

Step 7: Create the Loopback 1 interface on R2.

```
R2(config)# interface lo 1
Jul  5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
Jul  5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
```

Step 8: Remove the Loopback 1 interface from R2.

```
R2(config-if)# no interface lo 1
R2(config-if)#
Jul  5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to
administratively down
Jul  5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to down
```



Step 9: Observe the syslog server output. Compare this result with the results at trapping level 4. What is your observation?

Reflection

What is the problem with setting the level of severity too high (lowest level number) or too low (highest level number) for syslog?

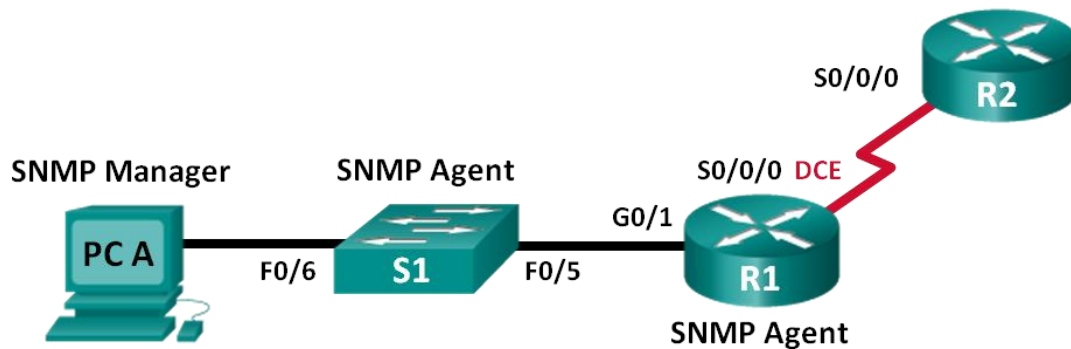
Router Interface Summary Table

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

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab12 – Configuring SNMP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.252	N/A
R2	S0/0/0	192.168.2.2	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure an SNMP Manager and Agents

Part 3: Convert OID Codes with the Cisco SNMP Object Navigator

Background / Scenario

Simple Network Management Protocol (SNMP) is a network management protocol and an IETF standard which can be used to both monitor and control clients on the network. SNMP can be used to get and set variables related to the status and configuration of network hosts like routers and switches, as well as network client computers. The SNMP manager can poll SNMP agents for data, or data can be automatically sent to the SNMP manager by configuring traps on the SNMP agents.

In this lab, you will download, install, and configure SNMP management software on PC-A. You will also configure a Cisco router and Cisco switch as SNMP agents. After capturing SNMP notification messages from the SNMP agent, you will convert the MIB/Object ID codes to learn the details of the messages using the Cisco SNMP Object Navigator.

