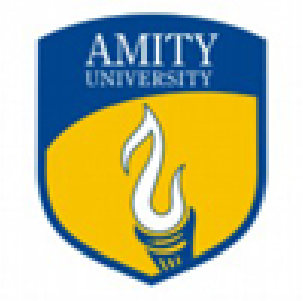
Lab File

Routing and Switching
[IT308]

DEPARTMENT
OF
COMPUTER SCIENCE AND ENGINEERING

BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING



Submitted To:

Dr. Sunil Kumar
Associate Professor
CSE Department, ASET

Submitted By:

Rishabh Sharma
A2345919013
B. Tech (CSE)
6CSE-EVNG-X

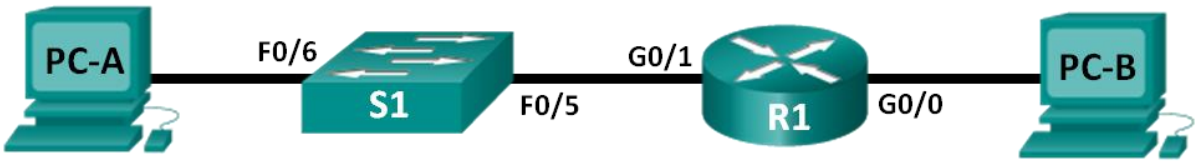
AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY
AMITY UNIVERSITY UTTAR PRADESH
NOIDA-201301

INDEX

Experiment-1

Objective: Configuring Basic Router Settings with IOS CLI.

1. **Topology**



1. **Addressing Table**

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

1. **Objectives**

Part 1: Set Up the Topology and Initialize Devices

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

Part 2: Configure Devices and Verify Connectivity

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

Part 3: Display Router Information

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

Part 4: Configure IPv6 and Verify Connectivity

1. **Background / Scenario**

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

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

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

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

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

1. **Required Resources**

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

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

1. **Set Up the Topology and Initialize Devices**

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

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

a. Power on all the devices in the topology.

1. **Initialize and reload the router and switch.**

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

1. **Configure Devices and Verify Connectivity**

1. **Configure the PC interfaces.**

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

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

1. Configure the router.

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

Router> **enable**

Router#

a. Enter into global configuration mode.

Router# **config terminal**

Router(config)#

a. Assign a device name to the router.

Router(config)# **hostname R1**

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

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

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

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

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

_____

_____

a. Assign **cisco12345** as the privileged EXEC encrypted password.

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

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

R1(config)# **line con 0**

R1(config-line)# **password ciscoconpass**

R1(config-line)# **exec-timeout 5 0**

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

R1(config-line)# **logging synchronous**

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

R1(config)#

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

_____

_____

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

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

R1(config-line)# **password ciscovtypass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **transport input telnet**

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

R1(config-line)# **logging synchronous**

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

R1(config)#

a. Encrypt the clear text passwords.

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

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

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

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

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

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

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

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

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

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

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

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

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

R1(config)# **exit**

R1#

a. Set the clock on the router; for example:

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

a. Save the running configuration to the startup configuration file.

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

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

_____
_____

_____
_____

1. **Verify network connectivity.**

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

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

Were the pings successful? _____

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

_____
_____

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

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

Was remote access successful? _____

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

_____
_____

_____
_____

1. **Configure the router for SSH access.**

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

R1# **configure terminal**

R1(config)# **ip domain-name CCNA-lab.com**

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

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

R1(config-line)# **transport input ssh**

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

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

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

R1(config)# **exit**

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

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

Was remote access successful? _____

1. Display Router Information

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

1. Establish an SSH session to R1.

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

1. Retrieve important hardware and software information.

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

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

_____ flash0:c1900-universalk9-mz.SPA.151-1.M4.bin _____

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

_____255K_____
_____

How much Flash memory does the router have?

_____249856K
_____

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

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

_____
_____

_____
_____

_____
_____

1. **Display the startup configuration.**

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

How are passwords presented in the output?

_____
_____

_____
_____

_____
_____

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

What is the result of using this command?

_____
_____

_____
_____

1. **Display the routing table on the router.**

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

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

_____
_____

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

1. **Display a summary list of the interfaces on the router.**

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

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

_____

_____

1. **Configure IPv6 and Verify Connectivity**

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

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

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

R1# **configure terminal**

R1(config)# **interface g0/0**

R1(config-if)# **ipv6 address 2001:db8:acad:a::1/64**

R1(config-if)# **ipv6 address fe80::1 link-local**

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

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

R1(config)# **ipv6 unicast-routing**

R1(config)# **exit**

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

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

_____

_____

_____

_____

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

What is the IPv6 address assigned to PC-B?

