



CCNA 3: Student Lab Manual v5.0

Student 1 name: _____

Student 1 number: _____

Student 2 name: _____

Student 2 number: _____

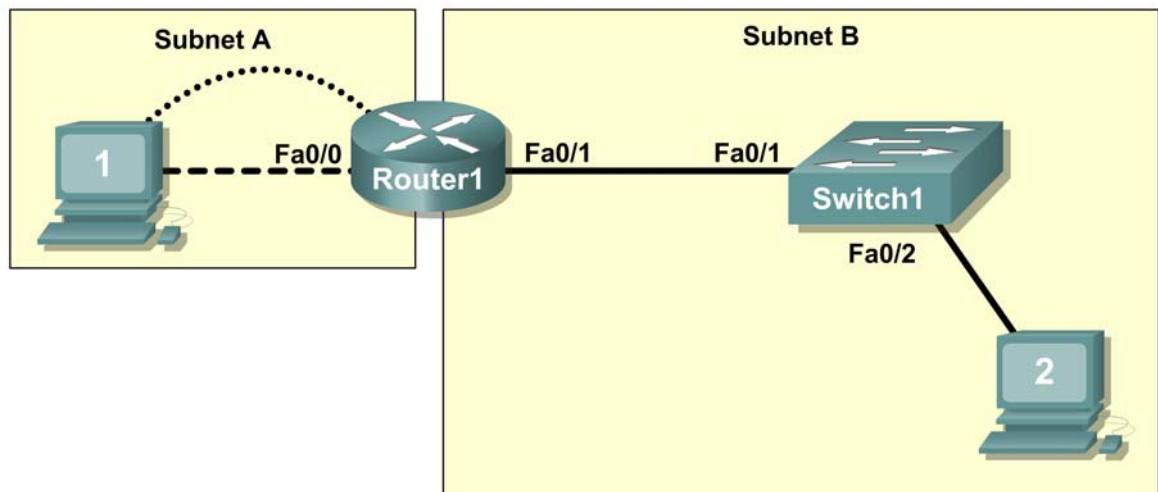
Student class ID: _____

Date when this workbook was submitted: _____

Lab 1.3.3: Troubleshooting a Small Network.....	3
Lab 2.5.1: Basic Switch Configuration.....	7
Appendix 1: Erasing and Reloading the Switch	19
Lab 2.5.3: Password Recovery – Challenge	21
Appendix 2: Password Recovery for the Catalyst 2960	24
Lab 3.5.1: Basic VLAN Configuration.....	29
Lab 4.4.1: Basic VTP Configuration	35
Lab 5.5.1: Basic Spanning Tree Protocol	44
Lab 5.5.2: Challenge Spanning Tree Protocol	52
Lab 6.4.1: Basic Inter-VLAN Routing	70
Lab 6.4.3: Troubleshooting Inter-VLAN Routing.....	82
Lab 7.5.1: Configuring Wireless LAN Access	88
Lab 7.5.2: Challenge Wireless Configuration.....	93

Lab 1.3.3: Troubleshooting a Small Network

Topology Diagram



Learning Objectives

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

- Verify that a paper design meets stated network requirements
- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers with supplied scripts
- Discover where communication is not possible
- Gather information about the misconfigured portion of the network along with any other errors
- Analyze information to determine why communication is not possible
- Propose solutions to network errors
- Implement solutions to network errors

Scenario

In this lab, you are given a completed configuration for a small routed network. The configuration contains design and configuration errors that conflict with stated requirements and prevent end-to-end communication. You will examine the given design and identify and correct any design errors. You will then cable the network, configure the hosts, and load configurations onto the router. Finally, you will troubleshoot the connectivity problems to determine where the errors are occurring and correct them using the appropriate commands. When all errors have been corrected, each host should be able to communicate with all other configured network elements and with the other host.

Task 1: Examine the Logical LAN Topology

The IP address block of 172.16.30.0 /23 is subnetted to meet the following requirements:

Subnet	Number of Hosts
Subnet A	174
Subnet B	60

Additional requirements and specifications:

- The 0 subnet is used.
- The smallest possible number of subnets that satisfy the requirements for hosts should be used, keeping the largest possible block in reserve for future use.
- Assign the first usable subnet to Subnet A.
- Host computers use the first IP address in the subnet. The network router uses the last network host address.

Based on these requirements, the following topology has been provided to you:

Subnet A	
Specification	Value
IP mask (decimal)	255.255.255.0
IP address	172.16.30.0
First IP host address	172.16.30.1
Last IP host address	172.16.30.254

Subnet B	
Specification	Value
IP mask (decimal)	255.255.255.128
IP address	172.16.31.0
First IP host address	172.16.31.1
Last IP host address	172.16.31.126

Examine each of the values in the tables above and verify that this topology meets all requirements and specifications. Are any of the given values incorrect? _____

If yes, correct the values in the table above and write the corrected values below:

Create a configuration table similar to the one below using your corrected values:

Device	IP address	Mask	Gateway
Host1	172.16.30.1	255.255.255.0	172.16.30.254
Router1–Fa0/0	172.16.30.254	255.255.255.0	N/A
Host2	172.16.31.1	255.255.255.128	172.16.31.126
Router1–Fa0/1	172.16.31.126	255.255.255.128	N/A

Task 2: Cable, Erase, and Reload the Routers

Step 1: Cable the network.

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

Step 2: Clear the configuration on each router.

Clear the configuration on the router using the **erase startup-config** command and then reload the router. Answer **no** if asked to save changes.

Task 3: Configure the Host Computers

Step 1: Configure host computers.

Configure the static IP address, subnet mask, and gateway for each host computer based on the configuration table created in Task 1. After configuring each host computer, display and verify the host network settings with the **ipconfig /all** command.

Task 4: Load the Router with the Supplied Scripts

```
enable
!
config term
!
hostname Router1
!
enable secret class
!
no ip domain-lookup
!
interface FastEthernet0/0
description connection to host1
ip address 172.16.30.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
description connection to switch1
ip address 192.16.31.1 255.255.255.192
duplex auto
speed auto
!
!
line con 0
password cisco
login
line vty 0
login
line vty 1 4
password cisco
login
!
end
```

Task 5: Identify Connectivity Problems

Step 1: Use the ping command to test network connectivity.

Use the following table to test the connectivity of each network device.

From	To	IP Address	Ping Results
Host1	NIC IP address	172.16.30.1	
Host1	Router1, Fa0/0	172.16.30.254	
Host1	Router1, Fa0/1	172.16.31.126	
Host1	Host2	172.16.31.1	
Host2	NIC IP address	172.16.30.1	
Host2	Router1, Fa0/1	172.16.31.126	
Host2	Router1, Fa0/0	172.16.30.254	
Host2	Host1	172.16.30.1	

Task 6: Troubleshoot Network Connections

Step 1: Begin troubleshooting at the host connected to the BRANCH router.

From host PC1, is it possible to ping PC2? _____

From host PC1, is it possible to ping the router fa0/1 interface? _____

From host PC1, is it possible to ping the default gateway? _____

From host PC1, is it possible to ping itself? _____

Where is the most logical place to begin troubleshooting the PC1 connection problems?

Step 2: Examine the router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

If there are problems with the status of the interfaces, record any commands that are necessary to correct the configuration errors.

Step 3: Use the necessary commands to correct the router configuration.

Step 4: View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces.

Does the information in the interface status summary indicate any configuration errors on Router1?

If the answer is **yes**, troubleshoot the interface status of the interfaces.

Has connectivity been restored? _____

Step 5: Verify the logical configuration.

Examine the full status of Fa 0/0 and 0/1. Is the IP addresses and subnet mask information in the interface status consistent with the configuration table? _____

If there are differences between the configuration table and the router interface configuration, record any commands that are necessary to correct the router configuration.

Has connectivity been restored? _____

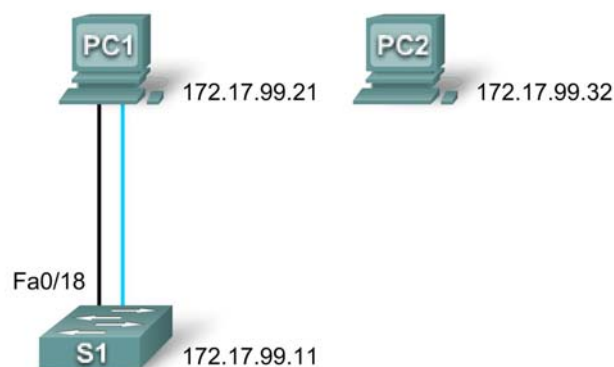
Why is it useful for a host to ping its own address?

Task 7: Clean Up

Unless directed otherwise by your instructor, 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 2.5.1: Basic Switch Configuration

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC	172.17.99.21	255.255.255.0	172.17.99.11
PC2	NIC	172.17.99.32	255.255.255.0	172.17.99.11
S1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Learning Objectives

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

- Cable a network according to the topology diagram
- Clear an existing configuration on a switch
- Examine and verify the default configuration
- Create a basic switch configuration, including a name and an IP address
- Configure passwords to ensure that access to the CLI is secured
- Configure switch port speed and duplex properties for an interface
- Configure basic switch port security
- Manage the MAC address table
- Assign static MAC addresses
- Add and move hosts on a switch

Scenario

In this lab, you will examine and configure a standalone LAN switch. Although a switch performs basic functions in its default out-of-the-box condition, there are a number of parameters that a network administrator should modify to ensure a secure and optimized LAN. This lab introduces you to the basics of switch configuration.

Task 1: Cable, Erase, and Reload the Switch

Step 1: Cable a network.

Cable a network that is similar to the one in the topology diagram. Create a console connection to the switch. If necessary, refer to Lab 1.3.1 on how to create a console connection.

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 from a 2960 switch. If you use other switches, the switch outputs and interface descriptions may appear different.

Note: PC2 is not initially connected to the switch. It is only used in Task 5.

Step 2: Clear the configuration on the switch.

Clear the configuration on the switch using the procedure in Appendix 1.

Task 2: Verify the Default Switch Configuration

Step 1: Enter privileged mode.

You can access all the switch commands in privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. You will set passwords in Task 3.

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#
```

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

Step 2: Examine the current switch configuration.

Examine the current running configuration file.

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

How many Fast Ethernet interfaces does the switch have? _____

How many Gigabit Ethernet interfaces does the switch have? _____

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

Examine the current contents of NVRAM:

```
Switch#show startup-config  
startup-config is not present
```

Why does the switch give this response?

Examine the characteristics of the virtual interface VLAN1:

```
Switch#show interface vlan1
```

Is there an IP address set on the switch? _____

What is the MAC address of this virtual switch interface? _____

Is this interface up? _____

Now view the IP properties of the interface:

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

What output do you see? _____

Step 3: Display Cisco IOS information.

Examine the following version information that the switch reports.

```
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? _____

Step 4: Examine the Fast Ethernet interfaces.

Examine the default properties of the Fast Ethernet interface used by PC1.

```
Switch#show interface fastethernet 0/18
```

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? _____

Step 5: Examine VLAN information.

Examine the default VLAN settings of the switch.

```
Switch#show vlan
```

What is the name of VLAN 1? _____

Which ports are in this VLAN? _____

Is VLAN 1 active? _____

What type of VLAN is the default VLAN? _____

Step 6 Examine flash memory.

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

```
Switch#dir flash:
```

or

```
Switch#show flash
```

Which files or directories are found?

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension. To examine the files in a directory, issue the following command using the filename displayed in the output of the previous command:

```
Switch#dir flash:c2960-lanbase-mz.122-25.SEE3
```

The output should look similar to this:

```
Directory of flash:/c2960-lanbase-mz.122-25.SEE3/
 6  drwx      4480   Mar 1 1993 00:04:42 +00:00  html
618 -rwx    4671175   Mar 1 1993 00:06:06 +00:00  c2960-lanbase-mz.122-25.SEE3.bin
619 -rwx      457    Mar 1 1993 00:06:06 +00:00  info
32514048 bytes total (24804864 bytes free)
```

What is the name of the Cisco IOS image file? _____

Step 7: Examine the startup configuration file.

To view the contents of the startup configuration file, issue the **show startup-config** command in privileged EXEC mode.

```
Switch#show startup-config
startup-config is not present
```

Why does this message appear? _____

Let's make one configuration change to the switch and then save it. Type the following commands:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
```

To save the contents of the running configuration file to non-volatile RAM (NVRAM), issue the the command **copy running-config startup-config**.

```
Switch#copy running-config startup-config
Destination filename [startup-config]? (enter)
Building configuration...
[OK]
```

Note: This command is easier to enter by using the **copy run start** abbreviation.

Now display the contents of NVRAM using the **show startup-config** command.

```
S1#show startup-config
Using 1170 out of 65536 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
!
<output omitted>
```

The current configuration has been written to NVRAM.

Task 3: Create a Basic Switch Configuration

Step 1: Assign a name to the switch.

In the last step of the previous task, you configured the hostname. Here's a review of the commands used.

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

Step 2: Set the access passwords.

Enter config-line mode for the console. Set the login password to **cisco**. Also configure the vty lines 0 to 15 with the password **cisco**.

S1#configure terminal

Enter the configuration commands, one for each line. When you are finished, return to global configuration mode by entering the **exit** command or pressing Ctrl-Z.

```
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)#exit
```

Why is the **login** command required? _____

Step 3. Set the command mode passwords.

Set the enable secret password to class. This password protects access to privileged EXEC mode.

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

Step 4. Configure the Layer 3 address of the switch.

Before you can manage S1 remotely from PC1, you need to 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. The implications and reasoning behind this action are explained in the next chapter.

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

First, you will create the new VLAN 99 on the switch. Then you will set the IP address of the switch to 172.17.99.11 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

```
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 172.17.99.11 255.255.255.0
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 command **no shutdown**. The interface is currently down because no switchports are assigned to VLAN 99.

Assign all user ports to VLAN 99.

```
S1#configure terminal
S1(config)#interface range fa0/1 - 24
S1(config-if-range)#switchport access vlan 99
S1(config-if-range)#exit
S1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

It is beyond the scope of this lab to fully explore VLANs. This subject is discussed in greater detail in the next chapter. However, 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 VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 will come up because at least one port is now assigned to VLAN 99.

Step 5: Set the switch default gateway.

S1 is a layer 2 switch, so it makes forwarding decisions based on the Layer 2 header. If multiple networks are connected to a switch, you need to specify how the switch forwards the internetwork frames, because the path must be determined at Layer three. This is done by specifying a default gateway address that points to a router or Layer 3 switch. 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 172.17.99.1, set the default gateway for the switch.

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

Step 6: Verify the management LANs settings.

Verify the interface settings on VLAN 99.

```
S1#show interface vlan 99
Vlan99 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.5302.4ec1 (bia 001b.5302.4ec1)
  Internet address is 172.17.99.11/24
  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 00:03:23, 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
    4 packets input, 1368 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 are the VLAN states? VLAN1 is _____ Line protocol is _____

What is the queuing strategy? _____

Step 7: Configure the IP address and default gateway for PC1.

Set the IP address of PC1 to 172.17.99.21, with a subnet mask of 255.255.255.0. Configure a default gateway of 172.17.99.11. (If needed, refer to Lab 1.3.1 to configure the PC NIC.)

Step 8: Verify connectivity.

To verify the host and switch are correctly configured, ping the IP address of the switch (172.17.99.11) from PC1.

Was the ping successful? _____

If not, troubleshoot the switch and host configuration. Note that this may take a couple of tries for the pings to succeed.

Step 9: Configure the port speed and duplex settings for a Fast Ethernet interface.

Configure the duplex and speed settings on Fast Ethernet 0/18. Use the **end** command to return to privileged EXEC mode when finished.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

The line protocol for both interface FastEthernet 0/18 and interface VLAN 99 will temporarily go down.