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

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

Note: The **snmp-server** commands in this lab will cause the Cisco 2960 switch to issue a warning message when saving the configuration file to NVRAM. To avoid this warning message verify that the switch is using the **lanbase-routing** template. The IOS template is controlled by the Switch Database Manager (SDM). When changing the preferred template, the new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Use the following commands to assign the **lanbase-routing** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer lanbase-routing
S1(config)# end
S1# reload
```

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS, Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- 1 PC (Windows 7, Vista, or XP with Internet access)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology
- SNMP Management Software (PowerSNMP Free Manager by Dart Communications, or SolarWinds Kiwi Syslog Server, Evaluation Version with 30 Day Trial)

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the devices with basic settings.

Task 1: Cable the network as shown in the topology.

Task 2: Configure the PC host.

Task 3: Initialize and reload the switch and routers as necessary.

Task 4: Configure basic settings for the routers and switch.

Step 1: Disable DNS lookup.

Step 2: Configure device names as shown in the topology.

Step 3: Configure IP addresses as shown in the Addressing Table. (Do not configure the S0/0/0 interface on R1 at this time.)

Step 4: Assign **cisco** as the console and vty password and enable login.

Step 5: Assign **class** as the encrypted privileged EXEC mode password.

Step 6: Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 7: Verify successful connectivity between the LAN devices by issuing the ping command.

Step 8: Copy the running configuration to the startup configuration.

Part 2: Configure SNMP Manager and Agents

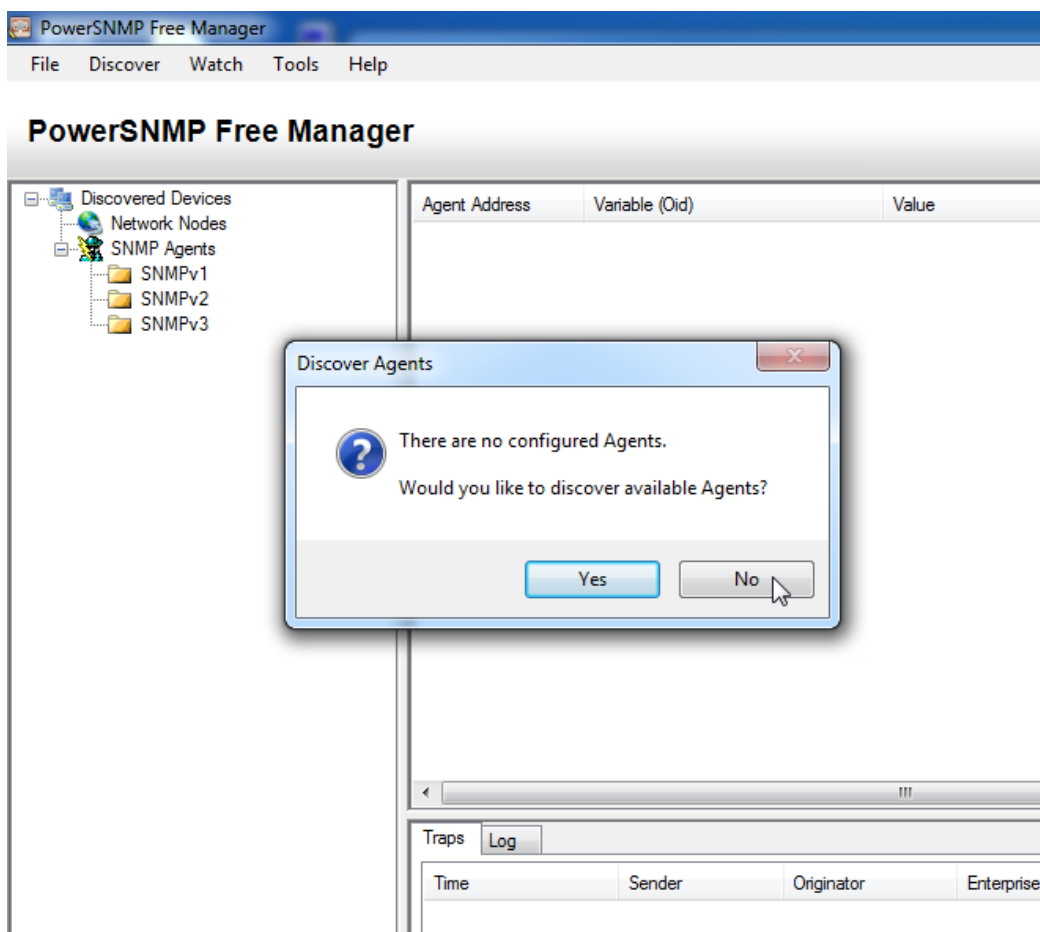
In Part 2, SNMP management software will be installed and configured on PC-A, and R1 and S1 will be configured as SNMP agents.

Task 1: Install an SNMP management program.

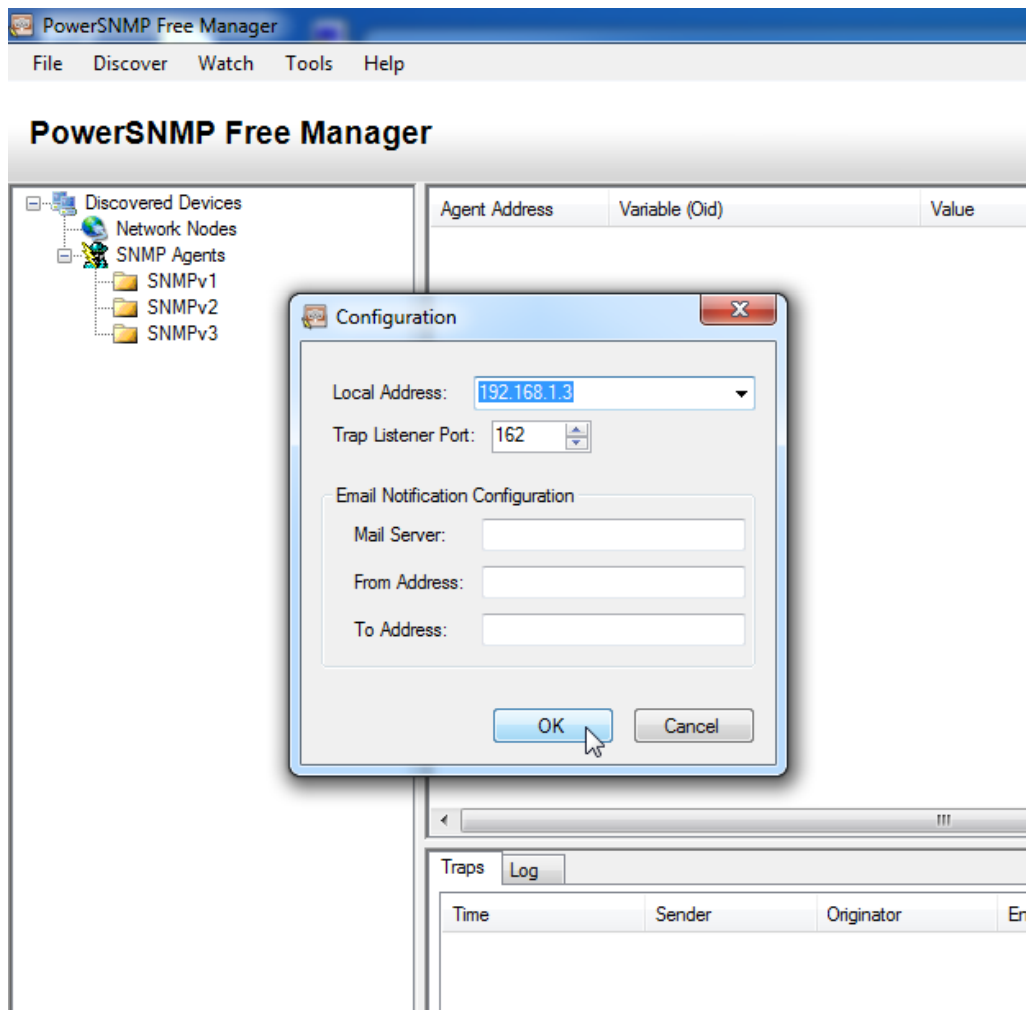
Step 1: Download and install the PowerSNMP Free Manager by Dart Communications from the following URL: <http://www.dart.com/snmp-free-manager.aspx>.

Step 2: Launch the PowerSNMP Free Manager program.

Step 3: Click **No** if prompted to discover available SNMP agents. You will discover SNMP agents after configuring SNMP on R1. PowerSNMP Free Manager supports SNMP version 1, 2, and 3. This lab uses SNMPv2.



Step 4: In the pop-up Configuration window (if no pop-up window appear, go to Tools > Configuration), set the local IP address to listen on 192.168.1.3 and click **OK**.



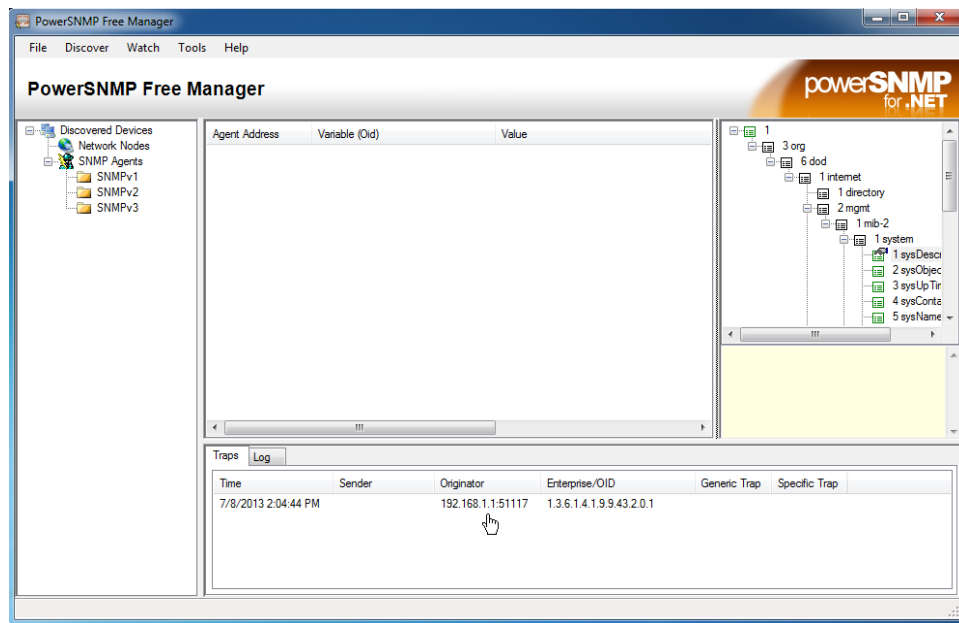
Note: If prompted to discover available SNMP agents, click **No** and continue to next part of the lab.

Task 2: Configure an SNMP agent.

Step 1: On R1, enter the following commands from the global configuration mode to configure the router as an SNMP agent. In line 1 below, the SNMP community string is **ciscolab**, with read-only privileges, and the named access list **SNMP_ACL** defines which hosts are allowed to get SNMP information from R1. In lines 2 and 3, the SNMP manager location and contact commands provide descriptive contact information. Line 4 specifies the IP address of the host that will receive SNMP notifications, the SNMP version, and the community string. Line 5 enables all default SNMP traps, and lines 6 and 7 create the named access list, to control which hosts are permitted to get SNMP information from the router.

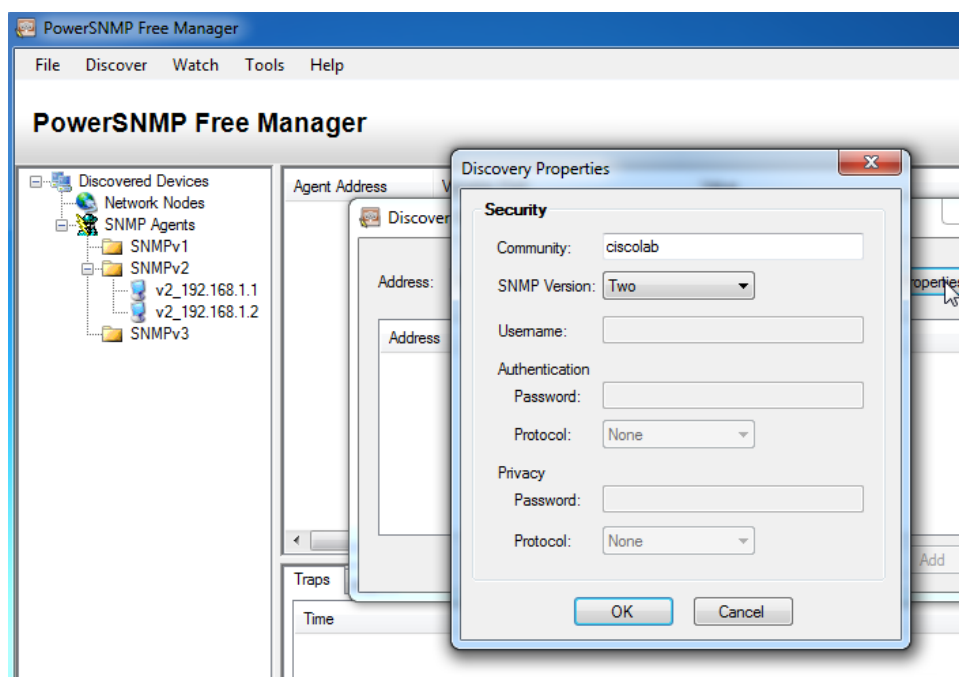
```
R1(config)# snmp-server community ciscolab ro SNMP_ACL
R1(config)# snmp-server location snmp_manager
R1(config)# snmp-server contact ciscolab_admin
R1(config)# snmp-server host 192.168.1.3 version 2c ciscolab
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

