



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Local Area Networks

M5X01046

Lab Manual

MComp/BSc (Hons) Computer Networks

HND Computer Networks

School of Applied Computing

Faculty of Architecture, Computing and Engineering

University of Wales Trinity Saint David

Swansea.



School of
Applied Computing

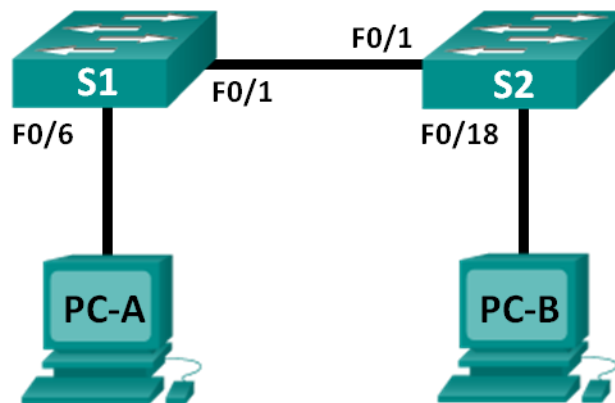
2016-2017

Module Leader

Dr Kapilan Radhakrishnan

Lab 1 - Building a Simple Network

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	N/A	N/A	N/A
S2	VLAN 1	N/A	N/A	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	N/A
PC-B	NIC	192.168.1.11	255.255.255.0	N/A

Objectives

Part 1: Set Up the Network Topology (Ethernet only)

- Identify cables and ports for use in the network.
- Cable a physical lab topology.

Part 2: Configure PC Hosts

- Enter static IP address information on the LAN interface of the hosts.
- Verify that PCs can communicate using the **ping** utility.

Part 3: Configure and Verify Basic Switch Settings

- Configure each switch with hostname, local passwords, and login banner.
- Save the running configurations.
- Display the running switch configuration.
- Display the IOS version for the running switch.
- Display the status of the interfaces.

Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. In this lab, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname,

local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations.

You will apply IP addressing for this lab to the PCs to enable communication between these two devices. Use the **ping** utility to verify connectivity.

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. Refer to Appendix A for the procedure to initialize and reload a switch.

Required Resources

- 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 cables as shown in the topology

Part 1: Set Up the Network Topology (Ethernet only)

In Part 1, you will cable the devices together according to the network topology.

Step 1: Power on the devices.

Power on all devices in the topology. The switches do not have a power switch; they will power on as soon as you plug in the power cord.

Step 2: Connect the two switches.

Connect one end of an Ethernet cable to F0/1 on S1 and the other end of the cable to F0/1 on S2. You should see the lights for F0/1 on both switches turn amber and then green. This indicates that the switches have been connected correctly.

Step 3: Connect the PCs to their respective switches.

- a. Connect one end of the second Ethernet cable to the NIC port on PC-A. Connect the other end of the cable to F0/6 on S1. After connecting the PC to the switch, you should see the light for F0/6 turn amber and then green, indicating that PC-A has been connected correctly.
- b. Connect one end of the last Ethernet cable to the NIC port on PC-B. Connect the other end of the cable to F0/18 on S2. After connecting the PC to the switch, you should see the light for F0/18 turn amber and then green, indicating that the PC-B has been connected correctly.

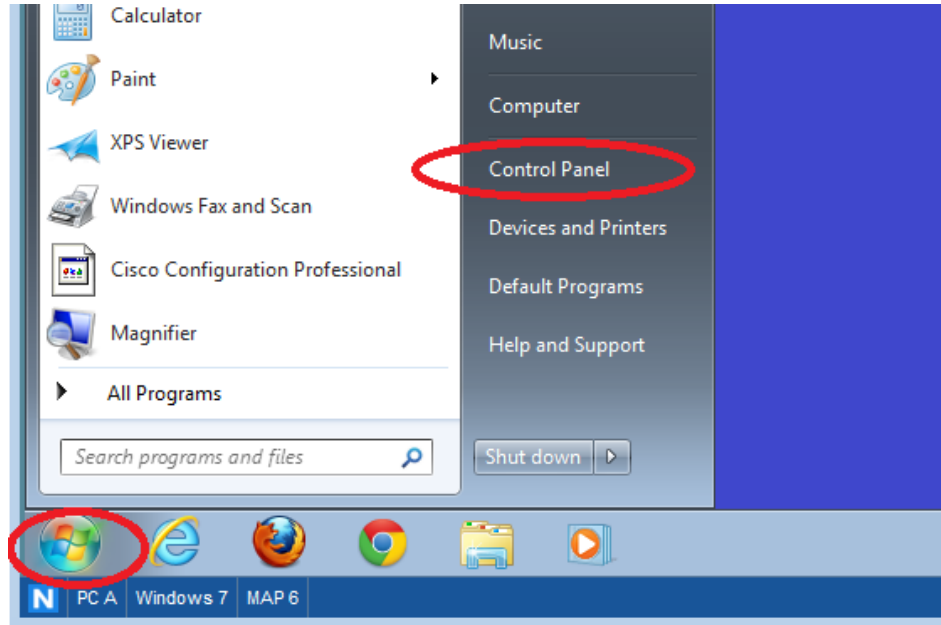
Step 4: Visually inspect network connections.

After cabling the network devices, take a moment to carefully verify the connections to minimize the time required to troubleshoot network connectivity issues later.

Part 2: Configure PC Hosts

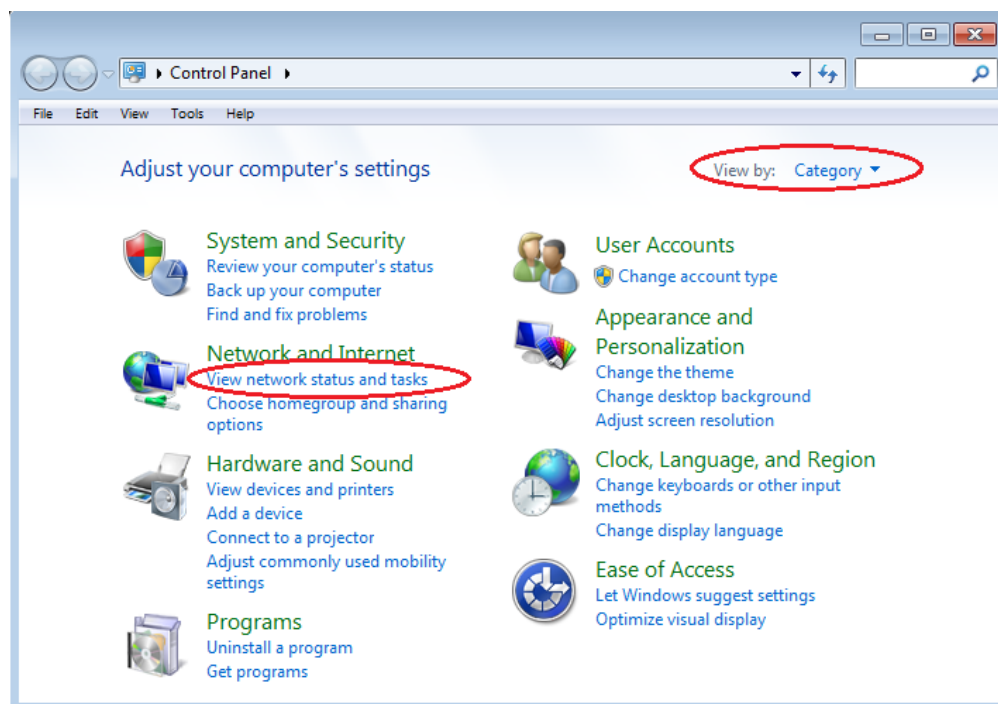
Step 1: Configure static IP address information on the PCs.

- a. Click the **Windows Start** icon and then select **Control Panel**.

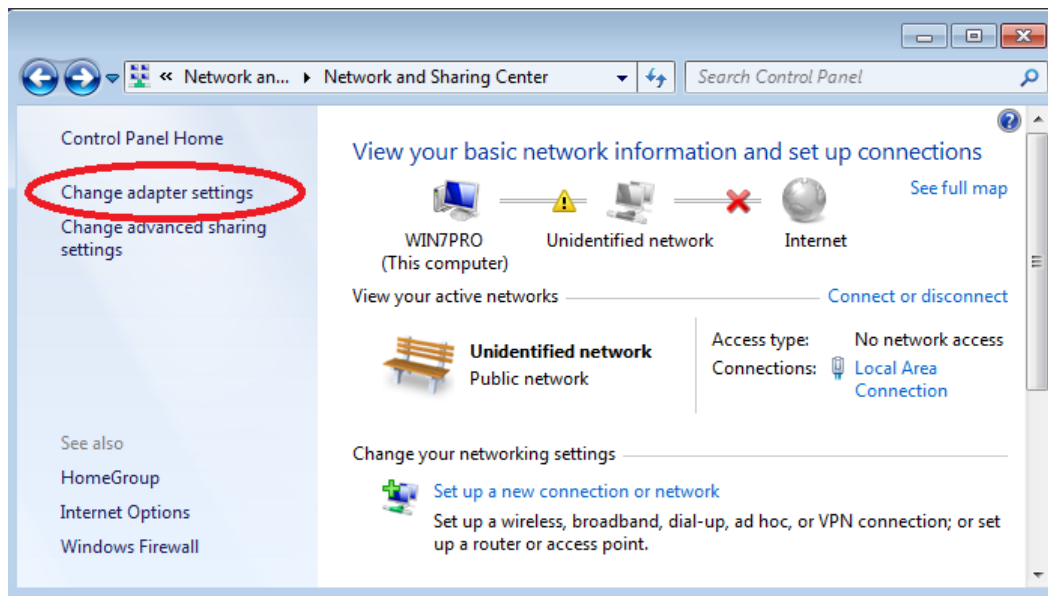


- b. In the Network and Internet section, click the **View network status and tasks** link.

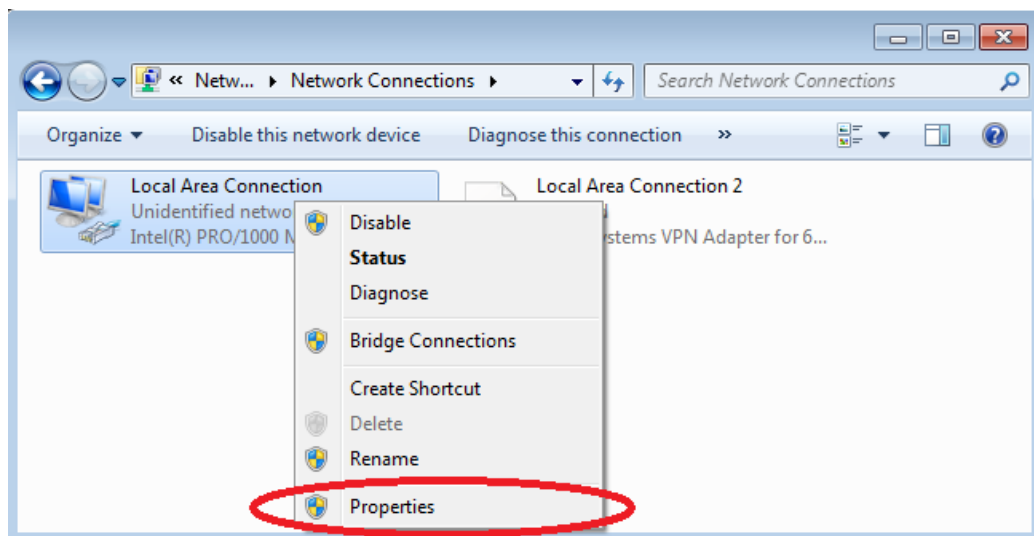
Note: If the Control Panel displays a list of icons, click the drop-down option next to the **View by:** and change this option to display by **Category**.



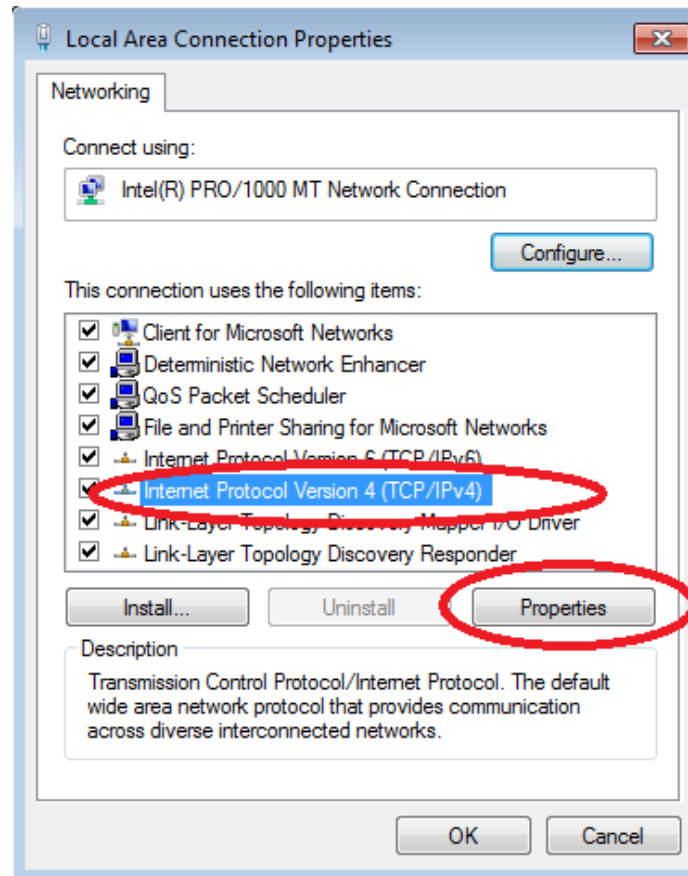
- c. In the left pane of the Network and Sharing Center window, click the **Change adapter settings** link.



- d. The Network Connections window displays the available interfaces on the PC. Right-click the **Local Area Connection** interface and select **Properties**.

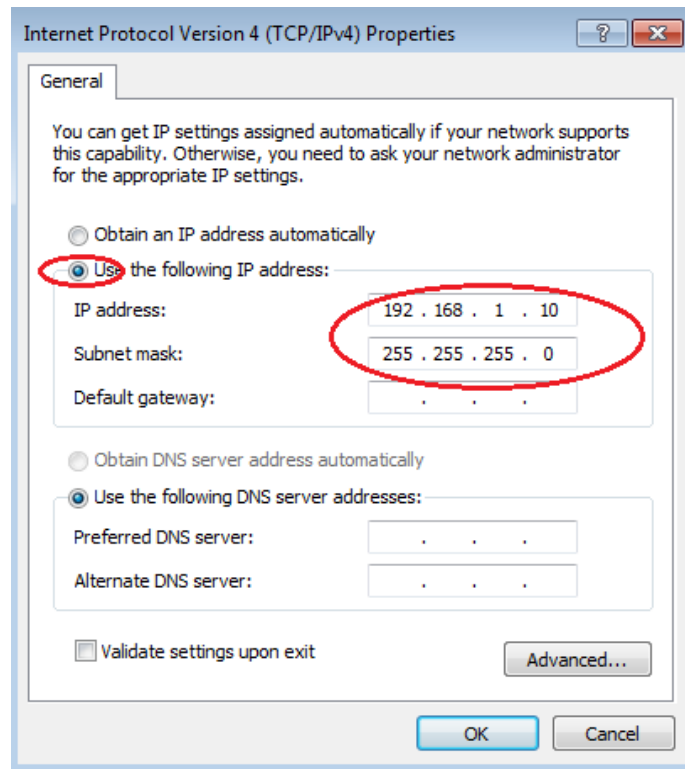


- e. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



Note: You can also double-click **Internet Protocol Version 4 (TCP/IPv4)** to display the Properties window.

- f. Click the **Use the following IP address** radio button to manually enter an IP address, subnet mask, and default gateway.



Note: In the above example, the IP address and subnet mask have been entered for PC-A. The default gateway has not been entered, because there is no router attached to the network. Refer to the Addressing Table on page 1 for PC-B's IP address information.

- g. After all the IP information has been entered, click **OK**. Click **OK** on the Local Area Connection Properties window to assign the IP address to the LAN adapter.
- h. Repeat the previous steps to enter the IP address information for PC-B.

Step 2: Verify PC settings and connectivity.

Use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

- a. From PC-A, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.



- b. The cmd.exe window is where you can enter commands directly to the PC and view the results of those commands. Verify your PC settings by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information.

```
C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PC-A
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 00-50-56-BE-6C-89
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-Local IPv6 Address . . . . . : fe80::d428:7de2:997c:b05a%11(Preferred)
    IPv4 Address. . . . . : 192.168.1.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
    DHCPv6 IAID . . . . . : 234884137
    DHCPv6 Client DUID. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

- c. Type **ping 192.168.1.11** and press Enter.

```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>
```

Were the ping results successful? _____

If not, troubleshoot as necessary.

Note: If you did not get a reply from PC-B, try to ping PC-B again. If you still do not get a reply from PC-B, try to ping PC-A from PC-B. If you are unable to get a reply from the remote PC, then have your instructor help you troubleshoot the problem.

Part 3: Configure and Verify Basic Switch Settings

Step 1: Console into the switch.

Using Tera Term, establish a console connection to the switch from PC-A.

Step 2: Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command.

```
Switch> enable
Switch#
```

The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode.

Step 3: Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

The prompt changed to reflect global configuration mode.

Step 4: Give the switch a name.

Use the **hostname** command to change the switch name to **S1**.

```
Switch(config)# hostname S1
S1(config)#
```

Step 5: Prevent unwanted DNS lookups.

To prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Step 6: Enter local passwords.

To prevent unauthorized access to the switch, passwords must be configured.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

Step 7: Enter a login MOTD banner.

A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated.

The **banner motd** command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the #, are often used.

```
S1(config)# banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited and prosecuted to the full extent
of the law. #
S1(config)# exit
S1#
```

Step 8: Save the configuration.

Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM).

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Step 9: Display the current configuration.

The **show running-config** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging. The commands configured in Steps 1 – 8 are highlighted below.

```
S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 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 S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
```

```
!  
  
<output omitted>  
  
!  
banner motd ^C  
Unauthorized access is strictly prohibited and prosecuted to the full extent of the  
law. ^C  
!  
line con 0  
password cisco  
login  
line vty 0 4  
login  
line vty 5 15  
login  
!  
end  
  
S1#
```

Step 10: Display the IOS version and other useful switch information.

Use the **show version** command to display the IOS version that the switch is running, along with other useful information. Again, you will need to use the spacebar to advance through the displayed information.

```
S1# show version  
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE  
SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2012 by Cisco Systems, Inc.  
Compiled Sat 28-Jul-12 00:29 by prod_rel_team  
  
ROM: Bootstrap program is C2960 boot loader  
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE  
(fc1)  
  
S1 uptime is 1 hour, 38 minutes  
System returned to ROM by power-on  
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.

Processor board ID FCQ1628Y5LE

Last reset from power-on

1 Virtual Ethernet interface

24 FastEthernet interfaces

2 Gigabit Ethernet interfaces

The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 0C:D9:96:E2:3D:00

Motherboard assembly number : 73-12600-06

Power supply part number : 341-0097-03

Motherboard serial number : FCQ16270N5G

Power supply serial number : DCA1616884D

Model revision number : R0

Motherboard revision number : A0

Model number : WS-C2960-24TT-L

System serial number : FCQ1628Y5LE

Top Assembly Part Number : 800-32797-02

Top Assembly Revision Number : A0

Version ID : V11

CLEI Code Number : COM3L00BRF

Hardware Board Revision Number : 0x0A

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
*	1 26	WS-C2960-24TT-L	15.0 (2) SE	C2960-LANBASEK9-M

Configuration register is 0xF

S1#

Step 11: Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the **show ip interface brief** command. Press the spacebar to advance to the end of the list.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down

```

FastEthernet0/4      unassigned      YES unset  down      down
FastEthernet0/5      unassigned      YES unset  down      down
FastEthernet0/6      unassigned      YES unset  up        up
FastEthernet0/7      unassigned      YES unset  down      down
FastEthernet0/8      unassigned      YES unset  down      down
FastEthernet0/9      unassigned      YES unset  down      down
FastEthernet0/10     unassigned      YES unset  down      down
FastEthernet0/11     unassigned      YES unset  down      down
FastEthernet0/12     unassigned      YES unset  down      down
FastEthernet0/13     unassigned      YES unset  down      down
FastEthernet0/14     unassigned      YES unset  down      down
FastEthernet0/15     unassigned      YES unset  down      down
FastEthernet0/16     unassigned      YES unset  down      down
FastEthernet0/17     unassigned      YES unset  down      down
FastEthernet0/18     unassigned      YES unset  down      down
FastEthernet0/19     unassigned      YES unset  down      down
FastEthernet0/20     unassigned      YES unset  down      down
FastEthernet0/21     unassigned      YES unset  down      down
FastEthernet0/22     unassigned      YES unset  down      down
FastEthernet0/23     unassigned      YES unset  down      down
FastEthernet0/24     unassigned      YES unset  down      down
GigabitEthernet0/1   unassigned      YES unset  down      down
GigabitEthernet0/2   unassigned      YES unset  down      down
S1#

```

Step 12: Repeat Steps 1 to 12 to configure switch S2.

The only difference for this step is to change the hostname to S2.

Step 13: Record the interface status for the following interfaces.

Interface	S1		S2	
	Status	Protocol	Status	Protocol
F0/1				
F0/6				
F0/18				
VLAN 1				

Why are some FastEthernet ports on the switches are up and others are down?

Reflection

What could prevent a ping from being sent between the PCs?

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

Appendix A: Initializing and Reloading a Switch

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

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

```
Switch# show flash
```

```
Directory of flash:/
```

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

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

```
Switch#
```

Step 3: Delete the VLAN file.

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

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

- When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

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

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

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

```
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

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

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

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

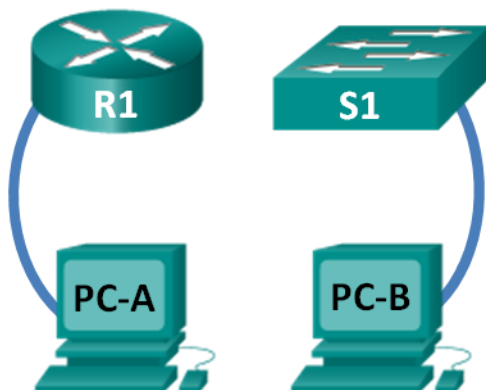
Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

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

Lab 2 - Initializing and Reloading a Router and Switch

Topology



Objectives

Part 1: Set Up Devices in the Network as Shown in the Topology

Part 2: Initialize the Router and Reload

Part 3: Initialize the Switch and Reload

Background / Scenario

Before starting a CCNA hands-on lab that makes use of either a Cisco router or switch, ensure that the devices in use have been erased and have no startup configurations present. Otherwise, the results of your lab may be unpredictable. This lab provides a detail procedure for initializing and reloading a Cisco router and a Cisco switch.

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.

Required Resources

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

Part 1: Set Up Devices in the Network as Shown in the Topology

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

Attach console cables to the devices shown in the topology diagram.

Step 2: Power on all the devices in the topology.

Wait for all devices to finish the software load process before moving to Part 2.

Part 2: Initialize the Router and Reload

Step 1: Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

```
Router> enable
Router#
```

Step 2: Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from nonvolatile random-access memory (NVRAM).

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

Step 3: Reload the router.

Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

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

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

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

Step 4: Bypass the initial configuration dialog.

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

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

Step 5: Terminate the autoinstall program.

You will be prompted to terminate the autoinstall program. Respond **yes** and then press Enter.

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

Part 3: Initialize the Switch and Reload

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

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

```
Switch# show flash
```

```
Directory of flash:/
```

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

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

```
Switch#
```

Step 3: Delete the VLAN file.

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

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

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

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

- b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

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

```
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

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

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

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload
```

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

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

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

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

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

Reflection

1. Why is it necessary to erase the startup configuration before reloading the router?

2. You find a couple configurations issues after saving the running configuration to the startup configuration, so you make the necessary changes to fix those issues. If you were to reload the device now, what configuration would be restored to the device after the reload?

Lab 3 - Building a Switch and Router Network

Topology



Addressing Table

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

Objectives

Part 1: Set Up the Topology and Initialize Devices

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

Part 2: Configure Devices and Verify Connectivity

- Assign static IP information to the PC interfaces.
- Configure the router.
- Verify network connectivity.

Part 3: Display Device Information

- Retrieve hardware and software information from the network devices.
- Interpret the output from the routing table.
- Display interface information on the router.
- Display a summary list of the interfaces on the router and switch.

Background / Scenario

This is a comprehensive lab to review previously covered IOS commands. In this lab, you will cable the equipment as shown in the topology diagram. You will then configure the devices to match the addressing table. After the configurations have been saved, you will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use IOS commands to retrieve information from the devices to answer questions about your network equipment.

This lab provides minimal assistance with the actual commands necessary to configure the router. 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 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: Ensure that the routers and switches have been erased and have no startup configurations. Refer to Appendix B for the procedure to initialize and reload a router and switch.

Required Resources

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

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

Part 1: Set Up Topology and Initialize Devices

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

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

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router and switch, initialize and reload these devices back to their basic configurations. For information on how to initialize and reload these devices, refer to Appendix B.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Note: Appendix A provides configuration details for the steps in Part 2. You should attempt to complete Part 2 prior to reviewing this appendix.

Step 1: Assign static IP information to the PC interfaces.

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

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

Why were the pings not successful?

Step 2: Configure the router.

- Console into the router and enable privileged EXEC mode.
- Enter configuration mode.
- Assign a device name to the router.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the clear text passwords.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- Configure and activate both interfaces on the router.
- Configure an interface description for each interface indicating which device is connected to it.
- Save the running configuration to the startup configuration file.
- Set the clock on the router.

Note: Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.

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

Were the pings successful? Why?

Part 3: Display Device Information

In Part 3, you will use **show** commands to retrieve information from the router and switch.

Step 1: Retrieve hardware and software information from the network devices.

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

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

How much DRAM memory does the router have?

How much NVRAM memory does the router have?

How much Flash memory does the router have?

- b. Use the **show version** command to answer the following questions about the switch.

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

How much dynamic random access memory (DRAM) does the switch have?

How much nonvolatile random-access memory (NVRAM) does the switch have?

What is the model number of the switch?

Step 2: Display the routing table on the router.

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

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

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

What interface types are associated to the C coded routes?

Step 3: Display interface information on the router.

Use the **show interface g0/1** to answer the following questions.

What is the operational status of the G0/1 interface?

What is the Media Access Control (MAC) address of the G0/1 interface?

How is the Internet address displayed in this command?

Step 4: Display a summary list of the interfaces on the router and switch.

There are several commands that can be used to verify an interface configuration. One of the most useful of these is the **show ip interface brief** command. The command output displays a summary list of the interfaces on the device and provides immediate feedback to the status of each interface.

- a. Enter the **show ip interface brief** command on the router.

```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down  down
GigabitEthernet0/0       192.168.0.1     YES manual  up              up
GigabitEthernet0/1       192.168.1.1     YES manual  up              up
Serial0/0/0              unassigned      YES unset  administratively down  down
Serial0/0/1              unassigned      YES unset  administratively down  down
R1#
```

- b. Enter the **show ip interface brief** command on the switch.

```
Switch# show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
Vlan1                    unassigned      YES manual  up          up
FastEthernet0/1          unassigned      YES unset   down        down
FastEthernet0/2          unassigned      YES unset   down        down
FastEthernet0/3          unassigned      YES unset   down        down
FastEthernet0/4          unassigned      YES unset   down        down
FastEthernet0/5          unassigned      YES unset   up          up
FastEthernet0/6          unassigned      YES unset   up          up
FastEthernet0/7          unassigned      YES unset   down        down
FastEthernet0/8          unassigned      YES unset   down        down
FastEthernet0/9          unassigned      YES unset   down        down
FastEthernet0/10         unassigned      YES unset   down        down
FastEthernet0/11         unassigned      YES unset   down        down
FastEthernet0/12         unassigned      YES unset   down        down
FastEthernet0/13         unassigned      YES unset   down        down
FastEthernet0/14         unassigned      YES unset   down        down
FastEthernet0/15         unassigned      YES unset   down        down
FastEthernet0/16         unassigned      YES unset   down        down
FastEthernet0/17         unassigned      YES unset   down        down
FastEthernet0/18         unassigned      YES unset   down        down
FastEthernet0/19         unassigned      YES unset   down        down
FastEthernet0/20         unassigned      YES unset   down        down
FastEthernet0/21         unassigned      YES unset   down        down
FastEthernet0/22         unassigned      YES unset   down        down
FastEthernet0/23         unassigned      YES unset   down        down
FastEthernet0/24         unassigned      YES unset   down        down
GigabitEthernet0/1       unassigned      YES unset   down        down
GigabitEthernet0/2       unassigned      YES unset   down        down
Switch#
```

Reflection

1. If the G0/1 interface showed administratively down, what interface configuration command would you use to turn the interface up?

2. What would happen if you had incorrectly configured interface G0/1 on the router with an IP address of 192.168.1.2?

Router Interface Summary Table

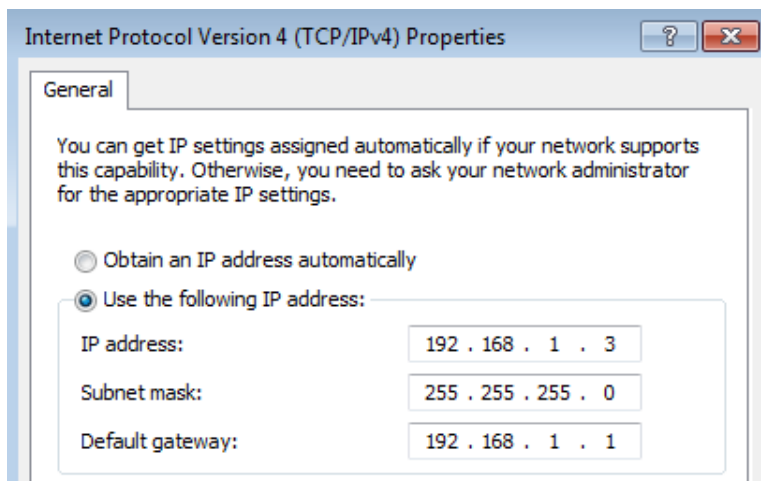
Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)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

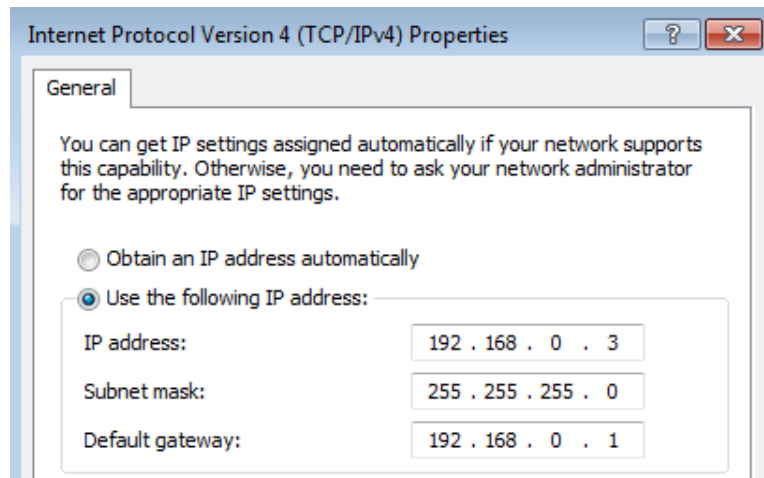
Appendix A: Configuration Details for Steps in Part 2

Step 1: Configure the PC interfaces.

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



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



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

```
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>
```

Step 2: Configure the router.

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

```
Router> enable
Router#
```

- b. Enter configuration mode.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

- c. Assign a device name to the router.

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

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

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

- e. Assign **class** as the privileged EXEC encrypted password.

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

- f. Assign **cisco** as the console password and enable login.

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

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

```
R1(config)#
```

- g. Assign **cisco** as the vty password and enable login.

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

```
R1(config-line)# password cisco
```

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

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

```
R1(config)#
```

- h. Encrypt the clear text passwords.

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

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

```
R1(config)# banner motd #
```

```
Enter TEXT message. End with the character '#'.  
Unauthorized access prohibited!
```

```
#
```

```
#
```

```
R1(config)#
```

- j. Configure and activate both interfaces on the router.

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

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

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

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

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

```
*Nov 29 23:49:44.195: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to  
down
```

```
*Nov 29 23:49:47.863: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to  
up
```

```
*Nov 29 23:49:48.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
GigabitEthernet0/0, changed state to up
```

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

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

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

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

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

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

```
*Nov 29 23:50:15.283: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to  
down
```

```
*Nov 29 23:50:18.863: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to  
up
```

```
*Nov 29 23:50:19.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
GigabitEthernet0/1, changed state to up
```

```
R1#
```

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

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

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

```
Building configuration...
```

[OK]

R1#

- l. Set the clock on the router.

R1# **clock set 17:00:00 29 Nov 2012**

R1#

*Nov 29 17:00:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:55:46 UTC Thu Nov 29 2012 to 17:00:00 UTC Thu Nov 29 2012, configured from console by console.

R1#

Note: Use the question mark (?) to help determine the correct sequence of the parameters needed to execute this command.

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

```
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Appendix B: Initializing and Reloading a Router and Switch

Part 4: Initialize the Router and Reload

Step 1: Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

Router> **enable**

Router#

Step 2: Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from nonvolatile random-access memory (NVRAM).

Router# **erase startup-config**

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

[OK]

Erase of nvram: complete

Router#

Step 3: Reload the router.

Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

Router# **reload**

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

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

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

Step 4: Bypass the initial configuration dialog.

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

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

Step 5: Terminate the autoinstall program.

You will be prompted to terminate the autoinstall program. Respond **yes** and then press Enter.

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

```
Router>
```

Part 5: Initialize the Switch and Reload

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
```

```
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

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

```
Switch# show flash
```

```
Directory of flash:/
```

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

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

```
Switch#
```

Step 3: Delete the VLAN file.

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

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

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

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

- b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

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

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

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

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

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

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

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

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

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

Lab 4 – Selecting Switching Hardware

Objectives

Part 1: Explore Cisco Switch Products

Part 2: Select an Access Layer Switch

Part 3: Select a Distribution/Core Layer Switch

Background / Scenario

As a Network Engineer, you are part of a team that selects appropriate devices for your network. You need to consider the network requirements for the company as they migrate to a converged network. This converged network supports voice over IP (VoIP), video streaming, and expansion of the company to support a larger customer base.

For a small- to medium-sized company, Cisco hierarchical network design suggests only using a two-tier LAN design. This design consists of an access layer and a collapsed core/distribution layer. Network switches come in different form factors, and with various features and functions. When selecting a switch, the team must choose between fixed configuration or modular configuration, and stackable or non-stackable switches.

Based on a given set of requirements, you will identify the Cisco switch models and features to support the requirements. The scope of this lab will limit the switch models to campus LAN only.

Required Resources

PC with Internet access

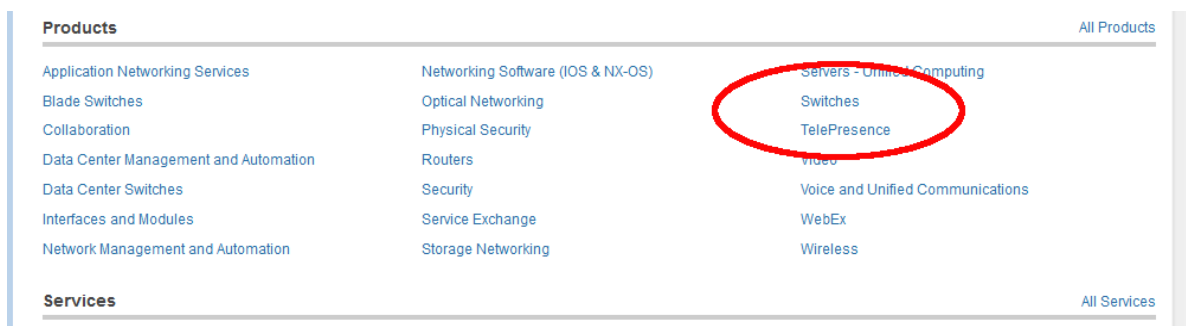
Part 1: Explore Cisco Switch Products

In Part 1, you will navigate the Cisco website and explore available switch products.

Step 1: Navigate the Cisco website.

At www.cisco.com, a list of available products and information about these products is available.

- a. From the home page, click **Products & Services > Switches**.



Step 2: Explore switch products.

In the Feature Products section, a list of different categories of switches is displayed. In this lab, you will explore the campus LAN switches. You can click different links to gather information about the different switch models. On this page, the information is organized in different ways. You can view all available switches by clicking **View All Switches**. If you click **Compare Series**, the switches are organized by types: modular vs. fixed configuration.

Featured Products

[View All Switches](#) | [For Small Business](#) | [Compare Series](#)



Campus LAN – Core and Distribution Switches
Scale network performance and reliability with industry- leading network services, integrated service modules, and validated design guides.

[Show Products](#) 



Campus LAN – Access Switches
Adapt your network to meet evolving business requirements and optimize new application deployments with Cisco access switches.

[Show Products](#) 



Campus LAN – Compact Switches
Securely and easily deploy services anywhere. These fanless, sleek, compact switches are ideal for spaces with limited wiring and cabling infrastructure, such as kiosks, conference rooms, and call centers.

[Show Products](#) 

a. Click the heading **Campus LAN – Core and Distribution Switches**.

List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

- b. Click the heading **Campus LAN – Access Switches**.

List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

- c. Click the heading **Campus LAN – Compact Switches**.

List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

Part 2: Select an Access Layer Switch

The main function of an access layer switch is to provide network access to end user devices. This switch connects to the core/distribution layer switches. Access switches are usually located in the intermediate distribution frame (IDF). An IDF is mainly used for managing and interconnecting the telecommunications cables between end user devices and a main distribution frame (MDF). There are typically multiple IDFs with uplinks to a single centralized MDF.