The default on the Ethernet interface of the switch is auto-sensing, so it automatically negotiates optimal settings. You should set duplex and speed manually only if a port must operate at a certain speed and duplex mode. Manually configuring ports can lead to duplex mismatches, which can significantly degrade performance.

Verify the new duplex and speed settings on the Fast Ethernet interface.

```
S1#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001b.5302.4e92 (bia 001b.5302.4e92)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, 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
    265 packets input, 52078 bytes, 0 no buffer
    Received 265 broadcasts (0 multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 32 multicast, 0 pause input
    0 input packets with dribble condition detected
  4109 packets output, 342112 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 PAUSE output
  0 output buffer failures, 0 output buffers swapped out
```

Step 10: Save the configuration.

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made will not be lost if the system is rebooted or loses power.

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

Step 11: Examine the startup configuration file.

To see the configuration that is stored in NVRAM, issue the **show startup-config** command from privileged EXEC mode.

```
S1#show startup-config
```

Are all the changes that were entered recorded in the file? _____

Task 4: Managing the MAC Address Table

Step 1: Record the MAC addresses of the hosts.

Determine and record the Layer 2 (physical) addresses of the PC network interface cards using the following commands:

Start > Run > cmd > ipconfig /all

PC1: _____

PC2: _____

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

Display the MAC addresses using the **show mac-address-table** command in privileged EXEC mode.

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

How many dynamic addresses are there? _____

How many MAC addresses are there in total? _____

Do the dynamic MAC addresses match the host MAC addresses? _____

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

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

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

Show only the MAC addresses from the table that were learned dynamically.

```
S1#show mac-address-table address <PC1 MAC here>
```

How many dynamic addresses are there? _____

Step 4: 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
```

Step 5: Verify the results.

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? _____

Step 6: Examine the MAC table again.

More than likely, an application running on your PC1 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 PC1

```
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 PC1, ping the VLAN 99 IP address of the switch from PC1 and then repeat Step 6.

Step 7: 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 Fast Ethernet interface 0/18 using the address that was recorded for PC1 in Step 1 of this task. The MAC address **00e0.2917.1884** is used as an example only. You must use the MAC address of your PC1, which is different than the one given here as an example.

```
S1(config)#mac-address-table static 00e0.2917.1884 interface fastethernet 0/18  
vlan 99
```

Step 8: Verify the results.

Verify the MAC address table entries.

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

How many total MAC addresses are there? _____

How many static addresses are there? _____

Step 10: Remove the static MAC entry.

To complete the next task, it will be necessary to remove the static MAC address table entry. Enter configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 00e0.2917.1884 is used in the example only. Use the MAC address for your PC1.

```
S1(config)#no mac-address-table static 00e0.2917.1884 interface fastethernet  
0/18 vlan 99
```

Step 10: Verify the results.

Verify that the static MAC address has been cleared.

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

How many total static MAC addresses are there? _____

Task 5 Configuring Port Security

Step 1: Configure a second host.

A second host is needed for this task. Set the IP address of PC2 to 172.17.99.32, with a subnet mask of 255.255.255.0 and a default gateway of 172.17.99.11. Do not connect this PC to the switch yet.

Step 2: Verify connectivity.

Verify that PC1 and the switch are still correctly configured by pinging the VLAN 99 IP address of the switch from the host.

Were the pings successful? _____

If the answer is no, troubleshoot the host and switch configurations.

Step 3: Copy the host MAC addresses.

Write down the MAC addresses from Task 4, Step 1.

PC1 _____

PC2 _____

Step 4: Determine which MAC addresses that the switch has learned.

Display the learned MAC addresses using the **show mac-address-table** command in privileged EXEC mode.

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

How many dynamic addresses are there? _____

Do the MAC addresses match the host MAC addresses? _____

Step 5: List the port security options.

Explore the options for setting port security on interface Fast Ethernet 0/18.

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#switchport port-security ?
    aging          Port-security aging commands
    mac-address     Secure mac address
    maximum         Max secure addresses
    violation       Security violation mode
    <cr>
```

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

Step 6: Configure port security on an access port.

Configure switch port Fast Ethernet 0/18 to accept only two devices, to learn the MAC addresses of those devices dynamically, and to block traffic from invalid hosts if a violation occurs.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation protect
S1(config-if)#exit
```

Step 7: Verify the results.

Show the port security settings.

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

How many secure addresses are allowed on Fast Ethernet 0/18? _____

What is the security action for this port? _____

Step 8: Examine the running configuration file.

```
S1#show running-config
```

Are there statements listed that directly reflect the security implementation of the running configuration?

Step 9: Modify the port security settings on a port.

On interface Fast Ethernet 0/18, change the port security maximum MAC address count to 1 and to shut down if a violation occurs.

```
S1(config-if)#switchport port-security maximum 1  
S1(config-if)#switchport port-security violation shutdown
```

Step 10: Verify the results.

Show the port security settings.

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

Have the port security settings changed to reflect the modifications in Step 9? _____

Ping the VLAN 99 address of the switch from PC1 to verify connectivity and to refresh the MAC address table. You should now see the MAC address for PC1 “stuck” to the running configuration.

```
S1#show run  
Building configuration...  
  
<output omitted>  
!  
interface FastEthernet0/18  
  switchport access vlan 99  
  switchport mode access  
  switchport port-security  
  switchport port-security mac-address sticky  
  switchport port-security mac-address sticky 00e0.2917.1884  
  speed 100  
  duplex full  
!
```

Step 11: Introduce a rogue host.

Disconnect PC1 and connect PC2 to port Fast Ethernet 0/18. Ping the VLAN 99 address 172.17.99.11 from the new host. Wait for the amber link light to turn green. Once it turns green, it should almost immediately turn off.

Record any observations: _____

Step 12: Show port configuration information.

To see the configuration information for just Fast Ethernet port 0/18, issue the following command in privileged EXEC mode:

```
S1#show interface fastethernet 0/18
```

What is the state of this interface?

Fast Ethernet0/18 is _____ Line protocol is _____

Step 13: Reactivate the port.

If a security violation occurs and the port is shut down, you can use the **no shutdown** command to reactivate it. However, as long as the rogue host is attached to Fast Ethernet 0/18, any traffic from the host disables the port. Reconnect PC1 to Fast Ethernet 0/18, and enter the following commands on the switch:

```
S1# configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)# no shutdown
S1(config-if)#exit
```

Note: Some IOS version may require a manual **shutdown** command before entering the **no shutdown** command.

Step 14: Cleanup

Unless directed otherwise, clear the configuration on the switches, turn off the power to the host computer and switches, and remove and store the cables.

Appendix 1: Erasing and Reloading the Switch

Erasing and Reloading the Switch

For the majority of the labs in Exploration 3, it is necessary to start with an unconfigured switch. Using a switch with an existing configuration may produce unpredictable results. These instructions show you how to prepare the switch prior to starting the lab. These instructions are for the 2960 switch; however, the procedure for the 2900 and 2950 switches is the same.

Step 1: Enter privileged EXEC mode by typing the enable command.

If prompted for a password, enter **class**. If that does not work, ask the instructor.

```
Switch>enable
```

Step 2: Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there is no VLAN file, this message is displayed:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

Step 3: Remove the switch startup configuration file from NVRAM.

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

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
Press Enter to confirm.
```

The response should be:

```
Erase of nvram: complete
```

Step 4: Check that the VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

If previous VLAN configuration information is still present (other than the default management VLAN 1), you must power-cycle the switch (hardware restart) instead of issuing the **reload** command. To power-cycle the switch, remove the power cord from the back of the switch or unplug it, and then plug it back in.

Step 5: Restart the software.

Note: This step is not necessary if the switch was restarted using the power-cycle method.

At the privileged EXEC mode prompt, enter the **reload** command.

```
Switch(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

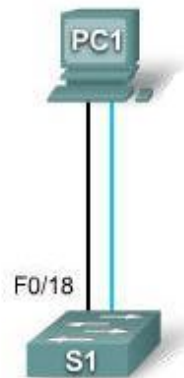
Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

Lab 2.5.3: Password Recovery – Challenge

Topology Diagram



Addressing Table

Device	Hostname / Interface	IP Address	Subnet Mask	Default Gateway
PC 1	Host-A	172.17.99.21	255.255.255.0	172.17.99.1
Switch1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Learning Objectives

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

- Create and save a basic switch configuration
- Set up a TFTP server on the network
- Configure a switch to load a configuration from a TFTP server
- Recover the password for a Cisco 2960 switch (2900 series)

Scenario

In this lab, you will explore file management and password recovery procedures on a Cisco Catalyst switch.

Task 1: Cable and Initialize the Network

Step 1: Cable a network.

Cable a network that is similar to the one in the topology diagram. Then, create a console connection to the switch. If necessary, refer to Lab 1.3.1. The output shown in this lab is from a 2960 switch. If you use other switches, the switch outputs and interface descriptions may appear different.

Step 2: Clear the configuration on the switch.

Set up a console connection to the switch. Erase the configuration on the switch.

Step 3: Create a basic configuration.

Configure the switch with the following hostname and access passwords. Then enable secret passwords on the switch.

Hostname	Console Password	Telnet Password	Command Password
ALSwitch	cisco	cisco	class

Create VLAN 99. Assign IP address 172.17.99.11 to this interface. Assign the Fast Ethernet 0/18 port to this VLAN.

Step 4: Configure the host attached to the switch.

Configure the host to use the IP address, mask, and default gateway identified in the Addressing table. This host acts as the TFTP server in this lab.

Step 5: Verify connectivity.

To verify that the host and switch are correctly configured, ping the switch IP address from the host.

Was the ping successful? _____

If the answer is no, troubleshoot the host and switch configurations.

Task 2: Starting and Configuring the TFTP Server

Step 1: Start up and configure the TFTP server.

The TFTP server that was used in the development of this lab is the Solar Winds server, available at <http://www.solarwindssoftware.com/toolsets/tools/tftp-server.aspx>

The labs in your classroom may be using a different TFTP server. If so, check with your instructor for the operating instructions for the TFTP server in use.

Start the server on the host using the Start menu: **Start > All Programs > SolarWinds 2003 Standard Edition > TFTP Server**.

The server should start up and acquire the IP address of the Ethernet interface. The server uses the C:\TFTP-Root directory by default.

Step 2: Verify connectivity to the TFTP server.

Verify that the TFTP server is running and that it can be pinged from the switch.

Task 3: Back Up and Restore a Configuration File from a TFTP Server

Step 1: Copy the startup configuration file to the TFTP server.

Verify that the TFTP server is running and that it can be pinged from the switch. Save the current configuration.

Back up the saved configuration file to the TFTP server.

Step 2: Verify the transfer to the TFTP server.

Verify the transfer to the TFTP server by checking the command window on the TFTP server. The output should look similar to the following:

```
Received alswitch-config from (172.17.99.11), 1452 bytes
```

Verify that the alswitch-config file is in the TFTP server directory C:\TFTP-root.

Step 3: Restore the startup configuration file from the TFTP server.

To restore the startup configuration file, first erase the existing startup configuration file, and then reload the switch.

When the switch has been reloaded, you must reestablish connectivity between the switch and the TFTP server before the configuration can be restored. To do this, reconfigure VLAN 99 with the correct IP address and assign port Fast Ethernet 0/18 to that VLAN (refer to Task 1).

After VLAN 99 is up, verify connectivity by pinging the server from the switch.

If the ping is unsuccessful, troubleshoot the switch and server configuration. Restore the configuration from the TFTP server by copying the alswitch-config file from the server to the switch.

Note: It is important that this process is not interrupted.

Was the operation successful? _____

Step 4: Verify the restored startup configuration file.

In privilege EXEC mode, reload the router again. When the reload is complete, the switch should show the ALSwitch prompt. Examine the running configuration to verify that the restored configuration is complete, including the access and enable secret passwords.

Task 7: Recover Passwords on the Catalyst 2960

Step 1: Reset the console password.

Have a classmate change the console, vty, and enable secret passwords on the switch. Save the changes to the startup-config file and reload the switch.

Now, without knowing the passwords, try to gain access to privilege EXEC mode on the switch.

Step 2: Recover access to the switch.

Detailed password recovery procedures are available in the online Cisco support documentation. In this case, they can be found in the troubleshooting section of the Catalyst 2960 Switch Software Configuration Guide. Follow the procedures to restore access to the switch.

Once the steps are completed, log off by typing **exit**, and turn all the devices off. Then remove and store the cables and adapter.

Appendix 2: Password Recovery for the Catalyst 2960

Recovering a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.



Note On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

These sections describes how to recover a forgotten or lost switch password:

- [Procedure with Password Recovery Enabled](#)
- [Procedure with Password Recovery Disabled](#)

You enable or disable password recovery by using the **service password-recovery** global configuration command. Follow the steps in this procedure if you have forgotten or lost the switch password.

Step 1 Connect a terminal or PC with terminal-emulation software to the switch console port.

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Power off the switch. Reconnect the power cord to the switch and, within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; then release the **Mode** button.

Several lines of information about the software appear with instructions, informing you if the password recovery procedure has been disabled or not.

- If you see a message that begins with this:

```
The system has been interrupted prior to initializing the flash  
file system. The  
following commands will initialize the flash file system
```

proceed to the "Procedure with Password Recovery Enabled" section, and follow the steps.

- If you see a message that begins with this:

```
The password-recovery mechanism has been triggered, but is  
currently disabled.
```


proceed to the "Procedure with Password Recovery Disabled" section, and follow the steps.

Step 4 After recovering the password, reload the switch:

```
Switch> reload
```

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

Procedure with Password Recovery Enabled

If the password-recovery mechanism is enabled, this message appears:

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software:

```
flash_init
load_helper
boot
```

Step 1 Initialize the flash file system:

```
switch: flash_init
```

Step 2 If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

Step 3 Load any helper files:

```
switch: load_helper
```

Step 4 Display the contents of flash memory:

```
switch: dir flash:
```

The switch file system appears:

Directory of flash:

13	drwx	192	Mar 01 1993 22:30:48	c2960-lanbase-
mz.122-25.FX				
11	-rwx	5825	Mar 01 1993 22:31:59	config.text
18	-rwx	720	Mar 01 1993 02:21:30	vlan.dat

```
16128000 bytes total (10003456 bytes free)
```

Step 5 Rename the configuration file to config.text.old.

This file contains the password definition.

```
switch: rename flash:config.text flash:config.text.old
```

Step 6 Boot the system:

```
switch: boot
```

You are prompted to start the setup program. Enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 7 At the switch prompt, enter privileged EXEC mode:

```
Switch> enable
```

Step 8 Rename the configuration file to its original name:

```
Switch# rename flash:config.text.old flash:config.text
```

Step 9 Copy the configuration file into memory:

```
Switch# copy flash:config.text system:running-config  
Source filename [config.text]?  
Destination filename [running-config]?
```

Press **Return** in response to the confirmation prompts.

The configuration file is now reloaded, and you can change the password.

Step 10 Enter global configuration mode:

```
Switch# configure terminal
```

Step 11 Change the password:

```
Switch (config)# enable secret password
```

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 12 Return to privileged EXEC mode:

```
Switch (config)# exit  
Switch#
```

Step 13 Write the running configuration to the startup configuration file:

```
Switch# copy running-config startup-config
```

The new password is now in the startup configuration.



Note This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the **show running-config** privileged EXEC command. To re-enable the interface, enter the **interface vlan *vlan-id*** global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the **no shutdown** command.

Step 14 Reload the switch:

```
Switch# reload
```

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:

The password-recovery mechanism has been triggered, but is currently disabled. Access to the boot loader prompt through the password-recovery mechanism is disallowed at this point. However, if you agree to let the system be reset back to the default system configuration, access to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?