_____

_____

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

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

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

_____

1. **Reflection**

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

_____

_____

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

_____

_____

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

_____

_____

_____

_____

1. **Router Interface Summary Table**

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

of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

1. **Appendix A: Initializing and Reloading a Router and Switch**

1. **Initialize and reload the router.**

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

Router> **enable**

Router#

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

Router# **erase startup-config**

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

[OK]

Erase of nvram: complete

Router#

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

Router# **reload**

Proceed with reload? [confirm]

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

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

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

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

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

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

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

1. **Initialize and reload the switch.**

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

Switch> **enable**

Switch#

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

Switch# **show flash**

Directory of flash:/

2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text

3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text

4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs

5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin

6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat

32514048 bytes total (20886528 bytes free)

Switch#

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

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

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

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

Delete flash:/vlan.dat? [confirm]

Switch#

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

Switch# **erase startup-config**

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

[OK]

Erase of nvram: complete

Switch#

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

Switch# **reload**

Proceed with reload? [confirm]

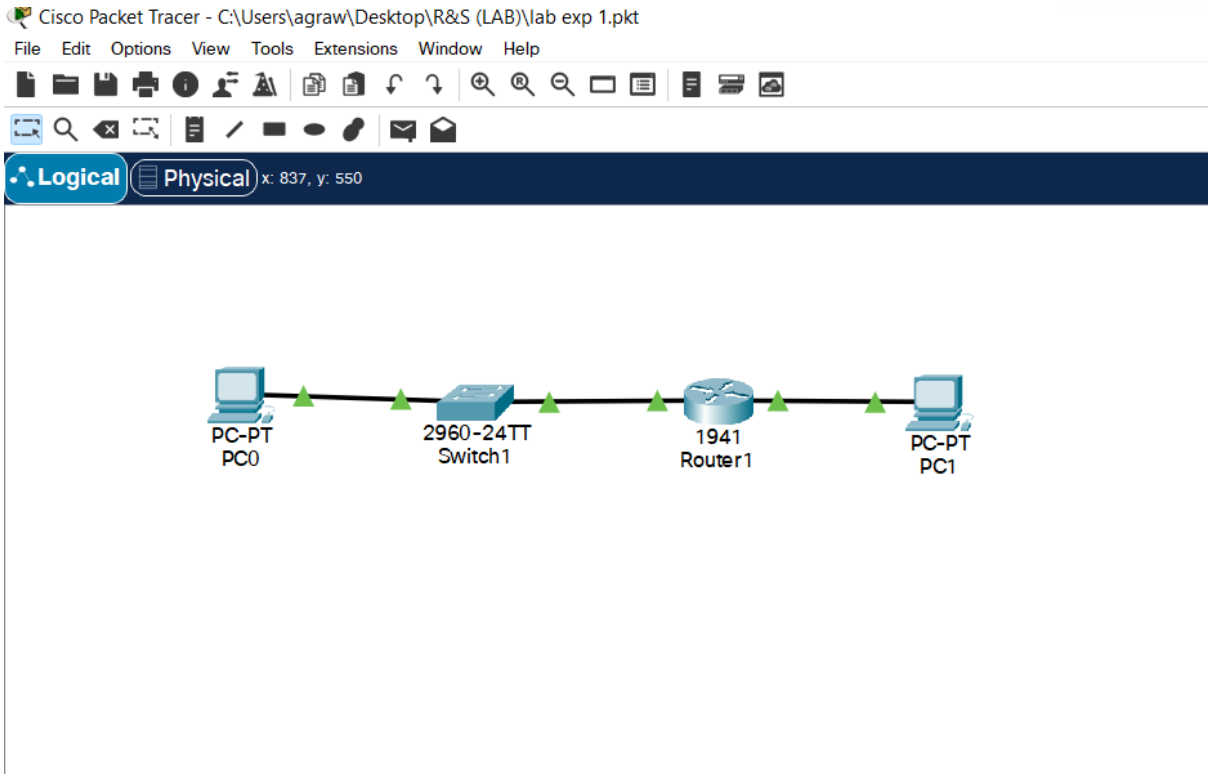
Note: You may be prompted to save the running configuration prior to reloading the switch. Type **no** and press Enter.