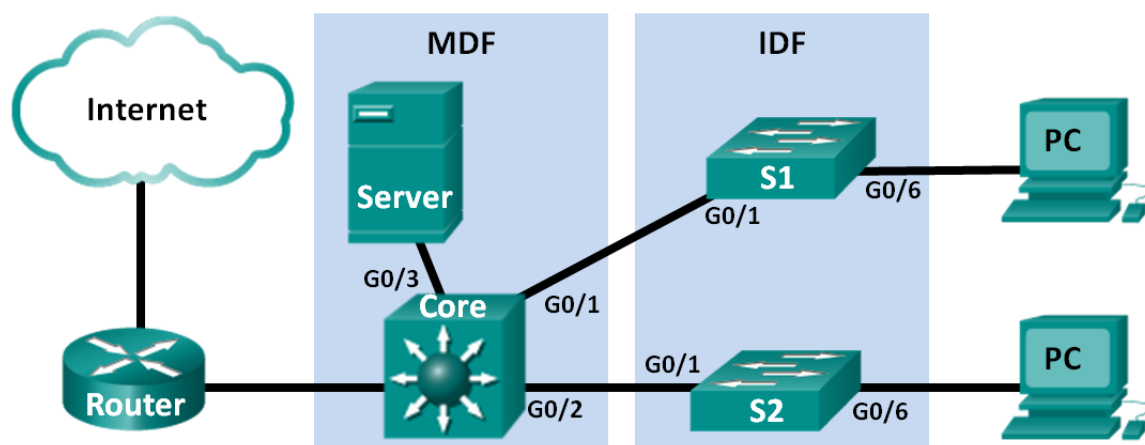
An access switch should have the following capabilities: low cost per switch port, high port density, scalable uplinks to higher layers, and user access functions and resiliency. In Part 2, you will select an access switch based on the requirements set by the company. You have reviewed and become familiar with Cisco switch product line.



- a. Company A requires a replacement access switch in the wiring closet. The company requires the switch to support VoIP and multicast, accommodate future growth of users and increased bandwidth usage. The switch must support a minimum of 35 current users and have a high-speed uplink. List a few of models that meet those requirements.
-
-
- b. Company B would like to extend services to a conference room on an as-needed basis. The switch will be placed on the conference room table, and switch security is a priority.
-
-

Part 3: Select a Distribution/Core Layer Switch

The distribution/core switch is the backbone of the network for the company. A reliable network core is of paramount importance for the function of the company. A network backbone switch provides both adequate capacity for current and future traffic requirements and resilience in the event of failure. They also require high throughput, high availability, and advanced quality of service (QoS). These switches usually reside in the main wiring closet (MDF) along with high speed servers, routers, and the termination point of your ISP.



- a. Company C will replace a backbone switch in the next budget cycle. The switch must provide redundancy features to minimize possible downtime in the event that an internal component fails. What features can accommodate these requirements for the replacement switch?

- b. Which Cisco Catalyst switches would you recommend?

- c. As Company C grows, high speed, such as 10 GB Ethernet, up to 8 uplink ports, and a modular configuration for the switch will become necessary. Which switch models would meet the requirement?

Reflection

What other factors should be considered during the selection process aside from network requirements and costs?

Layered Network Design Simulation

Objective

Explain the need to design a hierarchical network that is scalable.

Scenario

As the network administrator for a very small network, you want to prepare a simulated-network presentation for your branch manager to explain how the network currently operates.

The small network includes the following equipment:

- One Cisco 2911 series router
- One Cisco 3560 switch
- One Cisco 2960 switch
- Four user workstations (PCs or laptops)
- One printer

Resources

- Packet Tracer software

Directions

Step 2: Create a simple network topology using Packet Tracer software. Place the devices at the appropriate levels of the Cisco three-layer hierarchical model design, including:

- a. One Cisco 2911 series router
- b. One Cisco 3560 switch
- c. One Cisco 2960 switch

- d. Four user workstations (PCs or laptops)
- e. One printer

Step 3: Using Packet Tracer's drawing tool and indicate the hierarchical layers with different color coding and labels:

- a. Access layer
- b. Distribution layer
- c. Core layer

Step 4: Configure the network and user devices. Check for end-to-end connectivity.

Step 5: Share your configuration and hierarchical network design Packet Tracer file with another student, group, the class, or the instructor.

Lab 5 – Configuring Basic Switch Settings

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

- Configure basic switch settings.
- Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capabilities with Telnet.
- Save the switch running configuration file.

Part 4: Manage the MAC Address Table

- Record the MAC address of the host.
- Determine the MAC addresses that the switch has learned.
- List the **show mac address-table** command options.
- Set up a static MAC address.

Background / Scenario

Cisco switches can be configured with a special IP address known as Switched Virtual Interface (SVI). The SVI or management address can be used for remote access to the switch to display or configure settings. If the VLAN 1 SVI is assigned an IP address, by default, all ports in VLAN 1 have access to the SVI management IP address.

In this lab, you will build a simple topology using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will examine default switch configurations before configuring basic switch settings. These basic switch settings include device name, interface description, local passwords, message of the day (MOTD) banner, IP addressing, setting up a static MAC address, and demonstrating the

use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

Note: The switch used is a Cisco Catalyst 2960 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 switch has been erased and has no startup configuration. Refer to Appendix A for the procedures to initialize and reload devices.

Required Resources

- 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 Telnet capability)
- Console cable to configure the Cisco IOS device via the console port
- Ethernet cable as shown in the topology

Part 1: Cable the Network and Verify the Default Switch Configuration

In Part 1, you will set up the network topology and verify default switch settings.

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

- a. Cable the console connection as shown in the topology. Do not connect the PC-A Ethernet cable at this time.

Note: If you are using Netlab, you can shut down F0/6 on S1 which has the same effect as not connecting PC-A to S1.

- b. Create a console connection to the switch from PC-A using Tera Term or other terminal emulation program.

Why must you use a console connection to initially configure the switch? Why is it not possible to connect to the switch via Telnet or SSH?

Step 2: Verify the default switch configuration.

In this step, you will examine the default switch settings, such as current switch configuration, IOS information, interface properties, VLAN information, and flash memory.

You can access all the switch IOS commands in privileged EXEC mode. Access to privileged EXEC mode should be restricted by password protection to prevent unauthorized use because it provides direct access to global configuration mode and commands used to configure operating parameters. You will set passwords later in this lab.

The privileged EXEC mode command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained. Use the **enable** command to enter privileged EXEC mode.

- a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), you will be at the user EXEC mode prompt on the switch with a prompt of Switch>. Use the **enable** command to enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Verify a clean configuration file with the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address. If your switch does not have a default configuration, erase and reload the switch.

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

- b. Examine the current running configuration file.

```
Switch# show running-config
```

How many FastEthernet interfaces does a 2960 switch have? _____

How many Gigabit Ethernet interfaces does a 2960 switch have? _____

What is the range of values shown for the vty lines? _____

- c. Examine the startup configuration file in NVRAM.

```
Switch# show startup-config
```

```
startup-config is not present
```

Why does this message appear? _____

- d. Examine the characteristics of the SVI for VLAN 1.

```
Switch# show interface vlan1
```

Is there an IP address assigned to VLAN 1? _____

What is the MAC address of this SVI? Answers will vary. _____

Is this interface up?

- e. Examine the IP properties of the SVI VLAN 1.

```
Switch# show ip interface vlan1
```

What output do you see?

- f. Connect PC-A Ethernet cable to port 6 on the switch and examine the IP properties of the SVI VLAN 1. Allow time for the switch and PC to negotiate duplex and speed parameters.

Note: If you are using Netlab, enable interface F0/6 on S1.

```
Switch# show ip interface vlan1
```

What output do you see?

- g. Examine the Cisco IOS version information of the switch.

```
Switch# show version
```

What is the Cisco IOS version that the switch is running? _____

What is the system image filename? _____

What is the base MAC address of this switch? Answers will vary.

- h. Examine the default properties of the FastEthernet interface used by PC-A.

```
Switch# show interface f0/6
```

Is the interface up or down? _____

What event would make an interface go up? _____

What is the MAC address of the interface? _____

What is the speed and duplex setting of the interface? _____

- i. Examine the default VLAN settings of the switch.

```
Switch# show vlan
```

What is the default name of VLAN 1? _____

Which ports are in this VLAN? _____

Is VLAN 1 active? _____

What type of VLAN is the default VLAN? _____

- j. Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

```
Switch# show flash
```

```
Switch# dir flash:
```

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension.

What is the filename of the Cisco IOS image? _____

Part 2: Configure Basic Network Device Settings

In Part 2, you configure basic settings for the switch and PC.

Step 1: Configure basic switch settings including hostname, local passwords, MOTD banner, management address, and Telnet access.

In this step, you will configure the PC and basic switch settings, such as hostname and an IP address for the switch management SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch is managed. Telnet and SSH are the two most common management methods. However, Telnet is not a secure protocol. All information flowing between the two devices is sent in plain text. Passwords and other sensitive information can be easily looked at if captured by a packet sniffer.

- a. Assuming the switch had no configuration file stored in NVRAM, verify you are at privileged EXEC mode. Enter **enable** if the prompt has changed back to Switch>.

```
Switch> enable
```

```
Switch#
```

- b. Enter global configuration mode.

```
Switch# configure terminal
```

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

```
Switch(config)#
```

The prompt changed again to reflect global configuration mode.

- c. Assign the switch hostname.

```
Switch(config)# hostname S1
S1(config)#
```

- d. Configure password encryption.

```
S1(config)# service password-encryption
S1(config)#
```

- e. Assign **class** as the secret password for privileged EXEC mode access.

```
S1(config)# enable secret class
S1(config)#
```

- f. Prevent unwanted DNS lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

- g. Configure a MOTD banner.

```
S1(config)# banner motd #
Enter Text message. End with the character '#'.
Unauthorized access is strictly prohibited. #
```

- h. Verify your access settings by moving between modes.

```
S1(config)# exit
S1#
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available
```

Press RETURN to get started.

```
Unauthorized access is strictly prohibited.
S1>
```

Which shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

- i. Go back to privileged EXEC mode from user EXEC mode. Enter **class** as the password when prompted.

```
S1> enable
Password:
S1#
```

Note: The password does not display when entering.

- j. Enter global configuration mode to set the SVI IP address of the switch. This allows remote management of the switch.

Before you can manage S1 remotely from PC-A, you must assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies that you should always use VLAN 99.

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

Notice that the VLAN 99 interface is in the down state even though you entered the **no shutdown** command. The interface is currently down because no switch ports are assigned to VLAN 99.

- k. Assign all user ports to VLAN 99.

```
S1(config)# interface range f0/1 - 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. Notice in the above output that the VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 comes up because at least one active port (F0/6 with PC-A attached) is now assigned to VLAN 99.

- l. Issue **show vlan brief** command to verify that all the user ports are in VLAN 99.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
99	VLAN0099	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- m. Configure the IP default gateway for S1. If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. It does respond to pings from a remote network. Although this activity does not include an external IP gateway, assume that you will eventually connect

the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.1.1, set the default gateway for the switch.

```
S1(config)# ip default-gateway 192.168.1.1
S1(config)#
```

- n. Console port access should also be restricted. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the **logging synchronous** option.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config)#
```

- o. Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you are unable to telnet to the switch.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
Why is the login command required? _____
```

Step 2: Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. An abbreviated version of the procedure is described here. A default gateway is not required for this topology; however, you can enter **192.168.1.1** to simulate a router attached to S1.

- 1) Click the Windows **Start** icon > **Control Panel**.
- 2) Click **View By:** and choose **Small icons**.
- 3) Choose **Network and Sharing Center** > **Change adapter settings**.
- 4) Select **Local Area Network Connection**, right click and choose **Properties**.
- 5) Choose **Internet Protocol Version 4 (TCP/IPv4)** > **Properties**.
- 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Part 3: Verify and Test Network Connectivity

In Part 3, you will verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the switch's remote management capability.

Step 1: Display the switch configuration.

From your console connection on PC-A, display and verify your switch configuration. The **show run** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging.

- a. A sample configuration displays here. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
```

Building configuration...

Current configuration : 2206 bytes

```
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname S1  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2  
!  
no aaa new-model  
system mtu routing 1500  
!  
!  
no ip domain-lookup  
!  
<output omitted>  
!  
interface FastEthernet0/24  
    switchport access vlan 99  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
    no ip address  
    no ip route-cache  
!  
interface Vlan99  
    ip address 192.168.1.2 255.255.255.0  
    no ip route-cache  
!  
ip default-gateway 192.168.1.1  
ip http server  
ip http secure-server  
!  
banner motd ^C  
Unauthorized access is strictly prohibited. ^C  
!  
line con 0  
    password 7 104D000A0618
```

```
logging synchronous
login
line vty 0 4
password 7 14141B180F0B
login
line vty 5 15
password 7 14141B180F0B
login
!
end

S1#
```

- b. Verify the management VLAN 99 settings.

```
S1# show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:08:45, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    175 packets input, 22989 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

What is the bandwidth on this interface? _____

What is the VLAN 99 state? _____

What is the line protocol state? _____

Step 2: Test end-to-end connectivity with ping.

- a. From the command prompt on PC-A, ping your own PC-A address first.

```
C:\Users\User1> ping 192.168.1.10
```

- b. From the command prompt on PC-A, ping the SVI management address of S1.

```
C:\Users\User1> ping 192.168.1.2
```

Because PC-A needs to resolve the MAC address of S1 through ARP, the first packet may time out. If ping results continue to be unsuccessful, troubleshoot the basic device configurations. You should check both the physical cabling and logical addressing if necessary.

Step 3: Test and verify remote management of S1.

You will now use Telnet to remotely access the switch. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. In this step, you will use Telnet to remotely access switch S1 using its SVI management address. Telnet is not a secure protocol; however, you will use it to test remote access. With Telnet, all information, including passwords and commands, are sent across the session in plain text. In subsequent labs, you will use SSH to remotely access network devices.

Note: If you are using Windows 7, the administrator may need to enable the Telnet protocol. To install the Telnet client, open a cmd window and type **pkgmgr /iu:"TelnetClient"**. An example is shown below.

```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

- a. With the cmd window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

```
C:\Users\User1> telnet 192.168.1.2
```

- b. After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode.
- c. Type **exit** to end the Telnet session.

Step 4: Save the switch running configuration file.

Save the configuration.

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Part 4: Manage the MAC Address Table

In Part 4, you will determine the MAC address that the switch has learned, set up a static MAC address on one interface of the switch, and then remove the static MAC address from that interface.

Step 1: Record the MAC address of the host.

From a command prompt on PC-A, issue **ipconfig /all** command to determine and record the Layer 2 (physical) addresses of the PC NIC.

Step 2: Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac address-table** command.

```
S1# show mac address-table
```

How many dynamic addresses are there? _____

How many MAC addresses are there in total? _____

Does the dynamic MAC address match the PC-A MAC address? _____

Step 3: List the show mac address-table options.

- a. Display the MAC address table options.

```
S1# show mac address-table ?
```

How many options are available for the **show mac address-table** command? _____

- b. Issue the **show mac address-table dynamic** command to display only the MAC addresses that were learned dynamically.

```
S1# show mac address-table dynamic
```

How many dynamic addresses are there? _____

- c. View the MAC address entry for PC-A. The MAC address formatting for the command is xxxx.xxxx.xxxx.

```
S1# show mac address-table address <PC-A MAC here>
```

Step 4: Set up a static MAC address.

- a. Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table** command from privileged EXEC mode.

```
S1# clear mac address-table dynamic
```

- b. Verify that the MAC address table was cleared.

```
S1# show mac address-table
```

How many static MAC addresses are there? _____

How many dynamic addresses are there? _____

- c. Examine the MAC table again.

More than likely, an application running on your PC has already sent a frame out the NIC to S1. Look at the MAC address table again in privileged EXEC mode to see if S1 has relearned the MAC address for PC-A.

```
S1# show mac address-table
```

How many dynamic addresses are there? _____

Why did this change from the last display? _____

If S1 has not yet relearned the MAC address for PC-A, ping the VLAN 99 IP address of the switch from PC-A, and then repeat the **show mac address-table** command.

- d. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on F0/6 using the address that was recorded for PC-A in Part 4, Step 1. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of your PC-A, which is different than the one given here as an example.

```
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface  
fastethernet 0/6
```

- e. Verify the MAC address table entries.

```
S1# show mac address-table
```

How many total MAC addresses are there? _____

How many static addresses are there? _____

- f. Remove the static MAC entry. Enter global configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 0050.56BE.6C89 is used in the example only. Use the MAC address for your PC-A.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

- g. Verify that the static MAC address has been cleared.

```
S1# show mac address-table
```

How many total static MAC addresses are there? _____

Reflection

1. Why should you configure the vty lines for the switch?

2. Why change the default VLAN 1 to a different VLAN number?

3. How can you prevent passwords from being sent in plain text?

4. Why configure a static MAC address on a port interface?

Appendix A: Initializing and Reloading a Router and Switch

Step 5: Initialize and reload the router.

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

```
Router> enable
Router#
```

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

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

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

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

Note: You may receive a prompt asking to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

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

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

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

- e. Another prompt asks to terminate autoinstall. Respond by typing **yes** press Enter.

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

Step 6: Initialize and reload the switch.

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

```
Switch> enable
```

```
Switch#
```

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

```
Switch# show flash
```

```
Directory of flash:/
```

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

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

```
Switch#
```

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

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

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

- d. You are prompted to verify the filename. If you have entered the name correctly, press Enter; otherwise, you can change the filename.

- e. You are prompted to confirm to delete this file. Press Enter to confirm.

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

```
Switch#
```

- f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to remove the configuration file. Press Enter to confirm.

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

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

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#
```

- g. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm to reload the switch. Press Enter to proceed.

```
Switch# reload
```

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

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Respond by typing **no** and press Enter.

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

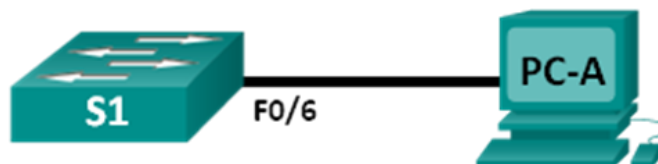
- h. After the switch reloads, you should see a prompt to enter the initial configuration dialog. Respond by entering **no** at the prompt and press Enter.

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

```
Switch>
```

Lab 6 - Configuring a Switch Management Address

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	N/A

Objectives

Part 1: Configure a Basic Network Device

- Cable the network as shown in the topology.
- Configure basic switch settings including hostname, management address, and Telnet access.
- Configure an IP address on the PC.

Part 2: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capability with Telnet.
- Save the switch running configuration file.

Background / Scenario

Cisco switches have a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address that is used for remote access to the switch to display or configure settings.

In this lab, you will build a simple network using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will configure basic switch settings and IP addressing, and demonstrate the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

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 available commands and output produced might vary from what is shown in the labs.

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

Required Resources

- 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 a Basic Network Device

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

Step 1: Cable the network.

- a. Cable the network as shown in the topology.
- b. Establish a console connection to the switch from PC-A.

Step 2: Configure basic switch settings.

In this step, you will configure basic switch settings, such as hostname and configuring an IP address for the SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch will be managed. Telnet and Secure Shell (SSH) are two of the most common management methods; however, Telnet is a very insecure protocol. All information flowing between the two devices is sent in plain text. Passwords and other sensitive information can be easily looked at if captured by a packet sniffer.

- a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), you will be at the user EXEC mode prompt on the switch with a prompt of `Switch>`. Enter privileged EXEC mode.

`Switch> enable`
`Switch#`
- b. Verify a clean configuration file with the `show running-config` privileged EXEC command. If a configuration file was previously saved, it will have to be removed. Depending on the switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address set. If your switch does not have a default configuration, ask your instructor for help.
- c. Enter global configuration mode and assign the switch hostname.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

- d. Configure the switch password access.

`S1(config)# enable secret class`
`S1(config)#`
- e. Prevent unwanted Domain Name System (DNS) lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

- f. Configure a login message-of-the-day (MOTD) banner.

```
S1(config)# banner motd #
Enter Text message. End with the character '#'.
Unauthorized access is strictly prohibited. #
```

- g. Verify your access setting by moving between modes.

```
S1(config)# exit
S1#
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

What shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

- h. Return to privileged EXEC mode from user EXEC mode.

```
S1> enable
Password: class
S1#
```

Note: Password will not show up on screen when entering.

- i. Enter global configuration mode to set the SVI IP address to allow remote switch management.

```
S1# config t
S1#(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

- j. Restrict console port access. The default configuration is to allow all console connections with no password needed.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

- k. Configure the virtual terminal (VTY) line for the switch to allow Telnet access. If you do not configure a VTY password, you will not be able to Telnet to the switch.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
```

```
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Step 3: Configure an IP address on PC-A.

- a. Assign the IP address and subnet mask to the PC, as shown in the Addressing Table on page 1. The procedure for assigning an IP address on a PC running Windows 7 is described below:
 - 1) Click the **Windows Start** icon > **Control Panel**.
 - 2) Click **View By:** > **Category**.
 - 3) Choose **View network status and tasks** > **Change adapter settings**.
 - 4) Right-click **Local Area Network Connection** and select **Properties**.
 - 5) Choose **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties** > **OK**.
 - 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Part 2: Verify and Test Network Connectivity

You will now verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the remote management capability of the switch.

Step 1: Display the S1 device configuration.

- a. Return to your console connection using Tera Term on PC-A to display and verify your switch configuration by issuing the **show run** command. A sample configuration is shown below. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
Building configuration...

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 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 S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
```

```

spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2

<output omitted>

interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
login
!
end

```

- b. Verify the status of your SVI management interface. Your VLAN 1 interface should be up/up and have an IP address assigned. Notice that switch port F0/6 is also up because PC-A is connected to it. Because all switch ports are initially in VLAN 1, by default, you can communicate with the switch using the IP address you configured for VLAN 1.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.2	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up

FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

Step 2: Test end-to-end connectivity.

Open a command prompt window (cmd.exe) on PC-A by clicking the **Windows Start** icon and enter **cmd** into the **Search for programs and files** field. Verify the IP address of PC-A by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information. Ping PC-A's own address and the management address of S1.

- Ping your own PC-A address first.

```
C:\Users\NetAcad> ping 192.168.1.10
```

Your output should be similar to the following screen:

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

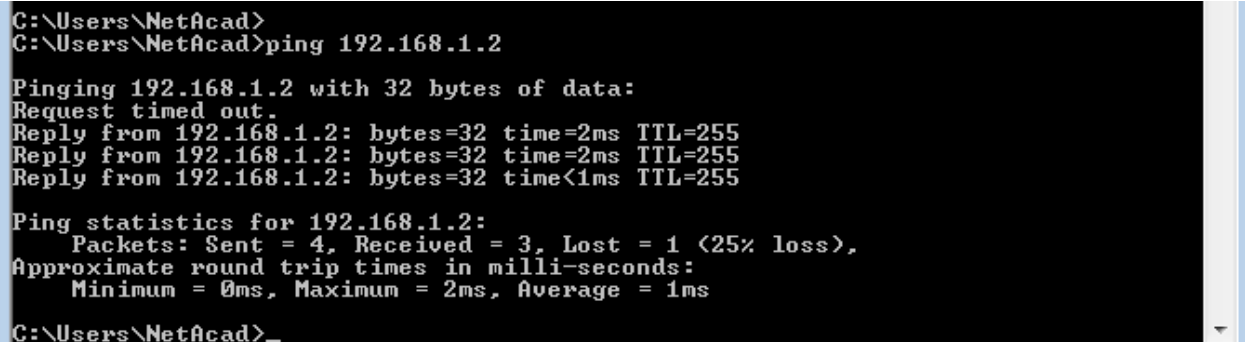
Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>_
  
```

- b. Ping the SVI management address of S1.

```
C:\Users\NetAcad> ping 192.168.1.2
```

Your output should be similar to the following screen. If ping results are not successful, troubleshoot the basic device configurations. You should check both the physical cabling and IP addressing, if necessary.



```
C:\Users\NetAcad>
C:\Users\NetAcad>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\NetAcad>
```

Step 3: Test and verify remote management of S1.

You will now use Telnet to remotely access the switch S1 using the SVI management address. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. Telnet is not a secure protocol. However, you will use it in this lab to test remote access. All information sent by Telnet, including passwords and commands, is sent across the session in plain text. In subsequent labs, you will use Secure Shell (SSH) to remotely access network devices.

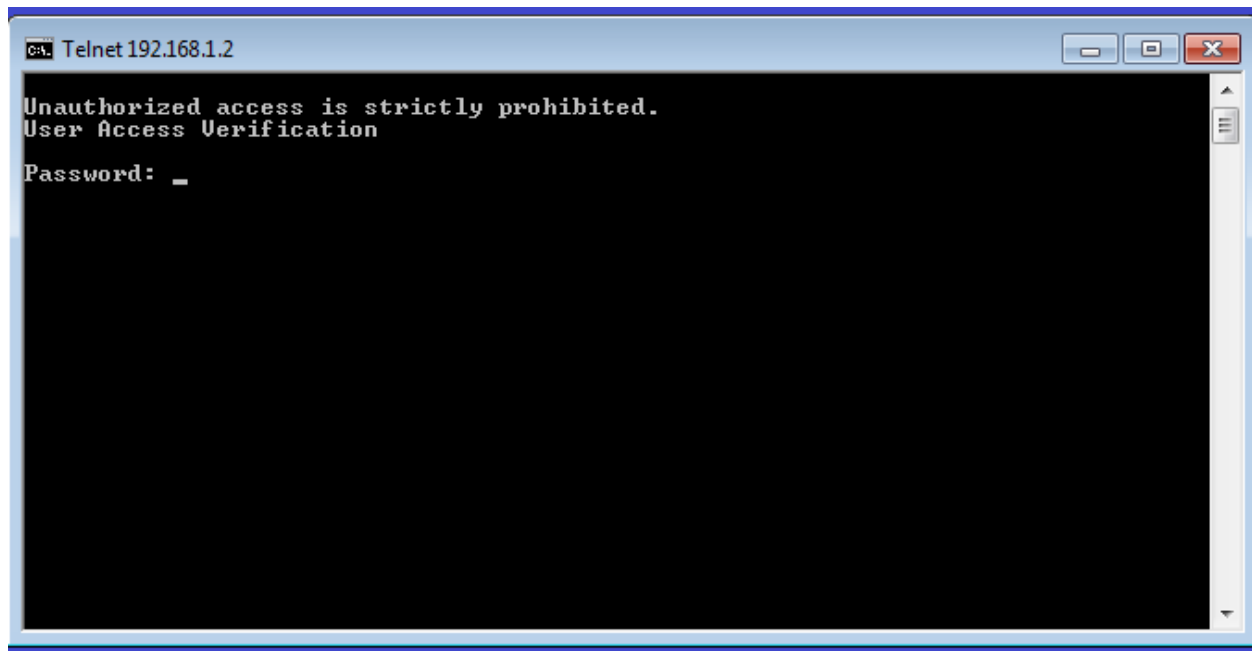
Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type `pkgmgr /iu:"TelnetClient"`.

```
C:\Users\NetAcad> pkgmgr /iu:"TelnetClient"
```

- a. With the command prompt window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

```
C:\Users\NetAcad> telnet 192.168.1.2
```

Your output should be similar to the following screen:



- b. After entering the **cisco** password, you will be at the user EXEC mode prompt. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode and issue a **show run** command.

Step 4: Save the configuration file.

- a. From your Telnet session, issue the **copy run start** command at the prompt.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```
- b. Exit the Telnet session by typing **quit**. You will be returned to the Windows 7 command prompt.

Reflection

Why must you use a console connection to initially configure the switch? Why not connect to the switch via Telnet or SSH?

Lab 7 – Configuring Switch Security Features

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure and Verify SSH Access on S1

- Configure SSH access.
- Modify SSH parameters.
- Verify the SSH configuration.

Part 4: Configure and Verify Security Features on S1

- Configure and verify general security features.
- Configure and verify port security.

Background / Scenario

It is quite common to lock down access and install good security features on PCs and servers. It is important that your network infrastructure devices, such as switches and routers, are also configured with security features.

In this lab, you will follow some best practices for configuring security features on LAN switches. You will only allow SSH and secure HTTPS sessions. You will also configure and verify port security to lock out any device with a MAC address not recognized by the switch.

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

Note: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, contact your instructor or refer to the previous lab for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 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: Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology and clear any configurations if necessary.

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

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router or switch, initialize and reload these devices back to their basic configurations.

Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you configure basic settings on the router, switch, and PC. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure an IP address on PC-A.

Step 2: Configure basic settings on R1.

- Configure the device name.
- Disable DNS lookup.
- Configure interface IP address as shown in the Addressing Table.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Encrypt plain text passwords.
- Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

A good security practice is to assign the management IP address of the switch to a VLAN other than VLAN 1 (or any other data VLAN with end users). In this step, you will create VLAN 99 on the switch and assign it an IP address.

- Configure the device name.
- Disable DNS lookup.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and vty password and then enable login.
- Configure a default gateway for S1 using the IP address of R1.
- Encrypt plain text passwords.

- g. Save the running configuration to startup configuration.
- h. Create VLAN 99 on the switch and name it **Management**.

```
S1(config)# vlan 99  
S1(config-vlan)# name Management  
S1(config-vlan)# exit  
S1(config)#
```

- i. Configure the VLAN 99 management interface IP address, as shown in the Addressing Table, and enable the interface.

```
S1(config)# interface vlan 99  
S1(config-if)# ip address 172.16.99.11 255.255.255.0  
S1(config-if)# no shutdown  
S1(config-if)# end  
S1#
```

- j. Issue the **show vlan** command on S1. What is the status of VLAN 99? _____
- k. Issue the **show ip interface brief** command on S1. What is the status and protocol for management interface VLAN 99?

Why is the protocol down, even though you issued the **no shutdown** command for interface VLAN 99?

- l. Assign ports F0/5 and F0/6 to VLAN 99 on the switch.

```
S1# config t  
S1(config)# interface f0/5  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# interface f0/6  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# end
```

- m. Issue the **show ip interface brief** command on S1. What is the status and protocol showing for interface VLAN 99? _____

Note: There may be a delay while the port states converge.

Step 4: Verify connectivity between devices.

- a. From PC-A, ping the default gateway address on R1. Were your pings successful? _____
- b. From PC-A, ping the management address of S1. Were your pings successful? _____
- c. From S1, ping the default gateway address on R1. Were your pings successful? _____
- d. From PC-A, open a web browser and go to <http://172.16.99.11>. If it prompts you for a username and password, leave the username blank and use **class** for the password. If it prompts for secured connection, answer **No**. Were you able to access the web interface on S1? _____
- e. Close the browser session on PC-A.

Note: The non-secure web interface (HTTP server) on a Cisco 2960 switch is enabled by default. A common security measure is to disable this service, as described in Part 4.

Part 3: Configure and Verify SSH Access on S1

Step 1: Configure SSH access on S1.

- a. Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.

```
S1(config)# ip domain-name CCNA-Lab.com
```

- b. Create a local user database entry for use when connecting to the switch via SSH. The user should have administrative level access.

Note: The password used here is NOT a strong password. It is merely being used for lab purposes.

```
S1(config)# username admin privilege 15 secret sshadmin
```

- c. Configure the transport input for the vty lines to allow SSH connections only, and use the local database for authentication.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# transport input ssh
```

```
S1(config-line)# login local
```

```
S1(config-line)# exit
```

- d. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

The name for the keys will be: S1.CCNA-Lab.com

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

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

```
[OK] (elapsed time was 3 seconds)
```

```
S1(config)#
```

```
S1(config)# end
```

- e. Verify the SSH configuration and answer the questions below.

```
S1# show ip ssh
```

What version of SSH is the switch using? _____

How many authentication attempts does SSH allow? _____

What is the default timeout setting for SSH? _____

Step 2: Modify the SSH configuration on S1.

Modify the default SSH configuration.

```
S1# config t
```

```
S1(config)# ip ssh time-out 75
```

```
S1(config)# ip ssh authentication-retries 2
```

How many authentication attempts does SSH allow? _____

What is the timeout setting for SSH? _____

Step 3: Verify the SSH configuration on S1.

- a. Using SSH client software on PC-A (such as Tera Term), open an SSH connection to S1. If you receive a message on your SSH client regarding the host key, accept it. Log in with **admin** for username and **cisco** for the password.

Was the connection successful? _____

What prompt was displayed on S1? Why?

- b. Type **exit** to end the SSH session on S1.

Part 4: Configure and Verify Security Features on S1

In Part 4, you will shut down unused ports, turn off certain services running on the switch, and configure port security based on MAC addresses. Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Configure general security features on S1.

- a. Configure a message of the day (MOTD) banner on S1 with an appropriate security warning message.
- b. Issue a **show ip interface brief** command on S1. What physical ports are up?

- c. Shut down all unused physical ports on the switch. Use the **interface range** command.

```
S1(config)# interface range f0/1 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

- d. Issue the **show ip interface brief** command on S1. What is the status of ports F0/1 to F0/4?
- _____

- e. Issue the **show ip http server status** command.

What is the HTTP server status? _____

What server port is it using? _____

What is the HTTP secure server status? _____

What secure server port is it using? _____

- f. HTTP sessions send everything in plain text. You will disable the HTTP service running on S1.

```
S1(config)# no ip http server
```

- g. From PC-A, open a web browser session to <http://172.16.99.11>. What was your result?
- _____

- h. From PC-A, open a secure web browser session at <https://172.16.99.11>. Accept the certificate. Log in with no username and a password of **class**. What was your result?
-
- i. Close the web session on PC-A.

Step 2: Configure and verify port security on S1.

- a. Record the R1 G0/1 MAC address. From the R1 CLI, use the **show interface g0/1** command and record the MAC address of the interface.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

What is the MAC address of the R1 G0/1 interface?

- b. From the S1 CLI, issue a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for ports F0/5 and F0/6. Record them below.

F0/5 MAC address: _____

F0/6 MAC address: _____

- c. Configure basic port security.

Note: This procedure would normally be performed on all access ports on the switch. F0/5 is shown here as an example.

- 1) From the S1 CLI, enter interface configuration mode for the port that connects to R1.

```
S1(config)# interface f0/5
```

- 2) Shut down the port.

```
S1(config-if)# shutdown
```

- 3) Enable port security on F0/5.

```
S1(config-if)# switchport port-security
```

Note: Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

- 4) Configure a static entry for the MAC address of R1 G0/1 interface recorded in Step 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(xxxx.xxxx.xxxx is the actual MAC address of the router G0/1 interface)

Note: Optionally, you can use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

- 5) Enable the switch port.

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

```
S1(config-if)# end
```

- d. Verify port security on S1 F0/5 by issuing a **show port-security interface** command.

```
S1# show port-security interface f0/5
```

```

Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

```

What is the port status of F0/5?

-
- e. From R1 command prompt, ping PC-A to verify connectivity.

```
R1# ping 172.16.99.3
```

- f. You will now violate security by changing the MAC address on the router interface. Enter interface configuration mode for G0/1 and shut it down.

```

R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown

```

- g. Configure a new MAC address for the interface, using **aaaa.bbbb.cccc** as the address.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

- h. If possible, have a console connection open on S1 at the same time that you do this step. You will see various messages displayed on the console connection to S1 indicating a security violation. Enable the G0/1 interface on R1.

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

- i. From R1 privilege EXEC mode, ping PC-A. Was the ping successful? Why or why not?

-
- j. On the switch, verify port security with the following commands shown below.

```
S1# show port-security
```

```

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----

```

```

Fa0/5          1          1          1          Shutdown
-----

```

```
Total Addresses in System (excluding one mac per port) :0
```

```
Max Addresses limit in System (excluding one mac per port) :8192
```

```
S1# show port-security interface f0/5
```

```

Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins

```

```

Aging Type           : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses   : 1
Configured MAC Addresses : 1
Sticky MAC Addresses  : 0
Last Source Address:Vlan : aaaa.bbbb.cccc:99
Security Violation Count : 1

```

S1# **show interface f0/5**

```

FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

```

S1# **show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
99	30f7.0da3.1821	SecureConfigured	Fa0/5	-

```

Total Addresses in System (excluding one mac per port) :0
Max Addresses limit in System (excluding one mac per port) :8192

```

- k. On the router, shut down the G0/1 interface, remove the hard-coded MAC address from the router, and re-enable the G0/1 interface.

```

R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end

```

- l. From R1, ping PC-A again at 172.16.99.3. Was the ping successful? _____
- m. Issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

- n. Clear the S1 F0/5 error disabled status.

```

S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown

```

Note: There may be a delay while the port states converge.

- o. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

```

S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)

```

```
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,  
    reliability 255/255, txload 1/255, rxload 1/255
```

p. From the R1 command prompt, ping PC-A again. You should be successful.

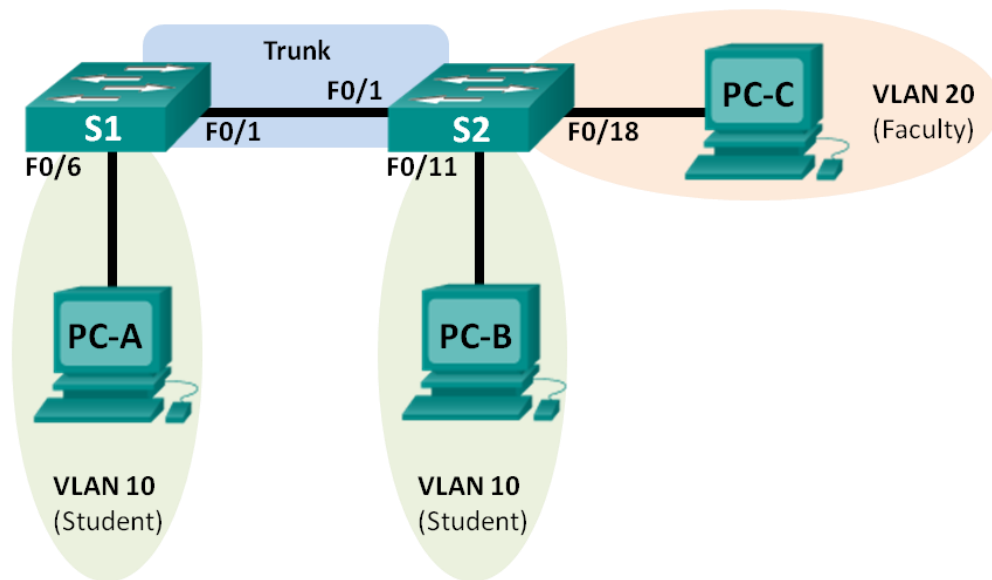
Reflection

1. Why would you enable port security on a switch?

2. Why should unused ports on a switch be disabled?

Lab 8 - Configuring VLANs and Trunking

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Maintain VLAN Port Assignments and the VLAN Database

Part 4: Configure an 802.1Q Trunk between the Switches

Part 5: Delete the VLAN Database

Background / Scenario

Modern switches use virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. VLANs can also be used as a security measure by controlling which hosts can communicate. In general, VLANs make it easier to design a network to support the goals of an organization.

VLAN trunks are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANs to travel over a single link, while keeping the VLAN identification and segmentation intact.

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

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: Ensure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 2 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: 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 switches.

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

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

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
- Configure **logging synchronous** for the console line.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure the IP address listed in the Addressing Table for VLAN 1 on both switches.
- Administratively deactivate all unused ports on the switch.
- Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

Verify that the PC hosts can ping one another.

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

Can PC-A ping PC-B? _____

Can PC-A ping PC-C? _____

Can PC-A ping S1? _____

Can PC-B ping PC-C? _____

Can PC-B ping S2? _____

Can PC-C ping S2? _____

Can S1 ping S2? _____

If you answered no to any of the above questions, why were the pings unsuccessful?

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create student, faculty, and management VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

Step 1: Create VLANs on the switches.

- a. Create the VLANs on S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

- b. Create the same VLANs on S2.

- c. Issue the **show vlan** command to view the list of VLANs on S1.