Caution Returning the switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup switch and VLAN configuration files.

- If you enter **n** (no), the normal boot process continues as if the **Mode** button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

Press Enter to continue.....

- If you enter **y** (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

Step 1 Elect to continue with password recovery and lose the existing configuration:

Would you like to reset the system back to the default configuration (y/n)? **Y**

Step 2 Load any helper files:

Switch: **load_helper**

Step 3 Display the contents of flash memory:

switch: **dir flash:**

The switch file system appears:

Directory of flash:

```
13  drwx          192   Mar 01 1993 22:30:48 c2960-lanbase-mz.122-25.FX.0
```

16128000 bytes total (10003456 bytes free)

Step 4 Boot the system:

Switch: **boot**

You are prompted to start the setup program. To continue with password recovery, enter **N** at the prompt:

Continue with the configuration dialog? [yes/no]: **N**

Step 5 At the switch prompt, enter privileged EXEC mode:

Switch> **enable**

Step 6 Enter global configuration mode:

Switch# **configure terminal**

Step 7 Change the password:

Switch (config)# **enable secret password**

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 8 Return to privileged EXEC mode:

Switch (config)# **exit**
Switch#

Step 9 Write the running configuration to the startup configuration file:

Switch# **copy running-config startup-config**

The new password is now in the startup configuration.

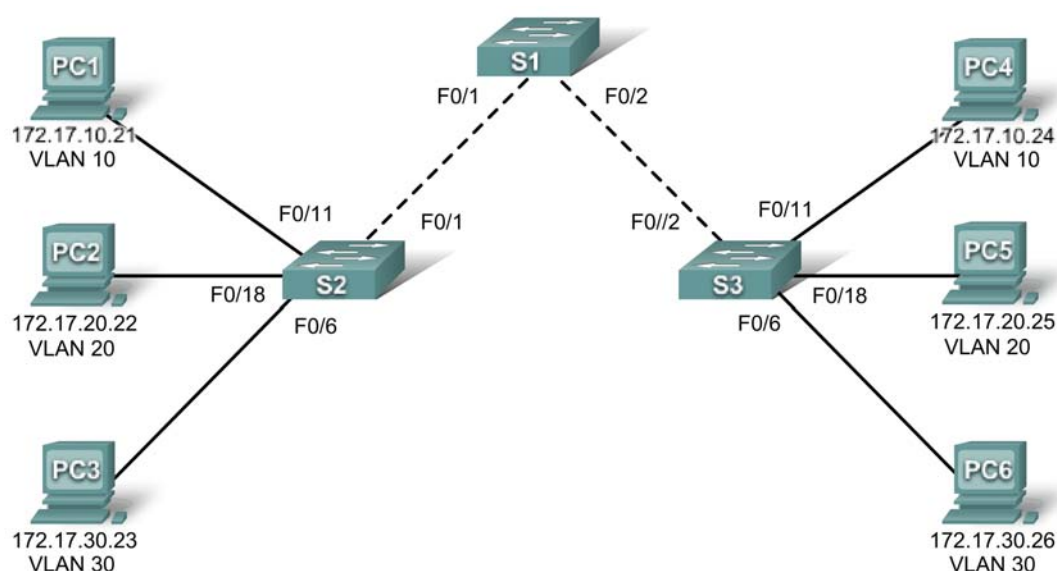


Note This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the **show running-config** privileged EXEC command. To re-enable the interface, enter the **interface vlan *vlan-id*** global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the **no shutdown** command.

Step 10 You must now reconfigure the switch. If the system administrator has the backup switch and VLAN configuration files available, you should use those.

Lab 3.5.1: 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 4: 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 id *vlan-name*** displays the same output.

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

Step 5: 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 6: 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 7: 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 8: 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 9: 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 10: Change the IP address and network on PC1.

Change the IP address on PC1 to 172.17.20.22. 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 7: Document the Switch Configurations

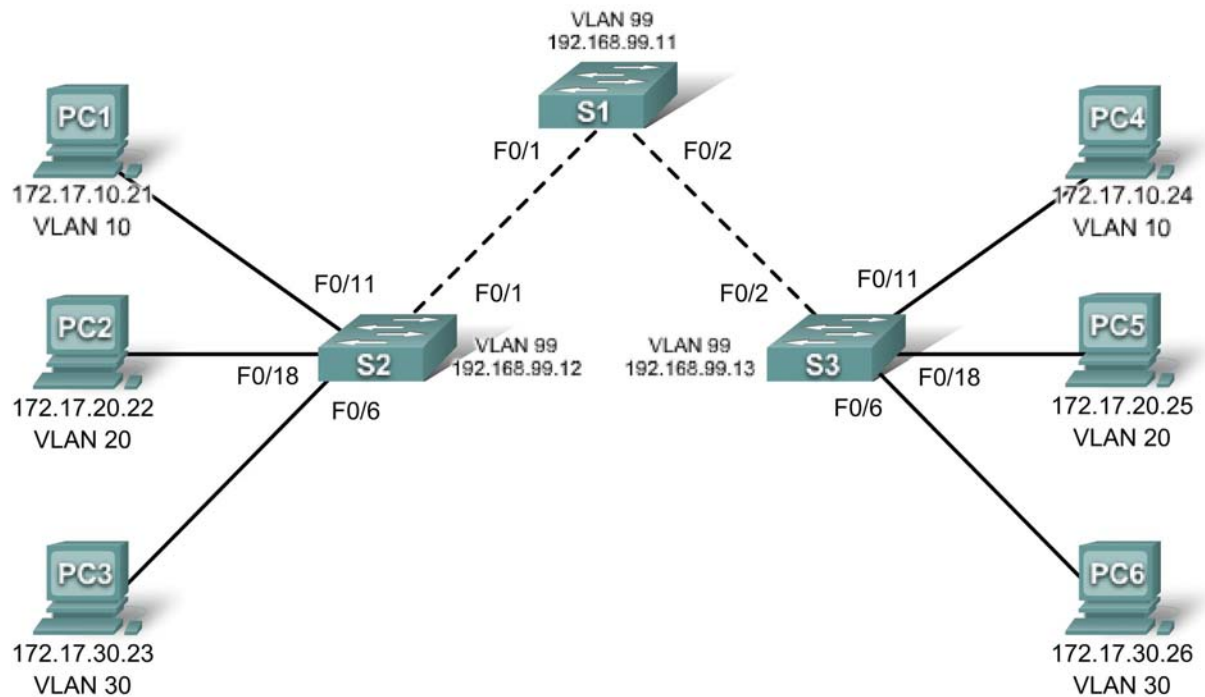
On each switch, capture the running configuration to a text file and save it for future reference.

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 4.4.1: 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 with another team
- 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 need to work with another team in the lab to build the topology.

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.

```
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 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.

```
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 4: 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
```

Task 2: Perform Basic Switch Configurations

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]
```

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. However, because S3 is in transparent mode, VTP pruning must be configured locally on that switch.

Confirm VTP pruning configuration on each switch using the **show vtp status** command. VTP pruning mode should be enabled on each switch.

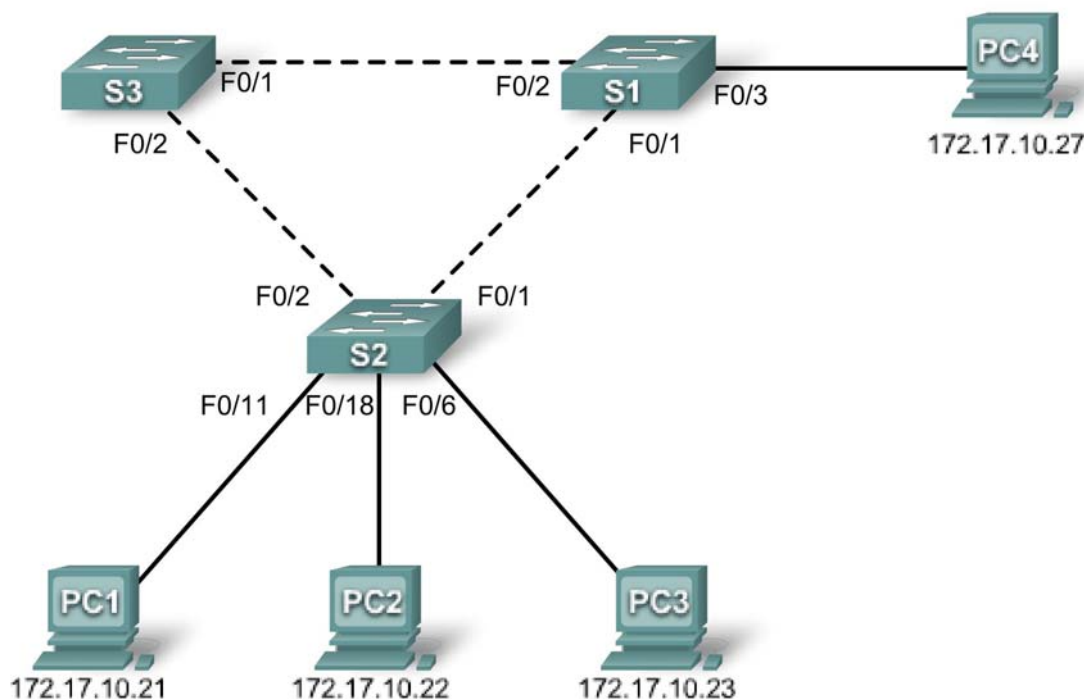
```
S1#show vtp status
VTP Version                : 2
Configuration Revision      : 17
Maximum VLANs supported locally : 255
Number of existing VLANs    : 9
VTP Operating Mode          : Server
VTP Domain Name             : Lab4
VTP Pruning Mode            : Enabled
<output omitted>
```

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 5.5.1: 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 is the MAC address of the root switch

           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? _____
- On S1, which spanning tree ports are in the blocking state on the root switch?

- On S3, which spanning tree 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 port Fa0/1 on S1

```
S1(config)#interface fa0/1
S1(config-if)#shutdown
```

Step 3: Record the debug output from S2 and S3

```
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
```

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
!
!
```

```

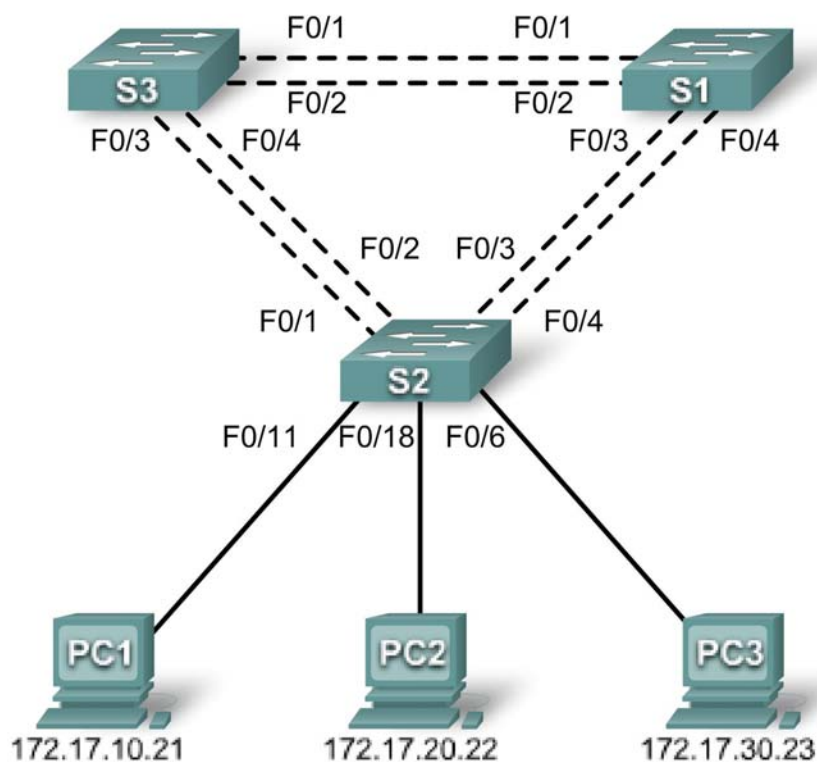
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode trunk
!
!
! <output omitted>
!
interface Vlan1
  ip address 172.17.10.3 255.255.255.0
!
end
  
```

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 5.5.2: 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. 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 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.

```
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 4: Re-enable the user ports on 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.

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no 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 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
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 access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
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]
```

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.

7. What is the bridge ID priority for switches S1, S2, and S3 on VLAN 99?
 - a. S1 _____
 - b. S2 _____
 - c. S3 _____
8. 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 _____
9. Which switch is the root for the VLAN 99 spanning tree? _____
10. On VLAN 99, which spanning tree ports are in the blocking state on the root switch?

11. On VLAN 99, which spanning tree ports are in the blocking state on the non-root switches?

12. How does STP elect the root switch? _____
13. 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 leave 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.

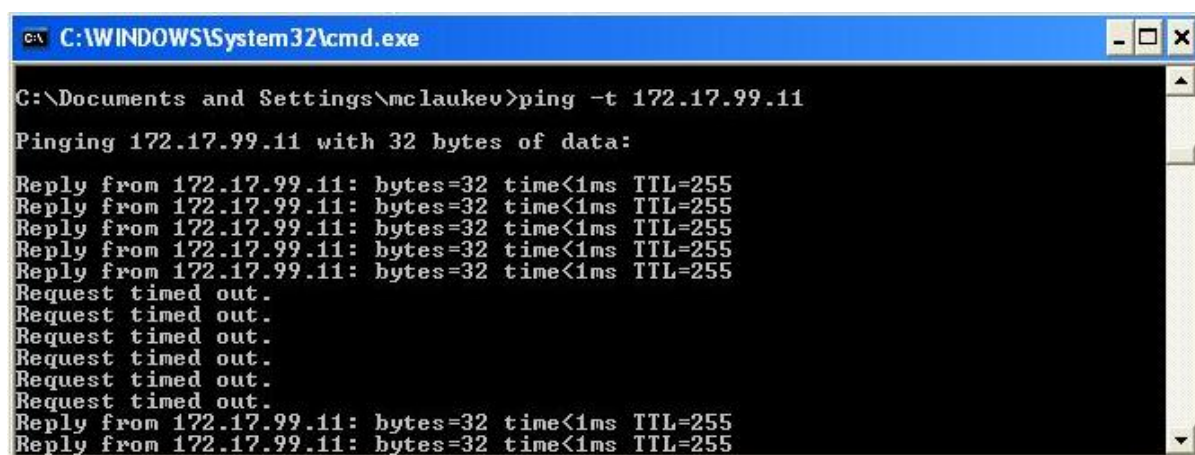


Figure 1. These pings show a 30-second lapse in connectivity while the spanning tree is recalculated.

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 dramatically. 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
!
interface FastEthernet0/6
switchport access vlan 30
!
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
!
interface FastEthernet0/12
switchport access vlan 10
!
interface FastEthernet0/13
```