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

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

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

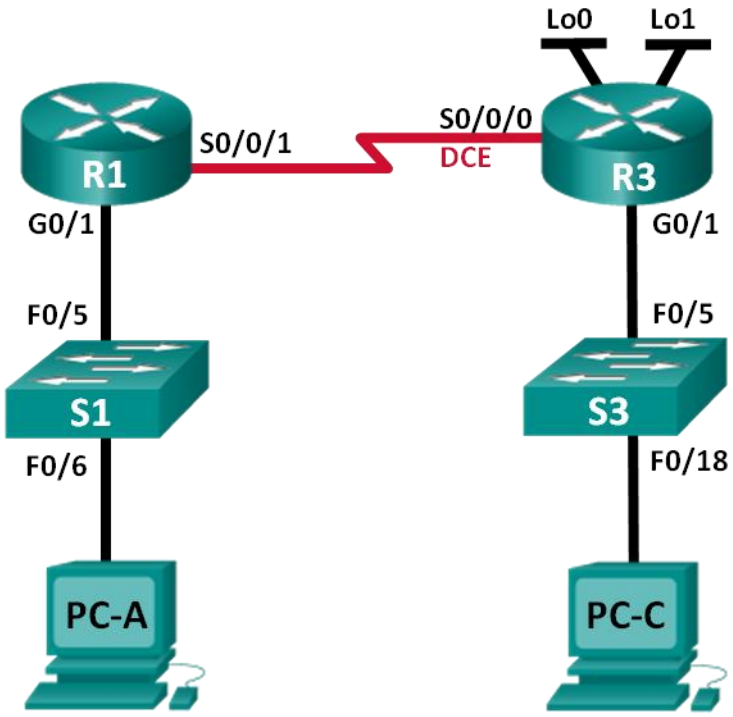
Switch>



Experiment-2

Objective: Configuring IPv4 Static and Default Routes

1. **Topology**



1. **Addressing Table**

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

1. **Objectives**

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure Static Routes

- Configure a recursive static route.
- Configure a directly connected static route.
- Configure and remove static routes.

Part 4: Configure and Verify a Default Route

1. **Background / Scenario**

A router uses a routing table to determine where to send packets. The routing table contains a set of routes that describe which gateway or interface the router uses to reach a specified network. Initially, the routing table contains only directly connected networks. To communicate with distant networks, routes must be specified and added to the routing table.

In this lab, you will manually configure a static route to a specified distant network based on a next-hop IP address or exit interface. You will also configure a static default route. A default route is a type of static route that specifies a gateway to use when the routing table does not contain a path for the destination network.

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

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

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

1. **Required Resources**

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

1. **Set Up the Topology and Initialize Devices**

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

1. **Initialize and reload the router and switch.**

1. **Configure Basic Device Settings and Verify Connectivity**

In Part 2, you will configure basic settings, such as the interface IP addresses, device access, and passwords. You will verify LAN connectivity and identify routes listed in the routing tables for R1 and R3.

1. **Configure the PC interfaces.**

1. **Configure basic settings on the routers.**

a. Configure device names, as shown in the Topology and Addressing Table.

a. Disable DNS lookup.

a. Assign **class** as the enable password and assign **cisco** as the console and vty password.

a. Save the running configuration to the startup configuration file.

1. **Configure IP settings on the routers.**

a. Configure the R1 and R3 interfaces with IP addresses according to the Addressing Table.

a. The S0/0/0 connection is the DCE connection and requires the **clock rate** command. The R3 S0/0/0 configuration is displayed below.

R3(config)# **interface s0/0/0**

R3(config-if)# **ip address 10.1.1.2 255.255.255.252**

R3(config-if)# **clock rate 128000**

R3(config-if)# **no shutdown**

1. **Verify connectivity of the LANs.**

a. Test connectivity by pinging from each PC to the default gateway that has been configured for that host.

From PC-A, is it possible to ping the default gateway? _____

From PC-C, is it possible to ping the default gateway? _____

a. Test connectivity by pinging between the directly connected routers.

From R1, is it possible to ping the S0/0/0 interface of R3? _____

If the answer is **no** to any of these questions, troubleshoot the configurations and correct the error.

a. Test connectivity between devices that are not directly connected.

From PC-A, is it possible to ping PC-C? _____

From PC-A, is it possible to ping Lo0? _____

From PC-A, is it possible to ping Lo1? _____

Were these pings successful? Why or why not?

_____
_____

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

1. **Gather information.**

a. Check the status of the interfaces on R1 with the **show ip interface brief** command.

How many interfaces are activated on R1? _____

a. Check the status of the interfaces on R3.

How many interfaces are activated on R3? _____

a. View the routing table information for R1 using the **show ip route** command.