```
S1# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
10	Student	active	
20	Faculty	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	

```

1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup

```

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
99	enet	100099	1500	-	-	-	-	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports

What is the default VLAN? _____

What ports are assigned to the default VLAN?

Step 2: Assign VLANs to the correct switch interfaces.

- a. Assign VLANs to the interfaces on S1.

- 1) Assign PC-A to the Student VLAN.

```

S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10

```

- 2) Move the switch IP address VLAN 99.

```

S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end

```

- b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/7, Fa0/8, Fa0/9
 Fa0/10, Fa0/11, Fa0/12, Fa0/13
 Fa0/14, Fa0/15, Fa0/16, Fa0/17
 Fa0/18, Fa0/19, Fa0/20, Fa0/21
 Fa0/22, Fa0/23, Fa0/24, Gi0/1
 Gi0/2

10	Student	active	Fa0/6
20	Faculty	active	
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Issue the **show ip interfaces brief** command.

What is the status of VLAN 99? Why?

- d. Use the Topology to assign VLANs to the appropriate ports on S2.
 e. Remove the IP address for VLAN 1 on S2.
 f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.
 g. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

S2# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/11
20	Faculty	active	Fa0/18
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Is PC-A able to ping PC-B? Why?

Is S1 able to ping S2? Why?

Part 3: Maintain VLAN Port Assignments and the VLAN Database

In Part 3, you will change VLAN assignments to ports and remove VLANs from the VLAN database.

Step 1: Assign a VLAN to multiple interfaces.

- On S1, assign interfaces F0/11 – 24 to VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```
- Issue the **show vlan brief** command to verify VLAN assignments.
- Reassign F0/11 and F0/21 to VLAN 20.
- Verify that VLAN assignments are correct.

Step 2: Remove a VLAN assignment from an interface.

- Use the **no switchport access vlan** command to remove the VLAN 10 assignment to F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```
- Verify that the VLAN change was made.
 Which VLAN is F0/24 is now associated with? _____

Step 3: Remove a VLAN ID from the VLAN database.

- Add VLAN 30 to interface F0/24 without issuing the VLAN command.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Note: Current switch technology no longer requires that the **vlan** command be issued to add a VLAN to the database. By assigning an unknown VLAN to a port, the VLAN adds to the VLAN database.

- Verify that the new VLAN is displayed in the VLAN table.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
30	VLAN0030	active	Fa0/24
99	Management	active	
1002	fddi-default	act/unsup	

```

1003 token-ring-default      act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default           act/unsup

```

What is the default name of VLAN 30? _____

- c. Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

```

S1(config)# no vlan 30
S1(config)# end

```

- d. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

After deleting VLAN 30, what VLAN is port F0/24 assigned to? What happens to the traffic destined to the host attached to F0/24?

```

S1# show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- e. Issue the **no switchport access vlan** command on interface F0/24.
- f. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24. To which VLAN is F0/24 assigned?

Note: Before removing a VLAN from the database, it is recommended that you reassign all the ports assigned to that VLAN.

Why should you reassign a port to another VLAN before removing the VLAN from the VLAN database?

Part 4: Configure an 802.1Q Trunk Between the Switches

In Part 4, you will configure interface F0/1 to use the Dynamic Trunking Protocol (DTP) to allow it to negotiate the trunk mode. After this has been accomplished and verified, you will disable DTP on interface F0/1 and manually configure it as a trunk.

Step 1: Use DTP to initiate trunking on F0/1.

The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a trunk if the neighboring interface is set to trunk or dynamic desirable mode.

- a. Set F0/1 on S1 to negotiate trunk mode.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar 1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar 1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#
*Mar 1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S1(config-if)#
*Mar 1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar 1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

You should also receive link status messages on S2.

```
S2#
*Mar 1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S2#
*Mar 1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S2#
*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

- b. Issue the **show vlan brief** command on S1 and S2. Interface F0/1 is no longer assigned to VLAN 1. Trunked interfaces are not listed in the VLAN table.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S1 is set to desirable, and the mode on S2 is set to auto.

S1# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,20,99

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,20,99

S2# **show interfaces trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,20,99

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,20,99

Note: By default, all VLANs are allowed on a trunk. The **switchport trunk** command allows you to control what VLANs have access to the trunk. For this lab, keep the default settings which allows all VLANs to traverse F0/1.

- d. Verify that VLAN traffic is traveling over trunk interface F0/1.

Can S1 ping S2? _____

Can PC-A ping PC-B? _____

Can PC-A ping PC-C? _____

Can PC-B ping PC-C? _____

Can PC-A ping S1? _____

Can PC-B ping S2? _____

Can PC-C ping S2? _____

If you answered no to any of the above questions, explain below.

Step 2: Manually configure trunk interface F0/1.

The **switchport mode trunk** command is used to manually configure a port as a trunk. This command should be issued on both ends of the link.

- a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

- b. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

```
S2# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

Why might you want to manually configure an interface to trunk mode instead of using DTP?

Part 5: Delete the VLAN Database

In Part 5, you will delete the VLAN Database from the switch. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Determine if the VLAN database exists.

Issue the **show flash** command to determine if a **vlan.dat** file exists in flash.

```
S1# show flash
```

```
Directory of flash:/
 2  -rwx      1285   Mar 1 1993 00:01:24 +00:00  config.text
 3  -rwx     43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
 4  -rwx         5   Mar 1 1993 00:01:24 +00:00  private-config.text
 5  -rwx    11607161  Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
 6  -rwx       736   Mar 1 1993 00:19:41 +00:00  vlan.dat
```

```
32514048 bytes total (20858880 bytes free)
```

Note: If there is a **vlan.dat** file located in flash, then the VLAN database does not contain its default settings.

Step 2: Delete the VLAN database.

- a. Issue the **delete vlan.dat** command to delete the vlan.dat file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the vlan.dat file. Press Enter both times.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```

- b. Issue the **show flash** command to verify that the vlan.dat file has been deleted.

```
S1# show flash
```

```
Directory of flash:/
```

```
 2  -rwx          1285   Mar 1 1993 00:01:24 +00:00  config.text
 3  -rwx         43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
 4  -rwx           5    Mar 1 1993 00:01:24 +00:00  private-config.text
 5  -rwx       11607161  Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
```

```
32514048 bytes total (20859904 bytes free)
```

To initialize a switch back to its default settings, what other commands are needed?

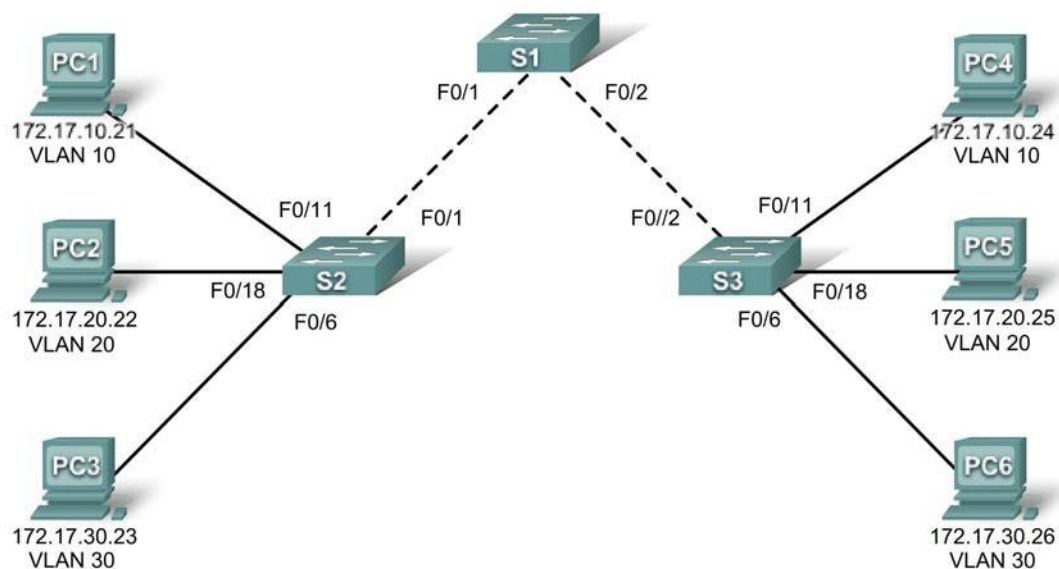
Reflection

1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 20?

2. What are some primary benefits that an organization can receive through effective use of VLANs?

Lab 9: Basic VLAN Configuration

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state
- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 2900 or 2950 switches, the outputs may appear different. Also, certain commands may be different or unavailable.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations.

It is a good practice to disable any unused ports on the switches by putting them in shutdown. Disable all ports on the switches:

```
Switch#config term
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

```

S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
S3(config)#interface range fa0/6, fa0/11, fa0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#no shutdown

```

Task 3: Configure and Activate Ethernet Interfaces**Step 1: Configure the PCs.**

You can complete this lab using only two PCs by simply changing the IP addressing for the two PCs specific to a test you want to conduct. For example, if you want to test connectivity between PC1 and PC2, then configure the IP addresses for those PCs by referring to the addressing table at the beginning of the lab. Alternatively, you can configure all six PCs with the IP addresses and default gateways.

Task 4: Configure VLANs on the Switch**Step 1: Create VLANs on switch S1.**

Use the **vlan *vlan-id*** command in global configuration mode to add a VLAN to switch S1. There are four VLANs configured for this lab: VLAN 10 (faculty/staff); VLAN 20 (students); VLAN 30 (guest); and VLAN 99 (management). After you create the VLAN, you will be in vlan configuration mode, where you can assign a name to the VLAN with the **name *vlan name*** command.

```

S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#

```

Step 2: Verify that the VLANs have been created on S1.

Use the **show vlan brief** command to verify that the VLANs have been created.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gi0/1
Gi0/2

10	faculty/staff	active
20	students	active
30	guest	active
99	management	active

Step 3: Configure and name VLANs on switches S2 and S3.

Create and name VLANs 10, 20, 30, and 99 on S2 and S3 using the commands from Step 1. Verify the correct configuration with the **show vlan brief** command.

What ports are currently assigned to the four VLANs you have created?

Step 4: Assign switch ports to VLANs on S2 and S3.

Refer to the port assignment table on page 1. Ports are assigned to VLANs in interface configuration mode, using the **switchport access vlan** *vlan-id* command. You can assign each port individually or you can use the **interface range** command to simplify this task, as shown here. The commands are shown for S3 only, but you should configure both S2 and S3 similarly. Save your configuration when done.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Step 5: Determine which ports have been added.

Use the **show vlan id** *vlan-number* command on S2 to see which ports are assigned to VLAN 10.

Which ports are assigned to VLAN 10?

Note: The **show vlan name** *vlan-name* displays the same output.

You can also view VLAN assignment information using the **show interfaces** *interface* **switchport** command.

Step 6: Assign the management VLAN.

A management VLAN is any VLAN that you configure to access the management capabilities of a switch. VLAN 1 serves as the management VLAN if you did not specifically define another VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Because the out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN, VLAN 1 is a bad choice as the management VLAN. You do not want an arbitrary user who is connecting

to a switch to default to the management VLAN. Recall that you configured the management VLAN as VLAN 99 earlier in this lab.

From interface configuration mode, use the **ip address** command to assign the management IP address to the switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Assigning a management address allows IP communication between the switches, and also allows any host connected to a port assigned to VLAN 99 to connect to the switches. Because VLAN 99 is configured as the management VLAN, any ports assigned to this VLAN are considered management ports and should be secured to control which devices can connect to these ports.

Step 7: Configure trunking and the native VLAN for the trunking ports on all switches.

Trunks are connections between the switches that allow the switches to exchange information for all VLANs. By default, a trunk port belongs to all VLANs, as opposed to an access port, which can only belong to a single VLAN. If the switch supports both ISL and 802.1Q VLAN encapsulation, the trunks must specify which method is being used. Because the 2960 switch only supports 802.1Q trunking, it is not specified in this lab.

A native VLAN is assigned to an 802.1Q trunk port. In the topology, the native VLAN is VLAN 99. An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). The 802.1Q trunk port places untagged traffic on the native VLAN. Untagged traffic is generated by a computer attached to a switch port that is configured with the native VLAN. One of the IEEE 802.1Q specifications for Native VLANs is to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For the purposes of this lab, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

Use the **interface range** command in global configuration mode to simplify configuring trunking.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
```

```
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Verify that the trunks have been configured with the **show interface trunk** command.

```
S1#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99
Fa0/2	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/2	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,30,99
Fa0/2	1,10,20,30,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,30,99
Fa0/2	1,10,20,30,99

Step 8: Verify that the switches can communicate.

From S1, ping the management address on both S2 and S3.

```
S1#ping 172.17.99.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#ping 172.17.99.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Step 9: Ping several hosts from PC2.

Ping from host PC2 to host PC1 (172.17.10.21). Is the ping attempt successful? _____

Ping from host PC2 to the switch VLAN 99 IP address 172.17.99.12. Is the ping attempt successful?

Because these hosts are on different subnets and in different VLANs, they cannot communicate without a Layer 3 device to route between the separate subnetworks.

Ping from host PC2 to host PC5. Is the ping attempt successful? _____

Because PC2 is in the same VLAN and the same subnet as PC5, the ping is successful

Step 10: Move PC1 into the same VLAN as PC2.

The port connected to PC2 (S2 Fa0/18) is assigned to VLAN 20, and the port connected to PC1 (S2 Fa0/11) is assigned to VLAN 10. Reassign the S2 Fa0/11 port to VLAN 20. You do not need to first remove a port from a VLAN to change its VLAN membership. After you reassign a port to a new VLAN, that port is automatically removed from its previous VLAN.

S2#**configure terminal**

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

S2(config)#**interface fastethernet 0/11**

S2(config-if)#**switchport access vlan 20**

S2(config-if)#**end**

Ping from host PC2 to host PC1. Is the ping attempt successful? _____

Even though the ports used by PC1 and PC2 are in the same VLAN, they are still in different subnetworks, so they cannot communicate directly.

Step 11: Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.21. The subnet mask and default gateway can remain the same. Once again, ping from host PC2 to host PC1, using the newly assigned IP address.

Is the ping attempt successful? _____

Why was this attempt successful?

Task 5: Document the Switch Configurations

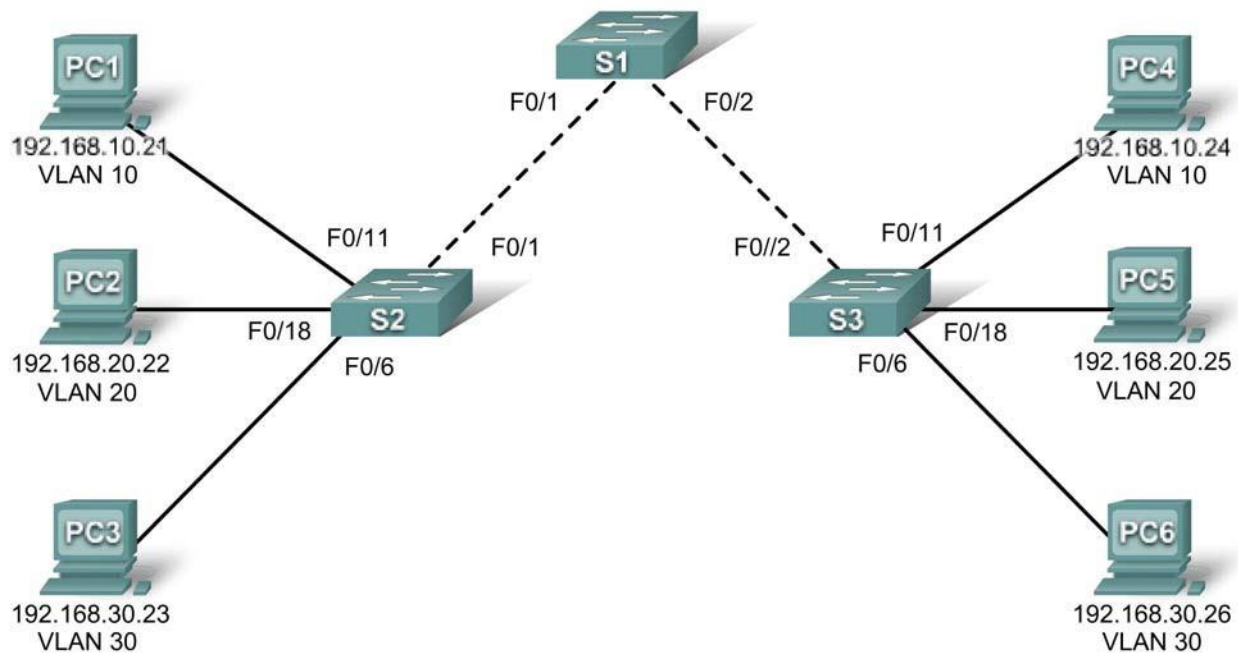
On each switch, capture the running configuration to a text file and save it for future reference.

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 10: Challenge VLAN Configuration

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 56	192.168.56.11	255.255.255.0	N/A
S2	VLAN 56	192.168.56.12	255.255.255.0	N/A
S3	VLAN 56	192.168.56.13	255.255.255.0	N/A
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
PC4	NIC	192.168.10.24	255.255.255.0	192.168.10.1
PC5	NIC	192.168.20.25	255.255.255.0	192.168.20.1
PC6	NIC	192.168.30.26	255.255.255.0	192.168.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 56)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state
- Perform basic configuration tasks on a switch
- Create VLANs
- Assign switch ports to a VLAN
- Add, move, and change ports
- Verify VLAN configuration
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Save the VLAN configuration

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

Task 3: Configure and Activate Ethernet Interfaces

Step 1: Configure the PCs.

Configure the Ethernet interfaces of the six PCs with the IP addresses and default gateways from the addressing table at the beginning of the lab.

Task 4: Configure VLANs on the Switch

Step 1: Create VLANs on switch S1.

Step 2: Verify that the VLANs have been created on S1.

Step 3: Configure, name, and verify VLANs on switches S2 and S3.

Step 4: Assign switch ports to VLANs on S2 and S3.

Step 5: Determine which ports have been added to VLAN 10 on S2.

Step 6: Configure management VLAN 56 on each of the switches. Use the IP addresses indicated in the Addressing Table.

Step 7: Configure trunking and the native VLAN for the trunking ports on all three switches. Verify that the trunks have been configured.

Step 8: Verify that S1, S2, and S3 can communicate.

Step 9: Ping several hosts from PC2. What is the result?

Step 10: Move PC1 into the same VLAN as PC2. Can PC1 successfully ping PC2?

Step 11: Change the IP address on PC1 to 192.168.20.21. Can PC1 successfully ping PC2?

Change the IP address on PC1 to 192.168.20.21. The default gateway should be changed to 192.168.20.1. Once again, ping from host PC2 to host PC1, using the newly assigned IP address. Is the ping attempt successful?

Why was this attempt successful?

Task 5: Document the Switch Configurations

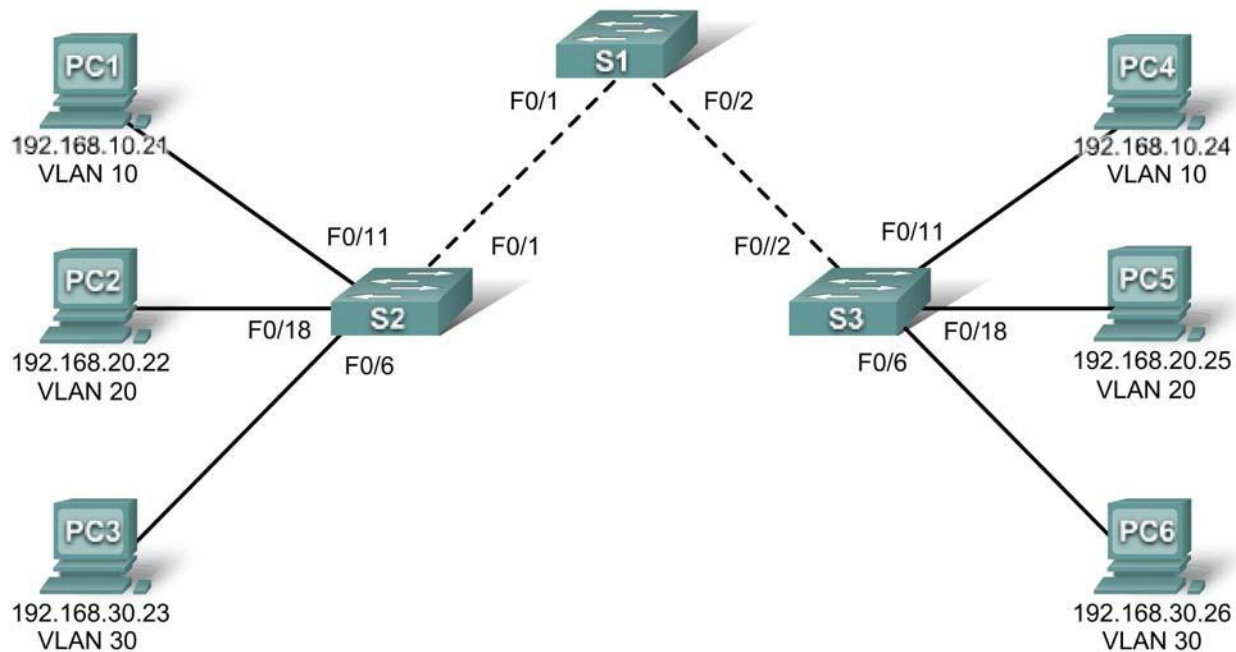
On each switch, capture the running configuration to a text file and save it for future reference.

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 11: Troubleshooting VLAN Configurations

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 56	192.168.56.11	255.255.255.0	N/A
S2	VLAN 56	192.168.56.12	255.255.255.0	N/A
S3	VLAN 56	192.168.56.13	255.255.255.0	N/A
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
PC4	NIC	192.168.10.24	255.255.255.0	192.168.10.1
PC5	NIC	192.168.20.25	255.255.255.0	192.168.20.1
PC6	NIC	192.168.30.26	255.255.255.0	192.168.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 56)	192.168.56.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	192.168.20.0 /24

Learning objective

Practice basic VLAN troubleshooting skills.

Scenario

In this lab, you will practice troubleshooting a misconfigured VLAN environment. Load or have your instructor load the configurations below into your lab gear. Your objective is to locate and correct any and all errors in the configurations and establish end-to-end connectivity. Your final configuration should match the topology diagram and addressing table. All passwords are set to **cisco**, except the enable secret password, which is set to **class**.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

Step 3: Import the configurations below.

Switch 1

```
hostname S1
no ip domain-lookup
enable secret class
!
!
interface range FastEthernet0/1-5
  switchport mode trunk
!
interface range FastEthernet0/6-24
  shutdown
!
interface Vlan1
  no ip address
  no ip route-cache
!
interface Vlan56
  ip address 192.168.56.11 255.255.255.0
  no ip route-cache
!
line con 0
  logging synchronous
line vty 0 4
  no login
```

```
line vty 5 15
  password cisco
  login
!
end
```

Switch 2

```
hostname S2
no ip domain-lookup
enable secret class
!
vlan 10,20,30,56
!
interface range FastEthernet0/1-5
  switchport trunk native vlan 56
  switchport mode access
!
interface range FastEthernet0/6-10
  switchport access vlan 30 switchport
  mode access
!
interface range FastEthernet0/11-17
  switchport access vlan 10 switchport
  mode access
!
interface range FastEthernet0/18-24
  switchport access vlan 20 switchport
  mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  ip address 192.168.56.12 255.255.255.0 no
  ip route-cache
  shutdown
!
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
line vty 5 15
  password cisco
  login
```

```
!  
end
```

Switch 3

```
hostname S3  
no ip domain-lookup  
enable secret class  
!  
vlan 10,20,30  
!  
interface range FastEthernet0/1-5  
    switchport trunk native vlan 56  
    switchport mode trunk  
!  
interface range FastEthernet0/6-10  
    switchport mode access  
!  
interface range FastEthernet0/11-17  
    switchport mode access  
!  
interface range FastEthernet0/18-24  
    switchport mode access  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
    no ip address  
    no ip route-cache  
    shutdown  
!  
interface Vlan56  
    no ip route-cache  
!  
line con 0  
    password cisco  
    login  
line vty 0 4  
    password cisco  
    login  
line vty 5 15  
    password cisco  
    login
```

```
!  
end
```

Task 2: Troubleshoot and Repair the VLAN Configuration**Task 3: Document the Switch Configurations**

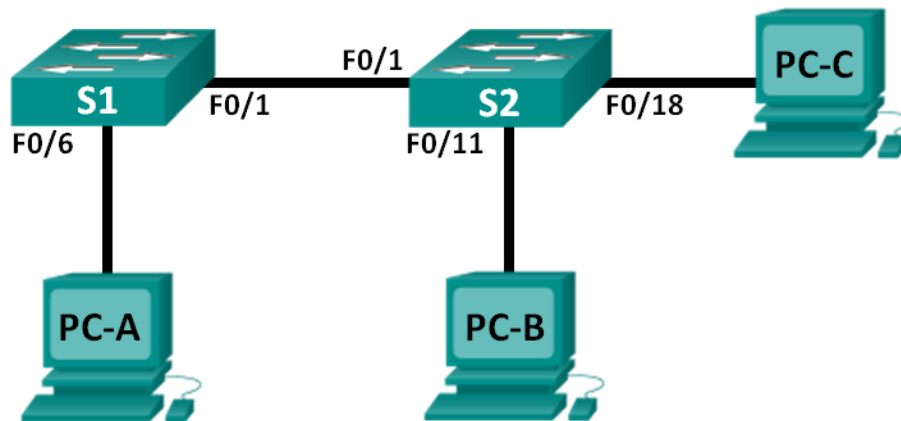
On each switch, capture the running configuration to a text file and save for future reference:

Task 4: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 12 - Troubleshooting VLAN Configurations

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
F0/1	802.1Q Trunk	N/A
F0/6-12	VLAN 10 – Students	192.168.10.0/24
F0/13-18	VLAN 20 – Faculty	192.168.20.0/24
F0/19-24	VLAN 30 – Guest	192.168.30.0/24

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot VLAN 10

Part 3: Troubleshoot VLAN 20

Background / Scenario

VLANs provide logical segmentation within an internetwork and improve network performance by separating large broadcast domains into smaller ones. By separating hosts into different networks, VLANs can be used to control which hosts can communicate. In this lab, a school has decided to implement VLANs in order to separate traffic from different end users. The school is using 802.1Q trunking to facilitate VLAN communication between switches.

The S1 and S2 switches have been configured with VLAN and trunking information. Several errors in the configuration have resulted in connectivity issues. You have been asked to troubleshoot and correct the configuration errors and document your work.

Note: The switches used with this lab 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

- 2 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: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the switches with some basic settings, such as passwords and IP addresses. Preset VLAN-related configurations, which contain errors, are provided for you for the initial switch configurations. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure IP address in Addressing Table.
- Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
- Assign **class** as the privileged EXEC password.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 5: Load switch configurations.

The configurations for the switches S1 and S2 are provided for you. There are errors within these configurations, and it is your job to determine the incorrect configurations and correct them.

Switch S1 Configuration:

```
hostname S1
vlan 10
name Students
vlan 2
!vlan 20
name Faculty
vlan 30
name Guest
interface range f0/1-24
switchport mode access
shutdown
interface range f0/7-12
switchport access vlan 10
interface range f0/13-18
switchport access vlan 2
interface range f0/19-24
switchport access vlan 30
end
```

Switch S2 Configuration:

```
hostname S2
vlan 10
Name Students
vlan 20
Name Faculty
vlan 30
Name Guest
interface f0/1
switchport mode trunk
switchport trunk allowed vlan 1,10,2,30
interface range f0/2-24
switchport mode access
shutdown
interface range f0/13-18
switchport access vlan 20
interface range f0/19-24
switchport access vlan 30
shutdown
end
```

Step 6: Copy the running configuration to the startup configuration.

Part 2: Troubleshoot VLAN 10

In Part 2, you must examine VLAN 10 on S1 and S2 to determine if it is configured correctly. You will troubleshoot the scenario until connectivity is established.

Step 1: Troubleshoot VLAN 10 on S1.

- a. Can PC-A ping PC-B? _____
- b. After verifying that PC-A was configured correctly, examine the S1 switch to find possible configuration errors by viewing a summary of the VLAN information. Enter the **show vlan brief** command.
- c. Are there any problems with the VLAN configuration?

- d. Examine the switch for trunk configurations using the **show interfaces trunk** and the **show interface f0/1 switchport** commands.
- e. Are there any problems with the trunking configuration?

- f. Examine the running configuration of the switch to find possible configuration errors.
Are there any problems with the current configuration?

- g. Correct the errors found regarding F0/1 and VLAN 10 on S1. Record the commands used in the space below.

- h. Verify the commands had the desired effects by issuing the appropriate **show** commands.
- i. Can PC-A ping PC-B? _____

Step 2: Troubleshoot VLAN 10 on S2.

- a. Using the previous commands, examine the S2 switch to find possible configuration errors.
Are there any problems with the current configuration?

- b. Correct the errors found regarding interfaces and VLAN 10 on S2. Record the commands below.

- c. Can PC-A ping PC-B? _____

Part 3: Troubleshoot VLAN 20

In Part 3, you must examine VLAN 20 on S1 and S2 to determine if it is configured correctly. To verify functionality, you will reassign PC-A into VLAN 20, and then troubleshoot the scenario until connectivity is established.

Step 1: Assign PC-A to VLAN 20.

- a. On PC-A, change the IP address to 192.168.20.2/24 with a default gateway of 192.168.20.1.
- b. On S1, assign the port for PC-A to VLAN 20. Write the commands needed to complete the configuration.

- c. Verify that the port for PC-A has been assigned to VLAN 20.
- d. Can PC-A ping PC-C? _____

Step 2: Troubleshoot VLAN 20 on S1.

- a. Using the previous commands, examine the S1 switch to find possible configuration errors.
Are there any problems with the current configuration?

- b. Correct the errors found regarding VLAN 20.
- c. Can PC-A ping PC-C? _____

Step 3: Troubleshoot VLAN 20 on S2.

- a. Using the previous commands, examine the S2 switch to find possible configuration errors.
Are there any problems with the current configuration?

- b. Correct the errors found regarding VLAN 20. Record the commands used below.

- c. Can PC-A ping PC-C? _____

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

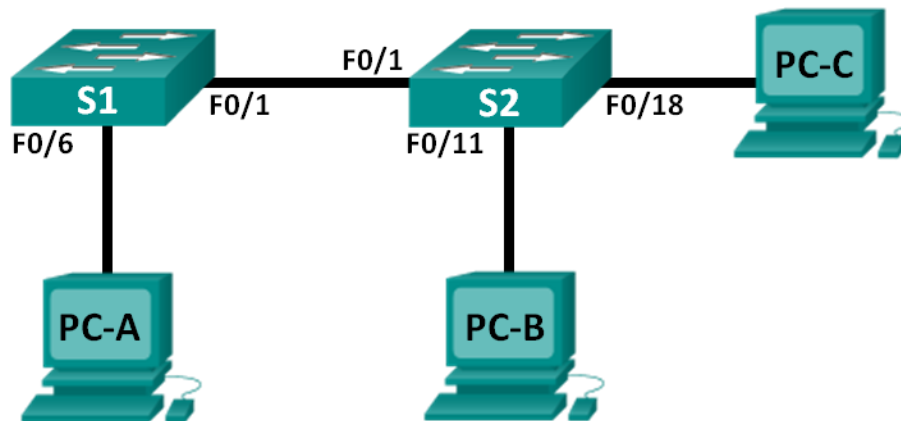
Reflection

1. Why is a correctly configured trunk port critical in a multi-VLAN environment?

2. Why would a network administrator limit traffic for specific VLANs on a trunk port?

Lab 13 – Implementing VLAN Security

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

VLAN Assignments

VLAN	Name
10	Data
99	Management&Native
999	BlackHole

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Implement VLAN Security on the Switches

Background / Scenario

Best practice dictates configuring some basic security settings for both access and trunk ports on switches. This will help guard against VLAN attacks and possible sniffing of network traffic within the network.

In this lab, you will configure the network devices in the topology with some basic settings, verify connectivity and then apply more stringent security measures on the switches. You will examine how Cisco switches behave by using various **show** commands. You will then apply security measures.

Note: The switches used with this lab 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

- 2 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: Build the Network and Configure Basic Device Settings

In Part 1, you will configure basic settings on the switches and PCs. Refer to the Addressing Table for device names and address information.

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

Step 2: Initialize and reload the switches.

Step 3: Configure IP addresses on PC-A, PC-B, and PC-C.

Refer to the Addressing Table for PC address information.

Step 4: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure the device names as shown in the topology.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and VTY password and enable login for console and vty lines.
- Configure synchronous logging for console and vty lines.

Step 5: Configure VLANs on each switch.

- Create and name VLANs according to the VLAN Assignments table.
- Configure the IP address listed in the Addressing Table for VLAN 99 on both switches.
- Configure F0/6 on S1 as an access port and assign it to VLAN 99.
- Configure F0/11 on S2 as an access port and assign it to VLAN 10.
- Configure F0/18 on S2 as an access port and assign it to VLAN 99.
- Issue **show vlan brief** command to verify VLAN and port assignments.

To which VLAN would an unassigned port, such as F0/8 on S2, belong?

Step 6: Configure basic switch security.

- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Encrypt all passwords.
- Shut down all unused physical ports.
- Disable the basic web service running.

```
S1(config)# no ip http server
```

```
S2(config)# no ip http server
```

- Copy the running configuration to startup configuration.

Step 7: Verify connectivity between devices and VLAN information.

- From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

- From S1, ping the management address of S2. Were the pings successful? Why?

- From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

- From a command prompt on PC-C, ping the management addresses on S1 and S2. Were you successful? Why?

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

Part 2: Implement VLAN Security on the Switches

Step 1: Configure trunk ports on S1 and S2.

- Configure port F0/1 on S1 as a trunk port.

```
S1(config)# interface f0/1
```

```
S1(config-if)# switchport mode trunk
```

- Configure port F0/1 on S2 as a trunk port.

```
S2(config)# interface f0/1
```

```
S2(config-if)# switchport mode trunk
```

- c. Verify trunking on S1 and S2. Issue the **show interface trunk** command on both switches.

```
S1# show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,99,999

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,99,999

Step 2: Change the native VLAN for the trunk ports on S1 and S2.

Changing the native VLAN for trunk ports from VLAN 1 to another VLAN is a good practice for security.

- a. What is the current native VLAN for the S1 and S2 F0/1 interfaces?

- b. Configure the native VLAN on the S1 F0/1 trunk interface to Management&Native VLAN 99.

```
S1# config t
```

```
S1(config)# interface f0/1
```

```
S1(config-if)# switchport trunk native vlan 99
```

- c. Wait a few seconds. You should start receiving error messages on the console session of S1. What does the %CDP-4-NATIVE_VLAN_MISMATCH: message mean?

- d. Configure the native VLAN on the S2 F0/1 trunk interface to VLAN 99.

```
S2(config)# interface f0/1
```

```
S2(config-if)# switchport trunk native vlan 99
```

- e. Verify that the native VLAN is now 99 on both switches. S1 output is shown below.

```
S1# show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,99,999

```
Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         10,999
```

Step 3: Verify that traffic can successfully cross the trunk link.

- a. From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

- b. From the console session on S1, ping the management address of S2. Were the pings successful? Why?

- c. From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

- d. From a command prompt on PC-C, ping the management addresses on S1 and S2 and the IP address of PC-A. Were you successful? Why?

Step 4: Prevent the use of DTP on S1 and S2.

Cisco uses a proprietary protocol known as the Dynamic Trunking Protocol (DTP) on its switches. Some ports automatically negotiate to trunking. A good practice is to turn off negotiation. You can see this default behavior by issuing the following command:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

- a. Turn off negotiation on S1.
S1(config)# **interface f0/1**
S1(config-if)# **switchport nonegotiate**
- b. Turn off negotiation on S2.
S2(config)# **interface f0/1**
S2(config-if)# **switchport nonegotiate**
- c. Verify that negotiation is off by issuing the **show interface f0/1 switchport** command on S1 and S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<Output Omitted>
```

Step 5: Secure access ports on S1 and S2.

Even though you shut down unused ports on the switches, if a device is connected to one of those ports and the interface is enabled, trunking could occur. In addition, all ports by default are in VLAN 1. A good practice is to put all unused ports in a “black hole” VLAN. In this step, you will disable trunking on all unused ports. You will also assign unused ports to VLAN 999. For the purposes of this lab, only ports 2 through 5 will be configured on both switches.

- a. Issue the **show interface f0/2 switchport** command on S1. Notice the administrative mode and state for trunking negotiation.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

- b. Disable trunking on S1 access ports.

```
S1(config)# interface range f0/2 - 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

- c. Disable trunking on S2 access ports.

- d. Verify that port F0/2 is set to access on S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>
```

- e. Verify that VLAN port assignments on both switches are correct. S1 is shown below as an example.