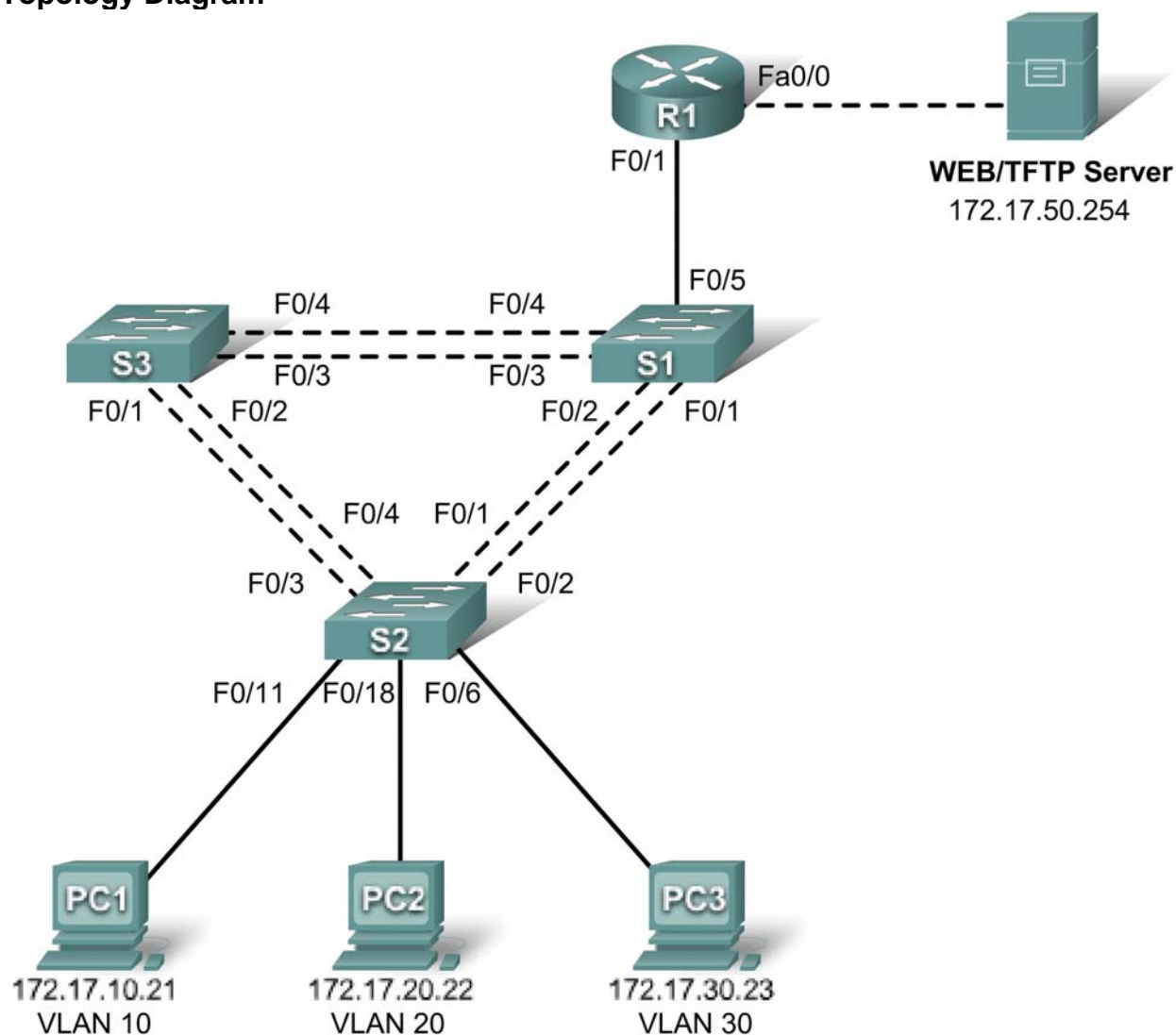
```
    switchport access vlan 10
!
interface FastEthernet0/14
    switchport access vlan 10
!
interface FastEthernet0/15
    switchport access vlan 10
!
interface FastEthernet0/16
    switchport access vlan 10
!
interface FastEthernet0/17
    switchport access vlan 10
!
interface FastEthernet0/18
    switchport access vlan 20
    switchport mode access
!
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 GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
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 6.4.1: 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 – 0/4	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

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.

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 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 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.

```
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 4: 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 2: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to 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...
```

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 fa0/1-4
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 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)#exit
```

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	
99	management	active	

Step 5: 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 6: Assign switch ports to VLANs on S2.

Refer to the port assignments table at the beginning of the lab to assign ports to VLANs on S2.

```
S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
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]
```

Step 7: Check connectivity between VLANs.

Open command windows on the three hosts connected to S2. Ping from PC1 (172.17.10.21) to PC2 (172.17.20.22). Ping from PC2 to PC3 (172.17.30.23).

Are the pings successful? _____

If not, why do these pings fail? _____

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 are 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.

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, FastEthernet0/1
C       172.17.30.0 is directly connected, FastEthernet0/0.30
C       172.17.20.0 is directly connected, FastEthernet0/0.20
C       172.17.10.0 is directly connected, FastEthernet0/0.10
C       172.17.1.0 is directly connected, FastEthernet0/0.1
C       172.17.99.0 is directly connected, FastEthernet0/0.99
```

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  
  no shutdown  
!  
<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  
!  
end
```

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 access vlan 30
  switchport mode access
!
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
```

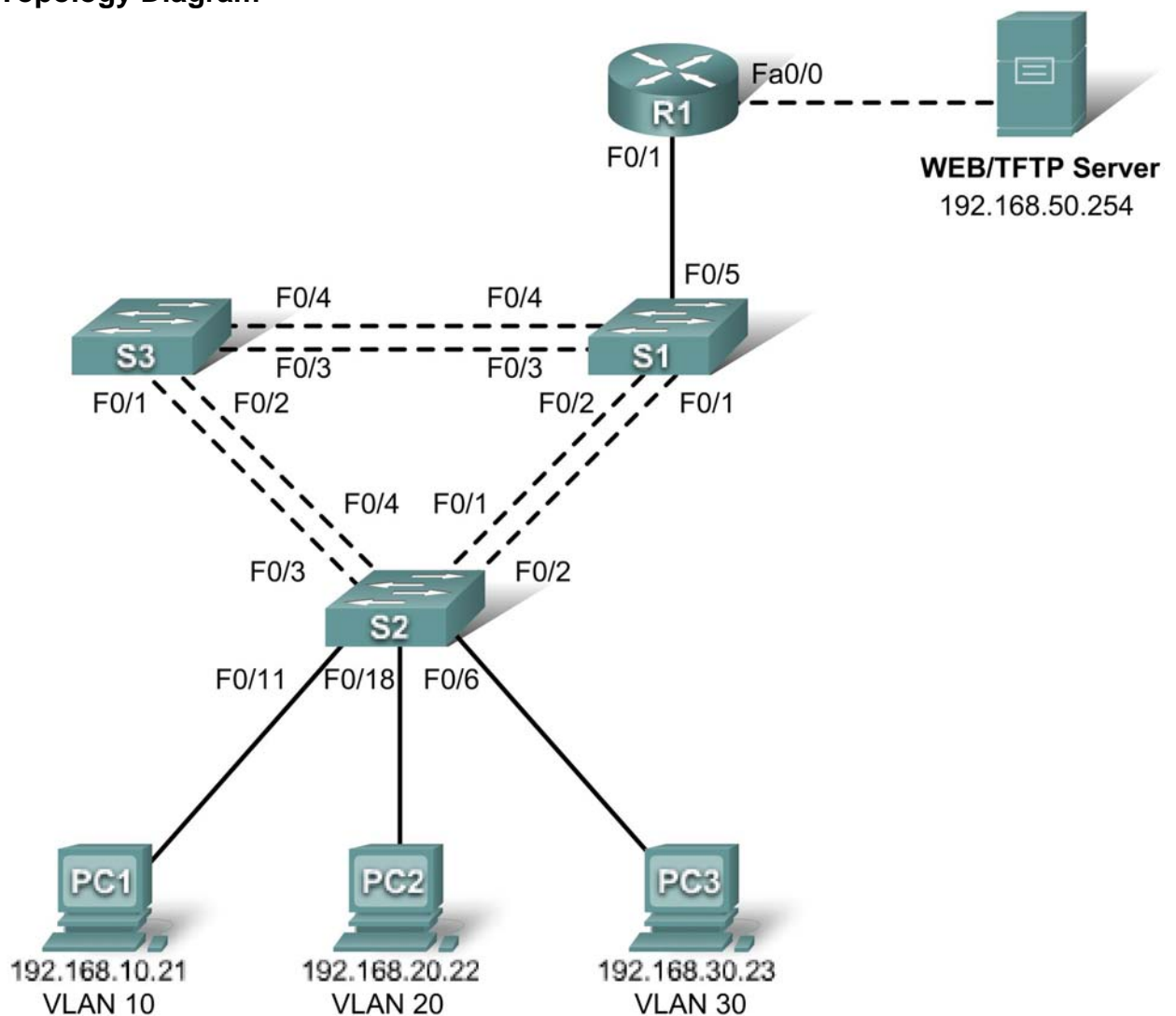
Switch 3

```
!
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
    shutdown
!
<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 6.4.3: 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 – 0/4	802.1q Trunks (Native VLAN 99)	192.168.99.0 /24
Fa0/5 – 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
Fa0/0.1	VLAN1	192.168.1.1
Fa0/0.10	VLAN 10	192.168.10.1
Fa0/0.20	VLAN 20	192.168.20.1
Fa0/0.30	VLAN 30	192.168.30.1
Fa0/0.99	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 range FastEthernet0/5 - 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 range FastEthernet0/5 - 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 range FastEthernet0/5 - 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

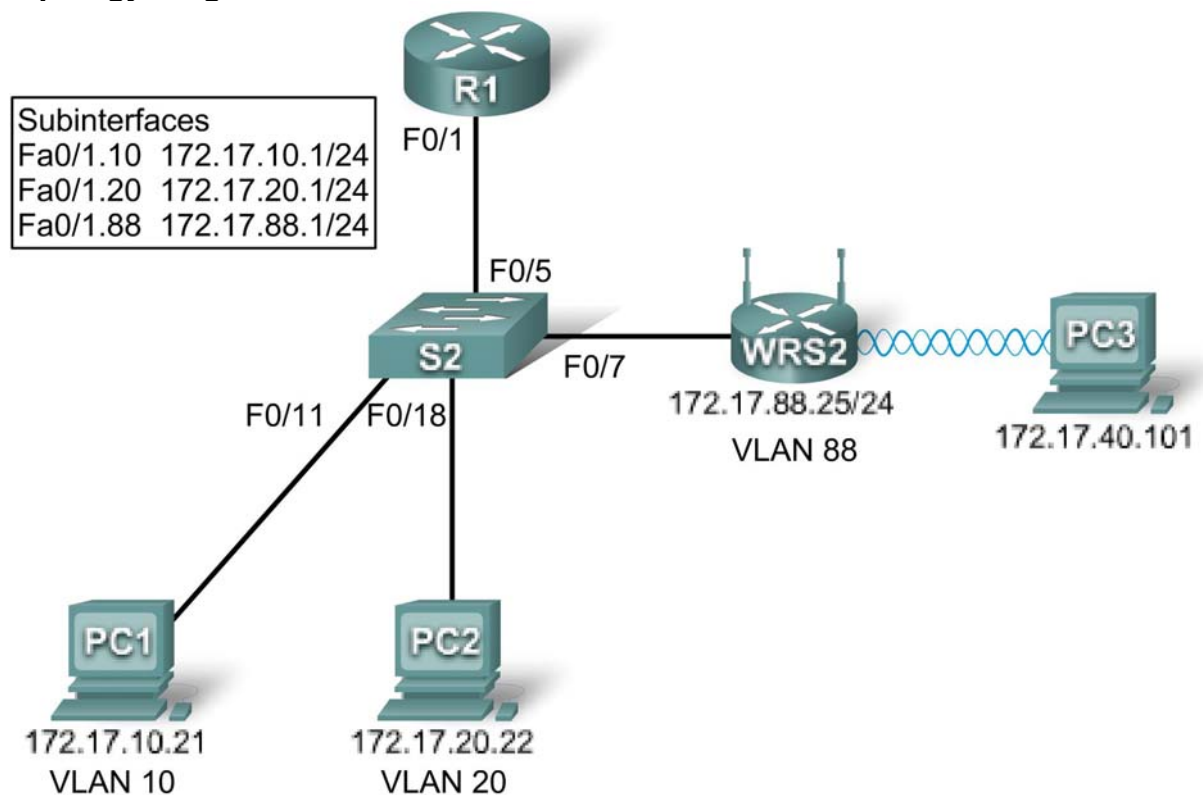
When you have successfully completed your troubleshooting, capture the output of the router and all three switches with the **show run** command and save it to a text file.

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 7.5.1: Configuring Wireless LAN Access

Topology Diagram



Learning Objectives

- Configure options in the Linksys Setup tab
- Configure options in the Linksys Wireless tab
- Configure options in the Linksys Administration tab
- Configure options in the Linksys Security tab
- Add wireless connectivity to a PC
- Test connectivity

Introduction

In this activity, you will configure a Linksys wireless router, allowing for remote access from PCs as well as wireless connectivity with WEP security.

Task 1: Load the starting configurations.

Step 1. Load R1's configurations.

```
hostname R1
!
interface FastEthernet0/0
 ip address 172.17.50.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
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 FastEthernet0/1.88
 encapsulation dot1Q 88
 ip address 172.17.88.1 255.255.255.0
!
```

Step 2. Load S2's configurations.

```
hostname S2
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no shutdown
!
interface FastEthernet0/7
 switchport access vlan 88
 switchport mode access
 no shutdown
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 no shutdown
```

```
!  
interface FastEthernet0/18  
  switchport access vlan 20  
  switchport mode access  
  no shutdown  
!
```

Task 2: Connect and log into the Wireless Router.

In order to configure the settings on the wireless router we will use its Web GUI utility. The GUI can be accessed by navigating to the router's LAN/Wireless IP address with a web browser. The factory default address is 192.168.1.1

Step 1. Establish physically connectivity.

Connect a straight through cable from the PC to one of the wireless router's LAN ports. The wireless router will provide an IP address to the PC using default DHCP configurations.

Step 2. Open a web browser.

Step 3. Navigate to the wireless router's Web Utility.

- Set the URL of the browser to <http://192.168.1.1>.

The default login credentials are a blank username and a password of: **admin**. Note that this is very insecure since it is the factory default and provided publicly. We will set our own unique password in a later task.

Step 4. Log in

- Leave the username blank and set the password to: admin.

Task 3: Configure Options in the Linksys Setup Tab.

Step 1. Set the Internet connection type to static IP.

- By default the start up page is the 'Setup' screen. In the menus at the top notice you are in the 'Setup' section and under the 'Basic Setup' tab.
- In the Setup screen for the Linksys router, locate the **Internet Connection Type** option under **Internet Setup** section of this page. Click the drop-down menu and select **Static IP** from the list.

Step 2. Configure the VLAN 88 IP address, subnet mask, and default gateway for WRS2.

- Set the Internet IP address to 172.17.88.25.
- Set the subnet mask to 255.255.255.0.
- Set the default gateway to 172.17.88.1.

Note: Typically in a home or small business network, this Internet IP address is assigned by the ISP through DHCP or PPPoE (the specifics of PPPoE are outside the scope of this course).

Step 3. Configure the router IP parameters.

- Still on this page, scroll down to **Network Setup**. For the **Router IP** fields do the following:
 - Set the IP address to 172.17.40.1 and the subnet mask to 255.255.255.0.
- Under the **DHCP Server Setting**, ensure that the DHCP server is enabled.

Step 4. Save settings.

Click the **Save Settings** button at the bottom of the **Setup** screen.

Note that the IP address range for the DHCP pool adjusts to a range of addresses to match the router IP parameters. These addresses are used for wireless clients and clients that connect to the wireless router's internal switch. Clients receive an IP address and mask and are given the router IP to use as a gateway.

Step 5. Reconnect to WRS2.

Since we have changed the router's IP address and DHCP pool, we will have to reconnect to it using the new address previously configured.

- Reconnect to the router. You will need to reacquire an IP address from the router via DHCP or manually set your own.
- Reconnect to the router's configuration GUI using an IP address of 172.17.88.1 (reference Task 1 for help).