What networks are present in the Addressing Table of this lab, but not in the routing table for R1?

_____
_____

a. View the routing table information for R3.

What networks are present in the Addressing Table in this lab, but not in the routing table for R3?

_____
_____

Why are all the networks not in the routing tables for each of the routers?

_____
_____

_____
_____

1. **Configure Static Routes**

In Part 3, you will employ multiple ways to implement static and default routes, you will confirm that the routes have been added to the routing tables of R1 and R3, and you will verify connectivity based on the introduced routes.

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

1. **Configure a recursive static route.**

With a recursive static route, the next-hop IP address is specified. Because only the next-hop IP is specified, the router must perform multiple lookups in the routing table before forwarding packets. To configure recursive static routes, use the following syntax:

Router(config)# **ip route** *network-address subnet-mask ip-address*

a. On the R1 router, configure a static route to the 192.168.1.0 network using the IP address of the Serial 0/0/0 interface of R3 as the next-hop address. Write the command you used in the space provided.

_____
_____

a. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

_____
_____

From host PC-A, is it possible to ping the host PC-C? _____

These pings should fail. If the recursive static route is correctly configured, the ping arrives at PC-C. PC-C sends a ping reply back to PC-A. However, the ping reply is discarded at R3 because R3 does not have a return route to the 192.168.0.0 network in the routing table.

1. **Configure a directly connected static route.**

With a directly connected static route, the *exit-interface* parameter is specified, which allows the router to resolve a forwarding decision in one lookup. A directly connected static route is typically used with a point-to-point serial interface. To configure directly connected static routes with an exit interface specified, use the following syntax:

Router(config)# **ip route** *network-address subnet-mask exit-intf*

a. On the R3 router, configure a static route to the 192.168.0.0 network using S0/0/0 as the exit interface. Write the command you used in the space provided.
_____

a. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

_____
_____

a. From host PC-A, is it possible to ping the host PC-C? _____

This ping should be successful.

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

1. **Configure a static route.**

a. On the R1 router, configure a static route to the 198.133.219.0 network using one of the static route configuration options from the previous steps. Write the command you used in the space provided.

_____
_____

a. On the R1 router, configure a static route to the 209.165.200.224 network on R3 using the other static route configuration option from the previous steps. Write the command you used in the space provided.

_____
_____

a. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

_____
_____

a. From host PC-A, is it possible to ping the R1 address 198.133.219.1? _____

This ping should be successful.

1. **Remove static routes for loopback addresses.**

a. On R1, use the **no** command to remove the static routes for the two loopback addresses from the routing table. Write the commands you used in the space provided.

_____
_____

_____
__

a. View the routing table to verify the routes have been removed.

How many network routes are listed in the routing table on R1? _____

Is the Gateway of last resort set? _____

1. **Configure and Verify a Default Route**

In Part 4, you will implement a default route, confirm that the route has been added to the routing table, and verify connectivity based on the introduced route.

A default route identifies the gateway to which the router sends all IP packets for which it does not have a learned or static route. A default static route is a static route with 0.0.0.0 as the destination IP address and subnet mask. This is commonly referred to as a “quad zero” route.

In a default route, either the next-hop IP address or exit interface can be specified. To configure a default static route, use the following syntax:

Router(config)# **ip route 0.0.0.0 0.0.0.0** {*ip-address or exit-intf*}

a. Configure the R1 router with a default route using the exit interface of S0/0/1. Write the command you used in the space provided.

_____
__

a. View the routing table to verify the new static route entry.

How is this new route listed in the routing table?

_____
_____

What is the Gateway of last resort?

_____
_____

a. From host PC-A, is it possible to ping the 209.165.200.225? _____

a. From host PC-A, is it possible to ping the 198.133.219.1? _____

These pings should be successful.

1. Reflection

1. A new network 192.168.3.0/24 is connected to interface G0/0 on R1. What commands could be used to configure a static route to that network from R3?

_____
_____

_____
_____

1. Is there a benefit to configuring a directly connected static route instead of a recursive static route?

_____
_____

_____
_____

1. Why is it important to configure a default route on a router?

_____
_____

1. **Router Interface Summary Table**

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

1.

1. **Appendix A: Configuration Commands for Parts 2, 3, and 4**

The commands listed in Appendix A are for reference only. This Appendix does not include all the specific commands necessary to complete this lab.

1. **Basic Device Settings**

Configure IP settings on the router.