```
S1# show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10

```

Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gi0/1, Gi0/2

10    Data                                active
99    Management&Native                  active    Fa0/6
999   BlackHole                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002  fddi-default                       act/unsup
1003  token-ring-default                 act/unsup
1004  fddinet-default                   act/unsup
1005  trnet-default                     act/unsup
Restrict VLANs allowed on trunk ports.

```

By default, all VLANs are allowed to be carried on trunk ports. For security reasons, it is a good practice to only allow specific desired VLANs to cross trunk links on your network.

- f. Restrict the trunk port F0/1 on S1 to only allow VLANs 10 and 99.

```

S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99

```

- g. Restrict the trunk port F0/1 on S2 to only allow VLANs 10 and 99.

- h. Verify the allowed VLANs. Issue a **show interface trunk** command in privileged EXEC mode on both S1 and S2.

```

S1# show interface trunk

```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	99

Port	Vlans allowed on trunk
Fa0/1	10,99

Port	Vlans allowed and active in management domain
Fa0/1	10,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	10,99

What is the result?

Reflection

What, if any, are the security problems with the default configuration of a Cisco switch?

Activity 13a - VLAN Plan

Objective

Implement VLANs to segment a small- to medium-sized network.

Scenario

You are designing a VLAN switched network for your small- to medium- sized business.

Your business owns space on two floors of a high-rise building. The following elements need VLAN consideration and access for planning purposes:

- Management
- Finance
- Sales
- Human Resources
- Network administrator
- General visitors to your business location

You have two Cisco 3560-24PS switches.

Use a word processing software program to design your VLAN-switched network scheme.

Section 1 of your design should include the regular names of your departments, suggested VLAN names and numbers, and which switch ports would be assigned to each VLAN.

Section 2 of your design should list how security would be planned for this switched network.

Once your VLAN plan is finished, complete the reflection questions from this activity.

Save your work. Be able to explain and discuss your VLAN design with another group or with the class.

Required Resources

Word processing program

Reflection

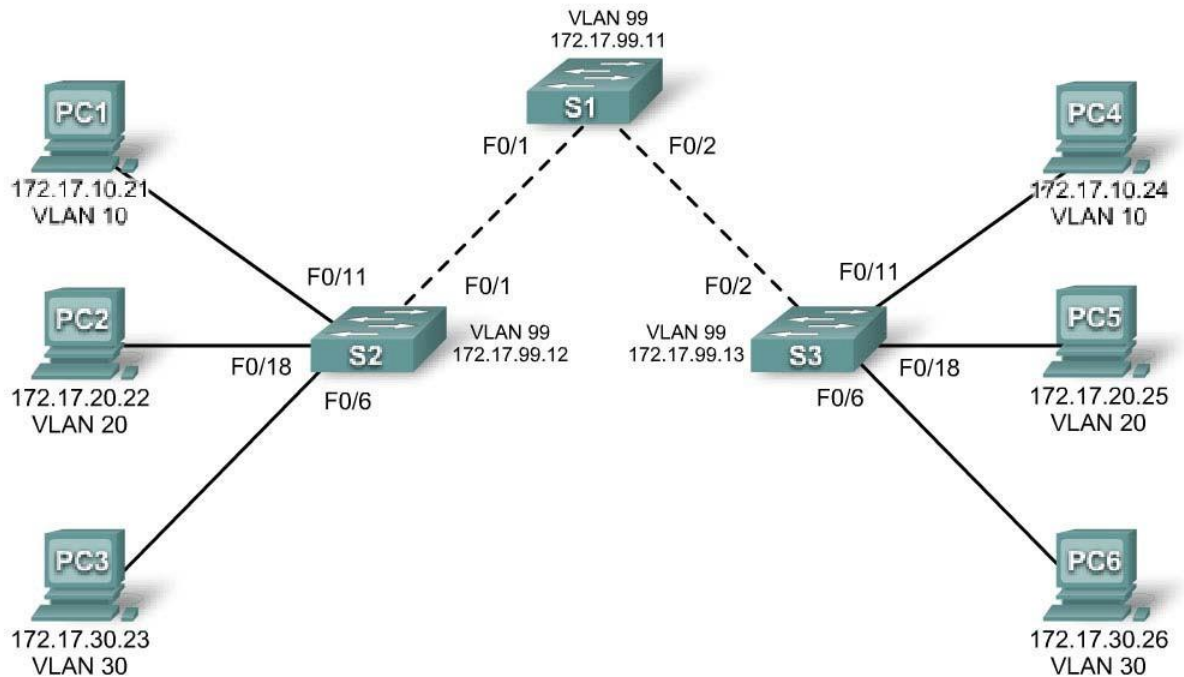
1. What criteria did you use for assigning ports to the VLANs?

2. How could these users access your network if the switches were not physically available to general users via direct connection?

3. Could you reduce the number of switch ports assigned for general users if you used another device to connect them to the VLAN network switch? What would be affected?

Lab 14: Basic VTP Configuration

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a switch to the default state
- Perform basic configuration tasks on a switch
- Configure VLAN Trunking Protocol (VTP) on all switches
- Enable trunking on inter-switch connections
- Verify trunk configuration
- Modify VTP modes and observe the impact
- Create VLANs on the VTP server, and distribute this VLAN information to switches in the network
- Explain the differences in operation between VTP transparent mode, server mode, and client mode
- Assign switch ports to the VLANs
- Save the VLAN configuration
- Enable VTP pruning on the network
- Explain how pruning reduces unnecessary broadcast traffic on the LAN

Task 1: Prepare the Network**Step 1: Cable a network that is similar to the one in the topology diagram.**

You can use any current switch in your lab as long as it has the required interfaces shown in the topology. The output shown in this lab is based on 2960 switches. Other switch types may produce different output. If you are using older switches, then some commands may be different or unavailable.

You will notice in the Addressing Table that the PCs have been configured with a default gateway IP address. This would be the IP address of the local router which is not included in this lab scenario. The default gateway, the router would be needed for PCs in different VLANs to be able to communicate. This is discussed in a later chapter.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations and VLANs. Use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Step 3: Disable all ports by using the shutdown command.

Repeat these commands for each switch in the topology.

```
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Step 1: Complete basic configuration of switches S1, S2, and S3.

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure the switch hostname as indicated on the topology.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

(Output for S1 shown)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
```

```
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Step 2: Re-enable the user ports on S2 and S3.

Configure the user ports in access mode. Refer to the topology diagram to determine which ports are connected to end-user devices.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

```
S3(config)#interface fa0/6
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/11
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
```

Step 3: Re-enable the trunk ports on S1, S2 and S3

```
S1(config)#interface fa0/1
S1(config-if)#no shutdown
S1(config)#interface fa0/2
S1(config-if)#no shutdown
```

```
S2(config)#interface fa0/1
S2(config-if)#no shutdown
```

```
S3(config)#interface fa0/2
S3(config-if)#no shutdown
```

Task 3: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, PC5, and PC6 with the IP addresses and default gateways indicated in the addressing table at the beginning of the lab.

Verify that PC1 can ping PC4, PC2 can ping PC5, and that PC3 can ping PC6.

Task 4: Configure VTP on the Switches

VTP allows the network administrator to control the instances of VLANs on the network by creating VTP domains. Within each VTP domain, one or more switches are configured as VTP servers. VLANs are then created on the VTP server and pushed to the other switches in the domain. Common VTP configuration tasks are setting the operating mode, domain, and password. In this lab, you will be using S1 as the VTP server, with S2 and S3 configured as VTP clients or in VTP transparent mode.

Step 1: Check the current VTP settings on the three switches.

S1#**show vtp status**

```
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

S2#**show vtp status**

```
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

S3#**show vtp status**

```
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 5
VTP Operating Mode          : Server
VTP Domain Name             :
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
```

```
MD5 digest                : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Note that all three switches are in server mode. Server mode is the default VTP mode for most Catalyst switches.

Step 2: Configure the operating mode, domain name, and VTP password on all three switches.

Set the VTP domain name to **Lab4** and the VTP password to **cisco** on all three switches. Configure S1 in server mode, S2 in client mode, and S3 in transparent mode.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end
```

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end
```

```
S3(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S3(config)#vtp domain Lab4
Changing VTP domain name from NULL to Lab4
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Note: The VTP domain name can be learned by a client switch from a server switch, but only if the client switch domain is in the null state. It does not learn a new name if one has been previously set. For that reason, it is good practice to manually configure the domain name on all switches to ensure that the domain name is configured correctly. Switches in different VTP domains do not exchange VLAN information.

Step 3: Configure trunking and the native VLAN for the trunking ports on all three switches.

Use the **interface range** command in global configuration mode to simplify this task.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

```
S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
```

```
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Step 4: Configure port security on the S2 and S3 access layer switches.

Configure ports fa0/6, fa0/11, and fa0/18 so that they allow only a single host and learn the MAC address of the host dynamically.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
```

```
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end
```

```
S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Step 5: Configure VLANs on the VTP server.

There are four additional VLANs required in this lab:

- VLAN 99 (management)
- VLAN 10 (faculty/staff)

- VLAN 20 (students)
- VLAN 30 (guest)

Configure these on the VTP server.

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
```

Verify that the VLANs have been created on S1 with the **show vlan brief** command.

Step 6: Check if the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to determine if the VTP server has pushed its VLAN configuration to all the switches.

S2#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10	faculty/staff	active	
20	students	active	
30	guest	active	
99	management	active	

S3#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17

```

Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gi0/1
Gi0/2
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
```

Are the same VLANs configured on all switches? _____

Explain why S2 and S3 have different VLAN configurations at this point. _____

Step 7: Create a new VLAN on switch 2 and 3.

```
S2(config)#vlan 88
%VTP VLAN configuration not allowed when device is in CLIENT mode.
```

```
S3(config)#vlan 88
S3(config-vlan)#name test
S3(config-vlan)#
```

Why are you prevented from creating a new VLAN on S2 but not S3? _____

Delete VLAN 88 from S3.

```
S3(config)#no vlan 88
```

Step 8: Manually configure VLANs.

Configure the four VLANs identified in Step 5 on switch S3.

```
S3(config)#vlan 99
S3(config-vlan)#name management
S3(config-vlan)#exit
S3(config)#vlan 10
S3(config-vlan)#name faculty/staff
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name students
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name guest
S3(config-vlan)#exit
```

Here you see one of the advantages of VTP. Manual configuration is tedious and error prone, and any error introduced here could prevent intra-VLAN communication. In addition, these types of errors can be difficult to troubleshoot.

Step 9: Configure the management interface address on all three switches.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? _____ If
not, troubleshoot the switch configurations and try again.

Step 10: Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the lab to assign ports to the VLANs. Use the **interface range** command to simplify this task. Port assignments are not configured through VTP. Port assignments must be configured on each switch manually or dynamically using a VMPS server. The commands are shown for S3 only, but both S2 and S1 switches should be similarly configured. Save the configuration when you are done.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...

[OK]

S3#
```

Task 5: Configure VTP Pruning on the Switches

VTP pruning allows a VTP server to suppress IP broadcast traffic for specific VLANs to switches that do not have any ports in that VLAN. By default, all unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is used to eliminate or prune this unnecessary traffic. Pruning saves LAN bandwidth because broadcasts do not have to be sent to switches that do not need them.

Pruning is configured on the server switch with the **vtp pruning** command in global configuration mode. The configuration is pushed to client switches.

Confirm VTP pruning configuration on each switch using the **show vtp status** command. VTP pruning mode should be enabled on each switch.

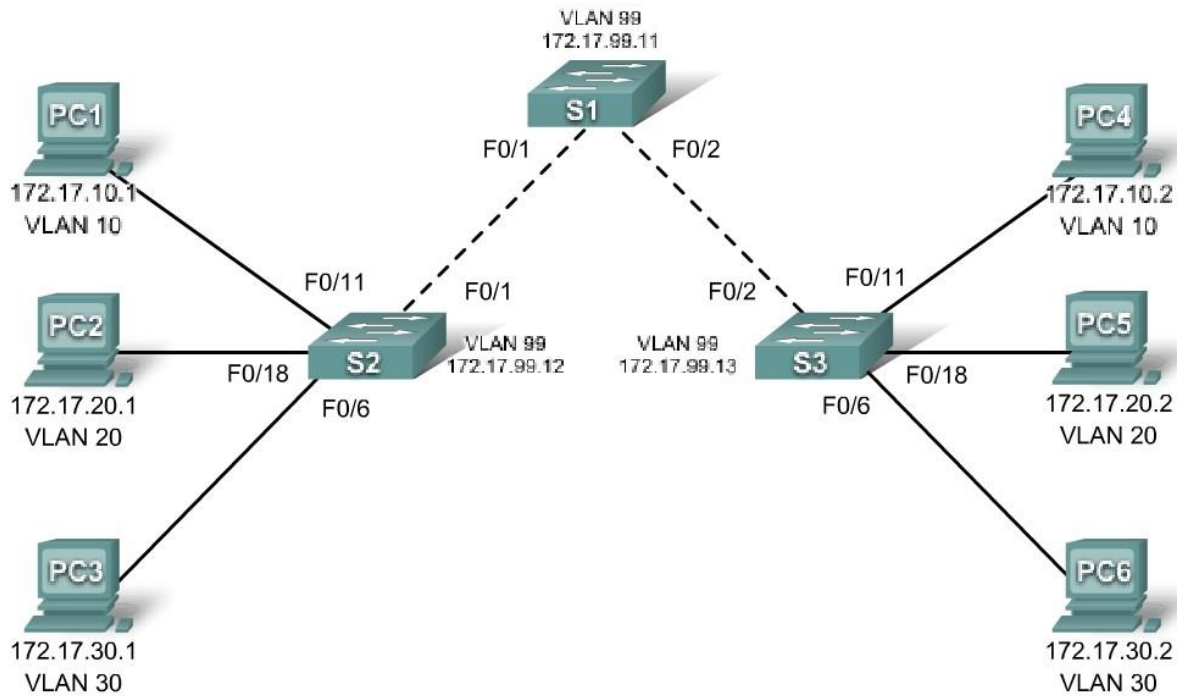
```
S1#show vtp status
VTP Version                : 2
Configuration Revision      : 17
Maximum VLANs supported locally : 255
Number of existing VLANs    : 9
VTP Operating Mode          : Server
VTP Domain Name             : Lab4
VTP Pruning Mode            : Enabled
<output omitted>
```

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 15: Challenge VTP Configuration

Topology



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.1	255.255.255.0	
PC2	NIC	172.17.20.1	255.255.255.0	
PC3	NIC	172.17.30.1	255.255.255.0	
PC4	NIC	172.17.10.2	255.255.255.0	
PC5	NIC	172.17.20.2	255.255.255.0	
PC6	NIC	172.17.30.2	255.255.255.0	

Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks	
Fa0/11 – 0/17	VLAN 10 – engineering	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – sales	172.17.20.0 /24
Fa0/6 – 0/10	VLAN 30 – administration	172.17.30.0 /24
None	VLAN 99 – network management	172.17.99.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram.
- Erase the startup configuration and reload a switch to the default state.
- Perform basic configuration tasks on a switch.
- Configure VLAN Trunking Protocol (VTP) on all switches.
- Enable trunking on inter-switch connections.
- Verify trunk configuration.
- Modify VTP modes and observe the impact.
- Create VLANs on the VTP server, and distribute this VLAN information to switches in the network.
- Explain the differences in operation between VTP transparent mode, server mode, and client mode.
- Assign switch ports to the VLANs.
- Save the VLAN configuration.

Task 1: Prepare the Network**Step 1: Cable a network that is similar to the one in the topology diagram.**

You can use any current switch in your lab as long as it has the required interfaces shown in the topology diagram. The output shown in this lab is based on 2960 switches. Other switch types may produce different output. If you are using older switches, then some commands may be different or unavailable.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

Erase existing configurations, VLANs, and reload the switch. Use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Step 3: Disable all ports by using the shutdown command.**Task 2: Perform Basic Switch Configurations.**

Step 1: Complete basic configuration of switches S1, S2, and S3.

Configure the S1, S2, and S3 switches according to the following guidelines and save all your configurations:

- Configure the switch hostname as indicated on the topology.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Save running-configuration to startup-configuration.

Step 2: Re-enable the user ports on S2 and S3 and put those ports in access mode. Refer to the topology diagram to determine which ports are connected to end-user devices.

Task 3: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1 through PC6 with the IP addresses indicated in the addressing table at the beginning of the lab.

Task 4: Configure VTP on the Switches

VTP allows the network administrator to control the instances of VLANs on the network by creating VTP domains. Within each VTP domain, one or more switches are configured as VTP servers. VLANs are then created on the VTP server and pushed to the other switches in the domain. Common VTP configuration tasks are operating mode, domain, and password. In this lab, you will be configuring S1 as a VTP server, with S2 and S3 configured as VTP clients.

Step 1: Check the current VTP settings on the three switches.

What is the current (default) VTP operating mode on the switches? _____

What is the configuration revision on S1 and S2? _____

Step 2: Configure the operating mode, the domain name, and VTP password on all three switches.

Set the VTP domain name to **access** and the VTP password to **lab4** on all three switches. Configure S1 in server mode, and S2 and S3 in client mode.

Note: The VTP domain name can be learned by a client switch from a server switch, but only if the client switch domain is in the null state. It does not learn a new name if one has been previously set. For that reason, it is good practice to manually configure the domain name on all switches to ensure that the domain name is configured correctly. Switches in different VTP domains do not exchange VLAN information. Recall that VTP domain names and passwords are case-sensitive.

Step 3: Configure trunking and the native VLAN for the trunking ports on all three switches.

Configure ports Fa0/1 through Fa0/5 in trunking mode. Configure VLAN 99 as the native VLAN for these trunks. You can use the **interface range** command to simplify this task. Do not forget to enable the trunk interfaces.

Step 4: Configure port security on the S2 and S3 access ports.

Configure ports Fa0/6, Fa0/11, and Fa0/18 on S2 and S3 so that they allow a maximum of two hosts to connect to these ports and learn the MAC addresses of the hosts dynamically.

Step 5: Configure VLANs on the VTP server.

There are four VLANs required in this lab:

1. VLAN 99 (network management)
2. VLAN 10(engineering)
3. VLAN 20 (sales)
4. VLAN 30 (administration)

Configure these VLANs only on the VTP server.

When you are done, verify that all four VLANs have been created on S1.

Step 6: Check if the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to determine if the VTP server has pushed its VLAN configuration to all these switches.

Are the same VLANs configured on all switches? _____

Explain why S2 and S3 have the same VLAN configurations at this point. _____

Step 7: Configure the management interface address on all three switches according to the addressing table at the beginning of the lab.

Assign these addresses to the network management VLAN (VLAN 99).

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and resolve.

Step 8: Assign switch ports to VLANs.

Refer to the port assignment table at the beginning of the lab to assign ports to VLANs. Use the **interface range** command to simplify this task. Note that port assignments are not configured through VTP. Port assignments must be configured on each switch manually or dynamically using a VMPs server. Save the configuration when you are done.

Step 9: Verify that the trunks are operating correctly.

From PC1, attempt to ping PC4, PC5, and PC6.

Were any of the pings successful? _____

Why did some of the pings fail? _____

Which hosts could be reached from PC3? _____

Task 5: Configure VTP Pruning on the Switches

VTP pruning allows a VTP server to suppress IP broadcast traffic for specific VLANs to switches that do not have any ports in that VLAN. By default, all unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning eliminates or prunes this unnecessary traffic. Pruning saves LAN bandwidth because broadcasts do not have to be sent to switches that do not need them.

Configure pruning on the server switch, which is then pushed to client switches.

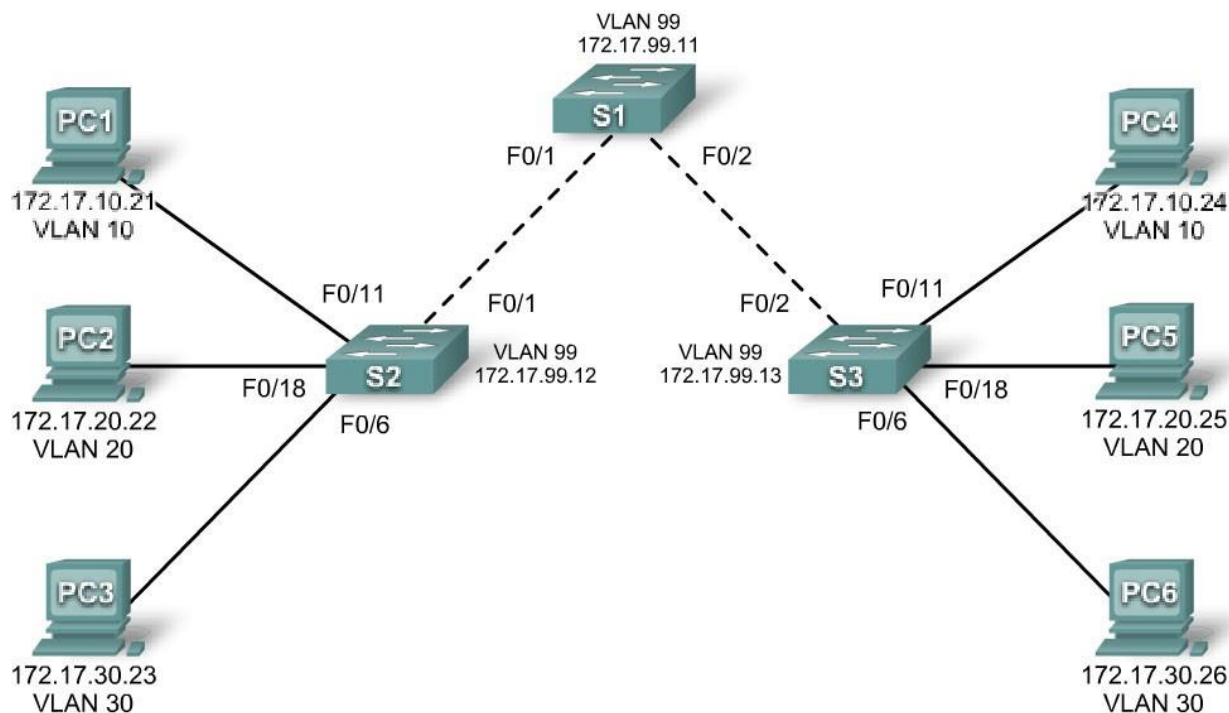
Confirm the VTP pruning configuration on each switch using the **show vtp status** command. VTP pruning mode should show “Enabled” on each switch.

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 16: Troubleshooting VTP Configuration

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask
S1	VLAN 99	172.17.99.11	255.255.255.0
S2	VLAN 99	172.17.99.12	255.255.255.0
S3	VLAN 99	172.17.99.13	255.255.255.0
PC1	NIC	172.17.10.21	255.255.255.0
PC2	NIC	172.17.20.22	255.255.255.0
PC3	NIC	172.17.30.23	255.255.255.0
PC4	NIC	172.17.10.24	255.255.255.0
PC5	NIC	172.17.20.25	255.255.255.0
PC6	NIC	172.17.30.26	255.255.255.0

Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and vlan.dat files and reload switches to the default state
- Load the switches with supplied scripts
- Find and correct all configuration errors
- Document the corrected network

Scenario

The VLAN Trunking Protocol (VTP) helps ensure uniform VLAN configurations on your switched network, but it must be configured correctly. In this lab, you will use the supplied scripts to configure S1 as a VTP server, and S2 and S3 as VTP clients. The VTP domain name is Lab4_3, and the VTP password is cisco. However, there are a number of errors in this configuration that you must troubleshoot and correct before end-to-end connectivity within the VLAN is restored.

You will have successfully resolved all errors when the same VLANs are configured on all three switches, and you can ping between any two hosts in the same VLAN or between any two switches.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology diagram. The output shown in this lab is based on 2960 switches. Other switch types may produce different output. If you are using older switches, then some commands may be different or unavailable.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

Clear switch configurations and VLANs on all three switches and reload them to restore the default state. Use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Step 3: Configure the Ethernet interfaces on the host PCs.

Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, PC5, and PC6 with the IP addresses indicated in the addressing table at the beginning of the lab. There is no need to configure the default gateways for this lab.

Task 2: Load Switches with Supplied Scripts

S1 Configuration

```
enable
!
config term
hostname S1
enable secret class no
ip domain-lookup
!
vtp mode server
vtp domain Lab4_3 vtp
password Cisco
!
vlan 99
name management
exit
!
vlan 10
name Faculty/Staff exit
!
vlan 20
name Students exit
!
vlan 30 name
Guest exit
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/2 switchport
trunk native vlan 99 switchport mode
access
!
interface FastEthernet0/3 switchport
trunk native vlan 99 switchport mode
access
!
interface FastEthernet0/4 switchport
trunk native vlan 99 switchport mode
trunk
!
```

```
interface FastEthernet0/5 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface range FastEthernet0/6-24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan99
  ip address 179.17.99.11 255.255.255.0 no
  shutdown
!
line con 0
  logging synchronous
  password cisco
  login
line vty 0 no
  login
line vty 1 4
  password cisco
  login
line vty 5 15
  password cisco
  login
!
end
```

S2 Configuration

```
hostname S2
!
enable secret class no
ip domain-lookup
!
vtp mode client
vtp domain Lab4
!
!
interface FastEthernet0/1 switchport
  trunk native vlan 99 switchport mode
  access
!
```

```
interface FastEthernet0/2 switchport
  trunk native vlan 99 switchport mode
  access
!
interface FastEthernet0/3 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface FastEthernet0/4 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface FastEthernet0/5
  switchport trunk native vlan 99
  switchport mode trunk
!
interface range FastEthernet0/6 - 10
  switchport access vlan 10
!
switchport mode access
!
interface range FastEthernet0/11 - 17
  switchport access vlan 20
switchport mode access
!
interface range FastEthernet0/18 - 24
  switchport access vlan 30
  switchport mode access
!
interface Vlan99
  ip address 172.17.99.12 255.255.255.0 no
  shutdown
!
ip http server
!
line con 0 password
  cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  login
line vty 5 15
  password cisco
```

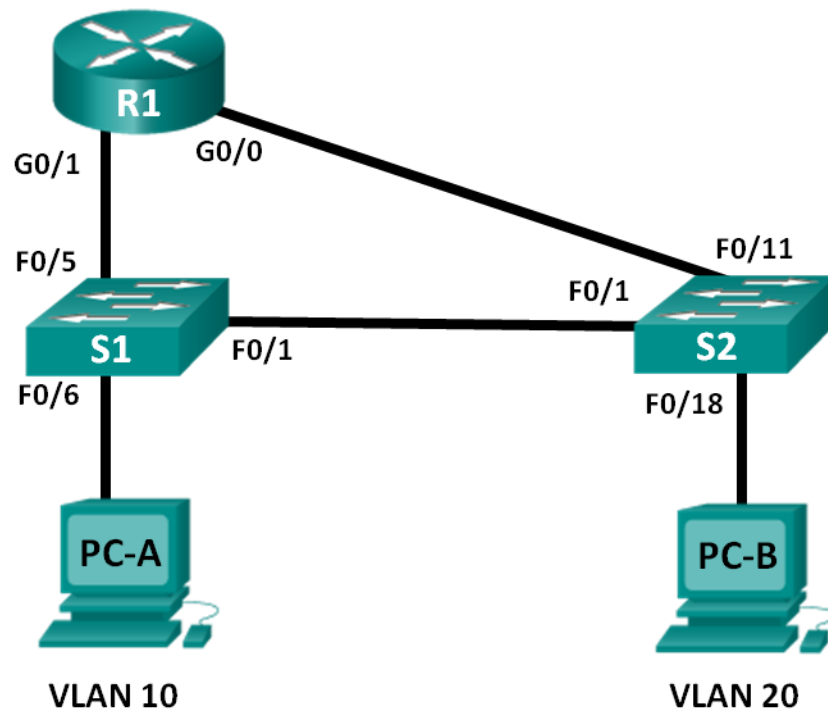
S3 Configuration

```
hostname S3
!
```

```
enable secret class no
ip domain-lookup
!
vtp mode client vtp
domain Lab4
!
!
interface FastEthernet0/1 switchport
trunk native vlan 99 switchport mode
trunk
!
interface FastEthernet0/2 switchport
trunk native vlan 99 switchport mode
trunk
!
interface FastEthernet0/3 switchport
trunk native vlan 99 switchport mode
trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/5 switchport
trunk native vlan 99 switchport mode
trunk
!
interface range FastEthernet0/6 - 10
switchport access vlan 30
```

Lab 17 – Configuring Per-Interface Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	192.168.10.1	255.255.255.0	N/A
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Switches with VLANs and Trunking

Part 3: Verify Trunking, VLANs, Routing, and Connectivity

Background / Scenario

Legacy inter-VLAN routing is seldom used in today's networks; however, it is helpful to configure and understand this type of routing before moving on to router-on-a-stick (trunk-based) inter-VLAN routing or

configuring Layer-3 switching. Also, you may encounter per-interface inter-VLAN routing in organizations with very small networks. One of the benefits of legacy inter-VLAN routing is ease of configuration.

In this lab, you will set up one router with two switches attached via the router Gigabit Ethernet interfaces. Two separate VLANs will be configured on the switches, and you will set up routing between the VLANs.

Note: This lab provides minimal assistance with the actual commands necessary to configure the router and switches. The required switch VLAN configuration commands are provided in Appendix A of this lab. Test your knowledge by trying to configure the devices without referring to the appendix.

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)
- 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 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 clear any configurations, if necessary.

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

Step 2: Initialize and reload the router and switches.

Step 3: Configure basic settings for R1.

- Disable DNS lookup.
- Assign the device name.
- Assign **class** as the privileged EXEC mode encrypted password.
- Assign **cisco** as the console and vty line password and enable login.
- Configure addressing on G0/0 and G0/1 and enable both interfaces.

Step 4: Configure basic settings on S1 and S2.

- Disable DNS lookup.
- Assign the device name.
- Assign **class** as the privileged EXEC mode encrypted password.
- Assign **cisco** as the console and vty line password and enable login.

Step 5: Configure basic settings on PC-A and PC-B.

Configure PC-A and PC-B with IP addresses and a default gateway address according to the Addressing Table.

Part 2: Configure Switches with VLANs and Trunking

In Part 2, you will configure the switches with VLANs and trunking.

Step 1: Configure VLANs on S1.

- On S1, create VLAN 10. Assign **Student** as the VLAN name.
- Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
- Configure F0/1 as a trunk port.
- Assign ports F0/5 and F0/6 to VLAN 10 and configure both F0/5 and F0/6 as access ports.
- Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
- Configure the default gateway according to the Addressing Table.

Step 2: Configure VLANs on S2.

- On S2, create VLAN 10. Assign **Student** as the VLAN name.
- Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
- Configure F0/1 as a trunk port.
- Assign ports F0/11 and F0/18 to VLAN 20 and configure both F0/11 and F0/18 as access ports.
- Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
- Configure the default gateway according to the Addressing Table.

Part 3: Verify Trunking, VLANs, Routing, and Connectivity**Step 1: Verify the R1 routing table.**

- On R1, issue the **show ip route** command. What routes are listed on R1?

- On both S1 and S2, issue the **show interface trunk** command. Is the F0/1 port on both switches set to trunk?

- Issue a **show vlan brief** command on both S1 and S2. Verify that VLANs 10 and 20 are active and that the proper ports on the switches are in the correct VLANs. Why is F0/1 not listed in any of the active VLANs?

- Ping from PC-A in VLAN 10 to PC-B in VLAN 20. If Inter-VLAN routing is functioning correctly, the pings between the 192.168.10.0 network and the 192.168.20.0 should be successful.
Note: It may be necessary to disable the PC firewall to ping between PCs.
- Verify connectivity between devices. You should be able to ping between all devices. Troubleshoot if you are not successful.

Reflection

What is an advantage of using legacy inter-VLAN routing?

Router Interface Summary Table

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

Appendix A: Configuration Commands

Switch S1

```

S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name Faculty-Admin
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface range f0/5 - 6
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# interface vlan 10

```

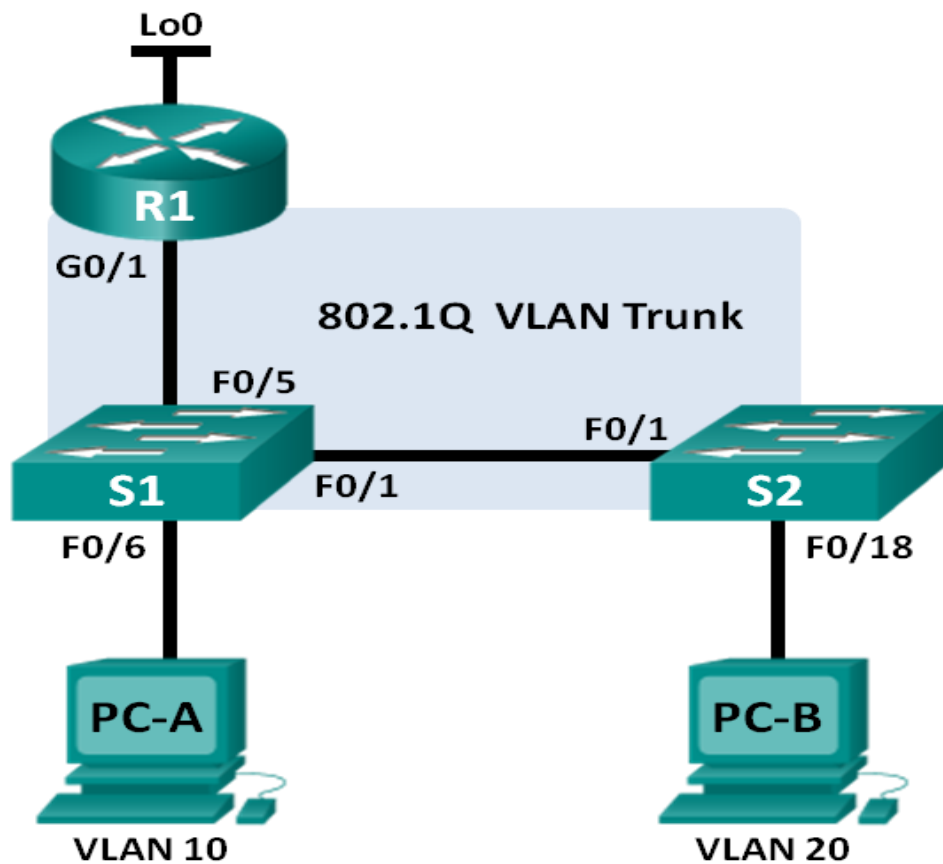
```
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1
```

Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name Student
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name Faculty-Admin
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/11
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if-range)# interface vlan 10
S2(config-if)# ip address 192.168.10.12 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.10.1
```

Lab 18 – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
S1 F0/1	802.1Q Trunk	N/A
S2 F0/1	802.1Q Trunk	N/A
S1 F0/5	802.1Q Trunk	N/A
S1 F0/6	VLAN 10 – Students	192.168.10.0/24
S2 F0/18	VLAN 20 – Faculty	192.168.20.0/24

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Switches with VLANs and Trunking

Part 3: Configure Trunk-Based Inter-VLAN Routing

Background / Scenario

A second method of providing routing and connectivity for multiple VLANs is through the use of an 802.1Q trunk between one or more switches and a single router interface. This method is also known as router-on-a-stick inter-VLAN routing. In this method, the physical router interface is divided into multiple subinterfaces that provide logical pathways to all VLANs connected.

In this lab, you will configure trunk-based inter-VLAN routing and verify connectivity to hosts on different VLANs as well as with a loopback on the router.

Note: This lab provides minimal assistance with the actual commands necessary to configure trunk-based inter-VLAN routing. However, the required configuration commands are provided in Appendix A of this lab. Test your knowledge by trying to configure the devices without referring to the appendix.

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.

Required Resources

- 1 Router (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 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, switches, and router.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the router and switches as necessary.

Step 4: Configure basic settings for each switch.

- a. Disable DNS lookup.
- b. Configure device names as shown in the topology.
- c. Assign **class** as the privileged EXEC password.
- d. Assign **cisco** as the console and vty passwords.
- e. Configure **logging synchronous** for the console line.
- f. Configure the IP address listed in the Addressing Table for VLAN 1 on both switches.
- g. Configure the default gateway on both switches.
- h. Administratively deactivate all unused ports on the switch.
- i. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for the router.

- a. Disable DNS lookup.
- b. Configure device names as shown in the topology.
- c. Configure the Lo0 IP address as shown in the Address Table. Do not configure subinterfaces at this time as they will be configured in Part 3.
- d. Assign **cisco** as the console and vty passwords.
- e. Assign **class** as the privileged EXEC password.
- f. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- g. Copy the running configuration to the startup configuration.

Part 2: Configure Switches with VLANs and Trunking

In Part 2, you will configure the switches with VLANs and trunking.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure S1 and S2 without referring to the appendix.

Step 1: Configure VLANs on S1.

- a. On S1, configure the VLANs and names listed in the Switch Port Assignment Specifications table. Write the commands you used in the space provided.

- b. On S1, configure the interface connected to R1 as a trunk. Also configure the interface connected to S2 as a trunk. Write the commands you used in the space provided.

- c. On S1, assign the access port for PC-A to VLAN 10. Write the commands you used in the space provided.

Step 2: Configure VLANs on Switch 2.

- a. On S2, configure the VLANs and names listed in the Switch Port Assignment Specifications table.
- b. On S2, verify that the VLAN names and numbers match those on S1. Write the command you used in the space provided.

- c. On S2, assign the access port for PC-B to VLAN 20.
- d. On S2, configure the interface connected to S1 as a trunk.

Part 3: Configure Trunk-Based Inter-VLAN Routing

In Part 3, you will configure R1 to route to multiple VLANs by creating subinterfaces for each VLAN. This method of inter-VLAN routing is called router-on-a-stick.

Note: The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure trunk-based or router-on-a-stick inter-VLAN routing without referring to the appendix.

Step 1: Configure a subinterface for VLAN 1.

- a. Create a subinterface on R1 G0/1 for VLAN 1 using 1 as the subinterface ID. Write the command you used in the space provided.

- b. Configure the subinterface to operate on VLAN 1. Write the command you used in the space provided.

- c. Configure the subinterface with the IP address from the Address Table. Write the command you used in the space provided.

Step 2: Configure a subinterface for VLAN 10.

- a. Create a subinterface on R1 G0/1 for VLAN 10 using 10 as the subinterface ID.
- b. Configure the subinterface to operate on VLAN 10.
- c. Configure the subinterface with the address from the Address Table.

Step 3: Configure a subinterface for VLAN 20.

- a. Create a subinterface on R1 G0/1 for VLAN 20 using 20 as the subinterface ID.
- b. Configure the subinterface to operate on VLAN 20.
- c. Configure the subinterface with the address from the Address Table.

Step 4: Enable the G0/1 interface.

Enable the G0/1 interface. Write the commands you used in the space provided.

Step 5: Verify connectivity.

Enter the command to view the routing table on R1. What networks are listed?

From PC-A, is it possible to ping the default gateway for VLAN 10? _____

From PC-A, is it possible to ping PC-B? _____

From PC-A, is it possible to ping Lo0? _____

From PC-A, is it possible to ping S2? _____

If the answer is **no** to any of these questions, troubleshoot the configurations and correct any errors.

Reflection

What are the advantages of trunk-based or router-on-a-stick inter-VLAN routing?

Router Interface Summary Table

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

Appendix A – Configuration Commands**Switch S1**