Task 4: Configure Options in the Linksys Wireless Tab.

Step 1. Set the network name (SSID).

- Click the **Wireless** tab.
- Under **Network Name (SSID)**, rename the network from **Default** to **WRS_LAN**.
- Click **Save Settings**.

Step 2. Set the security mode.

- Click **Wireless Security**. It is located next to **Basic Wireless Settings** in the main **Wireless** tab.
- Change **Security Mode** from **Disabled** to **WEP**.
- Using the default Encryption of 40/64-Bit, set **Key1** to **1234567890**,
- Click **Save Settings**.

Task 5: Configure Options in the Linksys Administration Tab

Step 1. Set the router password.

- Click the **Administration** tab.
- Under **Router Access**, change the router password to **cisco123**. Re-enter the same password to confirm.

Step 2. Enable remote management.

- Under **Remote Access**, enable **remote management**.
- Click **Save Settings**.
- You may be prompted to log in again. Use the new password of **cisco123** and still keep the username blank

Task 6: Configure Options in the Linksys Security Tab

By default ping requests to WRS2's LAN/Wireless interface (172.17.40.1) from sources on its WAN interface (for example PC1 & PC2) will be blocked for security reasons implemented by the wireless router. For the purpose of verifying connectivity in this lab we would like to allow them.

Step 1. Allow anonymous internet requests.

- Click the **Security** tab.
- Under **Internet Filter**, uncheck **Filter Anonymous Internet Requests**.

Task 7: Add Wireless Connectivity to a PC

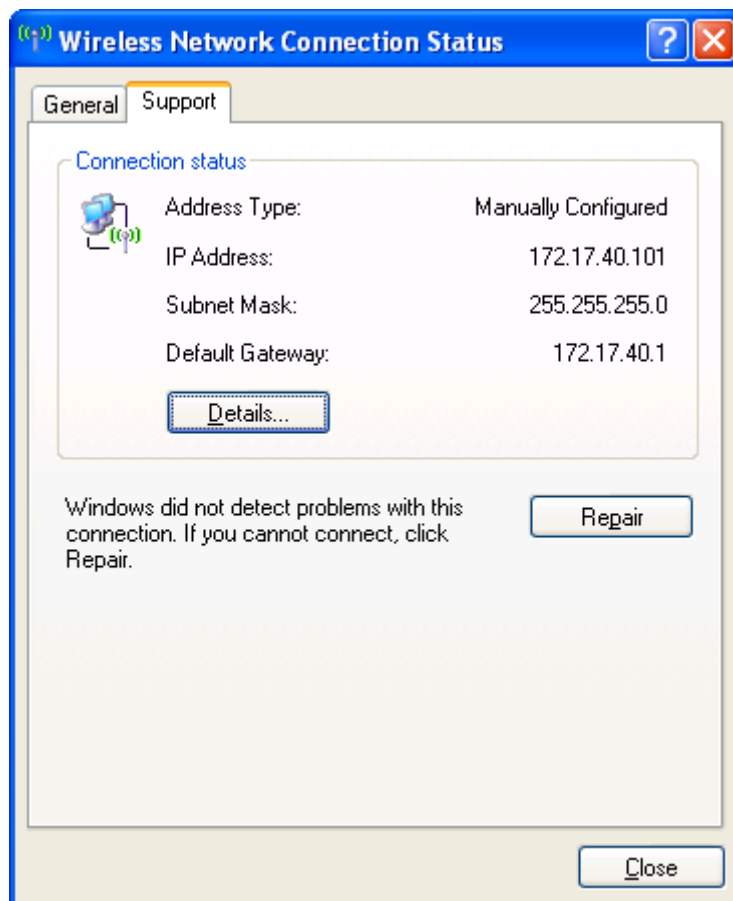
Step 1. Disconnect the Ethernet connection from PC3 to WRS2.

Step 2: Use Windows XP to connect to the wireless router.

- Locate the Wireless Network Connection icon in your taskbar, or go to **Start > Control Panel > Network Connections**.
- Select the **Wireless Network Connection**.
- Navigate to the **File** menu and select **Status**.
- Click **View Wireless Networks**.
- Locate the 'WRS_LAN' SSID in the list of available networks and connect to it.
- When prompted for the WEP key enter it as in Task 3, **1234567890** and click **Connect**.

Step 3: Verify the Connection.

- In the **Status** window, select the **Support** tab.
- Verify that PC3 has received an IP address from WRS2's DHCP address pool or has been manually configured.



Task 8: Test Connectivity

Step 1. Ping WRS2's LAN/Wireless interface.

- On PC3, click **Start->Run**
- Type **cmd** and select open. This will open the command prompt
- In the command prompt type (without quotes) "**ping 172.17.40.1**".

Step 2. Ping R1's Fa0/1.88 Interface.

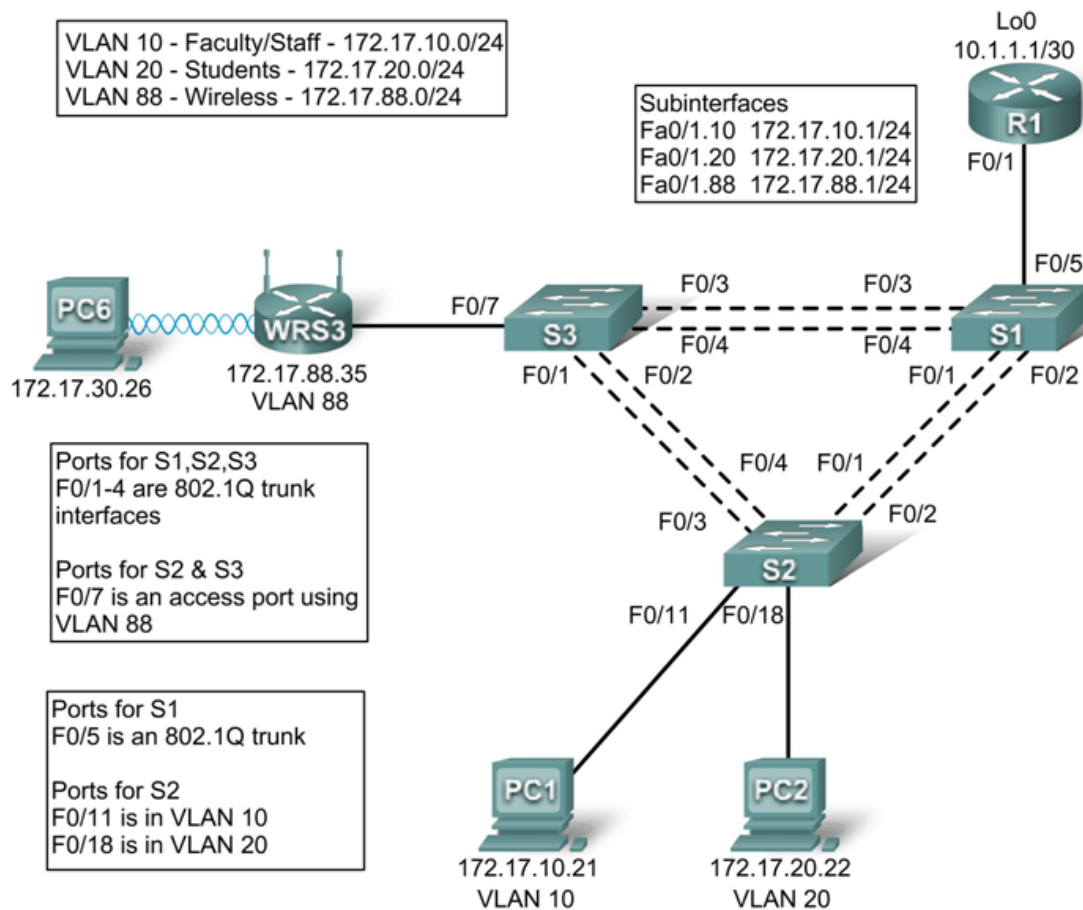
- In the command prompt type (without quotes) "**ping 172.17.88.1**"

Step 3. Ping PC1 and PC2 from PC3.

- In the command prompt type (without quotes) "**ping 172.17.10.21**" to ping PC1.
- Repeat on PC2's address, 172.17.20.22.

Lab 7.5.2: Challenge Wireless Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1.10	172.17.10.1	255.255.255.0	N/A
	Fa0/1.20	172.17.20.1	255.255.255.0	N/A
	Fa0/1.88	172.17.88.1	255.255.255.0	N/A
	Lo0	10.1.1.1	255.255.255.252	N/A
WRS3	WAN	172.17.88.35	255.255.255.0	172.17.88.1
	LAN/Wireless	172.17.30.1	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

Learning Objectives

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

- Configure switch port VLAN information and port security
- Hard reset a Linksys Wireless router
- Connect and verify connectivity to a wireless router
- Navigate to a Linksys Wireless router web utility page
- Configure the IP settings of a Linksys Wireless router
- Configure DHCP on a Linksys Wireless router
- Configure static routes on both standard Cisco routers and on a Wireless router
- Change the network mode and corresponding network channel on a Wireless router
- Learn how to enable WEP encryption and disable SSID broadcast
- Enable a wireless MAC filter
- Configure access restrictions on a Wireless router
- Configure router management password on a Wireless router
- Enable logging on a Wireless router
- Learn diagnosis, backup, restore, and confirmation mechanisms on a Wireless router

Scenario

In this lab, you will configure a Linksys WIRELESS, port security on a Cisco switch, and static routes on multiple devices. Make note of the procedures involved in connecting to a wireless network because some changes involve disconnecting clients, which may then have to reconnect after making changes to the configuration.

Task 1: Perform Basic Router Configurations

Configure R1 according to the following guidelines:

- Router hostname
- Disable DNS lookup
- EXEC mode password
- Fast Ethernet 0/1 and Fast Ethernet 0/0 and its subinterfaces
- Loopback0
- Synchronous logging, exec-timeout, and a login of **cisco** on the console port

Task 2: Configure Switch Interfaces

Set the switches to transparent, clear the VLAN information, and create VLANs 10, 20, and 88.

<For all three switches>

```
!  
vtp mode transparent  
no vlan 2-1001  
vlan 10,20,88  
!
```

Step 1: Configure switch port interfaces on S1, S2, and S3.

Configure the interfaces on the S1, S2, and S3 switches with the connections from topology diagram.

On connections between two switches configure trunks.

On connections to a wireless router configure them as access mode for vlan 88.

Configure S2's connection to PC1 in vlan 10 and PC2's connection in vlan 20.

Configure S1's connection to R1 as a trunk.

Allow all VLANS across trunking interfaces.

S1

```
!  
interface FastEthernet 0/1  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/2  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/3  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/4  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet0/5  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!
```

S2

```
!  
interface FastEthernet 0/1  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/2  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown
```

```
!  
interface FastEthernet 0/3  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/4  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet0/7  
  switchport mode access  
  switchport access vlan 88  
  no shutdown  
!
```

S3

```
!  
interface FastEthernet 0/1  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/2  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/3  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/4  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no shutdown  
!  
interface FastEthernet 0/7  
  switchport mode access  
  switchport access vlan 88  
  no shutdown  
!  
interface FastEthernet 0/11  
  switchport mode access  
  switchport access vlan 11  
  no shutdown  
!  
interface FastEthernet 0/18  
  switchport mode access  
  switchport access vlan 20  
  no shutdown  
!
```

Step 2: Verify VLANs and trunking.

Use the **show ip interface trunk** command on S1 and the **show vlan command** on S2 to verify that the switches are trunking correctly and the proper VLANs exist.

S1#show interface trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1
Fa0/3	on	802.1q	trunking	1
Fa0/4	on	802.1q	trunking	1
Fa0/5	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094
Fa0/2	1-4094
Fa0/3	1-4094
Fa0/4	1-4094
Fa0/5	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,88
Fa0/2	1,10,20,88
Fa0/3	1,10,20,88
Fa0/4	1,10,20,88
Fa0/5	1,10,20,88

Port	Vlans in spanning tree forwarding state and not pruned
------	--

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,88
Fa0/2	none ←-- blocked due to spanning tree
Fa0/3	1,10,20,88
Fa0/4	1,10,20,88
Fa0/5	1,10,20,88>

S2#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, 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	VLAN0010	active	Fa0/11
20	VLAN0020	active	Fa0/18
88	VLAN0088	active	Fa0/7
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

When you have finished, be sure to save the running configuration to the NVRAM of the router and switches.

Step 3: Configure the Ethernet interfaces of PC1 and PC2.

Configure the Ethernet interfaces of PC1 and PC2 with the IP addresses and default gateways according to the addressing table at the beginning of the lab.

Step 4: Test the PC configuration.

Ping the default gateway from the PC: 172.17.10.1 for PC1, and 172.17.20.1 from PC2.