R3(config)# **interface s0/0/0**

R3(config-if)# **ip address 10.1.1.2 255.255.255.252**

R3(config-if)# **clock rate 128000**

R3(config-if)# **no shutdown**

1. **Static Route Configurations**

Configure a recursive static route.

R1(config)# **ip route 192.168.1.0 255.255.255.0 10.1.1.2**

Configure a directly connected static route.

R3(config)# **ip route 192.168.0.0 255.255.255.0 s0/0/0**

Remove static routes.

R1(config)# **no ip route 209.165.200.224 255.255.255.224 serial0/0/1**

or

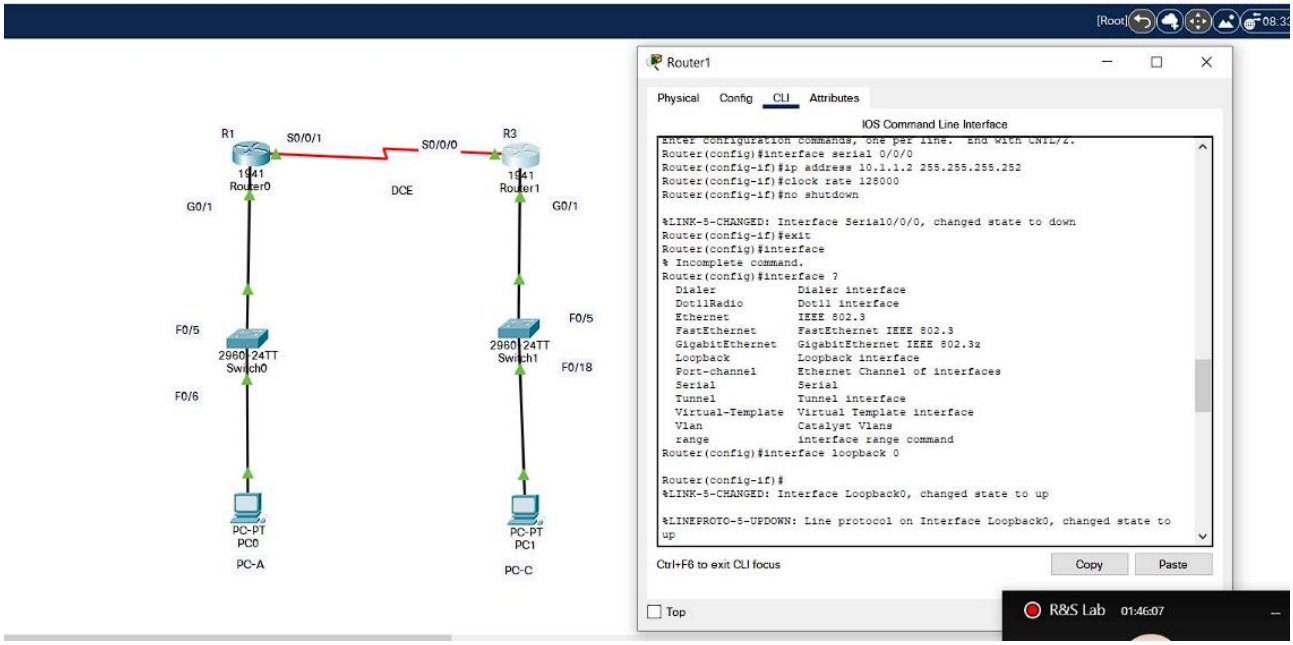
R1(config)# **no ip route 209.165.200.224 255.255.255.224 10.1.1.2**