```

S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10

```

Switch S2

```

S2(config)# vlan 10
S2(config-vlan)# name Students
S2(config-vlan)# vlan 20
S2(config-vlan)# name Faculty
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk

```

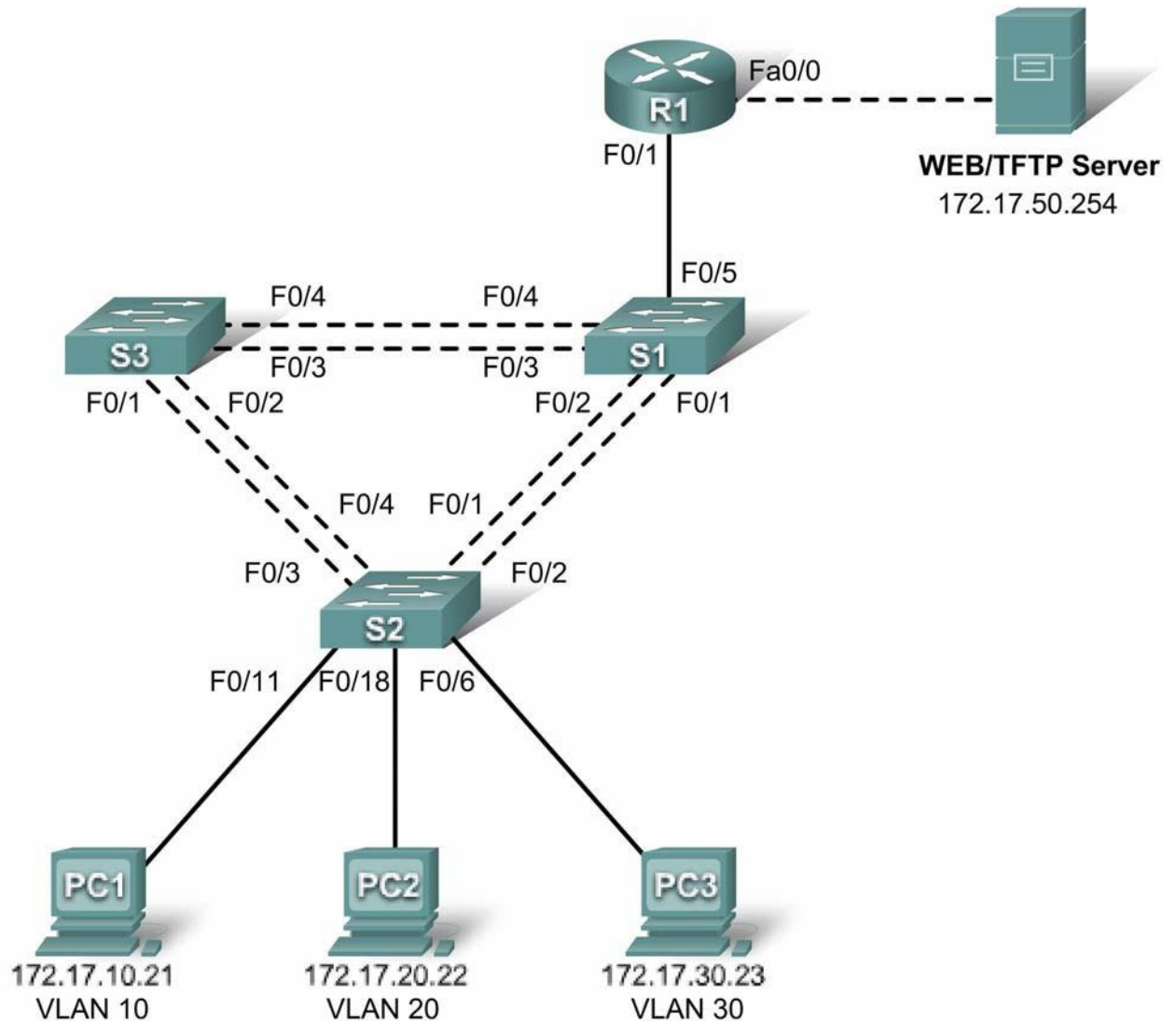
```
S2(config-if)# interface f0/18  
S2(config-if)# switchport mode access  
S2(config-if)# switchport access vlan 20
```

Router R1

```
R1(config)# interface g0/1.1  
R1(config-subif)# encapsulation dot1Q 1  
R1(config-subif)# ip address 192.168.1.1 255.255.255.0  
R1(config-subif)# interface g0/1.10  
R1(config-subif)# encapsulation dot1Q 10  
R1(config-subif)# ip address 192.168.10.1 255.255.255.0  
R1(config-subif)# interface g0/1.20  
R1(config-subif)# encapsulation dot1Q 20  
R1(config-subif)# ip address 192.168.20.1 255.255.255.0  
R1(config-subif)# exit  
R1(config)# interface g0/1  
R1(config-if)# no shutdown
```

Lab 19: Basic Inter-VLAN Routing

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
S3	VLAN 99	172.17.99.13	255.255.255.0	172.17.99.1

R1	Fa 0/0	172.17.50.1	255.255.255.0	N/A
R1	Fa 0/1	See Interface Configuration Table		N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
Server	NIC	172.17.50.254	255.255.255.0	172.17.50.1

Port Assignments – Switch 2

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 - Students	172.17.20.0 /24

Interface Configuration Table – Router 1

Interface	Assignment	IP Address
Fa0/1.1	VLAN1	172.17.1.1 /24
Fa0/1.10	VLAN 10	172.17.10.1 /24
Fa0/1.20	VLAN 20	172.17.20.1 /24
Fa0/1.30	VLAN 30	172.17.30.1 /24
Fa0/1.99	VLAN 99	172.17.99.1 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Clear configurations and reload a switch and a router to the default state
- Perform basic configuration tasks on a switched LAN and router
- Configure VLANs and VLAN Trunking Protocol (VTP) on all switches
- Demonstrate and explain the impact of Layer 3 boundaries imposed by creating VLANs
- Configure a router to support 802.1q trunking on a Fast Ethernet interface
- Configure a router with subinterfaces corresponding to the configured VLANs
- Demonstrate and explain inter-VLAN routing

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

The output shown in this lab is based on 2960 switches and an 1841 router. You can use any current switches or routers in your lab as long as they have the required interfaces shown in the topology diagram. Other device types may produce different output. Note that Ethernet (10Mb) LAN interfaces on routers do not support trunking, and Cisco IOS software earlier than version 12.3 may not support trunking on Fast Ethernet router interfaces. Set up console connections to all three switches and to the router.

Step 2: Clear any existing configurations on the switches.

Clear NVRAM, delete the vlan.dat file, and reload the switches. Refer to lab 2.2.1 if necessary for the procedure. After the reload is complete, use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Switch#**show vlan**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Step 3: Disable all ports using the shutdown command.

Ensure that the initial switch port states are inactive by disabling all ports. Use the **interface range** command to simplify this task. Repeat these commands on each switch in the topology.

```
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Step 1: Configure the S1, S2, and S3 switches.

Use the addressing table and the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
 - Configure an enable secret password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
 - Configure the default gateway on each switch

Output for S1 shown

```

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class S1(config)#no ip
domain-lookup S1(config)#ip default-gateway
172.17.99.1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...

```

Step 2: Re-enable the active user ports on S2 in access mode.

```

S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown

```

Task 3: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3 and the remote TFTP/Web Server with the IP addresses from the addressing table.

Task 4: Configure VTP on the Switches

Step 1: Configure VTP on the three switches using the following table. Remember that VTP domain names and passwords are case-sensitive.

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab6	cisco
S2	Client	Lab6	cisco
S3	Client	Lab6	cisco

S1:

```
S1(config)#vtp mode server Device
mode already VTP SERVER.
S1(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end
```

S2:

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end
```

S3:

```
S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Step 2: Configure trunking ports and designate the native VLAN for the trunks.

Configure Fa0/1 through Fa0/5 as trunking ports, and designate VLAN 99 as the native VLAN for these trunks. Use the **interface range** command in global configuration mode to simplify this task.

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end
```

```

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end

```

Step 3: Configure VLANs on the VTP server.

Configure the following VLANs on the VTP server:

VLAN	VLAN Name
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

```

S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit S1(config)#vlan 10
S1(config-vlan)#name faculty-staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#end

```

Verify that the VLANs have been created on S1 with the **show vlan brief** command.

Step 4: Verify that the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to verify that the four VLANs have been distributed to the client switches.

```
S2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10	faculty-staff	active	
20	students	active	
30	guest	active	

Task 5: Configure the Router and the Remote Server LAN

Step 1: Clear the configuration on the router and reload.

```
Router#erase nvram:
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
Erase of nvram: complete
Router#reload
System configuration has been modified. Save? [yes/no]: no
```

Step 2: Create a basic configuration on the router.

- Configure the router with hostname R1.
- Disable DNS lookup.
- Configure an EXEC mode password of **cisco**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 3: Configure the trunking interface on R1.

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute force approach. An L3 device, either a router or a Layer 3 capable switch, is connected to a LAN switch with multiple connections—a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the L3 device is configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the L3 device, the routing table has directly connected routes for all VLANs, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, under-utilization of ports on L3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

An alternative approach is to create one or more Fast Ethernet connections between the L3 device (the router) and the distribution layer switch, and to configure these connections as dot1q trunks. This allows all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the L3 interface be configured with multiple IP addresses. This can be done by creating “virtual” interfaces, called subinterfaces, on one of the router Fast Ethernet ports and configuring them to dot1q aware.

Using the subinterface configuration approach requires these steps:

- Enter subinterface configuration mode
- Establish trunking encapsulation
- Associate a VLAN with the subinterface
- Assign an IP address from the VLAN to the subinterface

The commands are as follows:

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown

R1(config-if)#interface fastethernet 0/1.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
```

```
R1(config-if)#interface fastethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
```

```
R1(config-if)#interface fastethernet 0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
```

```
R1(config-if)#interface fastethernet 0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
```

```
R1(config-if)#interface fastethernet 0/1.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Note the following points in this configuration:

- The physical interface is enabled using the **no shutdown** command, because router interfaces are down by default. The virtual interfaces are up by default.
- The subinterface can use any number that can be described with 32 bits, but it is good practice to assign the number of the VLAN as the interface number, as has been done here.
- The native VLAN is specified on the L3 device so that it is consistent with the switches. Otherwise, VLAN 1 would be the native VLAN by default, and there would be no communication between the router and the management VLAN on the switches.

Confirm creation and status of the subinterfaces with the **show ip interface brief** command:

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

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/1.1	172.17.1.1	YES	manual	up	up
FastEthernet0/1.10	172.17.10.1	YES	manual	up	up
FastEthernet0/1.20	172.17.20.1	YES	manual	up	up
FastEthernet0/1.30	172.17.30.1	YES	manual	up	up
FastEthernet0/1.99	172.17.99.1	YES	manual	up	up

Step 4: Configure the server LAN interface on R1.

```
R1(config)# interface FastEthernet0/0
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

There are now six networks configured. Verify that you can route packets to all six by checking the routing table on R1.

```
R1#show ip route
<output omitted>
```

Gateway of last resort is not set

```
172.17.0.0/24 is subnetted, 6 subnets
C      172.17.50.0 is directly connected, FastEthernet0/0
C      172.17.30.0 is directly connected, FastEthernet0/1.30
C      172.17.20.0 is directly connected, FastEthernet0/1.20
C      172.17.10.0 is directly connected, FastEthernet0/1.10
C      172.17.1.0 is directly connected, FastEthernet0/1.1
C      172.17.99.0 is directly connected, FastEthernet0/1.99
```

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 5: Verify Inter-VLAN routing.

From PC1, verify that you can ping the remote server (172.17.50.254) and the other two hosts (172.17.20.22 and 172.17.30.23). It may take a couple of pings before the end-to-end path is established.

Are the pings successful? _____

If not, troubleshoot your configuration. Check to make sure that the default gateways have been set on all PCs and all switches. If any of the hosts have gone into hibernation, the connected interface may go down.

Task 6: Reflection

In Task 5, it was recommended that you configure VLAN 99 as the native VLAN in the router Fa0/0.99 interface configuration. Why would packets from the router or hosts fail when trying to reach the switch management interfaces if the native VLAN were left in default?

Task 7: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Final Configurations

Router 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.17.50.1
 255.255.255.0 no shutdown
!
interface
 FastEthernet0/1 no
 shutdown
!
interface
 FastEthernet0/1.1
 encapsulation dot1Q 1
 ip address 172.17.1.1 255.255.255.0
!
interface
 FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.17.20.1 255.255.255.0
!
interface
 FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 172.17.30.1 255.255.255.0
!
interface FastEthernet0/1.99
 encapsulation dot1Q 99
 native
 ip address 172.17.99.1 255.255.255.0
!
```

```
<output omitted - serial interfaces not configured>
```

```
!
```

```
line con 0
```

```
line aux 0
```

```
line vty 0
```

```
4
```

```
login
```

```
password cisco
```

```
!
```

Switch 1

```
!
```

```
hostname S1
```

```
!
```

```
enable secret class
```

```
!
```

```
no ip domain lookup
```

```
!
```

```
interface FastEthernet0/1
```

```
switchport trunk native vlan 99
```

```
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/2
```

```
switchport trunk native vlan 99
```

```
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/3
```

```
switchport trunk native vlan 99
```

```
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/4
```

```
switchport trunk native vlan 99
```

```
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/5
```

```
switchport trunk native vlan 99
```

```
switchport mode trunk
```

```
!
```

```
<output omitted - all remaining ports in shutdown>
```

```
!
```

```
interface Vlan1
```

```
no ip address
```

```
no ip route-cache
```

```
!
```

```
interface Vlan99
```

```
ip address 172.17.99.11 255.255.255.0
```

```
no shutdown
```

```
!
```

```
ip default-gateway 172.17.99.1
```

```
ip http server
```

```
!  
line con 0  
  logging synchronous  
line vty 0 4  
  login  
  password cisco  
line vty 5 15  
  login  
  password cisco
```

Switch 2

```
!  
hostname S2  
!  
enable secret class  
!  
no ip domain lookup  
!  
interface FastEthernet0/1  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/2  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/3  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/4  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/5  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
  interface FastEthernet0/6  
    switchport access vlan 30  
    switchport mode access  
!  
interface FastEthernet0/7  
  switchport access vlan 30  
!  
interface FastEthernet0/8  
  switchport access vlan 30  
!  
interface FastEthernet0/9  
  switchport access vlan 30  
!
```

```
interface FastEthernet0/10
  switchport access vlan 30
!
interface FastEthernet0/11
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/12
  switchport access vlan 10
!
interface FastEthernet0/13
  switchport access vlan 10
!
interface FastEthernet0/14
  switchport access vlan 10
!
interface FastEthernet0/15
  switchport access vlan 10
!
interface FastEthernet0/16
  switchport access vlan 10
!
interface FastEthernet0/17
  switchport access vlan 10
!
interface FastEthernet0/18
  switchport access vlan 20
!
interface FastEthernet0/19
  switchport access vlan 20
!
interface FastEthernet0/20
  switchport access vlan 20
!
interface FastEthernet0/21
  switchport access vlan 20
!
interface FastEthernet0/22
  switchport access vlan 20
!
interface FastEthernet0/23
  switchport access vlan 20
!
interface FastEthernet0/24
  switchport access vlan 20
!
interface Vlan1
  no ip address
  no ip route-cache
!
```

```
interface Vlan99
  ip address 172.17.99.12 255.255.255.0
  no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
line con 0 password
  cisco logging
  synchronous login
line vty 0 4
  password cisco
  login
line vty 5 15
  password cisco
  login
!
end
```

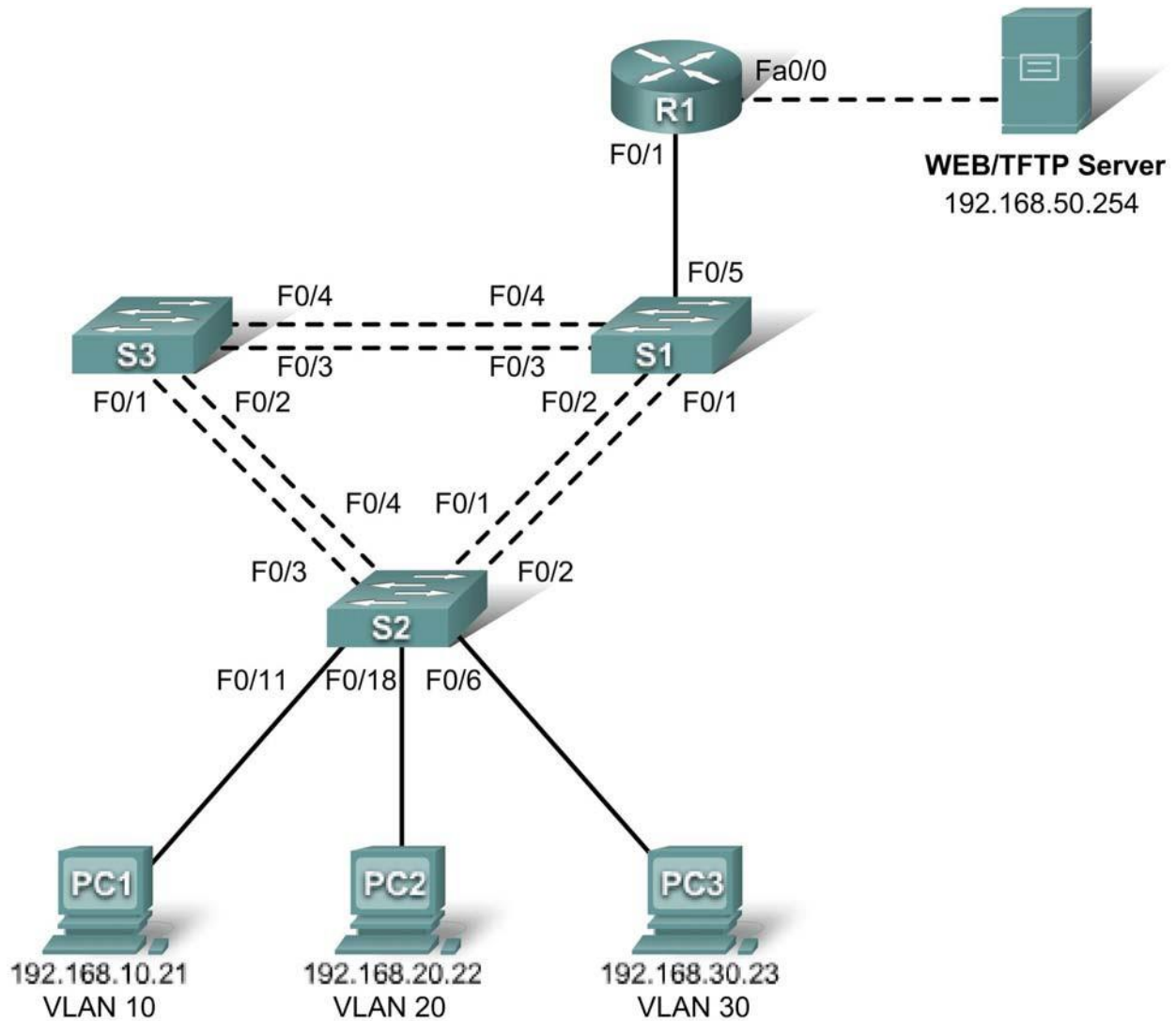
Switch 3

```
!
hostname S3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/5
  switchport trunk native vlan 99
  switchport mode trunk
!
<output omitted - all remaining ports in shutdown>
!
interface Vlan99
```

```
ip address 172.17.99.13 255.255.255.0
no shutdown
!
ip default-gateway 172.17.99.1
ip http server
!
control-plane
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

Lab 20: Challenge Inter-VLAN Routing

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.99.11	255.255.255.0	192.168.99.1
S2	VLAN 99	192.168.99.12	255.255.255.0	192.168.99.1
S3	VLAN 99	192.168.99.13	255.255.255.0	192.168.99.1
R1	Fa 0/0	192.168.50.1	255.255.255.0	N/A

R1	Fa 0/1	See Subinterface Configuration Table		N/A
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
Server	NIC	192.168.50.254	255.255.255.0	192.168.50.1

Port Assignments – Switch 2

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	192.168.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Sales	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Engineering	192.168.20.0 /24

Subinterface Configuration Table – Router 1

Router Interface	Assignment	IP Address
Fa0/1.1	VLAN1	192.168.1.1
Fa0/1.10	VLAN 10	192.168.10.1
Fa0/1.20	VLAN 20	192.168.20.1
Fa0/1.30	VLAN 30	192.168.30.1
Fa0/1.99	VLAN 99	192.168.99.1

Learning Objectives

Upon completion of this lab, you will be able to to:

- Cable a network according to the topology diagram
- Clear configurations and reload a switch and a router to the default state
- Perform basic configuration tasks on a switched LAN and a router
- Configure VLANs and VLAN Trunking Protocol (VTP) on all switches
- Configure a router to support 802.1q trunking on a Fast Ethernet interface
- Configure a router with subinterfaces corresponding to the configured VLANs
- Demonstrate inter-VLAN routing

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

The output shown in this lab is based on 2960 switches and an 1841 router. You can use any current switches or routers in your lab as long as they have the required interfaces shown in the topology diagram. Other device

types may produce different output. Note that Ethernet (10Mb) LAN interfaces on routers do not support trunking, and Cisco IOS software earlier than version 12.3 may not support trunking on Fast Ethernet router interfaces.

Set up console connections to all three switches and to the router.

Step 2: Clear any existing configurations on the switches.

Clear NVRAM, delete the vlan.dat file and reload the switches. Refer to Lab 2.2.1 if necessary for the procedure. After the reload is complete, use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Step 3: Disable all ports using the shutdown command.

Ensure that the initial switch port states are inactive by disabling all ports. Use the **interface-range** command to simplify this task. Remember to repeat the process on each switch in the topology.

Task 2: Perform Basic Switch Configurations

Step 1: Configure the S1, S2, and S3 switches.

Use the addressing table and the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Configure the default gateway on each switch.

Step 2: Re-enable the active user ports on S2 in access mode.

Enable ports Fa0/6, Fa0/11, and Fa0/18 on S2 using the **no shutdown** command, and configure them as access ports.

Task 3: Configure the Ethernet Interfaces on the Server and Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3 and the remote TFTP/Web Server with the IP addresses from the addressing table. Connect these devices using the correct cables and interfaces.

Task 4: Configure VTP on the Switches

Step 1: Configure VTP on the three switches.

Use the following table to configure the switches. Remember that VTP domain names and passwords are case-sensitive.

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab6	cisco
S2	Client	Lab6	cisco
S3	Client	Lab6	cisco

Step 2: Configure trunking ports and designate the native VLAN for the trunks.

Configure Fa0/1 through Fa0/5 as trunking ports, and designate VLAN 99 as the native VLAN for these trunks. Use the **interface range** command in global configuration mode to simplify this task.

Step 3: Configure VLANs on the VTP server.

Configure the following VLANs on the VTP server.

VLAN	VLAN Name
VLAN 99	Management
VLAN 10	R&D
VLAN 20	Engineering
VLAN 30	Sales

Verify that the VLANs have been created on S1 with the **show vlan brief** command.

Step 4: Verify that the VLANs created on S1 have been distributed to S2 and S3.

Use the **show vlan brief** command on S2 and S3 to verify that the four VLANs have been distributed to the client switches.

Step 5: Configure the Management interface address on all three switches.

Refer to the addressing table at the beginning of the lab to assign the management IP address on all three switches.

Verify that the switches are correctly configured by pinging between them. From S1, ping the Management interface on S2 and S3. From S2, ping the Management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and resolve.

Step 6: Assign switch ports to VLANs on S2.

Refer to the port assignment table at the beginning of the lab to assign ports to VLANs on S2.

Step 7: Check connectivity between VLANs.

Open command windows on the three hosts connected to S2. Ping from PC1 (192.168.10.21) to PC2 (192.168.20.22). Ping from PC2 to PC3 (192.168.30.23).

Are the pings successful? _____

If not, why do these pings fail? _____

Task 5: Configure the Router

Step 1: Clear the configuration on the router and reload.

Step 2: Create a basic configuration on the router.

- Configure the router with hostname R1.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 3: Configure the trunking interface on R1.

Configure the Fa0/1 interface on R1 with five subinterfaces, one for each VLAN identified in the Subinterface Configuration Table at the beginning of the lab. Configure these subinterfaces with dot1q encapsulation, and use the first address in each VLAN subnet on the router subinterface. Specify VLAN 99 as the native VLAN on its subinterface. Do not assign an IP address to the physical interface, but be sure to enable it. Document your subinterfaces and their respective IP addresses in the subinterface table.

Step 4: Configure the server LAN interface on R1.

Refer to the addressing table and configure Fa0/0 with the correct IP address and mask.

Step 5: Verify the routing configuration.

At this point, there should be six networks configured on R1. Verify that you can route packets to all six by checking the routing table on R1.

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 6: Verify inter-VLAN routing

From PC1, verify that you can ping the remote server (192.168.50.254) and the other two hosts (192.168.20.22 and 192.168.30.23). It may take a couple of pings before the end-to-end path is established.

Are the pings successful? _____

If not, troubleshoot your configuration. Check to make sure the default gateways have been set on all PCs and all switches. If any of the hosts have gone into hibernation, the connected interface may go down.

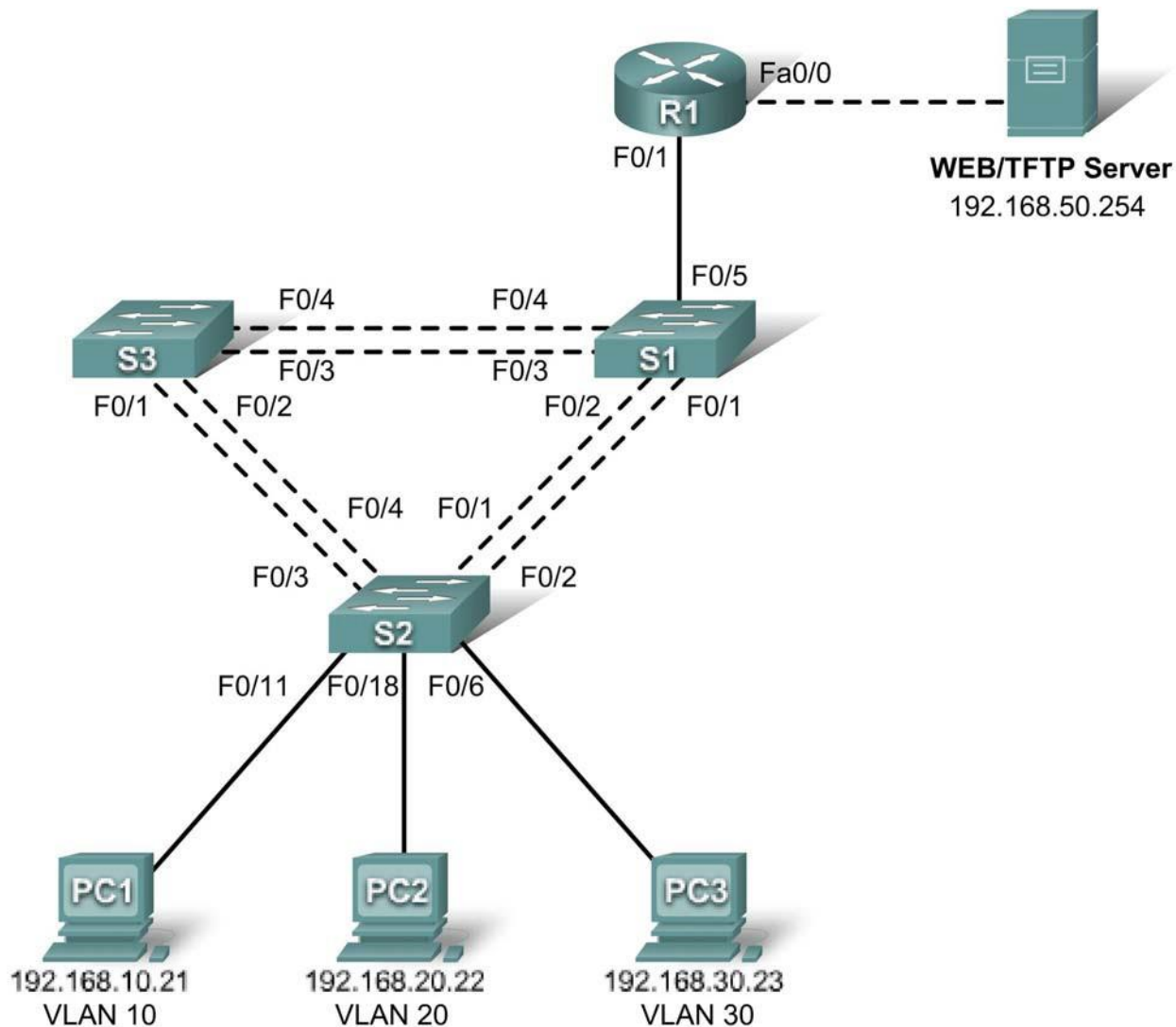
At this point, you should be able to ping any node on any of the six networks configured on your LAN, including the switch management interfaces.

Task 6: Clean Up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 21: Troubleshooting Inter-VLAN Routing

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.99.11	255.255.255.0	192.168.99.1
S2	VLAN 99	192.168.99.12	255.255.255.0	192.168.99.1
S3	VLAN 99	192.168.99.13	255.255.255.0	192.168.99.1
R1	Fa 0/0	192.168.50.1	255.255.255.0	N/A

R1	Fa 0/1	See Subinterface Configuration Table		N/A
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
Server	NIC	192.168.50.254	255.255.255.0	192.168.50.1

Port Assignments – Switch 2

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	192.168.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Sales	192.168.30.0 /24
Fa0/11 – 0/17	VLAN 10 – R&D	192.168.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Engineering	192.168.20.0 /24

Subinterface Configuration Table – Router 1

Router Interface	Assignment	IP Address
Fa0/1.1	VLAN1	192.168.1.1
Fa0/1.10	VLAN 10	192.168.10.1
Fa0/1.20	VLAN 20	192.168.20.1
Fa0/1.30	VLAN 30	192.168.30.1
Fa0/1.99	VLAN 99	192.168.99.1

Learning Objectives

To complete this lab:

- Cable a network according to the topology diagram
- Erase any existing configurations and reload switches and the router to the default state
- Load the switches and the router with supplied scripts
- Find and correct all configuration errors
- Document the corrected network

Scenario

The network has been designed and configured to support five VLANs and a separate server network. Inter-VLAN routing is being provided by an external router in a router-on-a-stick configuration, and the server network is routed across a separate Fast Ethernet interface. However, it is not working as designed, and complaints from your users have not given much insight into the source of the problems. You must first

define what is not working as expected, and then analyze the existing configurations to determine and correct the source of the problems.

This lab is complete when you can demonstrate IP connectivity between each of the user VLANs and the external server network, and between the switch management VLAN and the server network.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

The output shown in this lab is based on 2960 switches and an 1841 router. You can use any current switches or routers in your lab as long as they have the required interfaces shown in the topology diagram. Other device types may produce different output. Note that Ethernet (10Mb) LAN interfaces on routers do not support trunking, and Cisco IOS software earlier than version 12.3 may not support trunking on Fast Ethernet router interfaces.

Set up console connections to all three switches and to the router.

Step 2: Clear any existing configurations on the switches.

Clear switch configurations on all three switches, and reload to restore the default state. Use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Step 3: Configure the Ethernet interfaces on the host PCs and the server.

Configure the Ethernet interfaces of PC1, PC2, PC3 and the server with the IP addresses and default gateways listed in the addressing table.

Task 2: Load the Router and Switches with Supplied Scripts

Router 1 Configuration

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.50.1 255.255.255.192
!
interface FastEthernet0/1 no
 ip address
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1.10
 encapsulation dot1Q 11
 ip address 192.168.10.1 255.255.255.0
!
```

```
interface FastEthernet0/1.20
  encapsulation dot1Q 20
  ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1.30
  ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/1.99
  encapsulation dot1Q 99 native
  ip address 192.168.99.1 255.255.255.0
!
line con 0
  logging synchronous
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
end
```

Switch 1 Configuration

```
hostname S1
!
vtp mode server
vtp domain lab6_3 vtp
password cisco
!
vlan 99
  name Management
exit
!
vlan 10 name
  R&D exit
!
vlan 30 name
  Sales exit
!
interface FastEthernet0/1 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
```

```
!  
interface FastEthernet0/3  
    switchport trunk native vlan 99  
    switchport mode trunk  
    no shutdown  
!  
interface FastEthernet0/4  
    switchport trunk native vlan 99  
    switchport mode trunk  
    shutdown  
!  
interface FastEthernet0/5  
    switchport trunk native vlan 99  
    switchport mode trunk  
  
!  
interface range FastEthernet0/6 - 24  
    shutdown  
!  
interface Vlan99  
    ip address 192.168.99.11 255.255.255.0 no  
    shutdown  
!  
exit  
!  
ip default-gateway 192.168.99.1  
!  
line con 0  
    logging synchronous  
    password cisco  
    login  
!  
line vty 0 4  
    password cisco  
    login  
!  
line vty 5 15  
    password cisco  
    login  
!  
end
```

Switch 2 Configuration

```
!  
hostname S2  
no ip domain-lookup  
enable secret class  
!
```

```
vtp mode client vtp
domain lab6_3 vtp
password cisco
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/2 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface FastEthernet0/3 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface FastEthernet0/4 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface FastEthernet0/5 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface range FastEthernet0/6 - 11
  switchport access vlan 30
  switchport mode access
!
interface range FastEthernet0/12 - 17
  switchport access vlan 10
!
interface range FastEthernet0/18 -24
  switchport mode access
  switchport access vlan 20
!
interface Vlan99
  ip address 192.168.99.12 255.255.255.0 no
  shutdown
exit
!
ip default-gateway 192.168.99.1
ip http server
!
line con 0 password cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  login
```

```
line vty 5 15
  password cisco
  login
!
end
```

Switch 3 Configuration

```
!
hostname S3
!
enable secret class
!
vtp mode client vtp
domain lab6_3 vtp
password cisco
!
interface FastEthernet0/1 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/2 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/3 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/4 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/5 switchport
  trunk native vlan 99 switchport mode
  trunk
!
interface range FastEthernet0/6 - 24
  shutdown
  exit
!
ip default-gateway 192.168.99.1
!
line con 0
```

```
logging synchronous
password cisco
login
!
line vty 0 4
password cisco
login
!
line vty 5 15
password cisco
login
!
end
```

Task 3: Troubleshoot and Correct the Inter-VLAN Issues and Configuration Errors

Begin by identifying what is working and what is not. What is the state of the interfaces? What hosts can ping other hosts? Which hosts can ping the server? What routes should be in the R1 routing table? What could prevent a configured network from being installed in the routing table?

When all errors are corrected, you should be able to ping the remote server from any PC or any switch. In addition, you should be able to ping between the three PCs and ping the management interfaces on switches from any PC.

Task 4: Document the Network Configuration

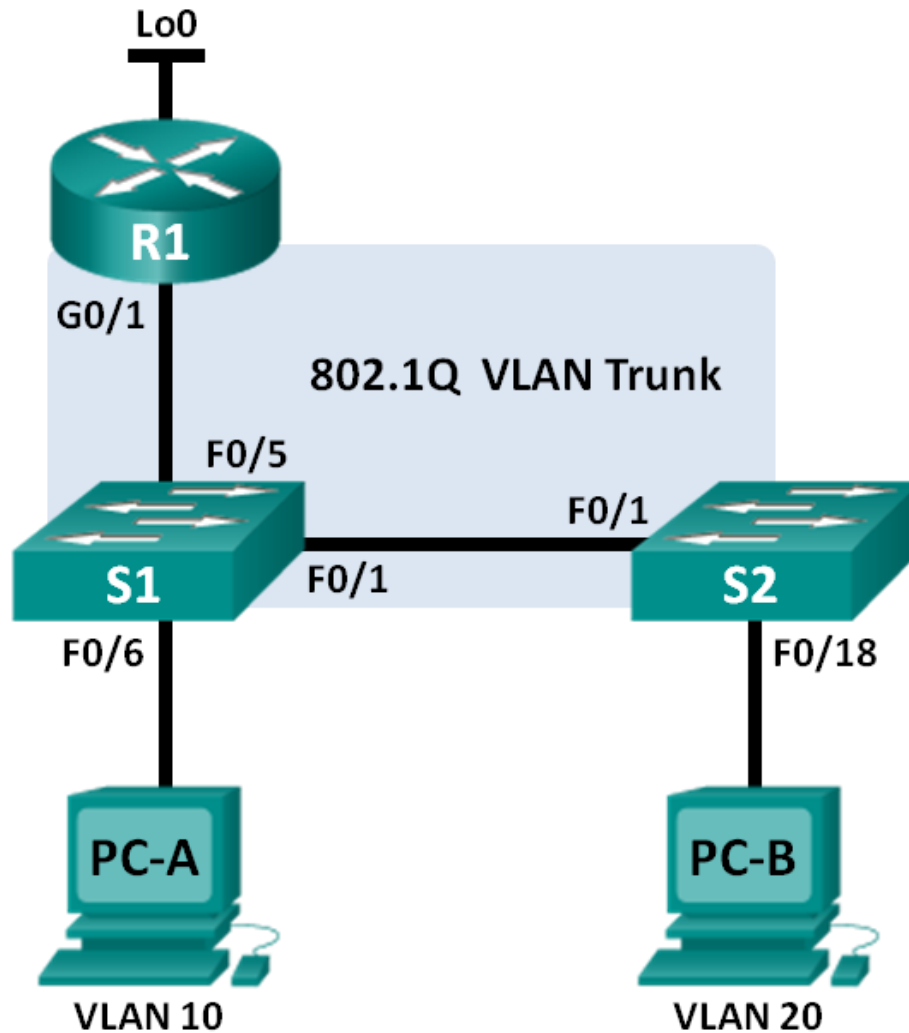
When you have successfully completed your troubleshooting, capture the output of the router and all three switches with the **show run** command and save it to a text file.