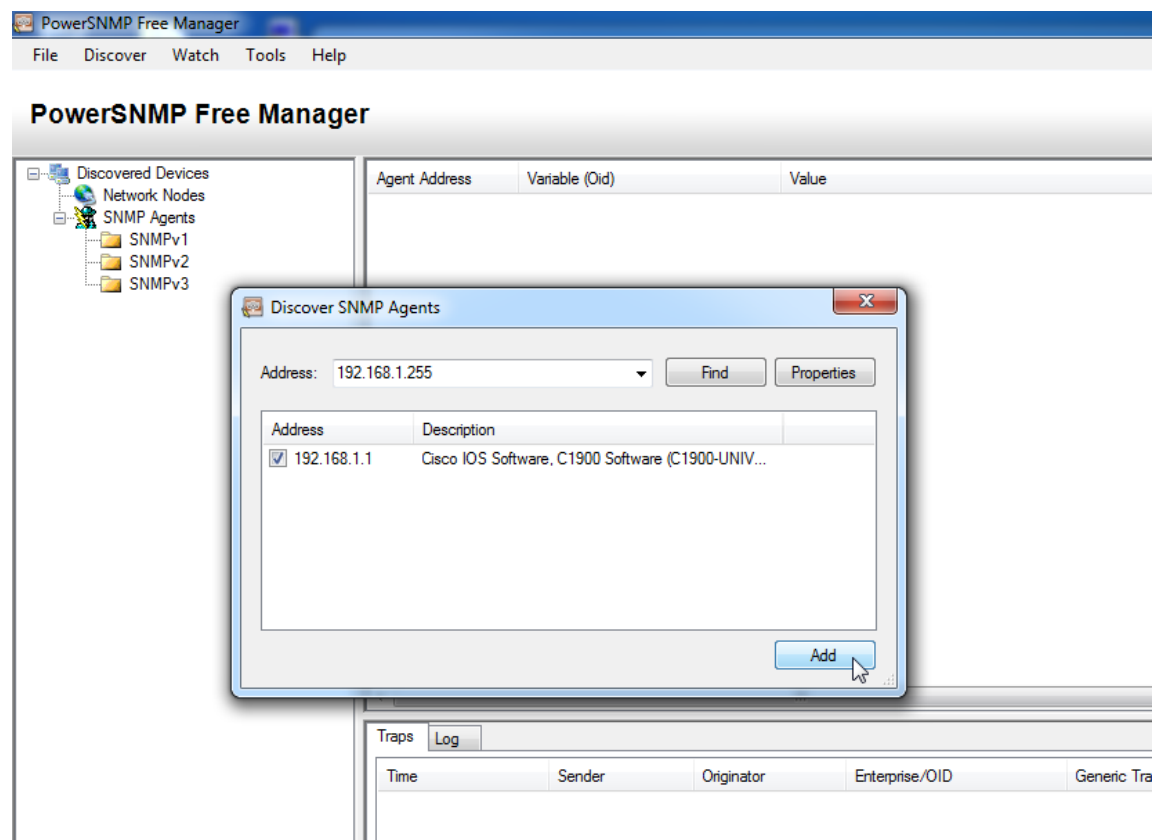
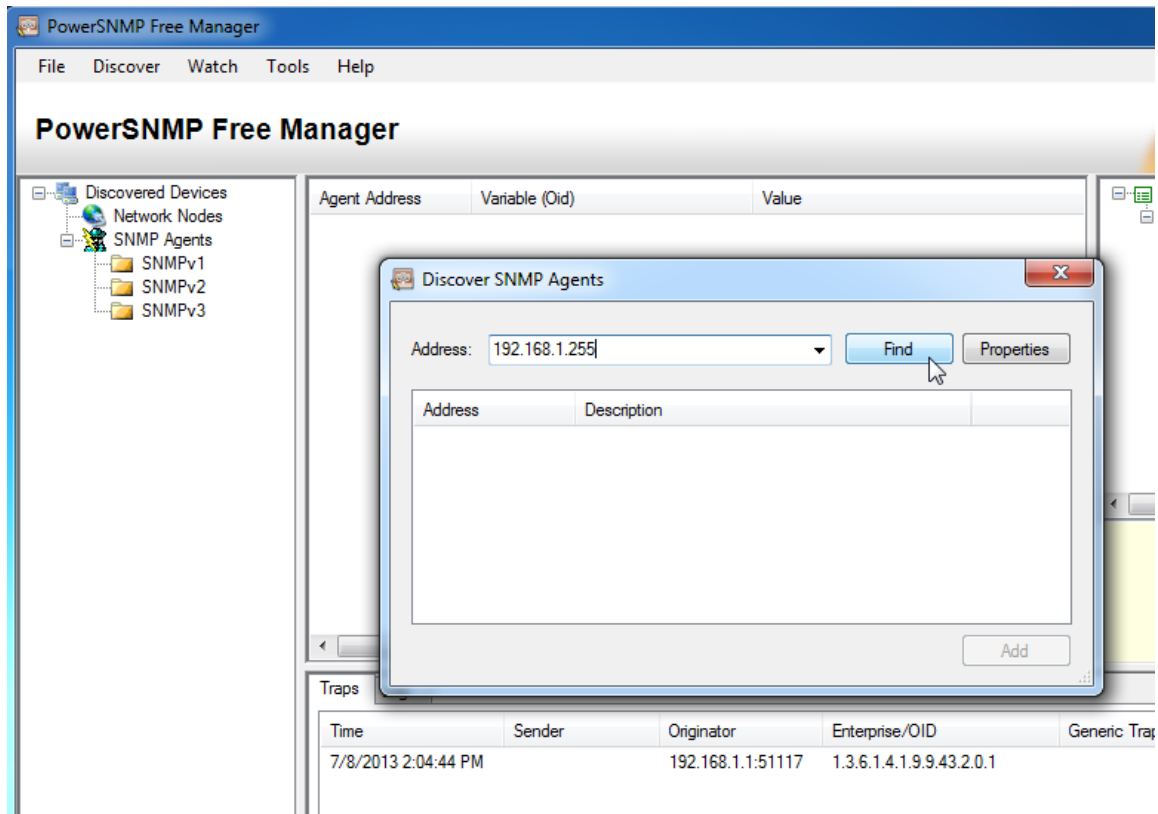
Step 2: At this point, you may notice that the PowerSNMP Free Manager is receiving notifications from R1. If it is not, you can try to force a SNMP notification to be sent by entering a **copy run start** command on R1. Continue to the next step if it is unsuccessful.