Go to Start->Run->cmd and type ping 172.17.x.x

```
C:\Documents and Settings\Administrator>ping 172.17.10.1

Pinging 172.17.10.1 with 32 bytes of data:

Reply from 172.17.10.1: bytes=32 time<1ms TTL=255
Reply from 172.17.10.1: bytes=32 time<1ms TTL=255
Reply from 172.17.10.1: bytes=32 time<1ms TTL=255
Reply from 172.17.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.17.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

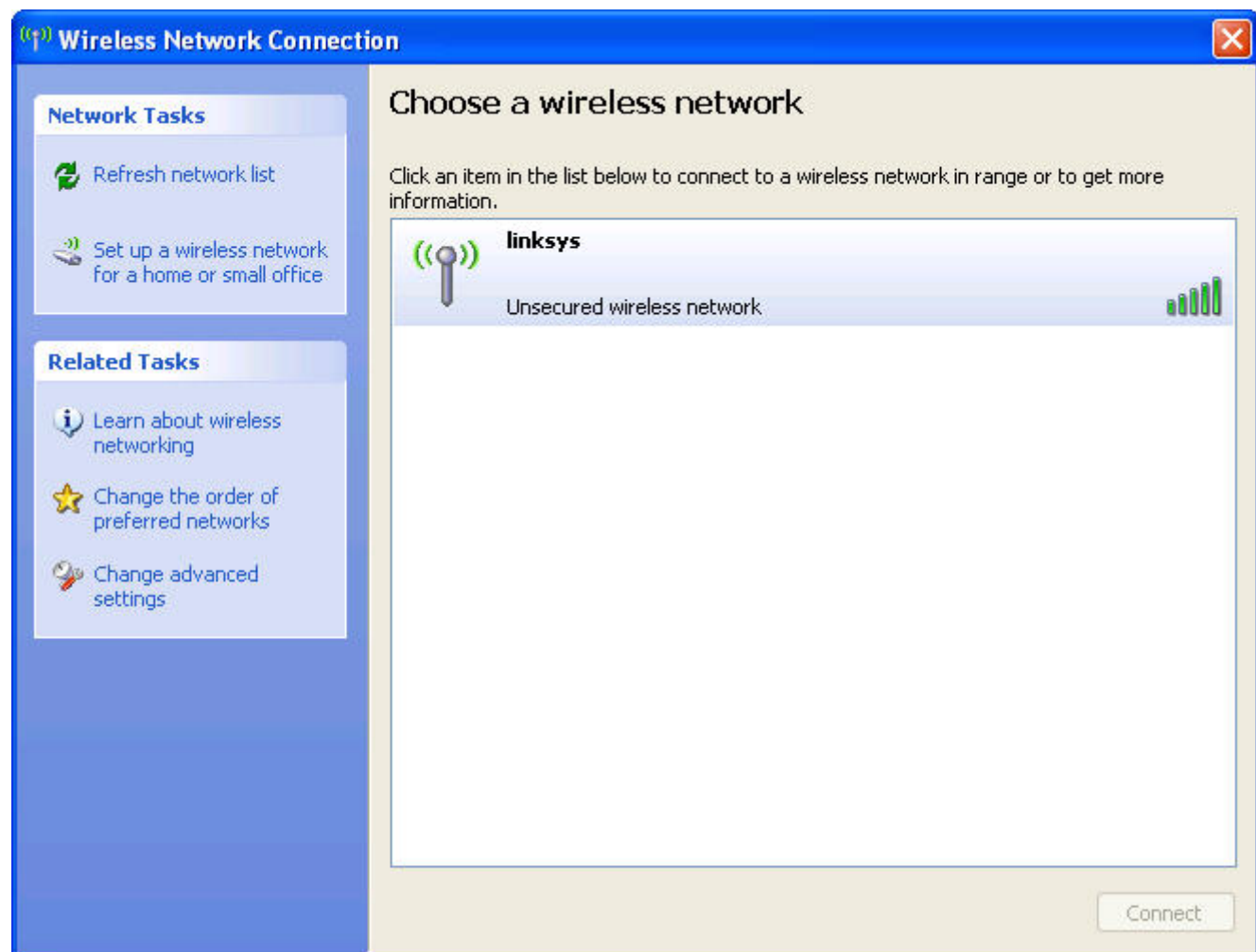
Task 3: Connect to the Linksys Wireless Router

Check with your instructor that the wireless router has its factory default settings. If it does not, you must hard reset the router. To do so, find the reset button on the back of the router. Using a pen or other thin instrument, hold down the reset button for 5 seconds. The router should now be restored to its factory default settings.

Step 1: Use Windows XP to connect to the wireless router.

Locate the Wireless Network Connection icon in your taskbar, or go to **Start > Control Panel > Network Connections**. Right-click the icon and select View Available Wireless Networks.

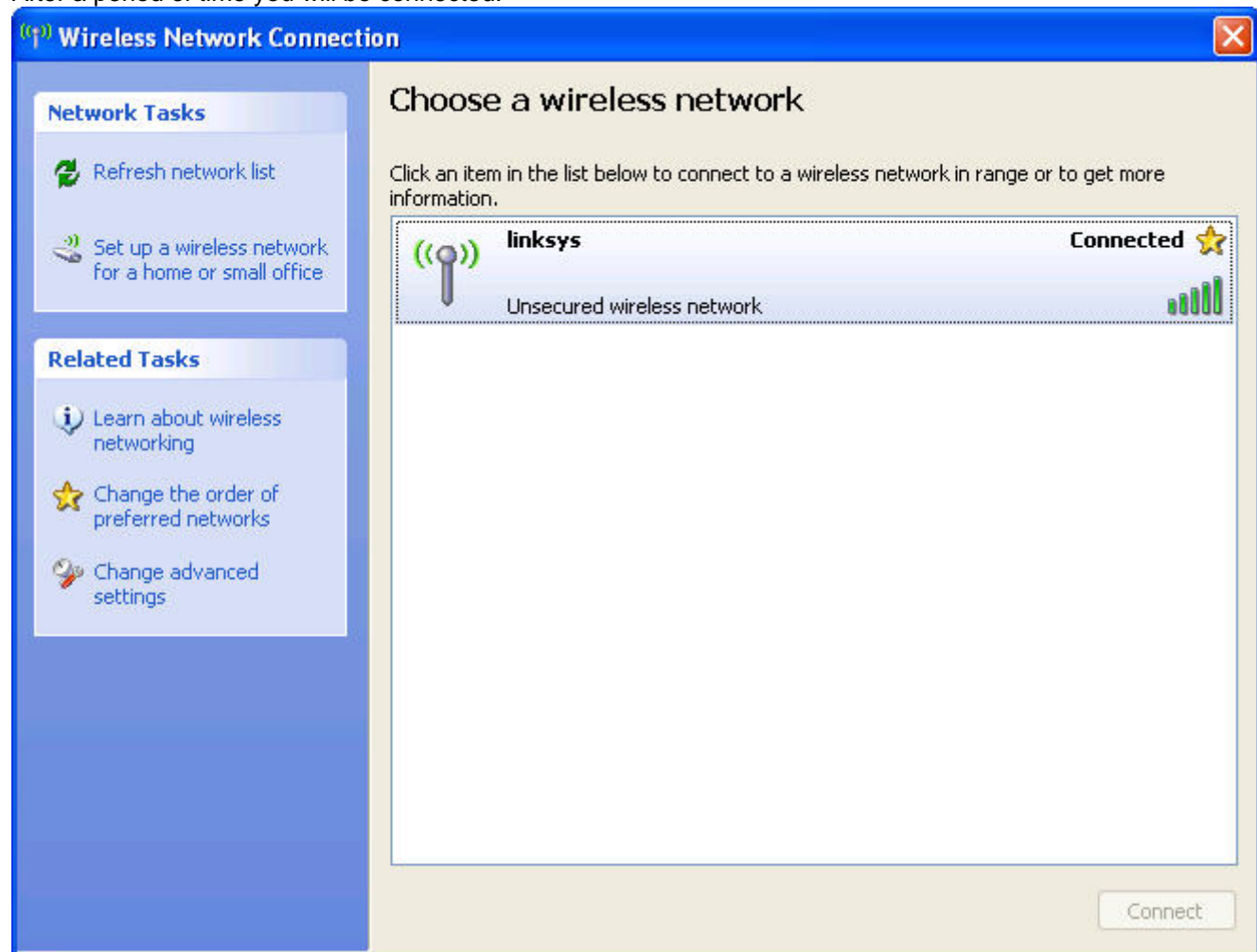
You are prompted with the following display. Note that the factory default SSID of the router is simply "Linksys."



Select **Linksys** and click **Connect**.



After a period of time you will be connected.



Step 2: Verify connectivity settings.

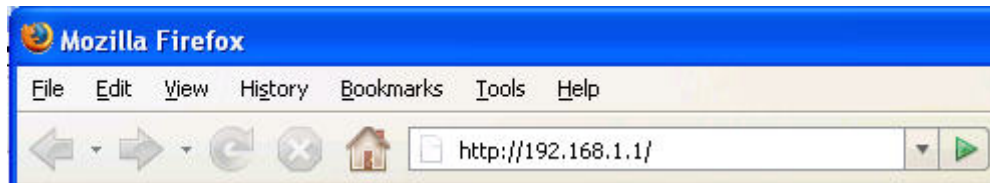
Verify the connectivity settings by going to **Start > Run** and typing **cmd**. At the command prompt, type the command **ipconfig** to view your network device information. Notice which IP address is the default gateway. This is the default IP address of a Linksys WIRELESS.

```
IP Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Task 4: Configure the WIRELESS Using the Web Utility

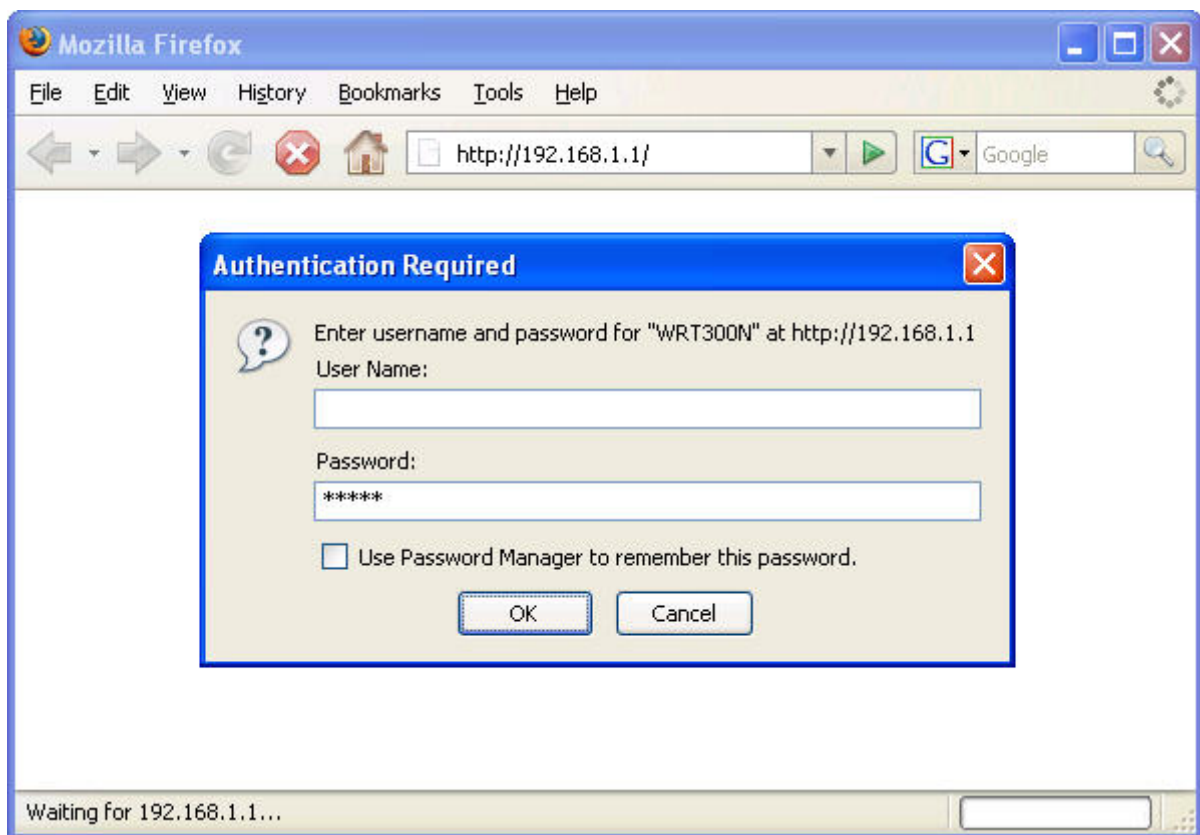
Step 1: Go to the default URL.

In your favorite web browser, navigate to <http://192.168.1.1> which is the default URL for the WIRELESS.




Step 2: Enter authentication information.

You are prompted for a username and password. Enter the WIRELESS factory default password of **admin** and leave the username field blank.



You should now be viewing the default page of the Linksys WIRELESS web utility.


A Division of Cisco Systems, Inc.

Firmware Version: v0.93.3

Wireless-N Broadband Router **WRT300N**

Setup

Setup **Wireless** **Security** **Access Restrictions** **Applications & Gaming** **Administration** **Status**

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Internet Setup

Internet Connection Type

Optional Settings
(required by some Internet Service Providers)

Network Setup

Router IP

DHCP Server Setting

Time Settings

Time Zone

Automatic Configuration - DHCP v

Host Name:

Domain Name:

MTU: Auto Size: 1500

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0 v

DHCP Server: ☒ **Enabled** ☐ **Disabled** DHCP Reservation

Start IP Address: 192 . 168 . 1 . 100

Maximum Number of Users: 50

IP Address Range: 192.168.1.100 ~ 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0


WINS: 0 . 0 . 0 . 0

(GMT-08:00) Pacific Time (USA & Canada) v

☒ Automatically adjust clock for daylight saving changes.

Save Settings Cancel Changes

[Help...](#)



Task 5: Configure IP Settings for the Linksys WIRELESS

The best way to understand the following settings is to think of the WIRELESS as being similar to a Cisco IOS-based router with two separate interfaces. One of the interfaces, the one configured under Internet Setup, acts as the connection to the switches and the interior of the network. The other interface, configured under Network Setup, acts as the interface connecting to the wireless clients, PC6 and PC3.

Step 1: Set the Internet connection type to static IP.

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: v0.93.3

Wireless-N Broadband Router WRT300N

Setup

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Internet Setup

Internet Connection Type

Optional Settings
(required by some Internet Service Providers)

Automatic Configuration - DHCP
Automatic Configuration - DHCP
Static IP
PPPoE
PPTP
L2TP
Telstra Cable

MTU: Auto Size: 1500

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

[Help...](#)

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version: v0.93.3

Wireless-N Broadband Router WRT300N

Setup

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Internet Setup

Internet Connection Type

Optional Settings
(required by some Internet Service Providers)

Static IP

Internet IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

DNS 1: 0 . 0 . 0 . 0

DNS 2 (Optional): 0 . 0 . 0 . 0

DNS 3 (Optional): 0 . 0 . 0 . 0

Host Name:

Domain Name:

MTU: Auto Size: 1500

[Help...](#)

Step 2: Set the IP address settings for Internet Setup.

- Set the Internet IP address to 172.17.88.35.
- Set the subnet mask to 255.255.255.0.
- Set the default gateway to the Fa 0/1 VLAN 88 IP address of R1, 172.17.88.1.

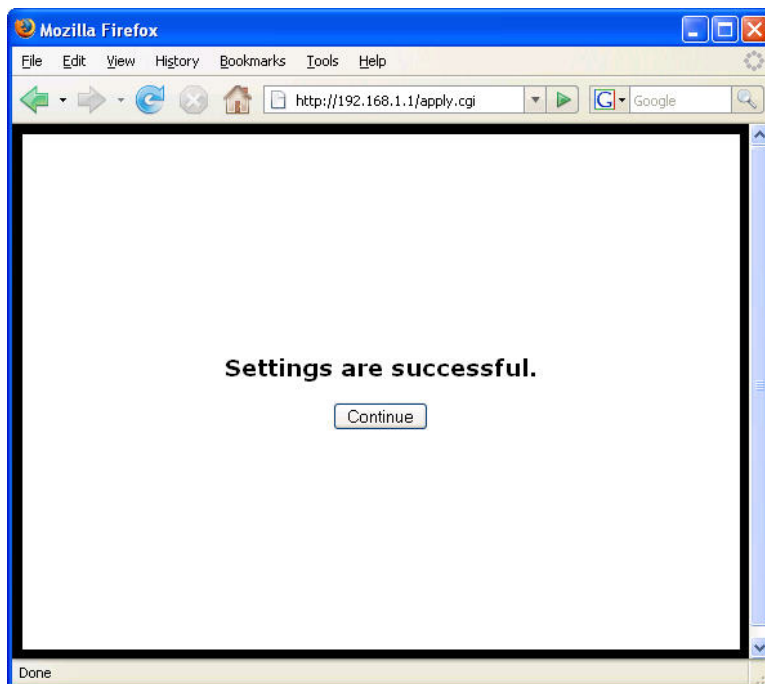
The image shows the Linksys Setup web utility interface. At the top, the Linksys logo is displayed with the text "A Division of Cisco Systems, Inc." Below the logo, there is a navigation bar with tabs for "Setup", "Wireless", "Security", and "Access Restrictions". The "Setup" tab is selected, and within it, the "Basic Setup" sub-tab is active. On the left side, there is a sidebar with "Internet Setup" selected. The main content area shows the "Internet Connection Type" dropdown set to "Static IP". Below this, there are three rows of input fields for IP configuration: "Internet IP Address" (172, 17, 88, 35), "Subnet Mask" (255, 255, 255, 0), and "Default Gateway" (172, 17, 88, 1).