Task 5: Clean Up

Erase the configurations and reload the switches and router. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 22 – Troubleshooting Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
S1 F0/1	802.1Q Trunk	N/A
S2 F0/1	802.1Q Trunk	N/A
S1 F0/5	802.1Q Trunk	N/A
S1 F0/6	VLAN 10 – R&D	192.168.10.0/24
S2 F0/18	VLAN 20 – Engineering	192.168.20.0/24

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot the Inter-VLAN Routing Configuration

Part 3: Verify VLAN Configuration, Port Assignment, and Trunking

Part 4: Test Layer 3 Connectivity

Background / Scenario

The network has been designed and configured to support three VLANs. Inter-VLAN routing is provided by an external router using an 802.1Q trunk, also known as router-on-a-stick. Routing to a remote web server, which is simulated by Lo0, is also provided by R1. However, it is not working as designed, and user complaints have not given much insight into the source of the problems.

In this lab, you must first define what is not working as expected, and then analyze the existing configurations to determine and correct the source of the problems. This lab is complete when you can demonstrate IP connectivity between each of the user VLANs and the external web server network, and between the switch management VLAN and the web server network.

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)
- 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 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 and configure basic settings on the PC hosts, switches, and router.

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

Step 2: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 3: Load router and switch configurations.

Load the following configurations into the appropriate router or switch. All devices have the same passwords; the enable password is **class**, and the line password is **cisco**.

Router R1 Configuration:

```
hostname R1
enable secret class
no ip domain lookup
line con 0
  password cisco
  login
  logging synchronous
line vty 0 4
  password cisco
  login
interface loopback0
  ip address 209.165.200.225 255.255.255.224
interface gigabitEthernet0/1
  no ip address
interface gigabitEthernet0/1.1
  encapsulation dot1q 11
  ip address 192.168.1.1 255.255.255.0
interface gigabitEthernet0/1.10
  encapsulation dot1q 10
```

```
ip address 192.168.11.1 255.255.255.0
interface gigabitEthernet0/1.20
encapsulation dot1q 20
ip address 192.168.20.1 255.255.255.0
end
```

Switch S1 Configuration:

```
hostname S1
enable secret class
no ip domain-lookup
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
vlan 10
name R&D
exit
interface fastethernet0/1
switchport mode access
interface fastethernet0/5
switchport mode trunk
interface vlan1
ip address 192.168.1.11 255.255.255.0
ip default-gateway 192.168.1.1
end
```

Switch S2 Configuration:

```
hostname S2
enable secret class
no ip domain-lookup
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
vlan 20
name Engineering
exit
interface fastethernet0/1
switchport mode trunk
interface fastethernet0/18
```

```
switchport access vlan 10
switchport mode access
interface vlan1
ip address 192.168.1.12 255.255.255.0
ip default-gateway 192.168.1.1
end
```

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

Part 2: Troubleshoot the Inter-VLAN Routing Configuration

In Part 2, you will verify the inter-VLAN routing configuration.

- a. On R1, enter the **show ip route** command to view the routing table.

Which networks are listed? _____

Are there any networks missing in the routing table? If so, which networks?

What is one possible reason that a route would be missing from the routing table?

- b. On R1, issue the **show ip interface brief** command.

Based on the output, are there any interface issues on the router? If so, what commands would resolve the issues?

- c. On R1, re-issue the **show ip route** command.

Verify that all networks are available in the routing table. If not, continue to troubleshoot until all networks are present.

Part 3: Verify VLAN Configuration, Port Assignment, and Trunking

In Part 3, you will verify that the correct VLANs exist on both S1 and S2 and that trunking is configured correctly.

Step 1: Verify VLAN configuration and port assignments.

- a. On S1, enter the **show vlan brief** command to view the VLAN database.

Which VLANs are listed? Ignore VLANs 1002 to 1005.

Are there any VLANs numbers or names missing in the output? If so, list them.

Are the access ports assigned to the correct VLANs? If not, list the missing or incorrect assignments.

If required, what commands would resolve the VLAN issues?

- b. On S1, re-issue the **show vlan brief** command to verify configuration.
- c. On S2, enter the **show vlan brief** command to view the VLAN database.
Which VLANs are listed? Ignore VLANs 1002 to 1005.

Are there any VLANs numbers or names missing in the output? If so, list them.

Are the access ports assigned to the correct VLANs? If not, list the missing or incorrect assignments.

If required, what commands would resolve the VLAN issues?

- d. On S2, re-issue the **show vlan brief** command to verify any configuration changes.

Step 2: Verify trunking interfaces.

- a. On S1, enter the **show interface trunk** command to view the trunking interfaces.

Which ports are in trunking mode? _____

Are there any ports missing in the output? If so, list them. _____

If required, what commands would resolve the port trunking issues?

- b. On S1, re-issue the **show interface trunk** command to verify any configuration changes.
- c. On S2, enter the **show interface trunk** command to view the trunking interfaces.

Which ports are in trunking mode? _____

Are there any ports missing in the output? If so, list them. _____

If required, what commands would resolve the port trunking issues?

Part 4: Test Layer 3 Connectivity

- a. Now that you have corrected multiple configuration issues, let's test connectivity.

From PC-A, is it possible to ping the default gateway for VLAN 10? _____

From PC-A, is it possible to ping PC-B? _____

From PC-A, is it possible to ping Lo0? _____

If the answer is **no** to any of these questions, troubleshoot the configurations and correct the error.

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

From PC-A, is it possible to ping S1? _____

From PC-A, is it possible to ping S2? _____

List some of the issues that could still be preventing successful pings to the switches.

- b. One way to help resolve where the error is occurring is to do a **tracert** from PC-A to S1.

```
C:\Users\User1> tracert 192.168.1.11
```

```
Tracing route to 192.168.1.11 over a maximum of 30 hops
```

```
 1    <1 ms    <1 ms    <1 ms    192.168.10.1
 2      *        *        *        Request timed out.
 3      *        *        *        Request timed out.
```

```
<output omitted>
```

This output shows that the request from PC-A is reaching the default gateway on R1 g0/1.10, but the packet stops at the router.

- c. You have already verified the routing table entries for R1, now execute the **show run | section interface** command to verify VLAN configuration. List any configuration errors.

What commands would resolve any issues found?

- d. Verify that that pings from PC-A now reach both S1 and S2.

From PC-A, is it possible to ping S1? _____

From PC-A, is it possible to ping S2? _____

Reflection

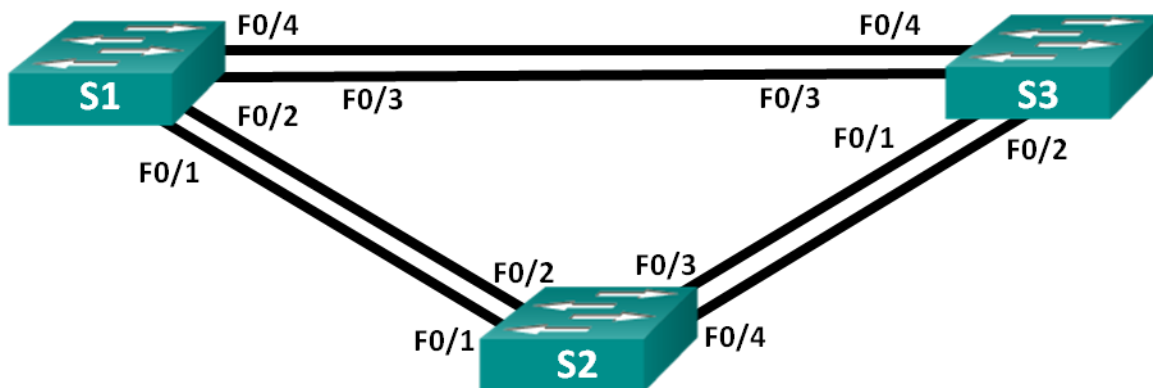
What are the advantages of viewing the routing table for troubleshooting purposes?

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.				

Lab 23 – 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.

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

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

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure the device name as shown in the topology.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
- Configure logging synchronous for the console line.
- Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.
- Configure the IP address listed in the Addressing Table for VLAN 1 on all switches.
- Copy the running configuration to the startup configuration.

Step 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.

Step 1: Deactivate all ports on the switches.

Step 2: Configure connected ports as trunks.

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

Step 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

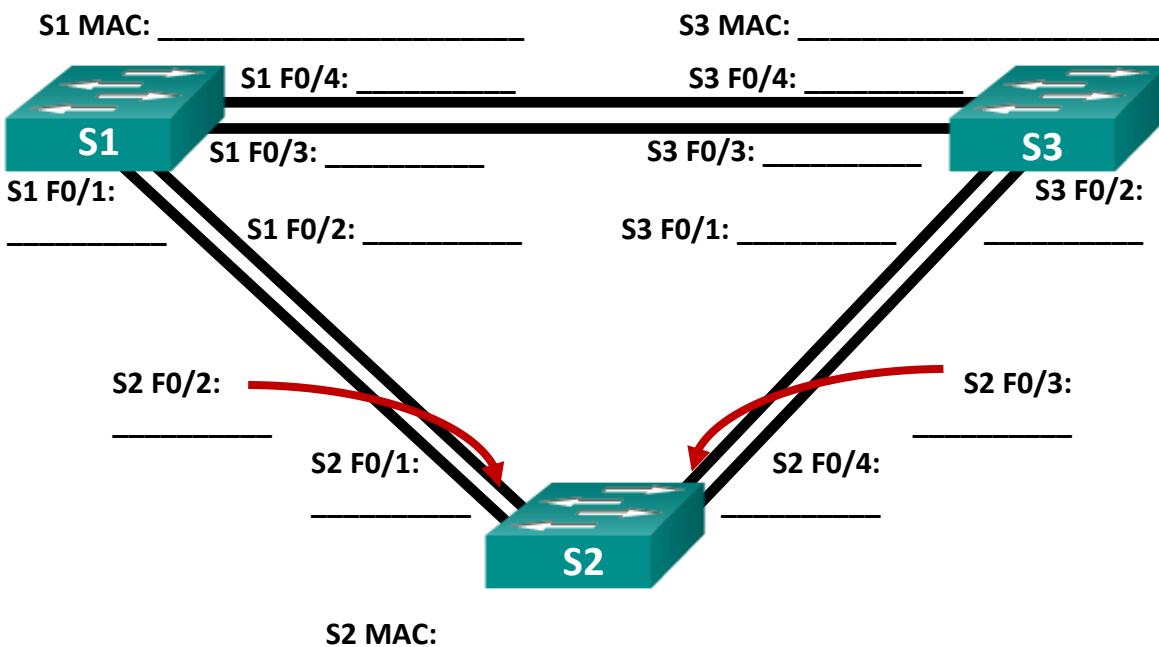
Root ID	Priority	32769			
	Address	0cd9.96d2.4000			
	Cost	19			
	Port	2 (FastEthernet0/2)			
Hello Time	2 sec	Max Age 20 sec	Forward Delay 15 sec		

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.

Step 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.

Step 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

```

Step 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?

Step 4: Remove port cost changes.

- 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

```
- 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.

- Activate ports F0/1 and F0/3 on all switches.
- 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

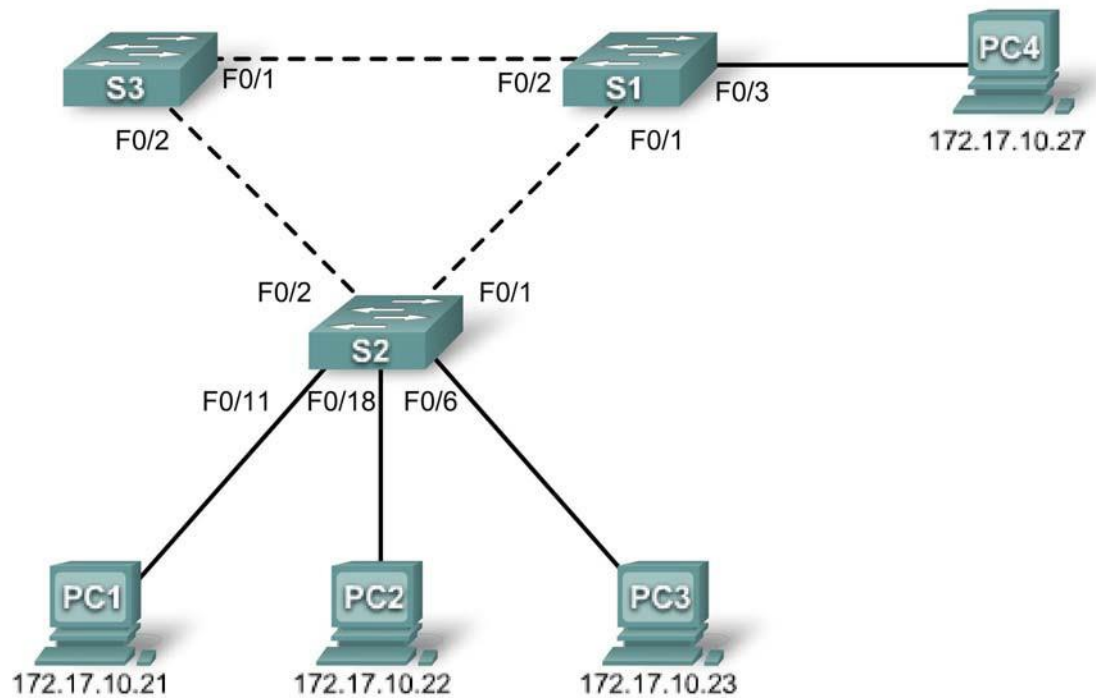
1. After a root bridge has been selected, what is the first value STP uses to determine port selection?

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?

Lab 24 - Basic Spanning Tree Protocol

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	172.17.10.1	255.255.255.0	N/A
S2	VLAN 1	172.17.10.2	255.255.255.0	N/A
S3	VLAN 1	172.17.10.3	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.254
PC2	NIC	172.17.10.22	255.255.255.0	172.17.10.254
PC3	NIC	172.17.10.23	255.255.255.0	172.17.10.254
PC4	NIC	172.17.10.27	255.255.255.0	172.17.10.254

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload the default configuration, setting a switch to the default state
- Perform basic configuration tasks on a switch
- Observe and explain the default behavior of Spanning Tree Protocol (STP, 802.1D)
- Observe the response to a change in the spanning tree topology

Task 1: Perform Basic Switch Configurations

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology diagram. The output shown in this lab is based on Cisco 2960 switches. Other switch models may produce different output.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

Clear NVRAM, delete the vlan.dat file, and reload the switches. Refer to Lab 2.5.1 for the procedure. After the reload is complete, use the **show vlan** privileged EXEC command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

S1#**show vlan**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Step 3: Configure basic switch parameters.

Configure the S1, S2, and S3 switches according to the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.

- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

(Output for S1 shown)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Task 2: Prepare the Network

Step 1: Disable all ports by using the shutdown command.

Ensure that the initial switch port states are inactive with the **shutdown** command. Use the **interface-range** command to simplify this task.

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown

S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown

S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Step 2: Re-enable the user ports on S1 and S2 in access mode.

Refer to the topology diagram to determine which switch ports on S2 are activated for end-user device access. These three ports will be configured for access mode and enabled with the **no shutdown** command.

```
S1(config)#interface fa0/3
S1(config-if)#switchport mode access
S1(config-if)#no shutdown

S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
```

Step 3: Enable trunk ports on S1, S2, and S3.

Only a single VLAN is being used in this lab, however trunking has been enabled on all links between switches to allow for additional VLANs to be added in the future.

```
S1(config-if-range)#interface range fa0/1, fa0/2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#no shutdown

S2(config-if-range)#interface range fa0/1, fa0/2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#no shutdown

S3(config-if-range)#interface range fa0/1, fa0/2
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#no shutdown
```

Step 4: Configure the management interface address on all three switches.

```
S1(config)#interface vlan1
S1(config-if)#ip address 172.17.10.1 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan1
S2(config-if)#ip address 172.17.10.2 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan1
S3(config-if)#ip address 172.17.10.3 255.255.255.0
S3(config-if)#no shutdown
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and try again.

Task 3: Configure Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, and PC4 with the IP address, subnet mask, and gateway indicated in the addressing table at the beginning of the lab.

Task 4: Configure Spanning Tree**Step 1: Examine the default configuration of 802.1D STP.**

On each switch, display the spanning tree table with the **show spanning-tree** command. Root selection varies depending on the BID of each switch in your lab resulting in varying outputs.

S1#**show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769
Address 0019.068d.6980

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 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type

Fa0/1	Desg	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p

S2#**show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769
Address 0019.068d.6980
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 001b.0c68.2080
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type

Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/11	Desg	FWD	19	128.11	P2p
Fa0/18	Desg	FWD	19	128.18	P2p

S3#**show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
             Address      0019.068d.6980
             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      001b.5303.1700
             Hello Time   2 sec   Max Age 20 sec   Forward Delay 15 sec
             Aging Time   300

```

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

Step 2: Examine the output.

The bridge identifier (bridge ID), stored in the spanning tree BPDU consists of the bridge priority, the system ID extension, and the MAC address. The combination or addition of the bridge priority and the system ID extension are known as the **bridge ID priority**. The system ID extension is always the number of the VLAN. For example, the system ID extension for VLAN 100 is 100. Using the default bridge priority value of 32768, the **bridge ID priority** for VLAN 100 would be 32868 (32768 + 100).

The **show spanning-tree** command displays the value of **bridge ID priority**. Note: The “priority” value within the parentheses represents the bridge priority value, which is followed by the value of the system ID extension.

Answer the following questions based on the output.

- What is the bridge ID priority for switches S1, S2, and S3 on VLAN 1?
 - S1
 - S2
 - S3
- Which switch is the root for the VLAN 1 spanning tree? _____
- Which spanning tree ports are in the blocking state on the root switch? _____
- Do either of the non-root switches have a blocking port? _____ Which switch and port is in the blocking state? _____
- How does STP elect the root switch? _____
- Since the bridge priorities are all the same, what else does the switch use to determine the root? _____

Task 5: Observe the response to the topology change in 802.1D STP

Now let's observe what happens when we intentionally simulate a broken link

Step 1: Place the switches in spanning tree debug mode using the command `debug spanning- tree events`.

```
S1#debug spanning-tree events
Spanning Tree event debugging is on
```

```
S2#debug spanning-tree events
Spanning Tree event debugging is on
```

```
S3#debug spanning-tree events
Spanning Tree event debugging is on
```

Step 2: Intentionally shutdown a port on the root switch. This example uses S1, since it is the root. Your root switch may vary.

```
S1(config)#interface fa0/1
S1(config-if)#shutdown
```

Step 3: Record the debug output from the non-root switches. In this example we record the output from S2 and S3, since they are the non-root switches.

```
S2#
1w2d: STP: VLAN0001 we are the spanning tree root
S2#
1w2d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
1w2d: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
S2#
1w2d: STP: VLAN0001 heard root 32769-0019.068d.6980 on Fa0/2
1w2d:      supersedes 32769-001b.0c68.2080
1w2d: STP: VLAN0001 new root is 32769, 0019.068d.6980 on port Fa0/2, cost 38
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/2

S3#
1w2d: STP: VLAN0001 heard root 32769-001b.0c68.2080 on Fa0/2
1w2d: STP: VLAN0001 Fa0/2 -> listening
S3#
1w2d: STP: VLAN0001 Topology Change rcvd on Fa0/2
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/1
S3#
1w2d: STP: VLAN0001 Fa0/2 -> learning
S3#
1w2d: STP: VLAN0001 sent Topology Change Notice on Fa0/1
1w2d: STP: VLAN0001 Fa0/2 -> forwarding
```

Based on the output from this example, when the link from S2 that is connected to the root switch goes down, what is its initial conclusion about the spanning tree root? _____

Once S2 receives new information on Fa0/2, what new conclusion does it draw? _____

Port Fa0/2 on S3 was previously in a blocking state before the link between S2 and S1 went down. What states does it go through as a result of the topology change? _____

Step 4: Examine what has changed in the spanning tree topology using the `show spanning-tree` command.

S2#**show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
              Address      0019.068d.6980
              Cost        38
              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      001b.0c68.2080
              Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

```

Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/2	Root	FWD	19	128.2	P2p
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/11	Desg	FWD	19	128.11	P2p
Fa0/18	Desg	FWD	19	128.18	P2p

S3#**show spanning-tree**

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
              Address      0019.068d.6980
              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      001b.5303.1700
              Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
              Aging Time  300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/1	Root	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p

Answer the following questions based on the output.

1. What has changed about the way that S2 forwards traffic? _____
2. What has changed about the way that S3 forwards traffic? _____

Task 6: Using the `show run` command, record the configuration of each switch.

```
S1#show run
!<output omitted>
!
hostname S1
!
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode trunk
!
interface FastEthernet0/3
  switchport mode access
!
! <output omitted>

!
interface Vlan1
  ip address 172.17.10.1 255.255.255.0
!
end
```

```
S2#show run
!<output omitted>
!
hostname S2
!
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode trunk
!
! <output omitted>
!
interface FastEthernet0/6
  switchport mode access
!
```

```
interface FastEthernet0/11
  switchport mode access
!
interface FastEthernet0/18
  switchport mode access
!
!
interface Vlan1
  ip address 172.17.10.2 255.255.255.0
!
end
```

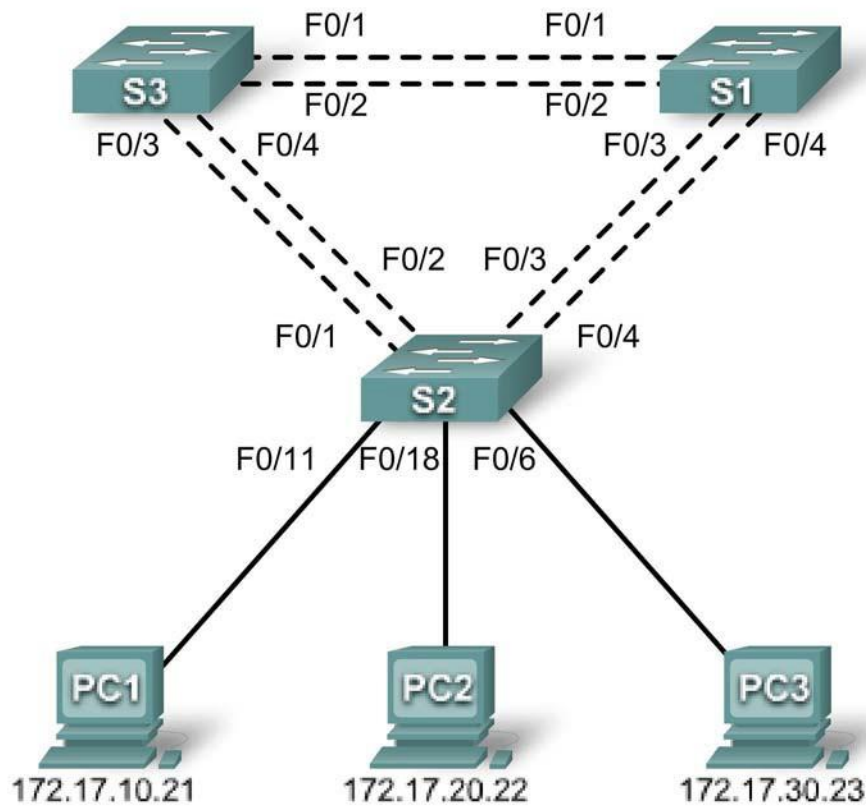
```
S3#show run
!<output omitted>
!
hostname S3
!
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode trunk
!
!
! <output omitted>
!
interface Vlan1
  ip address 172.17.10.3 255.255.255.0
!
end
```

Task 7: Clean Up

Erase the configurations and reload the default configurations for the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 25 - Challenge Spanning Tree Protocol

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.12
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.12
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.12

Port Assignments – Switch 2

Ports	Assignment	Network
Fa0/1 – 0/4	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload the default configuration, setting a switch to the default state
- Perform basic configuration tasks on a switch
- Configure VLAN Trunking Protocol (VTP) on all switches
- Observe and explain the default behavior of Spanning Tree Protocol (STP, 802.1D)
- Modify the placement of the spanning tree root
- Observe the response to a change in the spanning tree topology
- Explain the limitations of 802.1D STP in supporting continuity of service
- Configure Rapid STP (802.1W)
- Observe and explain the improvements offered by Rapid STP

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology diagram. The output shown in this lab is based on Cisco 2960 switches. Other switch models may produce different output.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

Clear NVRAM, delete the vlan.dat file, and reload the switches. After the reload is complete, use the **show vlan** privileged EXEC command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Switch#**show vlan**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Step 3: Disable all ports by using the shutdown command.

Ensure that the initial switch port states are inactive with the **shutdown** command. Use the **interface-range** command to simplify this task. Repeat these commands on each switch.

```
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Task 2: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

(Output for S1 shown)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Task 3: Configure Host PCs

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP address, subnet mask, and gateway indicated in the addressing table at the beginning of the lab.

Task 4: Configure VLANs**Step 1: Configure VTP.**

Configure VTP on the three switches using the following table. Remember that VTP domain names and passwords are case-sensitive. The default operating mode is server.

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end
```

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end
```

```
S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab5
Changing VTP domain name from NULL to Lab5
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Step 2: Configure Trunk Links and Native VLAN

Configure trunking ports and native VLAN. For each switch, configure ports Fa0/1 through Fa0/4 as trunking ports. Designate VLAN 99 as the native VLAN for these trunks. Use the **interface range** command in global configuration mode to simplify this task. Remember that these ports were disabled in a previous step and must be re-enabled using the **no shutdown** command.

```
S1(config)#interface range fa0/1-4
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

```
S2(config)# interface range fa0/1-4
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end
```

```

S3(config)# interface range fa0/1-4
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end

```

Step 3: Configure the VTP server with VLANs.

VTP allows you to configure VLANs on the VTP server and have those VLANs populated to the VTP clients in the domain. This ensures consistency in the VLAN configuration across the network.

Configure the following VLANS on the VTP server:

VLAN	VLAN Name
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

```

S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty-staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit

```

Step 4: Verify the VLANs.

Use the **show vlan brief** command on S2 and S3 to verify that all four VLANs have been distributed to the client switches.

S2#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1

```

10   faculty-staff      active
20   students           active
30   guest              active
99   management         active

```

S3#**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10	faculty-staff	active	
20	students	active	
30	guest	active	
99	management	active	

Step 5: Configure the management interface address on all three switches.

```

S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown

```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful? _____

If not, troubleshoot the switch configurations and try again.

Step 6: Assign switch ports to the VLANs.

Assign ports to VLANs on S2. Refer to the port assignments table at the beginning of the lab.

```

S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport mode access

```

```

S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S2#

```

Step 7: Re-enable the user ports on S2.

Refer to the topology diagram to determine which switch ports on S2 are activated for end-user device access. These three ports will be enabled with the **no shutdown** command.

```

S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#no shutdown

```

Task 5: Configure Spanning Tree

Step 1: Examine the default configuration of 802.1D STP.

On each switch, display the spanning tree table with the **show spanning-tree** command. The output is shown for S1 only. Root selection varies depending on the BID of each switch in your lab.

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

VLAN0001

```

Spanning tree enabled protocol ieee
Root ID    Priority      32769
           Address      0019.068d.6980
           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      0019.068d.6980
           Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
           Aging Time  300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

VLAN0010

```

Spanning tree enabled protocol ieee
Root ID    Priority      32778
           Address      0019.068d.6980
           This bridge is the root
Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

```

```

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

VLAN0020

```

Spanning tree enabled protocol ieee
Root ID Priority 32788
Address 0019.068d.6980

```

This bridge is the root

```

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```

```

Bridge ID Priority 32788 (priority 32768 sys-id-ext 20)
Address 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

VLAN0030

```

Spanning tree enabled protocol ieee
Root ID Priority 32798
Address 0019.068d.6980

```

This bridge is the root

```

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```

```

Bridge ID Priority 32798 (priority 32768 sys-id-ext 30)
Address 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

VLAN0099

Spanning tree enabled protocol ieee

Root ID Priority 32867
 Address 0019.068d.6980

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)

Address 0019.068d.6980

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/1	Desg	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

Note that there are five instances of the spanning tree on each switch. The default STP configuration on Cisco switches is Per-VLAN Spanning Tree (PVST+), which creates a separate spanning tree for each

VLAN (VLAN 1 and any user-configured VLANs).

Examine the VLAN 99 spanning tree for all three switches:

S1#**show spanning-tree vlan 99**

VLAN0099

Spanning tree enabled protocol ieee

Root ID Priority 32867
 Address 0019.068d.6980

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)

Address 0019.068d.6980

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
-----	----	---	-----	-----	-----
Fa0/1	Desg	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

S2#**show spanning-tree vlan 99**

VLAN0099

Spanning tree enabled protocol ieee

```

Root ID      Priority      32867
              Address      0019.068d.6980  This is the MAC address of the root switch (S1 in
              this case)
Cost          19
Port          3 (FastEthernet0/3)
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID     Priority      32867  (priority 32768 sys-id-ext 99)
              Address      001b.0c68.2080
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time    15

```

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

S3#show spanning-tree vlan 99

VLAN0099

Spanning tree enabled protocol ieee

```

Root ID      Priority      32867
              Address      0019.068d.6980  This is the MAC address of the root switch (S1 in
              this case)
Cost          19
Port          1 (FastEthernet0/1)
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID     Priority      32867  (priority 32768 sys-id-ext
              99) Address 001b.5303.1700
              Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time    300

```

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

Step 2: Examine the output.

Answer the following questions based on the output.

- What is the bridge ID priority for switches S1, S2, and S3 on VLAN 99?
 - S1 _____
 - S2 _____
 - S3 _____
- What is the bridge ID priority for S1 on VLANs 10, 20, 30, and 99?

- a. VLAN 10 ____ b.
- VLAN 20 ____ c.
- VLAN 30 ____ d.
- VLAN 99 ____
3. Which switch is the root for the VLAN 99 spanning tree? _____
4. On VLAN 99, which spanning tree ports are in the blocking state on the root switch?

5. On VLAN 99, which spanning tree ports are in the blocking state on the non-root switches?

6. How does STP elect the root switch? _____
7. Since the bridge priorities are all the same, what else does the switch use to determine the root?

Task 6: Optimizing STP

Because there is a separate instance of the spanning tree for every active VLAN, a separate root election is conducted for each instance. If the default switch priorities are used in root selection, the same root is elected for every spanning tree, as we have seen. This could lead to an inferior design. Some reasons to control the selection of the root switch include:

- The root switch is responsible for generating BPDUs in STP 802.1D and is the focal point for spanning tree control traffic. The root switch must be capable of handling this additional processing load.
- The placement of the root defines the active switched paths in the network. Random placement is likely to lead to suboptimal paths. Ideally the root is in the distribution layer.
- Consider the topology used in this lab. Of the six trunks configured, only two are carrying traffic. While this prevents loops, it is a waste of resources. Because the root can be defined on the basis of the VLAN, you can have some ports blocking for one VLAN and forwarding for another. This is demonstrated below.

In this example, it has been determined that the root selection using default values has led to under-utilization of the available switch trunks. Therefore, it is necessary to force another switch to become the root switch for VLAN 99 to impose some load-sharing on the trunks.

Selection of the root switch is accomplished by changing the spanning-tree priority for the VLAN. Because the default root switch may vary in your lab environment, we will configure S1 and S3 to be the root switches for specific VLANs. The default priority, as you have observed, is 32768 plus the VLAN ID. The lower number indicates a higher priority for root selection. Set the priority for VLAN 99 on S3 to 4096.

```
S3(config)#spanning-tree vlan 99 ?
forward-time  Set the forward delay for the spanning tree
hello-time    Set the hello interval for the spanning tree
max-age       Set the max age interval for the spanning tree
priority      Set the bridge priority for the spanning tree
root          Configure switch as root
<cr>
```

```
S3(config)#spanning-tree vlan 99 priority ?
<0-61440>    bridge priority in increments of 4096
```

```
S3(config)#spanning-tree vlan 99 priority 4096
S3(config)#exit
```

Set the priority for VLANs 1, 10, 20, and 30 on S1 to 4096. Once again, the lower number indicates a higher priority for root selection.

```
S1(config)#spanning-tree vlan 1 priority 4096
S1(config)#spanning-tree vlan 10 priority 4096
S1(config)#spanning-tree vlan 20 priority 4096
S1(config)#spanning-tree vlan 30 priority 4096
S1(config)#exit
```

Give the switches a little time to recalculate the spanning tree and then check the tree for VLAN 99 on switch S1 and switch S3.

```
S1#show spanning-tree vlan 99
```

```
VLAN0099
```

```
Spanning tree enabled protocol ieee
```

```
Root ID      Priority      4195
```

```
Address      001b.5303.1700 This is now the MAC address of S3, (the new root switch)
```

```
Cost          19
```

```
Port          3 (FastEthernet0/1)
```

```
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID     Priority      32867 (priority 32768 sys-id-ext 99)
```

```
Address        0019.068d.6980
```

```
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Aging Time    300
```

```
Interface      Role Sts Cost      Prio.Nbr Type
```

```
-----
```

Fa0/1	Root	FWD	19	128.3	P2p
Fa0/2	Altn	BLK	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

```
S3#show spanning-tree vlan 99
```

```
VLAN0099
```

```
Spanning tree enabled protocol ieee
```

```
Root ID      Priority      4195
```

```
Address      001b.5303.1700
```

```
This bridge is the root
```

```
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID     Priority      4195 (priority 4096 sys-id-ext 99)
```

```
Address        001b.5303.1700
```

```
Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Aging Time    300
```

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

Which switch is the root for VLAN 99?

On VLAN 99, which spanning tree ports are in the blocking state on the new root switch? _____

On VLAN 99, which spanning tree ports are in the blocking state on the old root switch? _____

Compare the S3 VLAN 99 spanning tree above with the S3 VLAN 10 spanning tree.

S3#**show spanning-tree vlan 10**

VLAN0010

Spanning tree enabled protocol ieee

```

Root ID      Priority      4106
             Address      0019.068d.6980
             Cost        19
             Port        1 (FastEthernet0/1)
             Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

```

```

Bridge ID    Priority      32778 (priority 32768 sys-id-ext 10)
             Address      001b.5303.1700
             Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
             Aging Time  300

```

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

Note that S3 can now use all four ports for VLAN 99 traffic as long as they are not blocked at the other end of the trunk. However, the original spanning tree topology, with three of four S3 ports in blocking mode, is still in place for the four other active VLANs. By configuring groups of VLANs to use different trunks as their primary forwarding path, we retain the redundancy of failover trunks, without having to leaves trunks totally unused.

Task 7: Observe the response to the topology change in 802.1D STP

To observe continuity across the LAN during a topology change, first reconfigure PC3, which is connected to port S2 Fa0/6, with IP address 172.17.99.23 255.255.255.0. Then reassign S2 port Fa0/6 to VLAN 99. This allows you to continuously ping across the LAN from the host.

```

S2(config)# interface fa0/6
S2(config-if)#switchport access vlan 99

```

Verify that the switches can ping the host.

```

S2#ping 172.17.99.23
Type escape sequence to abort.

```

```
Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms

S1#ping 172.17.99.23

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms
```

Put S1 in spanning-tree event debug mode to monitor changes during the topology change.

```
S1#debug spanning-tree events
Spanning Tree event debugging is on
```

Open a command window on PC3 and begin a continuous ping to the S1 management interface with the command **ping -t 172.17.99.11**. Now disconnect the trunks on S1 Fa0/1 and Fa0/3. Monitor the pings. They will begin to time out as connectivity across the LAN is interrupted. As soon as connectivity has been re-established, terminate the pings by pressing Ctrl-C.

Below is a shortened version of the debug output you will see on S1 (several TCNs are omitted for brevity).

```
S1#debug spanning-tree events
Spanning Tree event debugging is
on S1#
6d08h: STP: VLAN0099 new root port Fa0/2, cost 19
6d08h: STP: VLAN0099 Fa0/2 -> listening
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2
6d08h: STP: VLAN0030 Topology Change rcvd on Fa0/2
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/3, changed state to down
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4
6d08h: STP: VLAN0099 Fa0/2 -> learning
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2
6d08h: STP: VLAN0099 Fa0/2 -> forwarding
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4
```

Recall that when the ports are in listening and learning mode, they are not forwarding frames, and the LAN is essentially down. The spanning tree recalculation can take up to 50 seconds to complete – a significant interruption in network services. The output of the continuous pings shows the actual interruption time. In this case, it was about 30 seconds. While 802.1D STP effectively prevents switching loops, this long restoration time is considered a serious drawback in the high availability LANs of today.

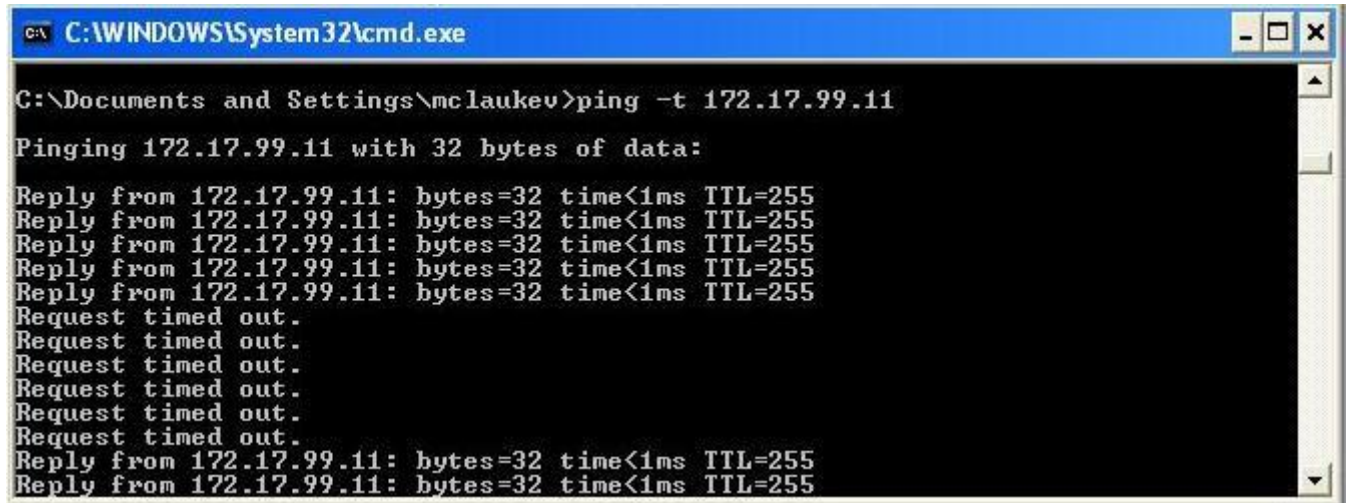


Figure 1. These pings show a 30-second lapse in connectivity while the spanning tree is recalculated.