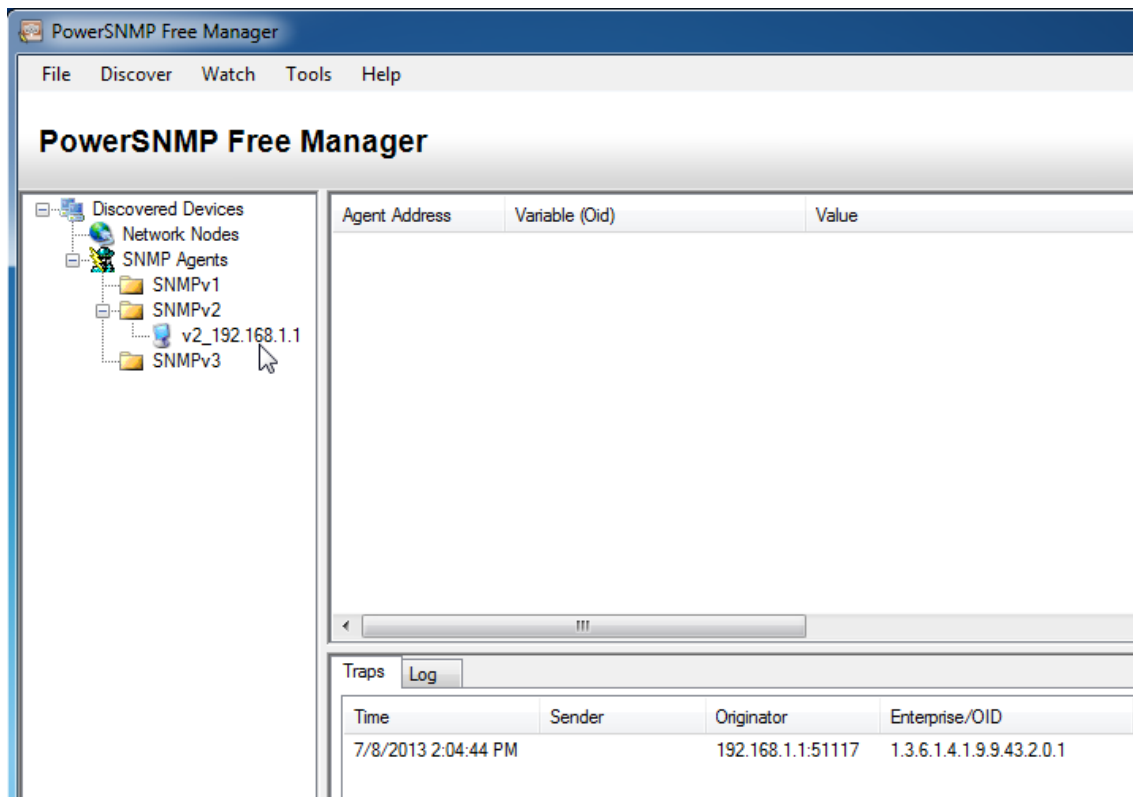
Task 3: Discover SNMP agents.