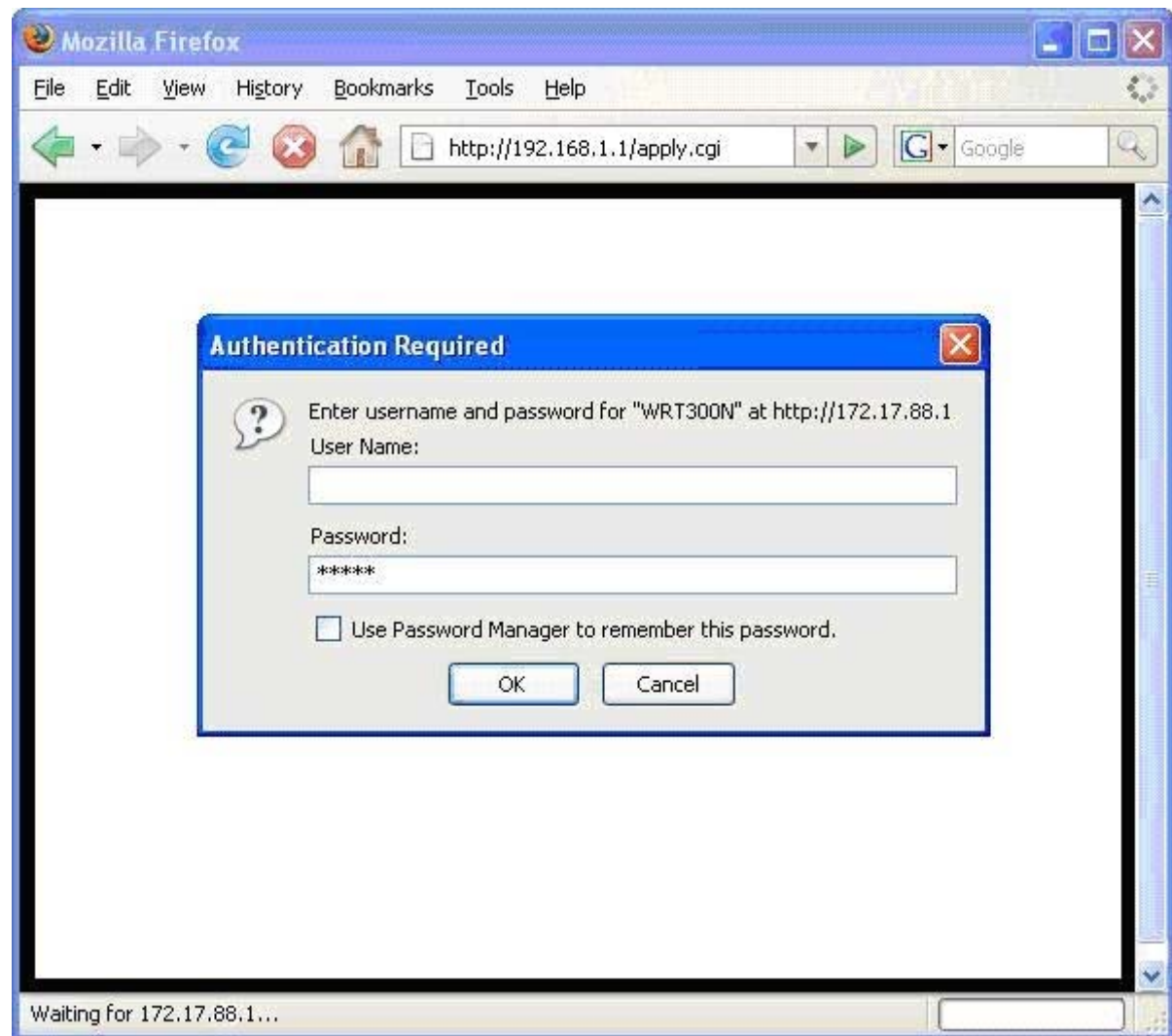
Step 3: Configure the Network Setup IP address to 172.17.30.1.

The image shows the "Network Setup" section of the Linksys web utility. The "Router IP" sub-tab is selected. It displays two rows of input fields: "IP Address" (172, 17, 30, 1) and "Subnet Mask" (255.255.255.0).

Step 4: Save the settings.

Click **Save Settings**. You are prompted with the following window. Click **Continue**. If you are not redirected to the new URL of the web utility (<http://172.17.30.1>), navigate your browser there as you did in Task 4, Step 1.





Step 5: Verify IP address changes.

Go back to the command prompt and notice the new IP addresses. Use the command **ipconfig**.

```
IP Address. . . . . : 172.17.30.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.17.30.1
```

Task 6: Configure DHCP Settings and Router Time Zone Settings

Step 1: Give Pc6 a static DHCP binding.

Click **DHCP Reservations** and find Pc6 in the list of current DHCP clients. Click **Add Clients**.

DHCP Reservation				
Select Clients from DHCP Tables				
Client Name	Interface	IP Address	MAC Address	Select
Pc6	Wireless	172.17.30.100	00:05:4E:49:64:F8	<input checked="" type="checkbox"/>

Add Clients

This gives Pc6, the computer with a MAC address of 00:05:4E:49:64:F8, the same IP address, 172.17.30.100, whenever it requests an address through DHCP. This is only an example of a quick way to permanently bind a client to its current DHCP-given IP address. Now, you will assign Pc6 the IP address in the topology diagram, not the one it received initially. Click **Remove** to assign a new address.

Clients Already Reserved			
Client Name	Assign IP Address	To This MAC Address	MAC Address
Pc6	172.17.30.100	00:05:4E:49:64:F8	Remove

Step 2: Assign Pc6 the 172.17.30.26 address.

By entering the Pc6 address under Manually Adding Client, whenever Pc6 connects to the wireless router, it receives the IP address 172.17.30.26 via DHCP. Save your changes.

Manually Adding Client			
Enter Client Name	Assign IP Address	To This MAC Address	
<input type="text" value="Pc6"/>	<input type="text" value="172.17.30.26"/>	<input type="text" value="00:05:4E:49:64:F8"/>	Add

Step 3: Verify the static IP address change.

Since we already have an IP address from DHCP we are not going to get the new address, 172.17.30.26, until we reconnect. We will wait and notice that later in Task 6, Step 5 and verify that this change has taken place.

Step 4: Configure the DHCP server.

Set the start address to 50, the maximum number of users to 25, and the lease time to 2 hours (or 120 minutes).

DHCP Server Setting	DHCP Server:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	DHCP Reservation
	Start IP Address:	<input type="text" value="172.17.30.50"/>	
	Maximum Number of Users:	<input type="text" value="25"/>	
	IP Address Range:	<input type="text" value="172.17.30.100 to 149"/>	
	Client Lease Time:	<input type="text" value="120"/> minutes (0 means one day)	

These settings give any PC that connects to this router wirelessly requesting an IP address through DHCP, an address between 172.17.30.50–74. Only 25 clients at a time are able to get an IP address and can only have the IP address for two hours, after which time they must request a new one.

Note: IP Address Range does not update until you click **Save Settings**.

Step 5: Configure the router for the appropriate time zone.

At the bottom of the Basic Setup page, change the time zone of the router to reflect your location.

Time Settings	Time Zone	<input type="text" value="(GMT-08:00) Pacific Time (USA & Canada)"/>
	<input checked="" type="checkbox"/> Automatically adjust clock for daylight saving changes.	

Step 6: Save your settings!

Task 7: Basic Wireless Settings

Step 1: Set the network mode.

The Linksys WIRELESS allows you to choose in which network mode to operate. Currently, the most used network mode for clients is Wireless-G and for routers is BG-Mixed. When a router is operating in BG-Mixed, it can accept both B and G clients. However, if a B client connects, the router must scale down to the slower level of B. For this lab, we are assuming all clients are running B only, so choose Wireless-B Only.



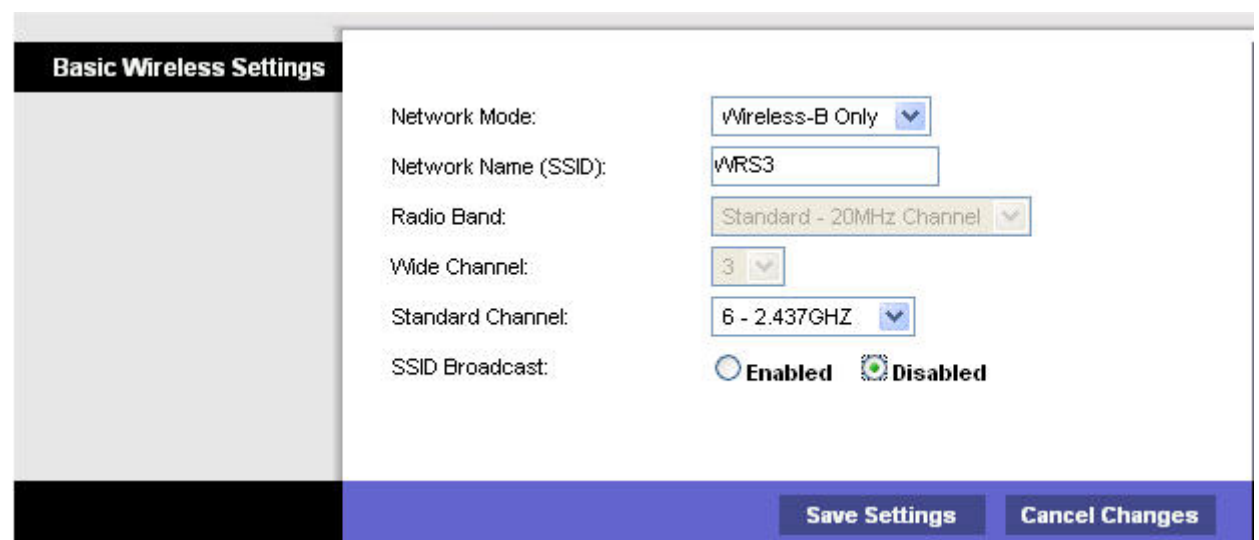
The screenshot shows the 'Basic Wireless Settings' page. The 'Network Mode' dropdown menu is open, showing options: Mixed, BG-Mixed, Wireless-G Only, Wireless-B Only (highlighted), Wireless-N Only, Disabled, and Auto. The 'SSID Broadcast' is currently set to 'Enabled'.

Step 2: Configure other settings.

Change the Network Name SSID to WRS3, Standard Channel to 6 – 2.437GHZ, and disable SSID Broadcast.

Why is it good to change the wireless channel to be different from the default channel?

Why is it recommended to disable SSID broadcast?



The screenshot shows the 'Basic Wireless Settings' page with the following configurations: Network Mode: Wireless-B Only; Network Name (SSID): WRS3; Radio Band: Standard - 20MHz Channel; Wide Channel: 3; Standard Channel: 6 - 2.437GHZ; SSID Broadcast: Disabled. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

Step 3: Click Save Settings.

Step 4: Verify that the SSID of the router is no longer being broadcast.

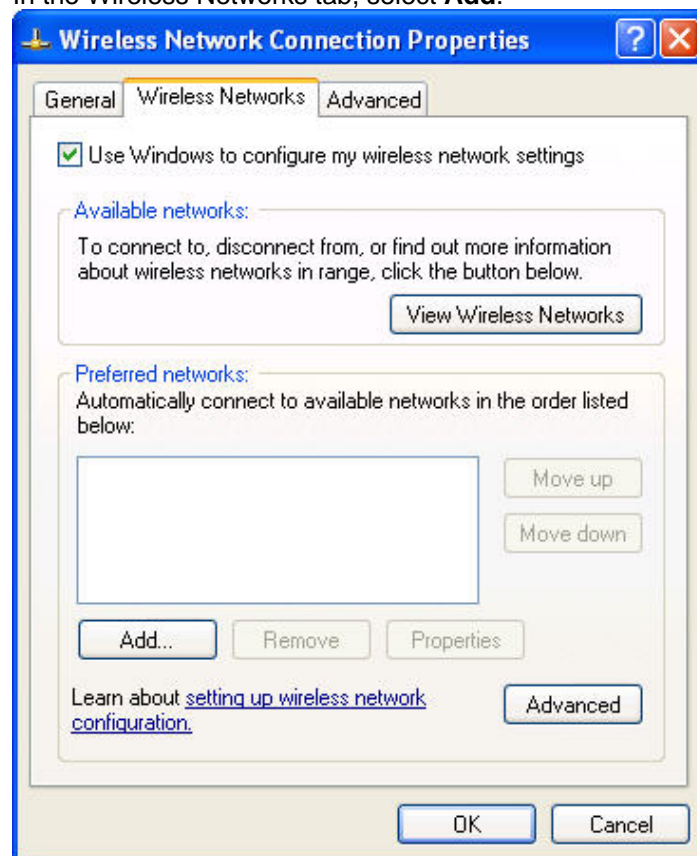
Scan for wireless networks, as done in Task 3, Step 1. Does the SSID of the wireless router appear?

Step 5: Reconnect to the wireless network.

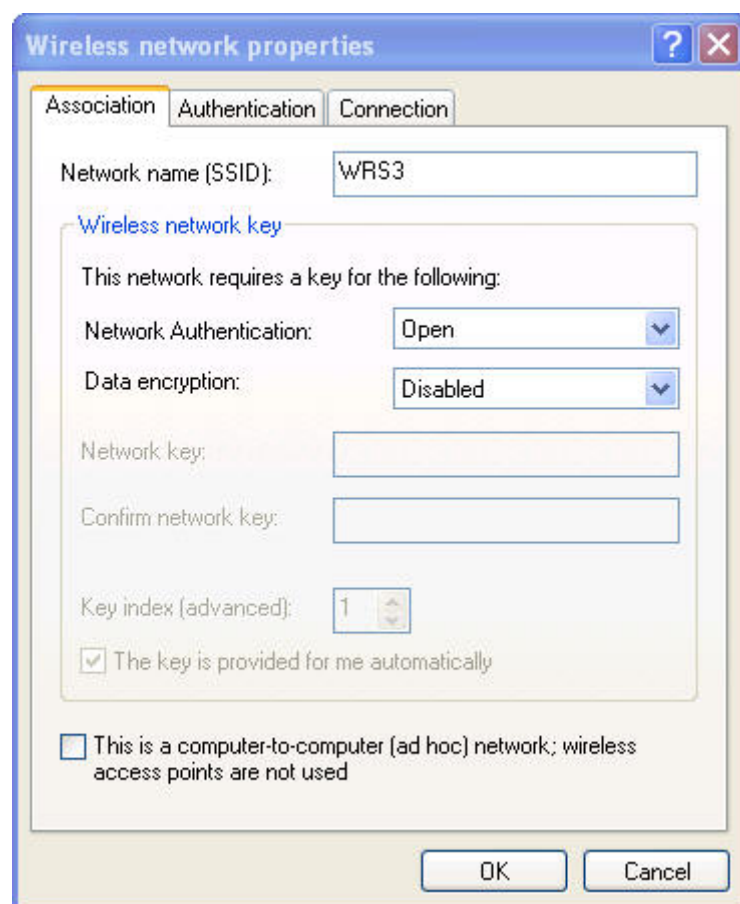
Navigate to **Start > Control Panel > Network Connections**, right-click the Wireless Network Connection icon, and select Properties.



In the Wireless Networks tab, select **Add**.



In the Association Tab, enter WR33 as the SSID, and set the Data Encryption to Disabled. Select OK, and then select OK again. Windows should now try to reconnect to the wireless router.



Step 6: Verify the settings.

Now that you have reconnected to the network, you have the new DHCP settings that you configured in Task 5, Step 3. Verify this at the command prompt with the **ipconfig** command.

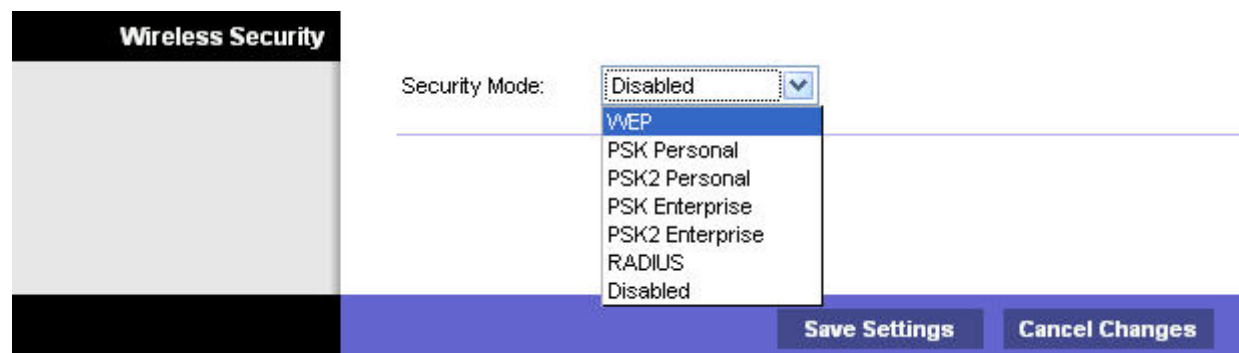
```
IP Address. . . . . : 172.17.30.26
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.17.30.1
```

Task 8: Enable Wireless Security

Step 1: Reconnect to the router setup page (<http://172.17.30.1>).