Task 8: Configure PVST Rapid Spanning Tree Protocol

Cisco has developed several features to address the slow convergence times associated with standard STP. PortFast, UplinkFast, and BackboneFast are features that, when properly configured, can dramatically reduce the time required to restore connectivity. Incorporating these features requires manual configuration, and care must be taken to do it correctly. The longer term solution is Rapid STP (RSTP), 802.1w, which incorporates these features among others. RSTP-PVST is configured as follows:

```
S1(config)#spanning-tree mode rapid-pvst
```

Configure all three switches in this manner.

Use the command **show spanning-tree summary** to verify that RSTP is enabled.

Task 9: Observe the convergence time of RSTP

Begin by restoring the trunks you disconnected in Task 7, if you have not already done so (ports Fa0/1 and Fa0/3 on S1). Then follow these steps in Task 7:

- Set up host PC3 to continuously ping across the network.
- Enable spanning-tree event debugging on switch S1.
- Disconnect the cables connected to ports Fa0/1 and Fa0/3.
- Observe the time required to re-establish a stable

spanning tree. Below is the partial debug output:

```
S1#debug spanning-tree
events Spanning Tree event
debugging is on S1#
6d10h: RSTP(99): updt rolesroot port Fa0/3 is going down
6d10h: RSTP(99): Fa0/2 is now root port Connectivity has been restored; less than 1
second interruption
6d10h: RSTP(99): syncing port Fa0/1
6d10h: RSTP(99): syncing port Fa0/4
6d10h: RSTP(99): transmitting a proposal on Fa0/1
6d10h: RSTP(99): transmitting a proposal on Fa0/4
```

```
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,  
changed state to down  
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,  
changed state to down
```

The restoration time with RSTP enabled was less than a second, and not a single ping was dropped.

Task 10: Clean Up

Erase the configurations and reload the default configurations for the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Final Configurations

Switch S1

```
hostname S1  
!  
enable secret class  
!  
no ip domain-lookup  
!  
spanning-tree mode rapid-pvst  
spanning-tree extend system-id  
spanning-tree vlan 1 priority 4096  
spanning-tree vlan 10 priority 4096  
spanning-tree vlan 20 priority 4096  
spanning-tree vlan 30 priority 4096  
!  
interface FastEthernet0/1  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/2  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/3  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/4  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/5  
    shutdown  
!
```

```
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
(remaining port configuration omitted - all non-used ports are shutdown)
!
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no ip route-cache
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

Switch S2

```
hostname S2
!
enable secret class
!
no ip domain-lookup
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
```

```
!  
interface FastEthernet0/4  
  switchport trunk native vlan 99  
  switchport mode trunk  
!  
interface FastEthernet0/5  
  switchport access vlan 30  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/6  
  switchport access vlan 30  
  switchport mode access  
!  
interface FastEthernet0/7  
  switchport access vlan 30  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/8  
  switchport access vlan 30  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/9  
  switchport access vlan 30  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/10  
  switchport access vlan 30  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/11  
  switchport access vlan 10  
  switchport mode access  
!  
interface FastEthernet0/12  
  switchport access vlan 10  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/13  
  switchport access vlan 10  
  switchport mode access  
  shutdown  
!  
interface FastEthernet0/14  
  switchport access vlan 10  
  switchport mode access  
  shutdown  
!
```

```
interface FastEthernet0/15
  switchport access vlan 10
  switchport mode access
  shutdown
!
interface FastEthernet0/16
  switchport access vlan 10
  switchport mode access
  shutdown
!
interface FastEthernet0/17
  switchport access vlan 10
  switchport mode access
  shutdown
!
interface FastEthernet0/18
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/19
  switchport access vlan 20
  switchport mode access
  shutdown
!
interface FastEthernet0/20
  switchport access vlan 20
  switchport mode access
  shutdown
!
interface FastEthernet0/21
  switchport access vlan 20
  switchport mode access
  shutdown
!
interface FastEthernet0/22
  switchport access vlan 20
  switchport mode access
  shutdown
!
interface FastEthernet0/23
  switchport access vlan 20
  switchport mode access
  shutdown
!
interface FastEthernet0/24
  switchport access vlan 20
  switchport mode access
  shutdown
!
interface GigabitEthernet0/1
  shutdown
!
```

```
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 172.17.99.12 255.255.255.0
 no ip route-cache
!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

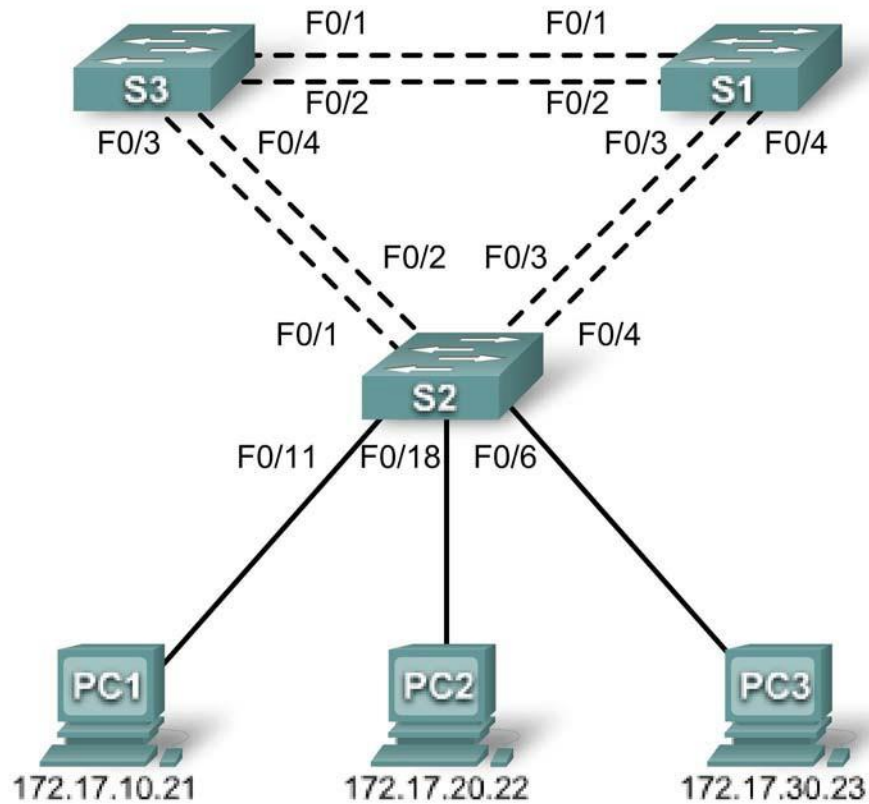
Switch S3

```
hostname S3
!
enable secret class
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 99 priority 4096
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
```

```
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
(remaining port configuration omitted - all non-used ports are shutdown)
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan99
ip address 172.17.99.13 255.255.255.0
no ip route-cache
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

Lab 26: Troubleshooting Spanning Tree Protocol

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1

Port Assignments – Switch 2

Ports	Assignment	Network
Fa0/1 – 0/4	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/5 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Learning Objectives

Upon completion of this lab, you will be able to:

- Analyze a congestion problem in a redundant, switched LAN network.
- Recognize the capabilities for per-VLAN load balancing with PVST.
- Modify the default STP configuration to optimize available bandwidth.
- Verify that modifications have had the intended effect.

Scenario

You are responsible for the operation of the redundant switched LAN shown in the topology diagram. You and your users have been observing increased latency during peak usage times, and your analysis points to congested trunks. You recognize that of the six trunks configured, only two are forwarding packets in the default STP configuration currently running. The solution to this problem requires more effective use of the available trunks. The PVST+ feature of Cisco switches provides the required flexibility to distribute the inter-switch traffic using all six trunks.

This lab is complete when all wired trunks are carrying traffic, and all three switches are participating in per-VLAN load balancing for the three user VLANs.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology diagram. The output shown in this lab is based on Cisco 2960 switches. Other switch models may produce different output.

Set up console connections to all three switches.

Step 2: Clear any existing configurations on the switches.

Clear NVRAM, delete the vlan.dat file, and reload the switches.

Step 3: Load the switches with the following script: S1**Configuration**

```
hostname S1
enable secret class
no ip domain-lookup
!
vtp mode server vtp
domain Lab5
vtp password cisco
!
vlan 99
name Management exit
!
vlan 10
name Faculty/Staff
exit
!
vlan 20
name Students exit
!
vlan 30 name
Guest exit
!
interface FastEthernet0/1 switchport
trunk native vlan 99 switchport mode
trunk
no shutdown
!
interface FastEthernet0/2 switchport
trunk native vlan 99 switchport mode
trunk
no shutdown
!
interface FastEthernet0/3 switchport
trunk native vlan 99 switchport mode
trunk
no shutdown
!
interface FastEthernet0/4 switchport
trunk native vlan 99 switchport mode
trunk
no shutdown
!
interface range FastEthernet0/5-24
shutdown
!
```

```
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 password cisco
 login
line vty 0 no
 login
line vty 1 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```

S2 Configuration

```
hostname S2
!
enable secret class no
ip domain-lookup
!
vtp mode client vtp
domain Lab5
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/3
```

```
switchport trunk native vlan 99
switchport mode trunk
no shutdown
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport mode trunk
no shutdown
!
interface range FastEthernet0/5 - 10
switchport access vlan 30
switchport mode access
!
interface range FastEthernet0/11 - 17
switchport access vlan 10
switchport mode access
!
interface range FastEthernet0/18 - 24
switchport access vlan 20
switchport mode access
!
interface fa0/6 no
shutdown interface
fa0/11 no shutdown
interface fa0/18 no
shutdown
!
interface Vlan99
ip address 172.17.99.12 255.255.255.0 no
shutdown
!
line con 0 password cisco
logging synchronous
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
```

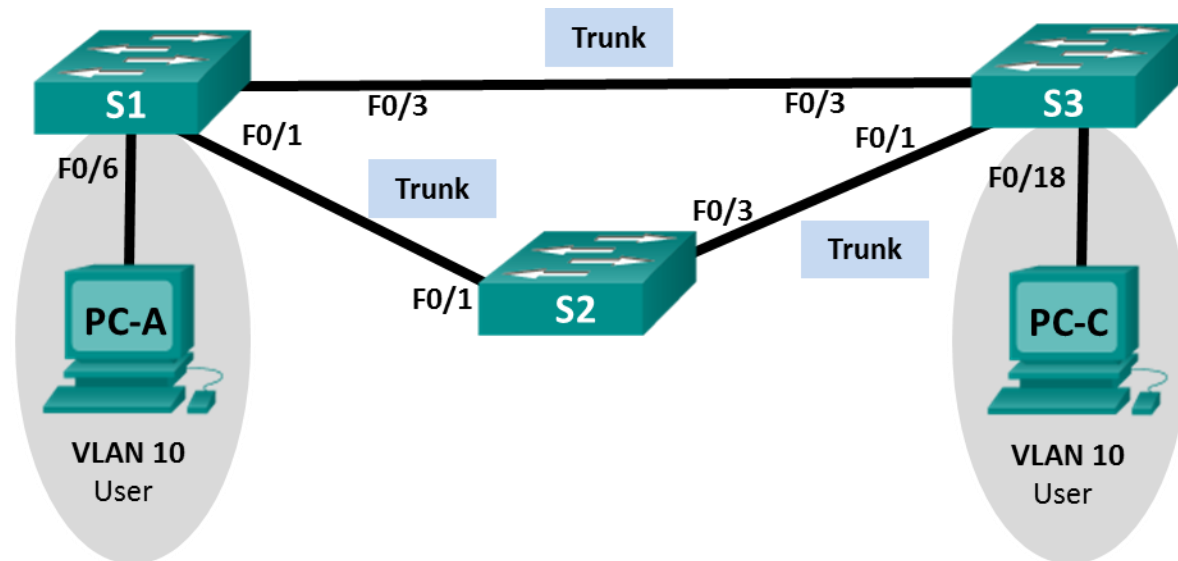
S3 Configuration

```
hostname S3
!
enable secret class no
ip domain-lookup
!
vtp mode client
```

```
vtp domain Lab5
vtp password cisco
!
interface FastEthernet0/1 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/2 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/3 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface FastEthernet0/4 switchport
  trunk native vlan 99 switchport mode
  trunk
  no shutdown
!
interface range FastEthernet0/5 - 10
```

Lab 27 – 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.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure the device name as shown in the Topology.
- Assign **cisco** as the console and vty passwords and enable login.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Shut down all switch ports.
- 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.

Step 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
```

Step 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.

Step 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.

Step 4: Configure the management interface on all switches.

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

Step 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.

Step 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?

Step 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.

- a. Configure switch S2 to be the primary root bridge for all existing VLANs. Write the command in the space provided.
-

- b. 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? _____

Step 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.

- a. 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
```

- b. 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.

Step 1: Configure Rapid PVST+.

- a. Configure S1 for Rapid PVST+. Write the command in the space provided.

- b. Configure S2 and S3 for Rapid PVST+.

- c. 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
```

Step 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.

- a. Configure interface F0/6 on S1 with PortFast. Write the command in the space provided.

- b. Configure interface F0/6 on S1 with BPDU guard. Write the command in the space provided.

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

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

Step 3: Examine Rapid PVST+ convergence.

- a. Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.
- b. 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
```

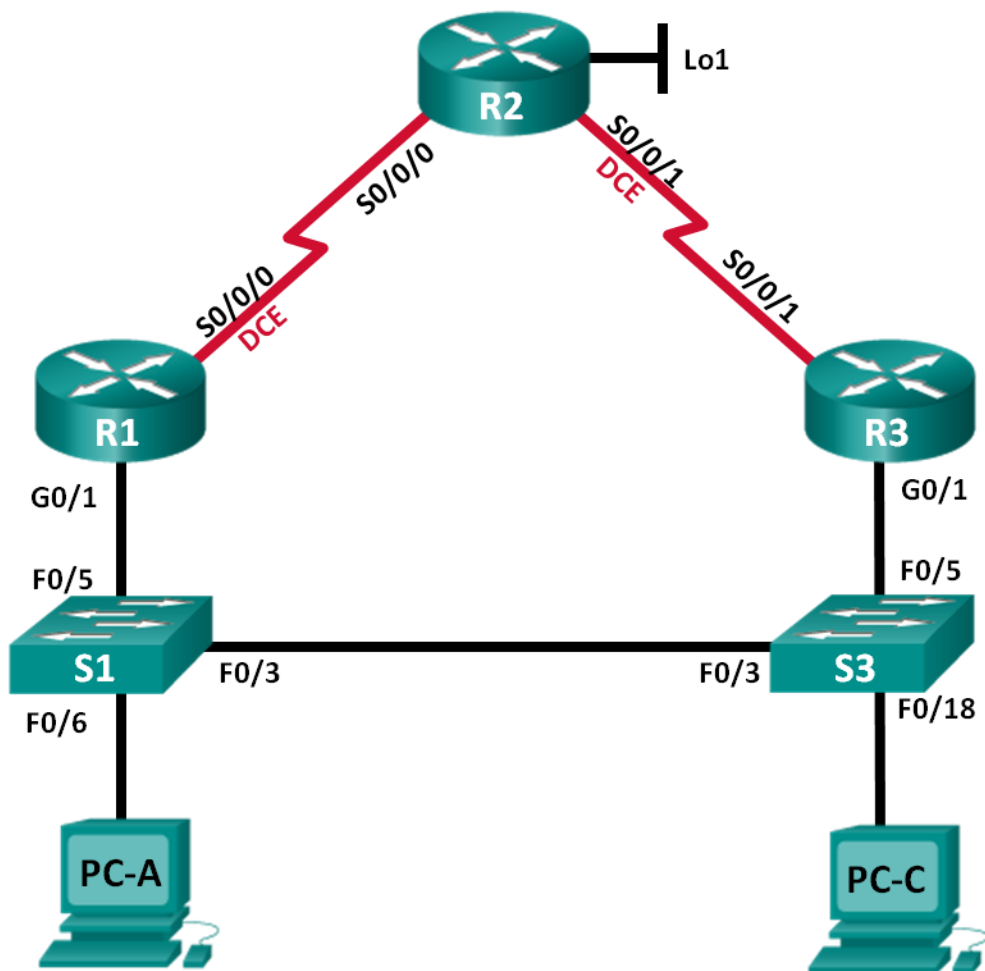
```
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface f0/3
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# 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
```

Lab 28 – 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.

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

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

Step 2: Configure PC hosts.

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

Step 4: Configure basic settings for each router.

- Disable DNS lookup.
- Configure the device name as shown in the topology.
- Configure IP addresses for the routers as listed in the Addressing Table.
- Set clock rate to **128000** for all DCE serial interfaces.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** for the console and vty password and enable login.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure the device name as shown in the topology.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure IP addresses for the switches as listed in the Addressing Table.
- Configure the default gateway on each switch.
- Assign **cisco** for the console and vty password and enable login.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Copy the running configuration to the startup configuration.

Step 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.

Step 7: Configure routing.

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

- b. 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.

Step 8: Verify connectivity.

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

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

- a. 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?

- b. 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?

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

- a. 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>
```

- b. 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?

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

What were your results?

- d. 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.

Step 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.

- a. 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
```

- b. Configure HSRP on R3.

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

- c. 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?

- d. 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

```

- e. 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? _____

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

- 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.
- 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?

Step 5: Verify HSRP settings on R1 and R3.

- a. Issue the **show standby brief** command on R1 and R3.

Which router is the active router? _____

- b. Reconnect the cable between the switch and the router or enable interface F0/5.
- c. 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.

Step 1: Configure GLBP on R1 and R3.

- a. 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
```

- b. 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
```

Step 2: Verify GLBP on R1 and R3.

- a. 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	-

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

- From a command prompt on PC-A, ping the 209.165.200.225 address of R2.
C:\> **ping 209.165.200.225**
 - Issue an **arp -a** command on PC-A. Which MAC address is used for the 192.168.1.254 address?
-
- 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.

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

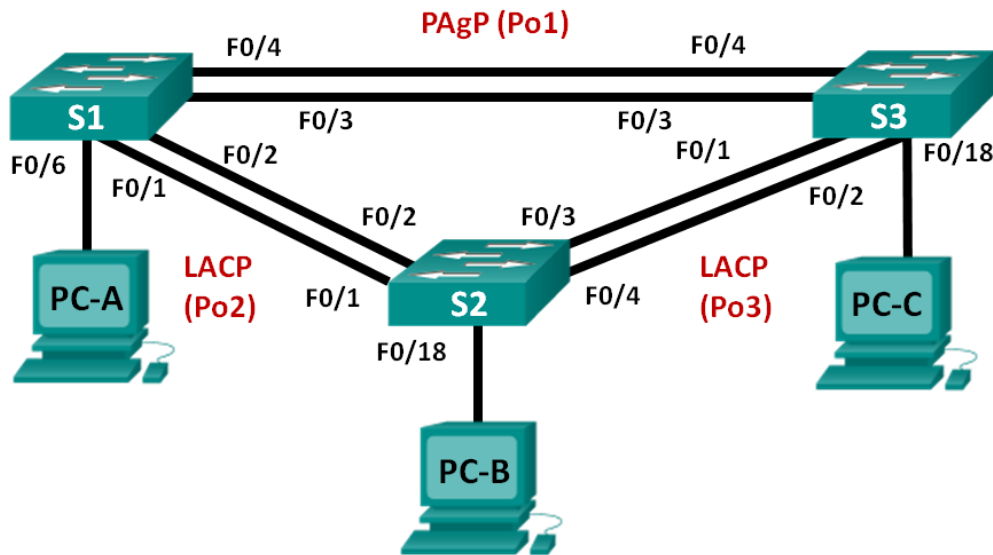
- From a command prompt on PC-A, issue a **ping -t** command to the 209.165.200.225 address on R2. Make sure you leave the command prompt window open.
 - As the ping continues, disconnect the Ethernet cable from F0/5 on S1 or shut down the F0/5 interface. What happened to the ping traffic?
-
-

Reflection

- Why would there be a need for redundancy in a LAN?
-
-
- If you had a choice, which protocol would you implement in your network, HSRP or GLBP? Explain your choice.
-
-

Lab 29 – 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.

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

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

Step 2: Initialize and reload the switches.

Step 3: Configure basic settings for each switch.

- Disable DNS lookup.
- Configure the device name as displayed in the topology.
- Encrypt plain text passwords.
- Create a MOTD banner warning users that unauthorized access is prohibited.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Configure logging synchronous to prevent console message from interrupting command entry.
- Shut down all switchports except the ports connected to PCs.
- Configure VLAN 99 and name it **Management**.
- Configure VLAN 10 and name it **Staff**.
- Configure the switch ports with attached hosts as access ports in VLAN 10.
- Assign the IP addresses according to the Addressing Table.
- Copy the running configuration to startup configuration.

Step 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.

Step 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
```

Step 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
```

Step 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?

Step 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
```

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

- 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.

- b. 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.

Step 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
```

Step 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.

Step 3: Configure LACP between S2 and S3.

- a. 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
```

- b. Verify that the EtherChannel has formed.

Step 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.

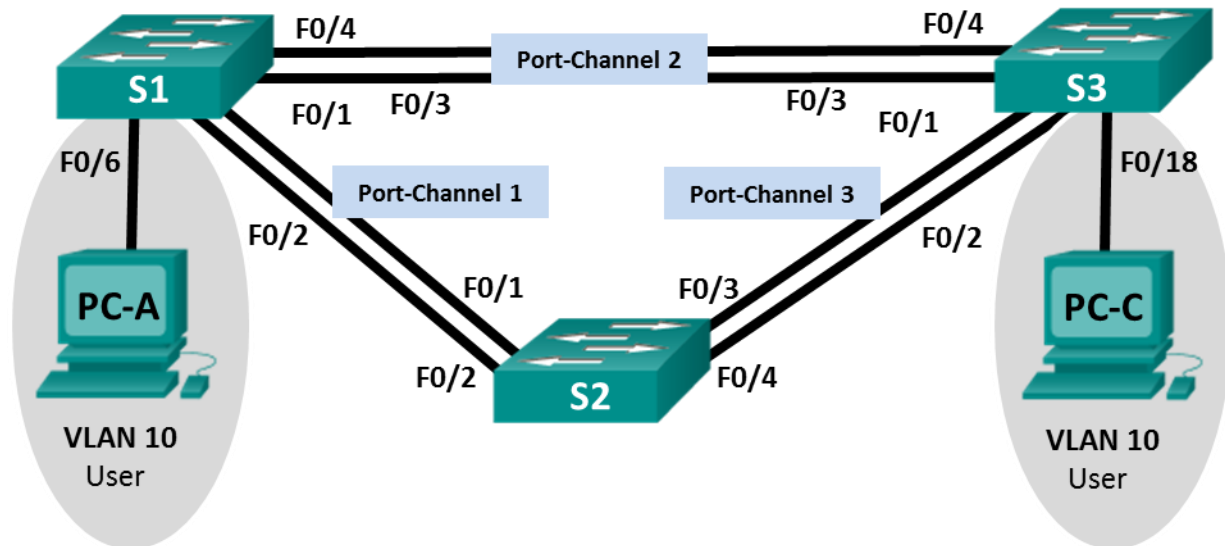
Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

What could prevent EtherChannels from forming?

Lab 30 – 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.

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

Step 2: Configure the PC hosts.

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

Step 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
```

Step 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.

Step 1: Troubleshoot S1.

- a. 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? _____
- b. 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.

- c. Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.
- d. Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configurations.

- e. Use the **show interfaces trunk** command to verify trunk settings.
- f. Use the **show etherchannel summary** command to verify that the port channels are up and in use.

Step 2: Troubleshoot S2.

- a. 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.

- b. 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.

- c. Use the command **show run | begin interface Port-channel** to view the running configuration beginning with the first port-channel interface.
- d. Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configuration.

- e. Issue the command to verify trunk settings.
- f. 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.

Step 3: Troubleshoot S3.

- a. 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.

- b. 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.

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

- d. Resolve all problems found. Record the commands used to correct the configuration.

- e. Issue the command to verify trunk settings. Record the command used in the space provided below.

- f. Issue the command to verify that the port channels are functioning. Record the command used in the space provided below.

Step 4: Verify EtherChannel and Connectivity.

- a. Use the **show interfaces etherchannel** command to verify full functionality of the port channels.

- b. Verify connectivity of the management VLAN.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

- c. Verify connectivity of PCs.

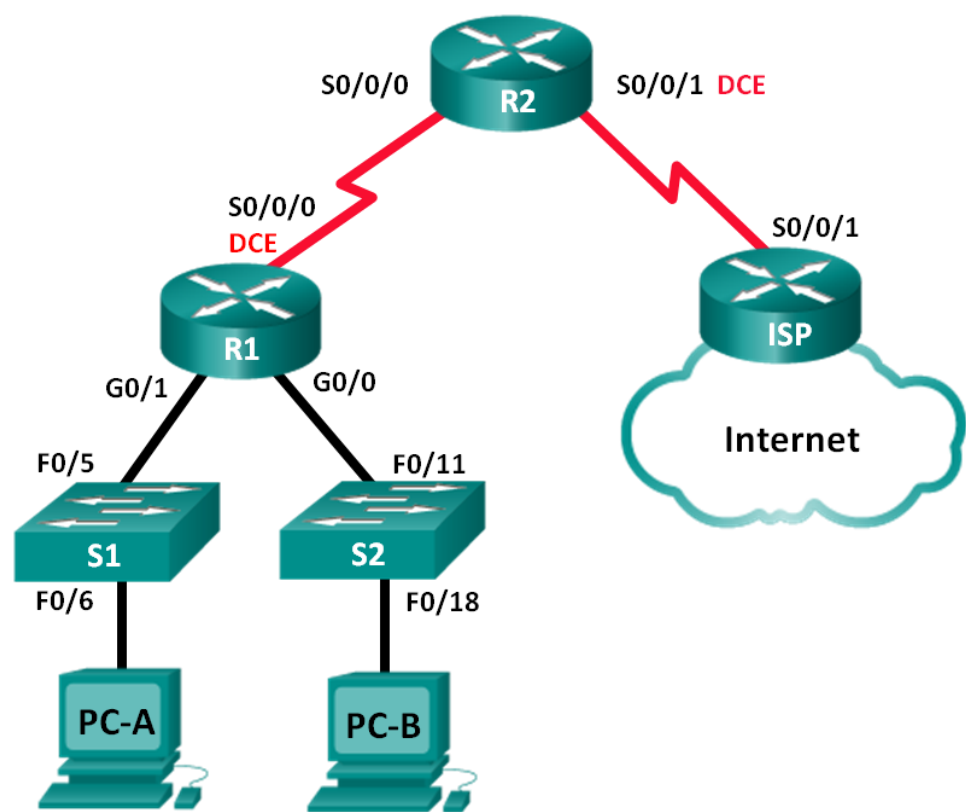
Can PC-A ping PC-C? _____

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.

Lab 31 - Configuring Basic DHCPv4 on a Router

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure a DHCPv4 Server and a DHCP Relay Agent

Background / Scenario

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that lets network administrators manage and automate the assignment of IP addresses. Without DHCP, the administrator must manually assign and configure IP addresses, preferred DNS servers, and default gateways. As the network grows in size, this becomes an administrative problem when devices are moved from one internal network to another.

In this scenario, the company has grown in size, and the network administrators can no longer assign IP addresses to devices manually. Your job is to configure the R2 router to assign IPv4 addresses on two different subnets connected to router R1.

Note: This lab provides minimal assistance with the actual commands necessary to configure DHCP. 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 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 Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers and switches with basic settings, such as passwords and IP addresses. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- Disable DNS lookup
- Configure the device name as shown in the topology.
- Assign **class** as the encrypted privileged EXEC mode password.
- Assign **cisco** as the console and vty passwords.
- Configure **logging synchronous** to prevent console messages from interrupting command entry.
- Configure the IP addresses for all the router interfaces according to the Addressing Table.
- Configure the serial DCE interface on R1 and R2 with a clock rate of 128000.
- Configure EIGRP for R1.

```
R1(config)# router eigrp 1
R1(config-router)# network 192.168.0.0 0.0.0.255
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# network 192.168.2.252 0.0.0.3
R1(config-router)# no auto-summary
```

- i. Configure EIGRP and a default route to the ISP on R2.

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- j. Configure a summary static route on ISP to reach the networks on the R1 and R2 routers.

```
ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
```

- k. Copy the running configuration to the startup configuration.

Step 4: Verify network connectivity between the routers.

If any pings between routers fail, correct the errors before proceeding to the next step. Use **show ip route** and **show ip interface brief** to locate possible issues.

Step 5: Verify the host PCs are configured for DHCP.

Part 2: Configure a DHCPv4 Server and a DHCP Relay Agent

To automatically assign address information on the network, you will configure R2 as a DHCPv4 server and R1 as a DHCP relay agent.

Step 1: Configure DHCPv4 server settings on router R2.

On R2, you will configure a DHCP address pool for each of the R1 LANs. Use the pool name **R1G0** for the G0/0 LAN and **R1G1** for the G0/1 LAN. You will also configure the addresses to be excluded from the address pools. Best practice dictates that excluded addresses be configured first, to guarantee that they are not accidentally leased to other devices.

Exclude the first 9 addresses in each R1 LAN starting with .1. All other addresses should be available in the DHCP address pool. Make sure that each DHCP address pool includes a default gateway, the domain **ccna-lab.com**, a DNS server (209.165.200.225), and a lease time of 2 days.

On the lines below, write the commands necessary for configuring DHCP services on router R2, including the DHCP-excluded addresses and the DHCP address pools.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure DHCP on R1 and R2 without referring to the appendix.

On PC-A or PC-B, open a command prompt and enter the **ipconfig /all** command. Did either of the host PCs receive an IP address from the DHCP server? Why?

Step 2: Configure R1 as a DHCP relay agent.

Configure IP helper addresses on R1 to forward all DHCP requests to the R2 DHCP server.

On the lines below, write the commands necessary to configure R1 as a DHCP relay agent for the R1 LANs.

Step 3: Record IP settings for PC-A and PC-B.

On PC-A and PC-B, issue the **ipconfig /all** command to verify that the PCs have received IP address information from the DHCP server on R2. Record the IP and MAC address for each PC.

Based on the DHCP pool that was configured on R2, what are the first available IP addresses that PC-A and PC-B can lease?

Step 4: Verify DHCP services and address leases on R2.

- a. On R2, enter the **show ip dhcp binding** command to view DHCP address leases.

Along with the IP addresses that were leased, what other piece of useful client identification information is in the output?

- b. On R2, enter the **show ip dhcp server statistics** command to view the DHCP pool statistics and message activity.

How many types of DHCP messages are listed in the output?

- c. On R2, enter the **show ip dhcp pool** command to view the DHCP pool settings.

In the output of the **show ip dhcp pool** command, what does the Current index refer to?

- d. On R2, enter the **show run | section dhcp** command to view the DHCP configuration in the running configuration.
- e. On R2, enter the **show run interface** command for interfaces G0/0 and G0/1 to view the DHCP relay configuration in the running configuration.

Reflection

What do you think is the benefit of using DHCP relay agents instead of multiple routers acting as DHCP servers?

Router Interface Summary Table

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

Appendix A – DHCP Configuration Commands

Router R1

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
```

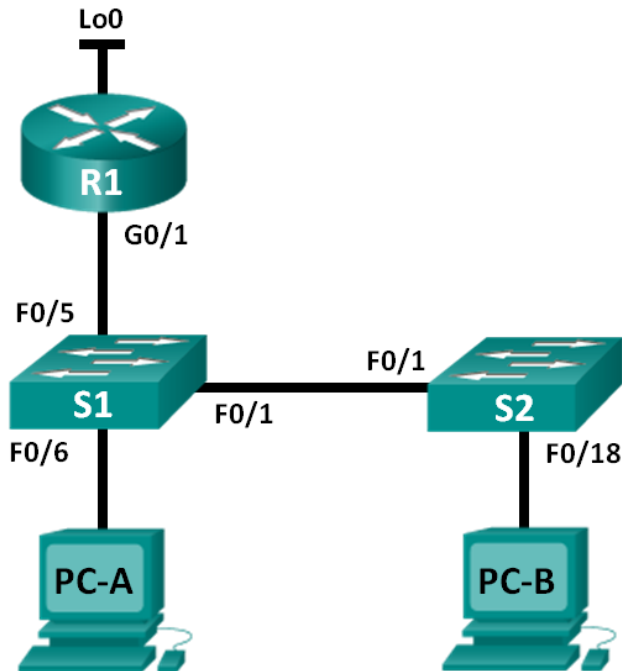
```
R1(config-if)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

Router R2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

Lab 30 – Configuring Basic DHCPv4 on a Switch

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.225	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Change the SDM Preference

- Set the SDM preference to lanbase-routing on S1.

Part 3: Configure DHCPv4

- Configure DHCPv4 for VLAN 1.
- Verify DHCPv4 and connectivity.

Part 4: Configure DHCP for Multiple VLANs

- Assign ports to VLAN 2.
- Configure DHCPv4 for VLAN 2.

- Verify DHCPv4 and connectivity.

Part 5: Enable IP Routing

- Enable IP routing on the switch.
- Create static routes.

Background / Scenario

A Cisco 2960 switch can function as a DHCPv4 server. The Cisco DHCPv4 server assigns and manages IPv4 addresses from identified address pools that are associated with specific VLANs and switch virtual interfaces (SVIs). The Cisco 2960 switch can also function as a Layer 3 device and route between VLANs and a limited number of static routes. In this lab, you will configure DHCPv4 for both single and multiple VLANs on a Cisco 2960 switch, enable routing on the switch to allow for communication between VLANs, and add static routes to allow for communication between all hosts.

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

Note: Make sure that the router and 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)
- 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 cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

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

Step 2: Initialize and reload the router and switches.

Step 3: Configure basic setting on devices.

- Assign device names as shown in the topology.
- Disable DNS lookup.
- Assign **class** as the enable password and assign **cisco** as the console and vty passwords.
- Configure the IP addresses on R1 G0/1 and Lo0 interfaces, according to the Addressing Table.
- Configure the IP addresses on S1 VLAN 1 and VLAN 2 interfaces, according to the Addressing Table.
- Save the running configuration to the startup configuration file.

Part 2: Change the SDM Preference

The Cisco Switch Database Manager (SDM) provides multiple templates for the Cisco 2960 switch. The templates can be enabled to support specific roles depending on how the switch is used in the network. In this lab, the sdm lanbase-routing template is enabled to allow the switch to route between VLANs and to support static routing.

Step 1: Display the SDM preference on S1.

On S1, issue the **show sdm prefer** command in privileged EXEC mode. If the template has not been changed from the factory default, it should still be the **default** template. The **default** template does not support static routing. If IPv6 addressing has been enabled, the template will be **dual-ipv4-and-ipv6 default**.

```
S1# show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

number of unicast mac addresses:          8K
number of IPv4 IGMP groups:              0.25K
number of IPv4/MAC qos aces:             0.125k
number of IPv4/MAC security aces:        0.375k
```

What is the current template?

Step 2: Change the SDM Preference on S1.

- a. Set the SDM preference to **lanbase-routing**. (If lanbase-routing is the current template, please proceed to Part 3.) From global configuration mode, issue the **sdm prefer lanbase-routing** command.

```
S1(config)# sdm prefer lanbase-routing
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

Which template will be available after reload? _____

- b. The switch must be reloaded for the template to be enabled.

```
S1# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

Note: The new template will be used after reboot even if the running configuration has not been saved. To save the running configuration, answer **yes** to save the modified system configuration.

Step 3: Verify that lanbase-routing template is loaded.

Issue the **show sdm prefer** command to verify that the lanbase-routing template has been loaded on S1.