Step 1: From the PowerSNMP Free Manager on PC-A, open the **Discover > SNMP Agents** window. Enter the IP address **192.168.1.255**. In the same window, click **Properties** and set the Community to **cisco123** and the SNMP Version to **Two**, and then click **OK**. Now you can click **Find** to discover all SNMP agents on the 192.168.1.0 network. The PowerSNMP Free Manager should find R1 at 192.168.1.1. Click the checkbox and then **Add** to add R1 as an SNMP agent.





Step 2: In the PowerSNMP Free Manager, R1 is added to the list of available SNMPv2 agents.



Step 3: Configure S1 as an SNMP agent. You can use the same **snmp-server** commands that you used to configure R1.

Step 4: After S1 is configured, SNMP notifications from 192.168.1.2 display in the Traps window of the PowerSNMP Free Manager. In the PowerSNMP Free Manager, add S1 as an SNMP agent using the same process that you used to discover R1.

Part 3: Convert OID Codes with the Cisco SNMP Object Navigator

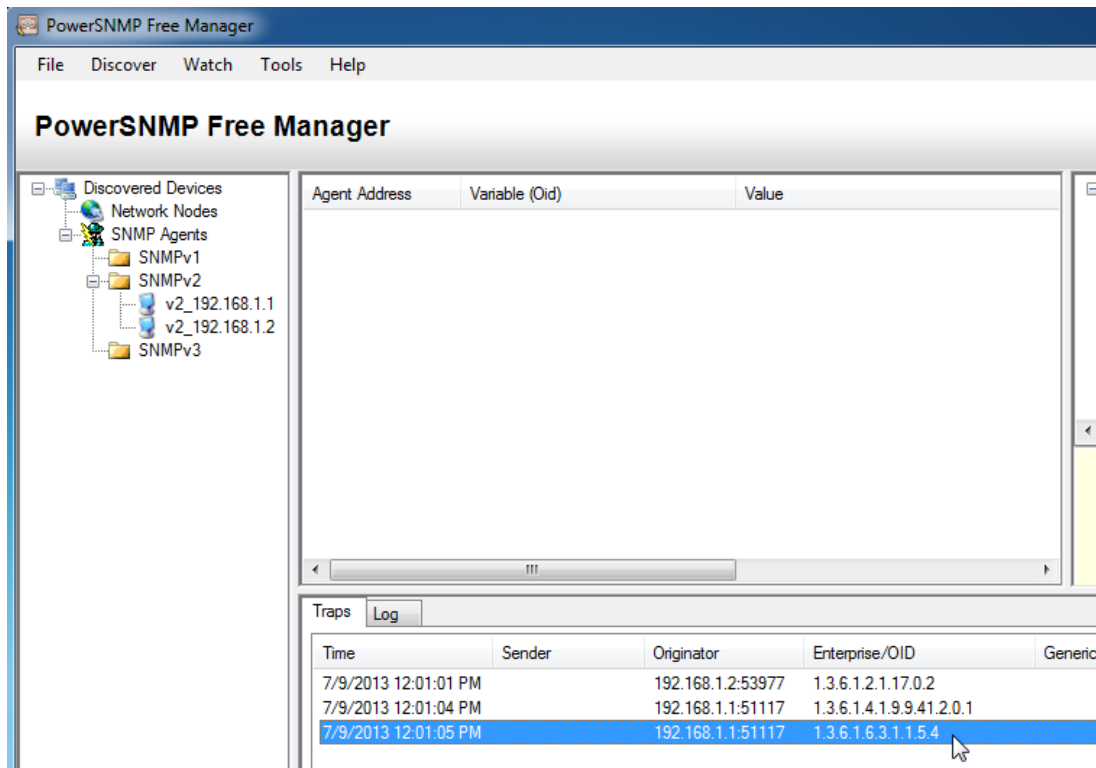
In Part 3, you will force SNMP notifications to be sent to the SNMP manager located at PC-A. You will then convert the received OID codes to names to learn the nature of the messages. The MIB/OID codes can be easily converted using the Cisco SNMP Object Navigator located at <http://www.cisco.com>.