Step 2: Navigate to the Wireless page and then select the Wireless Security tab.

Step 3: Under Security Mode, select WEP.

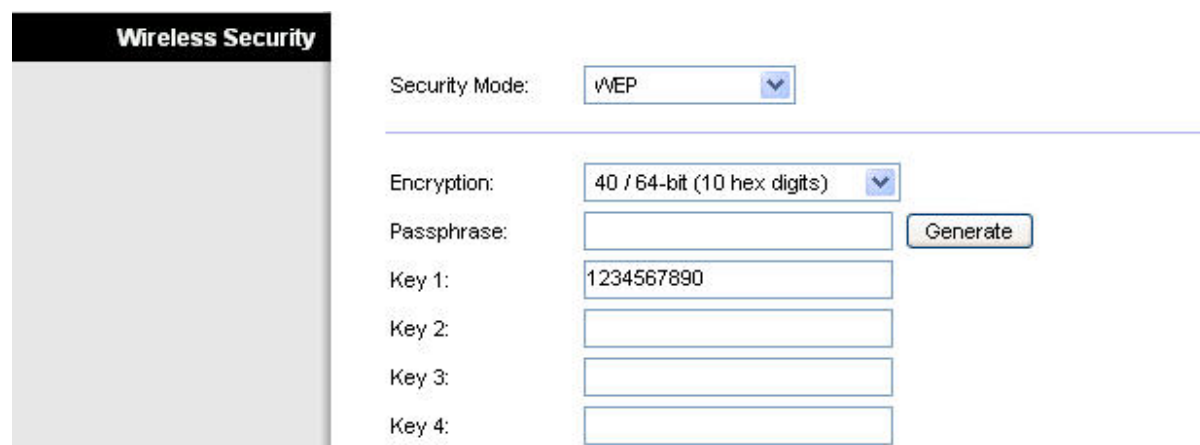


Step 4: Enter a WEP key.

A network is only as secure as its weakest point, and a wireless router is a very convenient place to start if someone wants to damage your network. By not broadcasting the SSID and requiring a WEP key to connect to the router, you are adding a few levels of security.

Unfortunately, there are tools that can discover networks that are not even broadcasting their SSID, and there are even tools that can crack WEP key encryption. A more robust form of wireless security is WPA and WPA-2, which are currently not supported on this router. Wireless MAC filters is more secure but sometimes impractical means of securing your network. It is discussed in the next task.

Add the WEP key 1234567890.



The image shows a 'Wireless Security' configuration page. On the left is a dark sidebar with the title 'Wireless Security'. The main area has a 'Security Mode' dropdown set to 'WEP'. Below this is a horizontal line. Under the line, 'Encryption' is set to '40 / 64-bit (10 hex digits)'. There is a 'Passphrase' field with a 'Generate' button to its right. Below the passphrase field are four 'Key' fields: 'Key 1' contains '1234567890', and 'Key 2', 'Key 3', and 'Key 4' are empty.

Step 5: Save your settings.

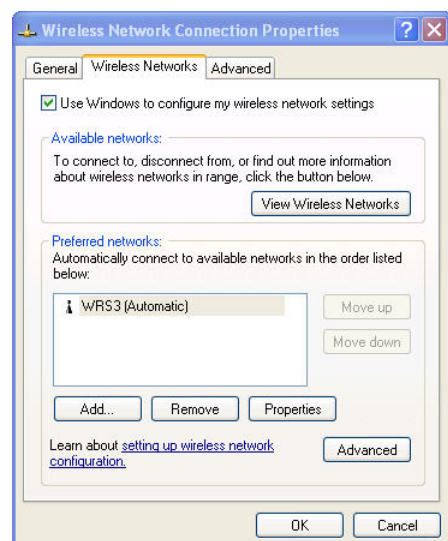
You will become disconnected from the network.

Step 6: Configure Windows to use WEP authentication.

Navigate to the Network Connections page again and right-click the **Wireless Network Connection** icon. In the Wireless Networks tab, locate the WRS3 network, and click **Properties**.

- Set Data Encryption to WEP.
- Uncheck This Key Is Provided For Me.
- Enter the network key of 1234567890, as configured before on the router.
- Click OK and OK.

Windows should now reconnect to the network.



Task 9: Configure a Wireless MAC Filter

Step 1: Add a Mac filter.

- Navigate back to the web utility page of the router (<http://172.17.30.1>).
- Navigate to the Wireless section and then to the Wireless MAC Filter tab.
- Check Enabled.
- Select **Prevent PCs listed below from accessing the wireless network**.
- Enter the MAC address 00:05:4E:49:64:87.

This prevents any client with the MAC address 00:05:4E:49:64:87 from accessing the wireless network.

Wireless Client List	
MAC 01:	00:05:4E:49:64:87
MAC 02:	00:00:00:00:00:00
MAC 26:	00:00:00:00:00:00
MAC 27:	00:00:00:00:00:00

Step 2: Click Wireless Client List.

The **Wireless Client List** shows anyone currently connected to the router via a wireless connection. Also take note of the option **Save to MAC filter list**. Checking this option automatically adds the MAC address of that client to the list of MAC addresses to prevent or permit access to the wireless network.

What is an extremely robust way of only allowing clients of your choosing to connect to the wireless network?

Why does this become not feasible in large networks?

What is a convenient way of adding MAC addresses if everyone to whom you wanted to allow access was already connected to the wireless network?

Task 10: Setting Access Restrictions

Configure an access restriction that prevents Telnet access Monday through Friday to users getting a DHCP address from the preset pool (172.17.30.50 – 74).

Step 1: Navigate to the Access Restrictions tab.

In the Access Restrictions tab, set the following:

- Policy Name – No_Telnet
- Status – Enabled
- Internet access – Allow
- Days – Check Monday through Friday
- Blocked List – Add Telnet

Internet Access Policy

Applied PCs

Access Restriction

Schedule

Website Blocking by URL Address

Website Blocking by Keyword

Blocked Applications

Access Policy: 1 () Delete This Entry Summary

Enter Policy Name:

Status: ☒ Enabled ☐ Disabled

Edit List (This Policy applies only to PCs on the List.)

☐ Deny ☒ Allow Internet access during selected days and hours.

Days: ☐ Everyday ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Times: ☒ 24 Hours ☐ 12 AM : 00 to 12 AM : 00

URL 1: URL 3:

URL 2: URL 4:

Keyword 1: Keyword 3:

Keyword 2: Keyword 4:

Note: only three applications can be blocked per policy.

Applications		Blocked List
<div style="display: flex; align-items: center;"> <div style="flex: 1;"> DNS (53 - 53) Ping (0 - 0) HTTP (80 - 80) HTTPS (443 - 443) FTP (21 - 21) POP3 (110 - 110) IMAP (143 - 143) </div> <div style="flex: 0.5; text-align: center;"> >> << </div> <div style="flex: 1;"> Telnet (23 - 23) </div> </div>		

Application Name	Telnet	
Port Range	23	to 23
Protocol	TCP	

Add
Modify
Delete

Step 2: Set the IP address range.

Apply this configuration to anyone that is using a default DHCP address in the range of 172.17.30.50 – 74.

Click the **Edit List** button at the top of the window and enter the IP address range. Save the settings.

IP Address Range	
01	172 . 17 . 30. 50 to 74
02	172 . 17 . 30. 0 to 0
03	172 . 17 . 30. 0 to 0
04	172 . 17 . 30. 0 to 0

Save the access restriction settings

Task 11: Managing and Securing the Web Utility of the Router

Step 1: Configure web access.

Navigate to the **Administration** section. Change the router password to **cisco**.

For **Web Utility Access**, select both HTTP and HTTPS. Selecting HTTPS access allows a network administrator to manage the router via <https://172.17.30.1> with SSL, a more secure form of HTTP. If you choose to do this in the lab, you may have to accept certificates.

Web Access	
Web Utility Access:	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS
Web Utility Access via Wireless:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

For **Web Utility Access via Wireless**, select Enabled. If you disabled this option, the Web Utility would not be available to clients connected wirelessly. Disabling access is another form of security, because it requires the user to be directly connected to the router before changing settings. However, in this lab scenario, you are configuring the router via wireless access, so disabling access would not be a good idea!

Now back up your configuration by clicking the **Backup Configurations** button. When prompted, save the file to your desktop.

Backup and Restore	
<input type="button" value="Backup Configurations"/>	<input type="button" value="Restore Configurations"/>

Step 2: Restore your configuration.

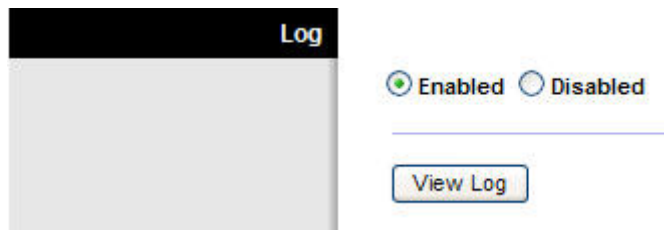
If your settings are accidentally or intentionally changed or erased, you can restore them from a working configuration using the **Restore Configurations** option located in the Backup and Restore section.

Click the **Restore Configuration** button now. In the Restore Configurations window, browse to the previously saved configuration file. Click the **Start to Restore** button. Your previous settings should be successfully restored.

Please select a file to Restore.: C:\Documents and Settings\... Browse...

Step 3: Enable logging.

Navigate to the **Log** tab and enable logging. You are now able to view the log of the router.



Step 4: Save your settings and end your wireless connection to the router.

Step 5: Plug an Ethernet cable into one of the wireless router's LAN ports and connect to it

Step 6: Navigate to the router's Web GUI.

Step 7: Navigate to the Administration section

```
R1#sh ip route
<output deleted>
```

Gateway of last resort is not set

```
      172.17.0.0/24 is subnetted, 5 subnets
S       172.17.40.0 [1/0] via 172.17.88.25
S       172.17.30.0 [1/0] via 172.17.88.35
C       172.17.20.0 is directly connected, FastEthernet0/1.20
C       172.17.10.0 is directly connected, FastEthernet0/1.10
C       172.17.88.0 is directly connected, FastEthernet0/1.88
      10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback0
```

```
R1#ping 172.17.30.26
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.30.26, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
R1#ping 172.17.40.23
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.40.23, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Verify that PC3 and PC6 can ping the loopback of R1.

Verify that PC3 and PC6 can ping each other.

Verify that PC3 and PC6 can ping PC1 and PC2.

```
IP Address. . . . . : 172.17.30.26
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.17.30.1
From PC6

C:\Documents and Settings\Administrator>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=1ms TTL=254
Reply from 10.1.1.1: bytes=32 time=1ms TTL=254
Reply from 10.1.1.1: bytes=32 time=1ms TTL=254
Reply from 10.1.1.1: bytes=32 time=1ms TTL=254
To R1's loopback

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 172.17.40.23

Pinging 172.17.40.23 with 32 bytes of data:

Reply from 172.17.40.23: bytes=32 time=1ms TTL=126
Reply from 172.17.40.23: bytes=32 time=1ms TTL=126
Reply from 172.17.40.23: bytes=32 time=1ms TTL=126
Reply from 172.17.40.23: bytes=32 time=1ms TTL=126
To PC3

Ping statistics for 172.17.40.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 172.17.10.21

Pinging 172.17.10.21 with 32 bytes of data:

Reply from 172.17.10.21: bytes=32 time=1ms TTL=126
Reply from 172.17.10.21: bytes=32 time<1ms TTL=126
Reply from 172.17.10.21: bytes=32 time<1ms TTL=126
Reply from 172.17.10.21: bytes=32 time<1ms TTL=126
To PC1

Ping statistics for 172.17.10.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Task 13: Configuring Port Security

Step 1: Configure PC1 port security.

Log on to switch S2. Configure the PC1 switch port 11, enable port security, and enable dynamic sticky MAC addresses.

Step 2: Configure PC2 port security.

Repeat Step 1 for switch port 18.

S2

```
!
interface FastEthernet 0/11
    switchport mode access
    switchport access vlan 10
    switchport port-security
    switchport port-security mac-address sticky
    no shutdown
!
!
interface FastEthernet 0/18
    switchport mode access
```

```
switchport access vlan 20
switchport port-security
switchport port-security mac-address sticky
no shutdown
!
```

Step 3: Generate traffic across the ports by pinging PC2 from PC1.

Step 4: Verify port security.

S1#show port-security address

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	0006.5b1e.33fa	SecureSticky	Fa0/11	-
20	0001.4ac2.22ca	SecureSticky	Fa0/18	-

```
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 6272
```

S1#sh port-security int fa 0/11

```
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 : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0006.5b1e.33fa:10
Security Violation Count : 0
```

Appendix Configurations

Hostname R1

```
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/1
 no shutdown
!
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 FastEthernet0/1.88
```

```
    encapsulation dot1Q 88
    ip address 172.17.88.1 255.255.255.0
!
!
ip route 172.17.30.0 255.255.255.0 172.17.88.35
ip route 172.17.40.0 255.255.255.0 172.17.88.25
!
!
!
!
line con 0
    exec-timeout 0 0
    logging synchronous
    password cisco
line aux 0
line vty 0 4
!
!
end
```

Hostname S1

```
!
!
vtp mode transparent
!
!
vlan 10,20,88
!
!
interface FastEthernet0/1
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
interface FastEthernet0/2
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
interface FastEthernet0/3
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
interface FastEthernet0/4
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
interface FastEthernet0/5
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
line con 0
    exec-timeout 0 0
    logging synchronous
!
end
```

Hostname S2

```
!  
vtp mode transparent  
!  
vlan 10,20,88  
!  
!  
interface FastEthernet0/1  
    switchport trunk encapsulation dot1q  
    switchport mode trunk  
!  
interface FastEthernet0/2  
    switchport trunk encapsulation dot1q  
    switchport mode trunk  
!  
interface FastEthernet0/3  
    switchport trunk encapsulation dot1q  
    switchport mode trunk  
!  
interface FastEthernet0/4  
    switchport trunk encapsulation dot1q  
    switchport mode trunk  
!  
interface FastEthernet0/7  
    switchport mode access  
    switchport access vlan 88  
!  
!  
! PC1 and PC2's MAC address will appear after 'sticky' on ports 11  
! and 18 respectively, after traffic traverses them  
!  
  
interface FastEthernet0/11  
    switchport access vlan 10  
    switchport mode access  
    switchport port-security  
    switchport port-security mac-address sticky  
    switchport port-security mac-address sticky ffff.ffff.ffff  
!  
interface FastEthernet0/18  
    switchport access vlan 20  
    switchport mode access  
    switchport port-security  
    switchport port-security mac-address sticky  
    switchport port-security mac-address sticky ffff.ffff.ffff  
!  
line con 0  
    exec-timeout 0 0  
    logging synchronous  
!  
end
```

Hostname S3

```
!  
vtp mode transparent  
!  
vlan 10,20,88  
!
```

```
interface FastEthernet0/1
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface FastEthernet0/7
  switchport mode access
  switchport access vlan 88
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
!
!
end
```