or

R1(config)# **no ip route 209.165.200.224 255.255.255.224**

1. **Default Route Configuration**

R1(config)# **ip route 0.0.0.0 0.0.0.0 s0/0/1**



Experiment-3

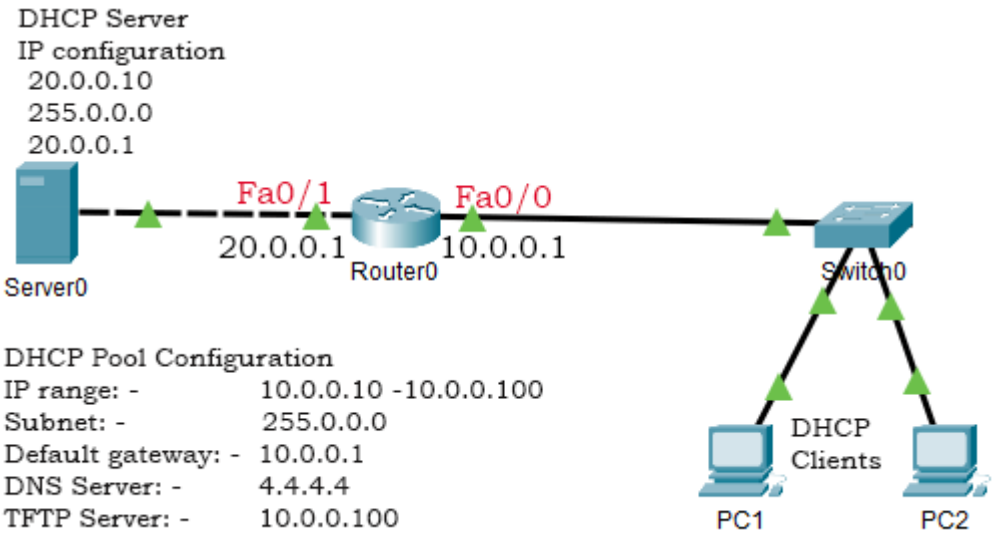
Objective: Configure DHCP Snooping on Cisco Switches

DHCP Snooping is a security feature of Layer 2 switches. It allows us to filter and block certain types of DHCP traffic. By using this feature, we can mitigate several security risks caused by rogue DHCP servers and attackers.

DHCP snooping works on a per-VLAN basis. By default, this feature is not enabled. To use this feature, first, we have to enable it. After enabling, we can configure it on some VLANs or all VLANs. Once configured, it actively monitors incoming traffic on all ports of the configured VLAN. If it detects any DHCP packet, based on its configuration either it allows the packet or drops the packet.

To learn how this process works in detail, you can check the previous parts of this tutorial. In this part, we will understand how to configure DHCP snooping on Cisco switches.

Create a packet tracer lab as shown in the following image.



Configure this lab as described below.

- Assign the IP address 10.0.0.1/8 to the Fa0/0 interface of router 0.
- Configure the Fa0/0 interface of the router to forward all DHCP requests to the Server0.
- Assign the IP address 20.0.0.1/8 to the Fa0/1 interface of the Router0.
- Assign the IP address 20.0.0.10/8 to the Server0.

- Configure a DHCP pool for the local network connected to the Switch0.
- Configure PCs of the local network as DHCP clients.

Configuring the router

Access the CLI prompt of the router and run the following commands.

Router>enable

Router#configure terminal

Router(config)#interface fastethernet 0/0

Router(config-if)#ip address 10.0.0.1 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastethernet 0/1

Router(config-if)#ip address 20.0.0.1 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastethernet 0/0

Router(config-if)#ip helper-address 20.0.0.10

Router(config-if)#exit

Router(config)#

The following table explains the commands used in the above configuration.

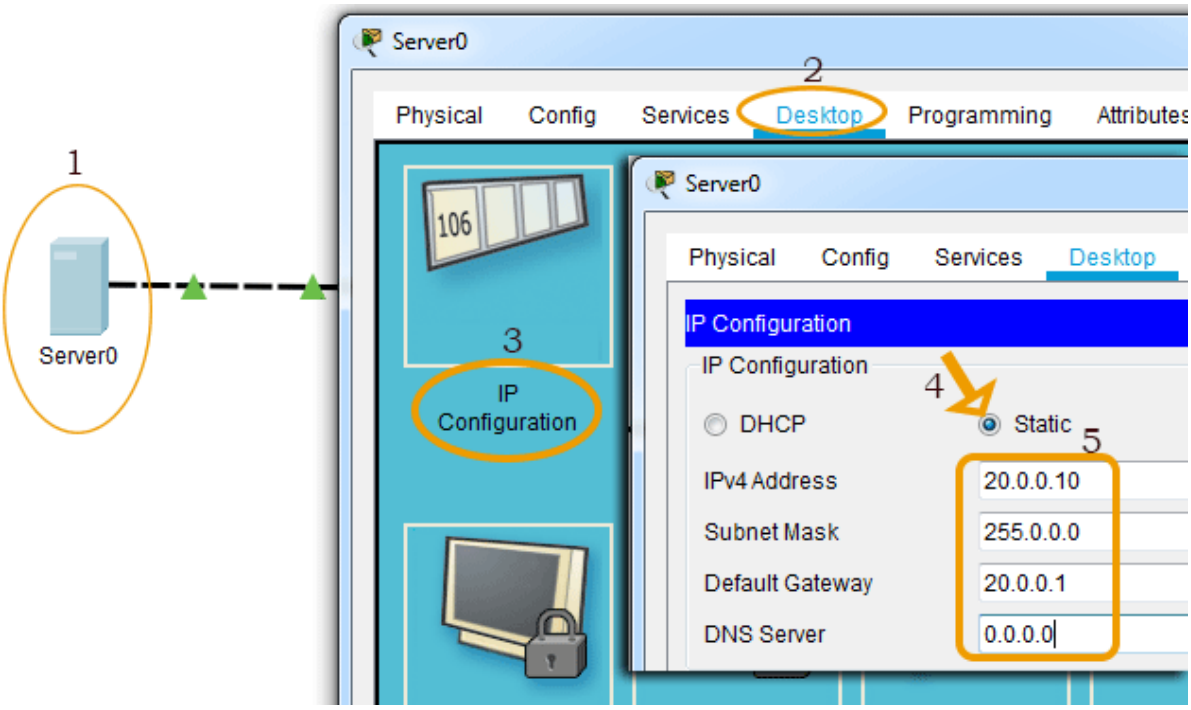
Command	Description
Router>enable	Enter privileged-exec mode.
Router#configure terminal	Enter global configuration mode.
Router(config)#interface [*interface*] [*slot/number*]	Enter interface configuration mode.
Router(config-if)#ip address [*IP address*] [*subnet mask*]	Assign an IP address to the interface.
Router(config-if)#ip helper-address [*IP address of the DHCP server*]	Configure the interface to forward DHCP requests to the DHCP server.