Task 1: Clear current SNMP messages.

In the PowerSNMP Free Manager, right-click the **Traps** window and select **Clear** to clear the SNMP messages.

Task 2: Generate an SNMP trap and notification.

On R1, configure the S0/0/0 interface according to the Addressing Table at the beginning of this lab. Accessing global configuration mode and enable an interface to generate an SNMP trap notification to be sent to the SNMP Manager at PC-A. Notice the Enterprise/OID code numbers that are visible in the traps window.



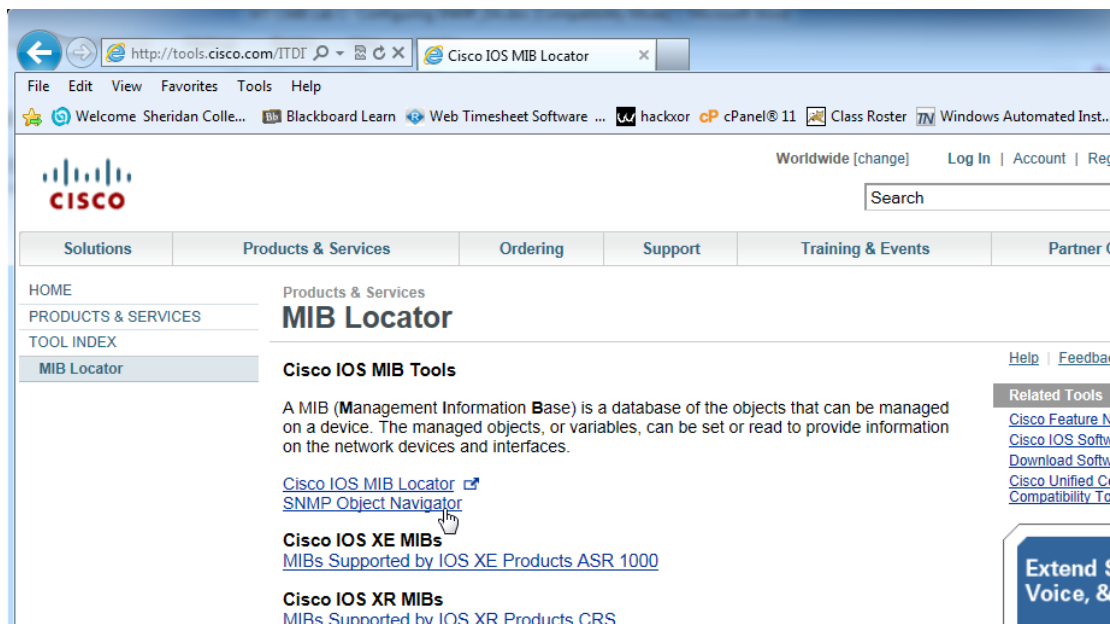
Task 3: Decode SNMP MIB/OID messages.

From a computer with Internet access, open a web browser and go to <http://www.cisco.com>.

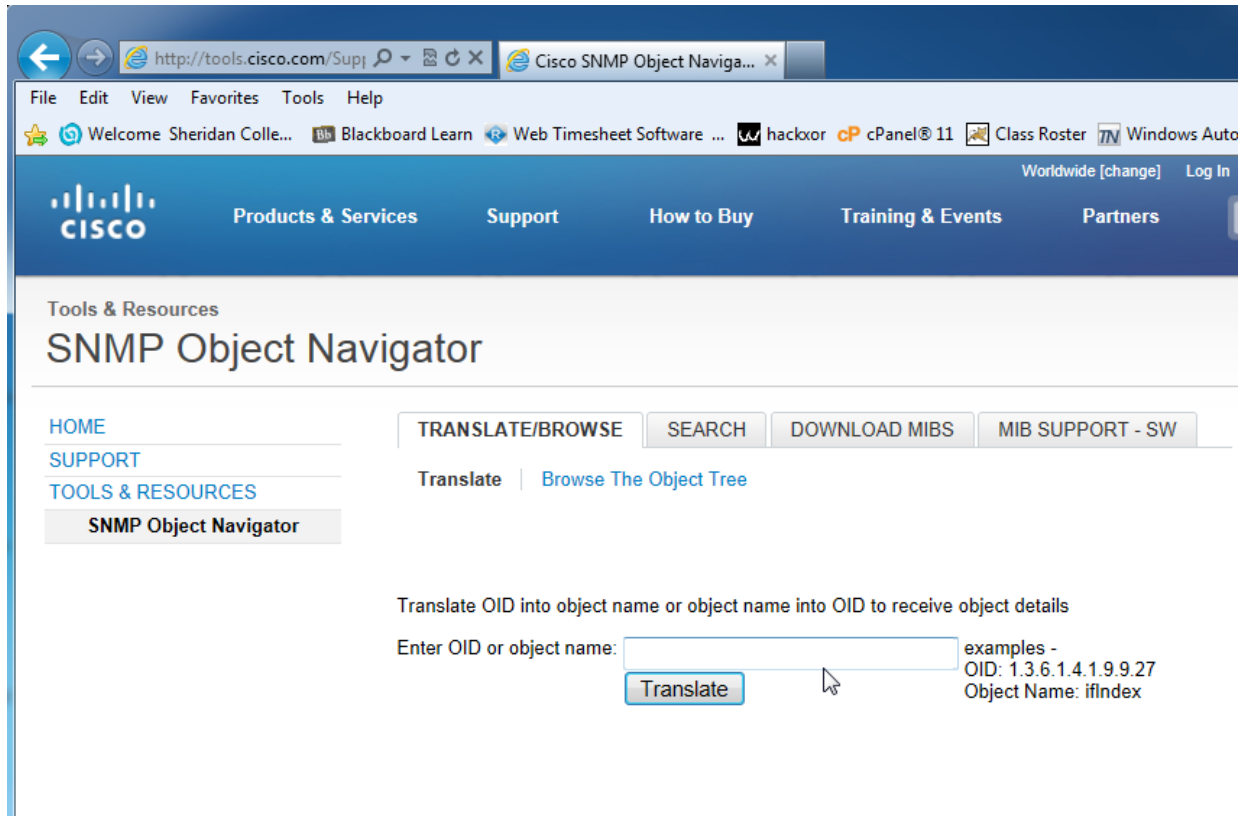
Step 1: Using the search tool at the top of the window, search for **SNMP Object Navigator**.