```
S1# show sdm prefer
The current template is "lanbase-routing" template.
The selected template optimizes the resources in
the switch to support this level of features for
```

0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	4K
number of IPv4 IGMP groups + multicast routes:	0.25K
number of IPv4 unicast routes:	0.75K
number of directly-connected IPv4 hosts:	0.75K
number of indirect IPv4 routes:	16
number of IPv6 multicast groups:	0.375k
number of directly-connected IPv6 addresses:	0.75K
number of indirect IPv6 unicast routes:	16
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.125k
number of IPv4/MAC security aces:	0.375k
number of IPv6 policy based routing aces:	0
number of IPv6 qos aces:	0.375k
number of IPv6 security aces:	127

Part 3: Configure DHCPv4

In Part 3, you will configure DHCPv4 for VLAN 1, check IP settings on host computers to validate DHCP functionality, and verify connectivity for all devices in VLAN 1.

Step 1: Configure DHCP for VLAN 1.

- Exclude the first 10 valid host addresses from network 192.168.1.0/24. Write the command you used in the space provided.

- Create a DHCP pool named **DHCP1**. Write the command you used in the space provided.

- Assign the network 192.168.1.0/24 for available addresses. Write the command you used in the space provided.

- Assign the default gateway as 192.168.1.1. Write the command you used in the space provided.

- Assign the DNS server as 192.168.1.9. Write the command you used in the space provided.

- Assign a lease time of 3 days. Write the command you used in the space provided.

- Save the running configuration to the startup configuration file.

Step 2: Verify DHCP and connectivity.

- On PC-A and PC-B, open the command prompt and issue the **ipconfig** command. If IP information is not present, or if it is incomplete, issue the **ipconfig /release** command, followed by the **ipconfig /renew** command.

For PC-A, list the following:

IP Address: _____

Subnet Mask: _____

Default Gateway: _____

For PC-B, list the following:

IP Address: _____

Subnet Mask: _____

Default Gateway: _____

- b. Test connectivity by pinging from PC-A to the default gateway, PC-B, and R1.

From PC-A, is it possible to ping the VLAN 1 default gateway? _____

From PC-A, is it possible to ping PC-B? _____

From PC-A, is it possible to ping R1 G0/1? _____

If the answer is no to any of these questions, troubleshoot the configurations and correct the error.

Part 4: Configure DHCPv4 for Multiple VLANs

In Part 4, you will assign PC-A to a port accessing VLAN 2, configure DHCPv4 for VLAN 2, renew the IP configuration of PC-A to validate DHCPv4, and verify connectivity within the VLAN.

Step 1: Assign a port to VLAN 2.

Place port F0/6 into VLAN 2. Write the command you used in the space provided.

Step 2: Configure DHCPv4 for VLAN 2

- a. Exclude the first 10 valid host addresses from network 192.168.2.0. Write the command you used in the space provided.

- b. Create a DHCP pool named **DHCP2**. Write the command you used in the space provided.

- c. Assign the network 192.168.2.0/24 for available addresses. Write the command you used in the space provided.

- d. Assign the default gateway as 192.168.2.1. Write the command you used in the space provided.

- e. Assign the DNS server as 192.168.2.9. Write the command you used in the space provided.

- f. Assign a lease time of 3 days. Write the command you used in the space provided.

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

Step 3: Verify DHCPv4 and connectivity.

- a. On PC-A, open the command prompt and issue the **ipconfig /release** command, followed by **ipconfig /renew** command.

For PC-A, list the following:

IP Address: _____

Subnet Mask: _____

Default Gateway: _____

- b. Test connectivity by pinging from PC-A to the VLAN 2 default gateway and PC-B.

From PC-A, is it possible to ping the default gateway? _____

From PC-A, is it possible to ping PC-B? _____

Were these pings successful? Why?

- c. Issue the **show ip route** command on S1.

What was the result of this command?

Part 5: Enable IP Routing

In Part 5, you will enable IP routing on the switch, which will allow for inter-VLAN communication. For all networks to communicate, static routes on S1 and R1 must be implemented.

Step 1: Enable IP routing on S1.

- a. From global configuration mode, use the **ip routing** command to enable routing on S1.

`S1(config)# ip routing`

- b. Verify inter-VLAN connectivity.

From PC-A, is it possible to ping PC-B? _____

What function is the switch performing? _____

- c. View the routing table information for S1.

What route information is contained in the output of this command?

- d. View the routing table information for R1.

What route information is contained in the output of this command?

- e. From PC-A, is it possible to ping R1? _____

From PC-A, is it possible to ping Lo0? _____

Consider the routing table of the two devices, what must be added to communicate between all networks?

Step 2: Assign static routes.

Enabling IP routing allows the switch to route between VLANs assigned on the switch. For all VLANs to communicate with the router, static routes must be added to the routing table of both the switch and the router.

- a. On S1, create a default static route to R1. Write the command you used in the space provided.

- b. On R1, create a static route to VLAN 2. Write the command you used in the space provided.

- c. View the routing table information for S1.

How is the default static route represented?

- d. View the routing table information for R1.

How is the static route represented?

- e. From PC-A, is it possible to ping R1? _____

From PC-A, is it possible to ping Lo0? _____

Reflection

1. In configuring DHCPv4, why would you exclude the static addresses prior to setting up the DHCPv4 pool?

2. If multiple DHCPv4 pools are present, how does the switch assign the IP information to hosts?

3. Besides switching, what functions can the Cisco 2960 switch perform?

Router Interface Summary Table

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

Appendix A: Configuration Commands

Configure DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

Configure DHCPv4 for Multiple VLANs

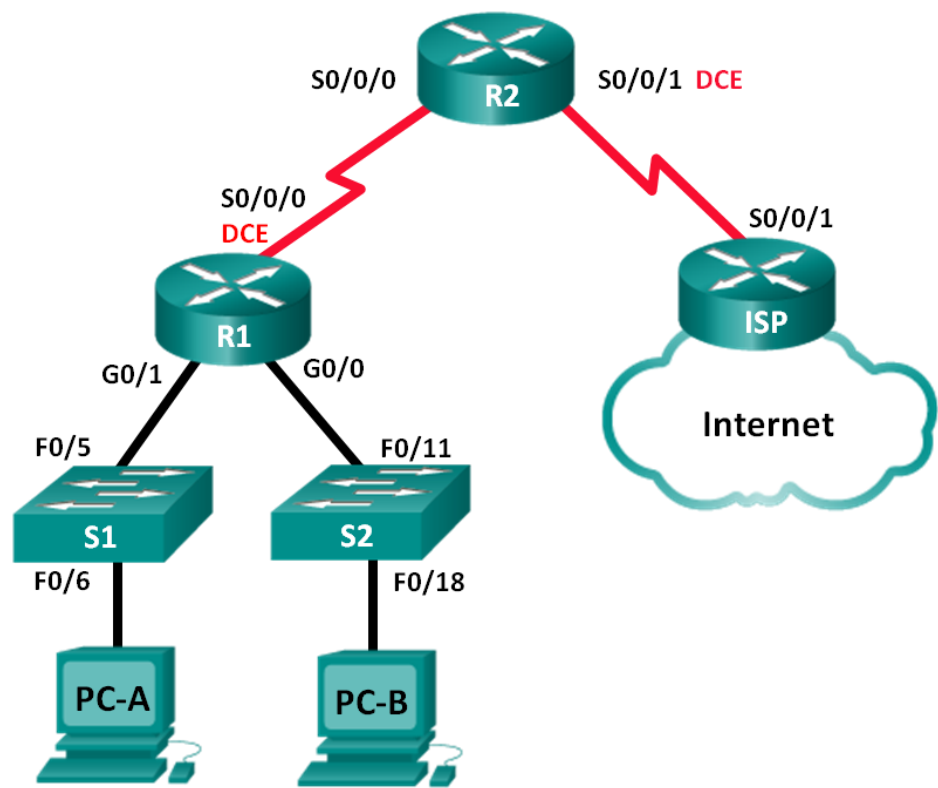
```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)# ip dhcp pool DHCP2
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.2.1
S1(dhcp-config)# dns-server 192.168.2.9
S1(dhcp-config)# lease 3
```

Enable IP Routing

```
S1(config)# ip routing
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

Lab 31 - Troubleshooting DHCPv4

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.128	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.253	255.255.255.252	N/A
R2	S0/0/0	192.168.0.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.252	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.0.2	255.255.255.128	192.168.0.1
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot DHCPv4 Issues

Background / Scenario

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that lets the network administrators manage and automate the assignment of IP addresses. Without DHCP, the administrator must manually assign and configure IP addresses, preferred DNS servers, and the default gateway. As the network grows in size, this becomes an administrative problem when devices are moved from one internal network to another.

In this scenario, the company has grown in size, and the network administrators can no longer assign IP addresses to devices manually. The R2 router has been configured as a DHCP server to assign IP addresses to the host devices on router R1 LANs. Several errors in the configuration have resulted in connectivity issues. You are asked to troubleshoot and correct the configuration errors and document your work.

Ensure that the network supports the following:

- 1) The router R2 should function as the DHCP server for the 192.168.0.0/25 and 192.168.1.0/24 networks connected to R1.
- 2) All PCs connected to S1 and S2 should receive an IP address in the correct network via DHCP.

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 Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers and switches with basic settings, such as passwords and IP addresses. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- a. Disable DNS lookup.
- b. Configure device name as shown in the topology.

- c. Assign **class** as the privileged EXEC password.
- d. Assign **cisco** as the console and vty passwords.
- e. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- f. Configure the IP addresses for all the router interfaces.
- g. Set clock rate to **128000** for all DCE router interfaces.
- h. Configure EIGRP for R1.

```
R1(config)# router eigrp 1
R1(config-router)# network 192.168.0.0 0.0.0.127
R1(config-router)# network 192.168.0.252 0.0.0.3
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
```

- i. Configure EIGRP and a static default route on R2.

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.0.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- j. Configure a summary static route on ISP to the networks on R1 and R2 routers.

```
ISP(config)# ip route 192.168.0.0 255.255.254.0 209.165.200.226
```

Step 4: Verify network connectivity between the routers.

If any pings between the routers fail, correct the errors before proceeding to the next step. Use **show ip route** and **show ip interface brief** to locate possible issues.

Step 5: Configure basic settings for each switch.

- a. Disable DNS lookup.
- b. Configure device name as shown in the topology.
- c. Configure the IP address for the VLAN 1 interface and the default gateway for each switch.
- d. Assign **class** as the privileged EXEC mode password.
- e. Assign **cisco** as the console and vty passwords.
- f. Configure **logging synchronous** for the console line.

Step 6: Verify the hosts are configured for DHCP.

Step 7: Load the initial DHCP configuration for R1 and R2.

Router R1

```
interface GigabitEthernet0/1
ip helper-address 192.168.0.253
```

Router R2

```
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
```

```

ip dhcp pool R1G1
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
ip dhcp pool R1G0
  network 192.168.0.0 255.255.255.128
  default-router 192.168.11.1

```

Part 2: Troubleshoot DHCPv4 Issues

After configuring routers R1 and R2 with DHCPv4 settings, several errors in the DHCP configurations were introduced and resulted in connectivity issues. R2 is configured as a DHCP server. For both pools of DHCP addresses, the first nine addresses are reserved for the routers and switches. R1 relays the DHCP information to all the R1 LANs. Currently, PC-A and PC-B have no access to the network. Use the **show** and **debug** commands to determine and correct the network connectivity issues.

Step 1: Record IP settings for PC-A and PC-B.

- For PC-A and PC-B, at the command prompt, enter **ipconfig /all** to display the IP and MAC addresses.
- Record the IP and MAC addresses in the table below. The MAC address can be used to determine which PC is involved in the debug message.

	IP Address/Subnet Mask	MAC Address
PC-A		
PC-B		

Step 2: Troubleshoot DHCP issues for the 192.168.1.0/24 network on router R1.

Router R1 is a DHCP relay agent for all the R1 LANs. In this step, only the DHCP process for the 192.168.1.0/24 network will be examined. The first nine addresses are reserved for other network devices, such as routers, switches, and servers.

- Use a DHCP **debug** command to observe the DHCP process on R2 router.

```
R2# debug ip dhcp server events
```

- On R1, display the running configuration for the G0/1 interface.

```

R1# show run interface g0/1
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  ip helper-address 192.168.0.253
  duplex auto
  speed auto

```

If there are any DHCP relay issues, record any commands that are necessary to correct the configurations errors.

- In a command prompt on PC-A, type **ipconfig /renew** to receive an address from the DHCP server. Record the configured IP address, subnet mask, and default gateway for PC-A.

- d. Observe the debug messages on R2 router for the DHCP renewal process for PC-A. The DHCP server attempted to assign 192.168.1.1/24 to PC-A. This address is already in use for G0/1 interface on R1. The same issue occurs with IP address 192.168.1.2/24 because this address has been assigned to S1 in the initial configuration. Therefore, an IP address of 192.168.1.3/24 has been assigned to PC-A. The DHCP assignment conflict indicates there may be an issue with the excluded-address statement on the DHCP server configuration on R2.

```
*Mar  5 06:32:16.939: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.939: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.943: DHCPD: Allocated binding 2944C764
*Mar  5 06:32:16.943: DHCPD: Adding binding to radix tree (192.168.1.1)
*Mar  5 06:32:16.943: DHCPD: Adding binding to hash tree
*Mar  5 06:32:16.943: DHCPD: assigned IP address 192.168.1.1 to client
0100.5056.be76.8c.
*Mar  5 06:32:16.951: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged
192.168.1.1.
*Mar  5 06:32:16.951: DHCPD: returned 192.168.1.1 to address pool R1G1.
*Mar  5 06:32:16.951: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:16.951:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.951:
R2#6.951: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:16.951:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.951: DHCPD: Allocated binding 31DC93C8
*Mar  5 06:32:16.951: DHCPD: Adding binding to radix tree (192.168.1.2)
*Mar  5 06:32:16.951: DHCPD: Adding binding to hash tree
*Mar  5 06:32:16.951: DHCPD: assigned IP address 192.168.1.2 to client
0100.5056.be76.8c.
*Mar  5 06:32:18.383: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged
192.168.1.2.
*Mar  5 06:32:18.383: DHCPD: returned 192.168.1.2 to address pool R1G1.
*Mar  5 06:32:18.383: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Allocated binding 2A40E074
*Mar  5 06:32:18.383: DHCPD: Adding binding to radix tree (192.168.1.3)
*Mar  5 06:32:18.383: DHCPD: Adding binding to hash tree
*Mar  5 06:32:18.383: DHCPD: assigned IP address 192.168.1.3 to client
0100.5056.be76.8c.
<output omitted>
```

- e. Display the DHCP server configuration on R2. The first nine addresses for 192.168.1.0/24 network are not excluded from the DHCP pool.

```
R2# show run | section dhcp
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
    network 192.168.1.0 255.255.255.0
    default-router 192.168.1.1
ip dhcp pool R1G0
    network 192.168.0.0 255.255.255.128
    default-router 192.168.1.1
```

Record the commands to resolve the issue on R2.

- f. At the command prompt on PC-A, type **ipconfig /release** to return the 192.168.1.3 address back to the DHCP pool. The process can be observed in the debug message on R2.

```
*Mar  5 06:49:59.563: DHCPD: Sending notification of TERMINATION:
*Mar  5 06:49:59.563:  DHCPD: address 192.168.1.3 mask 255.255.255.0
*Mar  5 06:49:59.563:  DHCPD: reason flags: RELEASE
*Mar  5 06:49:59.563:  DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:49:59.563:  DHCPD: lease time remaining (secs) = 85340
*Mar  5 06:49:59.563: DHCPD: returned 192.168.1.3 to address pool R1G1.
```

- g. At the command prompt on PC-A, type **ipconfig /renew** to be assigned a new IP address from the DHCP server. Record the assigned IP address and default gateway information.
-

The process can be observed in the debug message on R2.

```
*Mar  5 06:50:11.863: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:50:11.863:  DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:50:11.863:  DHCPD: circuit id 00000000
*Mar  5 06:50:11.863: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:50:11.863:  DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:50:11.863:  DHCPD: circuit id 00000000
*Mar  5 06:50:11.863: DHCPD: requested address 192.168.1.3 has already been assigned.
*Mar  5 06:50:11.863: DHCPD: Allocated binding 3003018C
*Mar  5 06:50:11.863: DHCPD: Adding binding to radix tree (192.168.1.10)
*Mar  5 06:50:11.863: DHCPD: Adding binding to hash tree
*Mar  5 06:50:11.863: DHCPD: assigned IP address 192.168.1.10 to client
0100.5056.be76.8c.
<output omitted>
```

- h. Verify network connectivity.

Can PC-A ping the assigned default gateway? _____

Can PC-A ping the R2 router? _____

Can PC-A ping the ISP router? _____

Step 3: Troubleshoot DHCP issues for 192.168.0.0/25 network on R1.

Router R1 is a DHCP relay agent for all the R1 LANs. In this step, only the DHCP process for the 192.168.0.0/25 network is examined. The first nine addresses are reserved for other network devices.

- a. Use a DHCP **debug** command to observe the DHCP process on R2.

```
R2# debug ip dhcp server events
```

- b. Display the running configuration for the G0/0 interface on R1 to identify possible DHCP issues.

```
R1# show run interface g0/0
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.128
 duplex auto
 speed auto
```

Record the issues and any commands that are necessary to correct the configurations errors.

- c. From the command prompt on PC-B, type **ipconfig /renew** to receive an address from the DHCP server. Record the configured IP address, subnet mask, and default gateway for PC-B.
-

- d. Observe the debug messages on R2 router for the renewal process for PC-A. The DHCP server assigned 192.168.0.10/25 to PC-B.

```
*Mar  5 07:15:09.663: DHCPD: Sending notification of DISCOVER:
*Mar  5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar  5 07:15:09.663: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar  5 07:15:09.707: DHCPD: Sending notification of ASSIGNMENT:
*Mar  5 07:15:09.707:   DHCPD: address 192.168.0.10 mask 255.255.255.128
*Mar  5 07:15:09.707:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.707:   DHCPD: lease time remaining (secs) = 86400
```

- e. Verify network connectivity.

Can PC-B ping the DHCP assigned default gateway? _____

Can PC-B ping its default gateway (192.168.0.1)? _____

Can PC-B ping the R2 router? _____

Can PC-B ping the ISP router? _____

- f. If any issues failed in Step e, record the problems and any commands to resolve the issues.
-
-
-

- g. Release and renew the IP configurations on PC-B. Repeat Step e to verify network connectivity.

- h. Discontinue the debug process by using the **undebug all** command.

```
R2# undebug all
All possible debugging has been turned off
```

Reflection

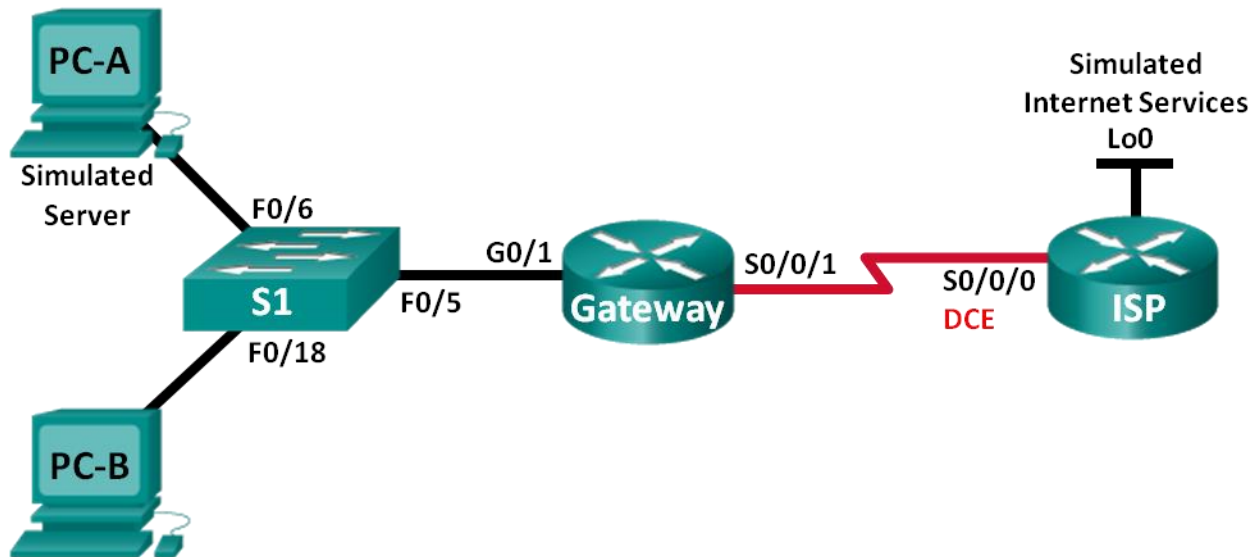
What are the benefits of using DHCP?

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.				

Lab 32 – Configuring Dynamic and Static NAT

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (Simulated Server)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify Static NAT

Part 3: Configure and Verify Dynamic NAT

Background / Scenario

Network Address Translation (NAT) is the process where a network device, such as a Cisco router, assigns a public address to host devices inside a private network. The main reason to use NAT is to reduce the number of public IP addresses that an organization uses because the number of available IPv4 public addresses is limited.

In this lab, an ISP has allocated the public IP address space of 209.165.200.224/27 to a company. This provides the company with 30 public IP addresses. The addresses, 209.165.200.225 to 209.165.200.241, are

for static allocation and 209.165.200.242 to 209.165.200.254 are for dynamic allocation. A static route is used from the ISP to the gateway router, and a default route is used from the gateway to the ISP router. The ISP connection to the Internet is simulated by a loopback address on the ISP router.

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

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

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

Step 2: Configure PC hosts.

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

Step 4: Configure basic settings for each router.

- Disable DNS lookup.
- Configure IP addresses for the routers as listed in the Addressing Table.
- Set the clock rate to **1280000** for the DCE serial interfaces.
- Configure device name as shown in the topology.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure **logging synchronous** to prevent console messages from interrupting the command entry.

Step 5: Create a simulated web server on ISP.

- Create a local user named **webuser** with an encrypted password of **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```
- Enable the HTTP server service on ISP.

```
ISP(config)# ip http server
```

- c. Configure the HTTP service to use the local user database.

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

Step 6: Configure static routing.

- a. Create a static route from the ISP router to the Gateway router using the assigned public network address range 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

- b. Create a default route from the Gateway router to the ISP router.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

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

Step 8: Verify network connectivity.

- a. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.
- b. Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

Part 2: Configure and Verify Static NAT

Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant. Static NAT is particularly useful for web servers or devices that must have static addresses that are accessible from the Internet.

Step 1: Configure a static mapping.

A static map is configured to tell the router to translate between the private inside server address 192.168.1.20 and the public address 209.165.200.225. This allows a user from the Internet to access PC-A. PC-A is simulating a server or device with a constant address that can be accessed from the Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

Step 2: Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Step 3: Test the configuration.

- a. Display the static NAT table by issuing the **show ip nat translations** command.

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20      ---                ---
```

What is the translation of the Inside local host address?

192.168.1.20 = _____

The Inside global address is assigned by?

The Inside local address is assigned by?

- b. From PC-A, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:1	192.168.1.20:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.225	192.168.1.20	---	---

A NAT entry was added to the table with ICMP listed as the protocol when PC-A sent an ICMP request (ping) to 192.31.7.1 on ISP.

What port number was used in this ICMP exchange? _____

Note: It may be necessary to disable the PC-A firewall for the ping to be successful.

- c. From PC-A, telnet to the ISP Lo0 interface and display the NAT table.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:1	192.168.1.20:1	192.31.7.1:1	192.31.7.1:1
tcp	209.165.200.225:1034	192.168.1.20:1034	192.31.7.1:23	192.31.7.1:23
---	209.165.200.225	192.168.1.20	---	---

Note: The NAT for the ICMP request may have timed out and been removed from the NAT table.

What was the protocol used in this translation? _____

What are the port numbers used?

Inside global / local: _____

Outside global / local: _____

- d. Because static NAT was configured for PC-A, verify that pinging from ISP to PC-A at the static NAT public address (209.165.200.225) is successful.
- e. On the Gateway router, display the NAT table to verify the translation.

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:12	192.168.1.20:12	209.165.201.17:12	209.165.201.17:12
---	209.165.200.225	192.168.1.20	---	---

Notice that the Outside local and Outside global addresses are the same. This address is the ISP remote network source address. For the ping from the ISP to succeed, the Inside global static NAT address 209.165.200.225 was translated to the Inside local address of PC-A (192.168.1.20).

- f. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

Gateway# **show ip nat statistics**

Total active translations: 2 (1 static, 1 dynamic; 1 extended)

Peak translations: 2, occurred 00:02:12 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 39 Misses: 0

```
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Note: This is only a sample output. Your output may not match exactly.

Part 3: Configure and Verify Dynamic NAT

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Dynamic NAT results in a many-to-many address mapping between local and global addresses.

Step 1: Clear NATs.

Before proceeding to add dynamic NATs, clear the NATs and statistics from Part 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

Step 2: Define an access control list (ACL) that matches the LAN private IP address range.

ACL 1 is used to allow 192.168.1.0/24 network to be translated.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 3: Verify that the NAT interface configurations are still valid.

Issue the **show ip nat statistics** command on the Gateway router to verify the NAT configurations.

Step 4: Define the pool of usable public IP addresses.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

Step 5: Define the NAT from the inside source list to the outside pool.

Note: Remember that NAT pool names are case-sensitive and the pool name entered here must match that used in the previous step.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Step 6: Test the configuration.

- From PC-B, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.165.200.225    192.168.1.20      ---               ---
icmp 209.165.200.242:1 192.168.1.21:1    192.31.7.1:1      192.31.7.1:1
--- 209.165.200.242    192.168.1.21      ---               ---
```

What is the translation of the Inside local host address for PC-B?

192.168.1.21 = _____

A dynamic NAT entry was added to the table with ICMP as the protocol when PC-B sent an ICMP message to 192.31.7.1 on ISP.

What port number was used in this ICMP exchange? _____

- b. From PC-B, open a browser and enter the IP address of the ISP-simulated web server (Lo0 interface). When prompted, log in as **webuser** with a password of **webpass**.
- c. Display the NAT table.

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1041	192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042	192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043	192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044	192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1045	192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046	192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047	192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048	192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049	192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050	192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1051	192.168.1.21:1051	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1052	192.168.1.21:1052	192.31.7.1:80	192.31.7.1:80
---	209.165.200.242	192.168.1.22	---	---

What protocol was used in this translation? _____

What port numbers were used?

Inside: _____

outside: _____

What well-known port number and service was used? _____

- d. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

Gateway# **show ip nat statistics**

Total active translations: 3 (1 static, 2 dynamic; 1 extended)

Peak translations: 17, occurred 00:06:40 ago

Outside interfaces:

Serial0/0/1

Inside interfaces:

GigabitEthernet0/1

Hits: 345 Misses: 0

CEF Translated packets: 345, CEF Punted packets: 0

Expired translations: 20

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public_access refcount 2

```
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13, allocated 1 (7%), misses 0
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Note: This is only a sample output. Your output may not match exactly.

Step 7: Remove the static NAT entry.

In Step 7, the static NAT entry is removed and you can observe the NAT entry.

- a. Remove the static NAT from Part 2. Enter **yes** when prompted to delete child entries.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225
```

```
Static entry in use, do you want to delete child entries? [no]: yes
```

- b. Clear the NATs and statistics.
- c. Ping the ISP (192.31.7.1) from both hosts.
- d. Display the NAT table and statistics.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 2 (15%), misses 0
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

```
Gateway# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243     192.168.1.20     ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
```

```

--- 209.165.200.242    192.168.1.21    ---

```

Note: This is only a sample output. Your output may not match exactly.

Reflection

1. Why would NAT be used in a network?

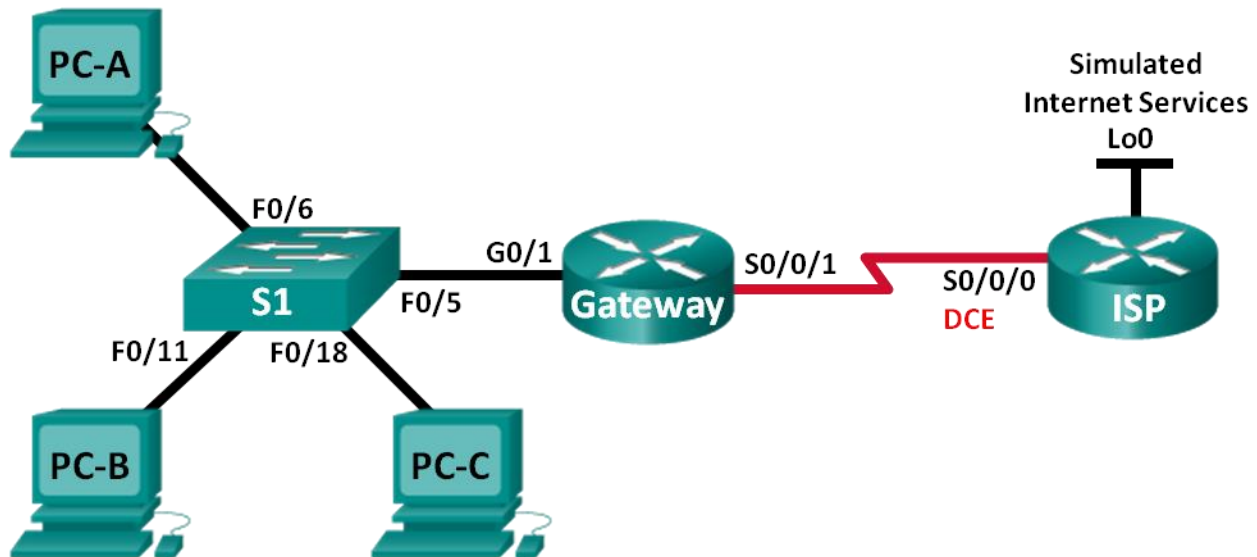
2. What are the limitations of NAT?

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.				

Lab 33 – Configuring NAT Pool Overload and PAT

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify NAT Pool Overload

Part 3: Configure and Verify PAT

Background / Scenario

In the first part of the lab, your company is allocated the public IP address range of 209.165.200.224/29 by the ISP. This provides the company with six public IP addresses. Dynamic NAT pool overload uses a pool of IP addresses in a many-to-many relationship. The router uses the first IP address in the pool and assigns connections using the IP address plus a unique port number. After the maximum number of translations for a single IP address have been reached on the router (platform and hardware specific), it uses the next IP address in the pool.

In Part 2, the ISP has allocated a single IP address, 209.165.201.18, to your company for use on the Internet connection from the company Gateway router to the ISP. You will use the Port Address Translation (PAT) to convert multiple internal addresses into the one usable public address. You will test, view, and verify that the translations are taking place, and you will interpret the NAT/PAT statistics to monitor the process.

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 switch 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 Switch (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 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.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches.

Step 4: Configure basic settings for each router.

- Disable DNS lookup.
- Configure IP addresses for the routers as listed in the Addressing Table.
- Set the clock rate to **128000** for DCE serial interface.
- Configure device name as shown in the topology.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure **logging synchronous** to prevent console messages from interrupting the command entry.

Step 5: Configure static routing.

- Create a static route from the ISP router to the Gateway router.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```
- Create a default route from the Gateway router to the ISP router.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Step 6: Verify network connectivity.

- a. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.
- b. Verify that the static routes are configured correctly on both routers.

Part 2: Configure and Verify NAT Pool Overload

In Part 2, you will configure the Gateway router to translate the IP addresses from the 192.168.1.0/24 network to one of the six usable addresses in the 209.165.200.224/29 range.

Step 1: Define an access control list that matches the LAN private IP addresses.

ACL 1 is used to allow the 192.168.1.0/24 network to be translated.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 2: Define the pool of usable public IP addresses.

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Step 3: Define the NAT from the inside source list to the outside pool.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Step 4: Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Step 5: Verify the NAT pool overload configuration.

- a. From each PC host, ping the 192.31.7.1 address on the ISP router.
- b. Display NAT statistics on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
pool public_access: netmask 255.255.255.248
```

```
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6, allocated 1 (16%), misses 0
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

c. Display NATs on the Gateway router.

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:0 192.168.1.20:1    192.31.7.1:1      192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1    192.31.7.1:1      192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1    192.31.7.1:1      192.31.7.1:2
```

Note: Depending on how much time has elapsed since you performed the pings from each PC, you may not see all three translations. ICMP translations have a short timeout value.

How many Inside local IP addresses are listed in the sample output above? _____

How many Inside global IP addresses are listed? _____

How many port numbers are used paired with the Inside global addresses? _____

What would be the result of pinging the Inside local address of PC-A from the ISP router? Why?

Part 3: Configure and Verify PAT

In Part 3, you will configure PAT by using an interface instead of a pool of addresses to define the outside address. Not all of the commands in Part 2 will be reused in Part 3.

Step 1: Clear NATs and statistics on the Gateway router.

Step 2: Verify the configuration for NAT.

- Verify that statistics have been cleared.
- Verify that the outside and inside interfaces are configured for NATs.
- Verify that the ACL is still configured for NATs.

What command did you use to confirm the results from steps a to c?

Step 3: Remove the pool of useable public IP addresses.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Step 4: Remove the NAT translation from inside source list to outside pool.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Step 5: Associate the source list with the outside interface.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload
```

Step 6: Test the PAT configuration.

- a. From each PC, ping the 192.31.7.1 address on the ISP router.
- b. Display NAT statistics on the Gateway router.

```
Gateway# show ip nat statistics
```

```
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
```

```
Peak translations: 3, occurred 00:00:19 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

```
GigabitEthernet0/1
```

```
Hits: 24 Misses: 0
```

```
CEF Translated packets: 24, CEF Punted packets: 0
```

```
Expired translations: 0
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3
```

```
Total doors: 0
```

```
Appl doors: 0
```

```
Normal doors: 0
```

```
Queued Packets: 0
```

- c. Display NAT translations on Gateway.

```
Gateway# show ip nat translations
```

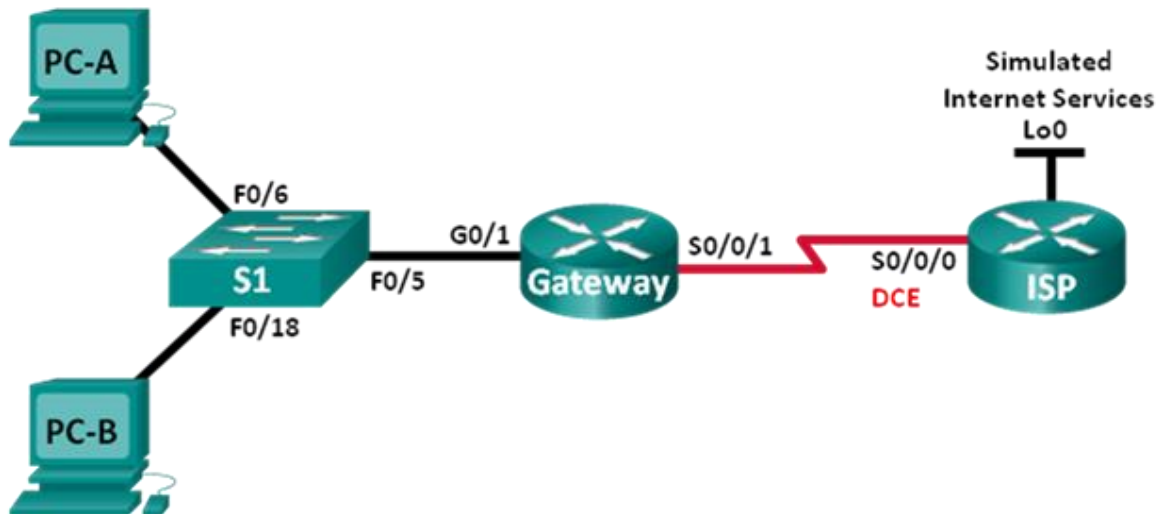
Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:3	192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp	209.165.201.18:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.201.18:4	192.168.1.22:1	192.31.7.1:1	192.31.7.1:4

Reflection

What advantages does PAT provide?

Lab 34 - Troubleshooting NAT Configurations

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.4	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot Static NAT

Part 3: Troubleshoot Dynamic NAT

Background / Scenario

In this lab, the Gateway router was configured by an inexperienced network administrator at your company. Several errors in the configuration have resulted in NAT issues. Your boss has asked you to troubleshoot and correct the NAT errors and document your work. Ensure that the network supports the following:

- PC-A acts as a web server with a static NAT and will be reachable from the outside using the 209.165.200.254 address.
- PC-B acts as a host computer and dynamically receives an IP address from the created pool of addresses called NAT_POOL, which uses the 209.165.200.240/29 range.

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 switch 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 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet 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 the routers with basic settings. Additional NAT-related configurations are provided. The NAT configurations for the Gateway router contains errors that you will identify and correct as you proceed through the lab.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switch and routers.

Step 4: Configure basic settings for each router.

- Disable DNS lookup.
- Configure device name as shown in the topology.
- Configure IP addresses as listed in the Address Table.
- Set the clock rate to **128000** for DCE serial interfaces.
- Assign **cisco** as the console and vty password.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure **logging synchronous** to prevent console messages from interrupting the command entry.

Step 5: Configure static routing.

- Create a static route from the ISP router to the Gateway router-assigned public network address range 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 s0/0/0
```

- Create a default route from the Gateway router to the ISP router.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

Step 6: Load router configurations.

The configurations for the routers are provided for you. There are errors with the configuration for the Gateway router. Identify and correct the configurations errors.

Gateway Router Configuration

```
interface g0/1
  ip nat outside
  no shutdown
interface s0/0/0
  ip nat outside
interface s0/0/1
  no shutdown
ip nat inside source static 192.168.2.3 209.165.200.254
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL
ip access-list standard NAT_ACL
  permit 192.168.10.0 0.0.0.255
banner motd $AUTHORIZED ACCESS ONLY$
end
```

Step 7: Save the running configuration to the startup configuration.**Part 2: Troubleshoot Static NAT**

In Part 2, you will examine the static NAT for PC-A to determine if it is configured correctly. You will troubleshoot the scenario until the correct static NAT is verified.

- a. To troubleshoot issues with NAT, use the **debug ip nat** command. Turn on NAT debugging to see translations in real-time across the Gateway router.

Gateway# **debug ip nat**

- b. From PC-A, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

- c. On the Gateway router, enter the command that allows you to see all current NAT translations on the Gateway router. Write the command in the space below.

Why are you seeing a NAT translation in the table, but none occurred when PC-A pinged the ISP loopback interface? What is needed to correct the issue?

- d. Record any commands that are necessary to correct the static NAT configuration error.

- e. From PC-A, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

- f. On the Gateway router, enter the command that allows you to observe the total number of current NATs. Write the command in the space below.

Is the static NAT occurring successfully? Why?

- g. On the Gateway router, enter the command that allows you to view the current configuration of the router. Write the command in the space below.

- h. Are there any problems with the current configuration that prevent the static NAT from occurring?

- i. Record any commands that are necessary to correct the static NAT configuration errors.

- j. From PC-A, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

- k. Use the **show ip nat translations verbose** command to verify static NAT functionality.

Note: The timeout value for ICMP is very short. If you do not see all the translations in the output, redo the ping.

Is the static NAT translation occurring successfully? _____

If static NAT is not occurring, repeat the steps above to troubleshoot the configuration.

Part 3: Troubleshoot Dynamic NAT

- a. From PC-B, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

- b. On the Gateway router, enter the command that allows you to view the current configuration of the router. Are there any problems with the current configuration that prevent dynamic NAT from occurring?

- c. Record any commands that are necessary to correct the dynamic NAT configuration errors.

- d. From PC-B, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

- e. Use the **show ip nat statistics** to view NAT usage.

Is the NAT occurring successfully? _____

What percentage of dynamic addresses has been allocated? _____

- f. Turn off all debugging using the **undebug all** command.

Reflection

1. What is the benefit of a static NAT?

2. What issues would arise if 10 host computers in this network were attempting simultaneous Internet communication?

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.				