Router(config-if)#no shutdown	Enable interface.
Router(config-if)#exit	Exit interface configuration mode.

Assigning a static IP address to the Server0

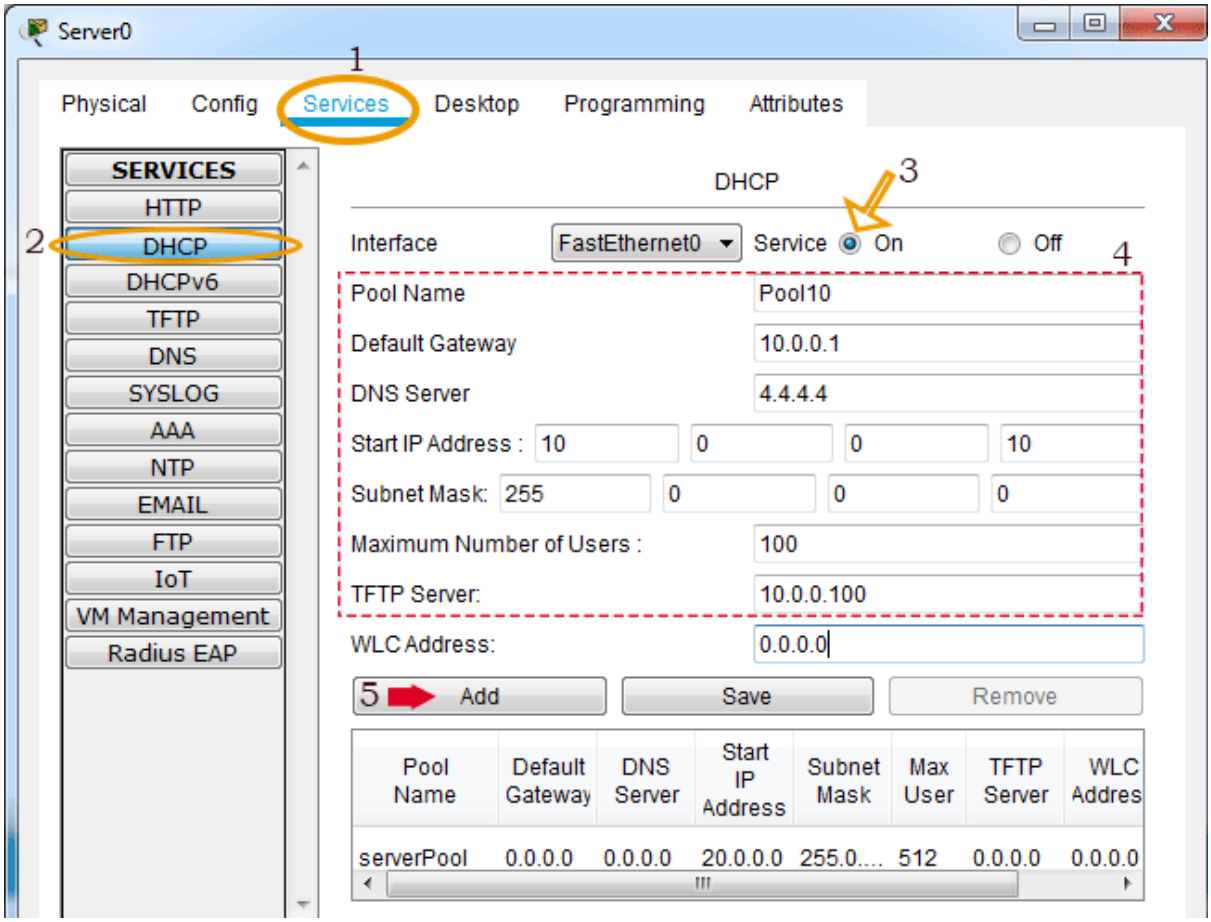
To assign a static IP address to the Server0, click **Server0** and click the **IP configuration** option of the **Desktop** menu. In the IP configuration option, select the **Static** option and set the static configuration.