Step 2: Choose **SNMP Object Navigator MIB Download MIBs OID OIDs** from the results.

Step 3: Navigate to the **MIB Locator** page. Click the **SNMP Object Navigator**.



Step 4: Using the **SNMP Object Navigator** page, decode the OID code number from the PowerSNMP Free Manager generated in Part 3, Step 2. Enter the OID code number and click **Translate**.



Step 5: Record the OID code numbers and their corresponding message translations below.

Reflection

1. What are some of the potential benefits of monitoring a network with SNMP?

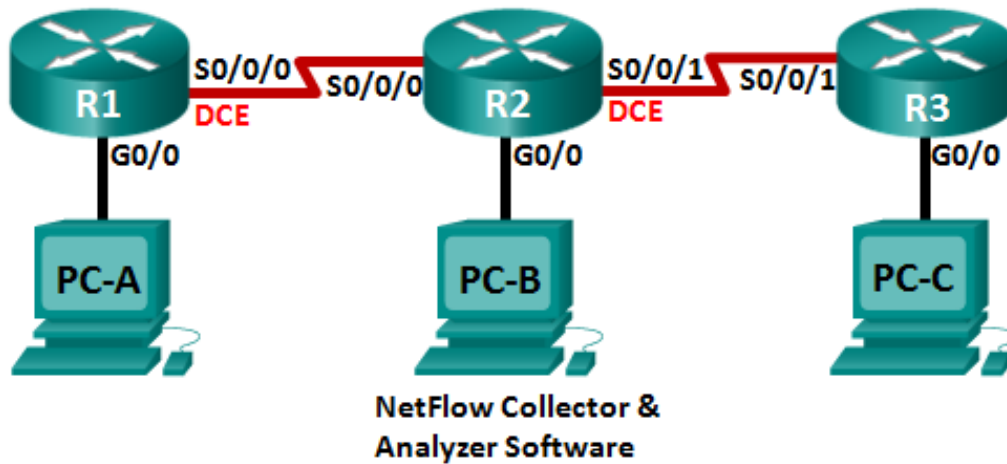
2. Why is it preferable to solely use read-only access when working with SNMPv2?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab13 – Collecting and Analyzing NetFlow Data

Topology



Addressing Table

Device	Interface	IP Address	Default Gateway
R1	G0/0	192.168.1.1/24	N/A
	S0/0/0 (DCE)	192.168.12.1/30	N/A
R2	G0/0	192.168.2.1/24	N/A
	S0/0/0	192.168.12.2/30	N/A
	S0/0/1 (DCE)	192.168.23.1/30	N/A
R3	G0/0	192.168.3.1/24	N/A
	S0/0/1	192.168.23.2/30	N/A
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure NetFlow on a Router

Part 3: Analyze NetFlow Using the CLI

Part 4: Explore NetFlow Collector and Analyzer Software

Background / Scenario

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch. NetFlow enables network and security monitoring, network planning, traffic analysis, and IP

accounting. It is important not to confuse NetFlow's purpose and results with that of packet capture hardware and software. Packet capturing records all possible information exiting or entering a network device for later analysis, NetFlow targets specific statistical information.

Flexible NetFlow is the latest NetFlow technology, improving on the original NetFlow by adding the capability to customize the traffic analysis parameters. Flexible NetFlow uses the Version 9 export format. Starting with Cisco IOS Release 15.1, many useful Flexible NetFlow commands are supported.

In this lab, you will configure NetFlow to capture both ingress (incoming) and egress (outgoing) packets. You will use **show** commands to verify that NetFlow is operational and gathering statistical information. You will also explore available options for NetFlow collection and analysis software.

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

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

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and routers.

Task 1: Cable the network as shown in the topology.

Task 2: Initialize and reload the routers as necessary.

Task 3: Configure basic settings for each router.

Step 1: Disable DNS lookup.

Step 2: Configure device names as shown in the topology.

Step 3: Assign **class** as the encrypted privileged EXEC mode password.

Step 4: Assign **cisco** as the console and vty passwords and enable login.

Step 5: Encrypt the plain text passwords.

Step 6: Configure a MOTD banner to warn users that unauthorized access is prohibited.

Step 7: Configure **logging synchronous** for the console line.

Step 8: Set the clock rate for all DCE serial interfaces at **128000**.

Step 9: Configure the IP addresses as listed in the Addressing Table.

Step 10: Configure OSPF using Process ID 1 and advertise all networks. Ethernet interfaces should be passive.

Step 11: Create a local database on R3 with the username **admin** and password **cisco** with the privilege level at **15**.

Step 12: On R3, enable the HTTP service and authenticate HTTP users by using the local database.

Step 13: Copy the running configuration to the startup configuration.

Task 4: Configure PC hosts.

Task 5: Verify end-to-end connectivity.

All devices should be able to ping other devices in the topology. Troubleshoot as necessary until end-to-end connectivity is established.

Note: It may be necessary to disable the PC firewall for pings between PCs to be successful.

Part 2: Configure NetFlow on a Router

In Part 2, you will configure NetFlow on router R2. NetFlow will capture all ingress and egress traffic on the R2 serial interfaces and export the data to the NetFlow collector, PC-B. Flexible NetFlow Version 9 will be used to export to the NetFlow collector.

Task 1: Configure NetFlow capture.

Configure NetFlow data capture on both serial interfaces. Capture data from ingress and egress packets.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Task 2: Configure NetFlow data export.

Use the **ip flow-export destination** command to identify the IP address and the UDP port of the NetFlow collector to which the router should export NetFlow data. UDP Port number 9996 will be used for this configuration.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

Task 3: Configure the NetFlow export version.

Cisco routers running IOS 15.1 support NetFlow versions 1, 5, and 9. Version 9 is the most versatile export data format, but is not backward-compatible with earlier versions. Use the **ip flow-export version** command to set the NetFlow version.

```
R2(config)# ip flow-export version 9
```

Task 4: Verify the NetFlow configuration.

Step 1: Issue the **show ip flow interface** command to review the NetFlow capture interface information.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
Serial0/0/1
  ip flow ingress
  ip flow egress
```

Step 2: Issue the **show ip flow export** command to review the NetFlow data export information.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
Export source and destination details :
VRF ID : Default
Destination(1) 192.168.2.3 (9996)
Version 9 flow records
388 flows exported in 63 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
```

Part 3: Analyze NetFlow Using the CLI

In Part 3, you will generate data traffic between R1 and R3 to observe NetFlow technology.

Task 1: Generate data traffic between R1 and R3.

Step 1: Telnet from R1 to R3 using the IP address 192.168.3.1. Enter the password **cisco** to enter the user EXEC mode. Enter the password **class** to enable global EXEC mode. Issue the **show run** command to generate some Telnet traffic. Keep your Telnet session active for now.

Step 2: From R3, issue the **ping 192.168.1.1 repeat 1000** command to ping the R1 G0/0 interface. This will generate ICMP traffic through R2.

Step 3: From PC-A, browse to R3 using the 192.168.3.1 IP address. Login as **admin** with the password **cisco**. Keep the browser open after you have logged into R3.

Note: Make sure the pop-up blocker is disabled on your browser.

Task 2: Display a summary of the NetFlow accounting statistics.

On R2, issue the **show ip cache flow** command to display changes to the summary of NetFlow data, including packet size distribution, IP flow information, captured protocols, and interface activity. Notice the protocols now display in the summary data.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
1546 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
```

```

0 alloc failures, 0 force free
1 chunk, 1 chunk added
last clearing of statistics 00:07:35

```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	4	0.0	27	43	0.2	5.0	15.7
TCP-WWW	104	0.2	14	275	3.4	2.1	1.5
ICMP	4	0.0	1000	100	8.8	27.9	15.4

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Total:	112	0.2	50	146	12.5	3.1	2.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Se0/0/0	192.168.12.1	Null	224.0.0.5	59	0000	0000	43
Se0/0/1	192.168.23.2	Null	224.0.0.5	59	0000	0000	40

Task 3: End the Telnet and browser sessions.

Step 1: Issue the **exit** command on R1 to disconnect from the Telnet session to R3.

Step 2: Close the browser session on PC-A.

Task 4: Clear NetFlow accounting statistics.

Step 1: On R2, issue the **clear ip flow stats** command to clear NetFlow accounting statistics.

```
R2# clear ip flow stats
```

Step 2: Re-issue the **show ip cache flow** command to verify that the NetFlow accounting statistics have been reset. Notice that, even though you are no longer generating data through R2, data is being picked up by NetFlow. In the example below, the destination address for this traffic is multicast address 224.0.0.5, or OSPF LSA data.

```
R2# show ip cache flow
```

```

IP packet size distribution (124 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512   544   576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

```

```
IP Flow Switching Cache, 278544 bytes
```

```
2 active, 4094 inactive, 2 added
```

```
1172 ager polls, 0 flow alloc failures
```

```
Active flows timeout in 30 minutes
```

```
Inactive flows timeout in 15 seconds
```

```
IP Sub Flow Cache, 34056 bytes
```

```
2 active, 1022 inactive, 2 added, 2 added to flow
```

```
0 alloc failures, 0 force free
```

```
1 chunk, 0 chunks added
```

```
last clearing of statistics 00:09:48
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active (Sec)	Idle (Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
IP-other	2	0.0	193	79	0.6	1794.8	5.7
Total:	2	0.0	193	79	0.6	1794.8	5.7

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Se0/0/0	192.168.12.1	Null	224.0.0.5	59	0000	0000	35

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Se0/0/1	192.168.23.2	Null	224.0.0.5	59	0000	0000	33

Part 4: Explore NetFlow Collector and Analyzer Software

NetFlow Collector and Analyzer Software is available from many vendors. Some software is provided as freeware, others are not. The following URL provides a summary web page of some of the Freeware NetFlow software available:

http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html

Review this web page to acquaint yourself with some of the available NetFlow Collector and Analyzer software products.

Reflection

1. What is the purpose of NetFlow collector software?

2. What is the purpose of NetFlow analyzer software?

3. What are the seven critical fields used by the original NetFlow to distinguish flows?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				