The following image shows this procedure.



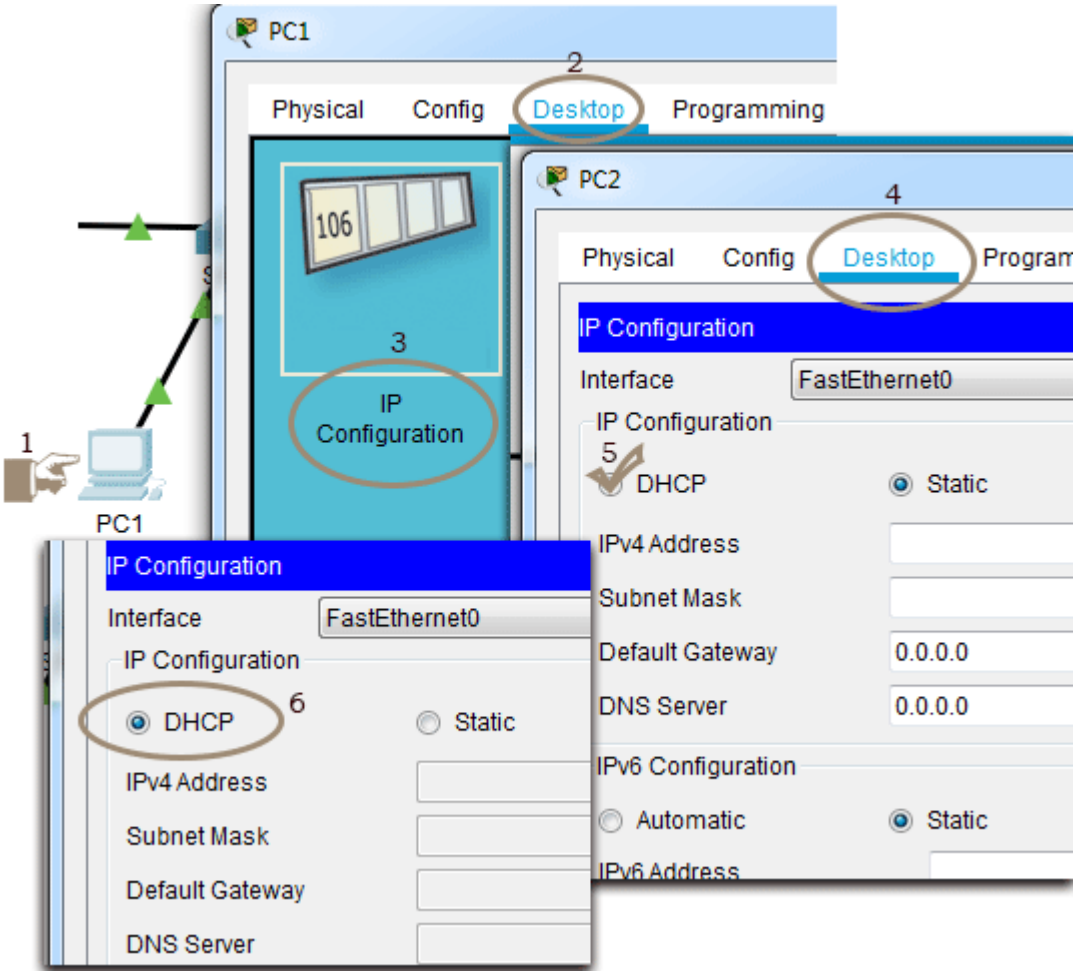
Enabling DHCP service and adding a DHCP pool

Click the **Services** menu icon and click the **DHCP Service** in the left pane and select the **on** option in the right pane. Set the value in the DHCP Pool Options and click the **Add** button. The following image shows this procedure.



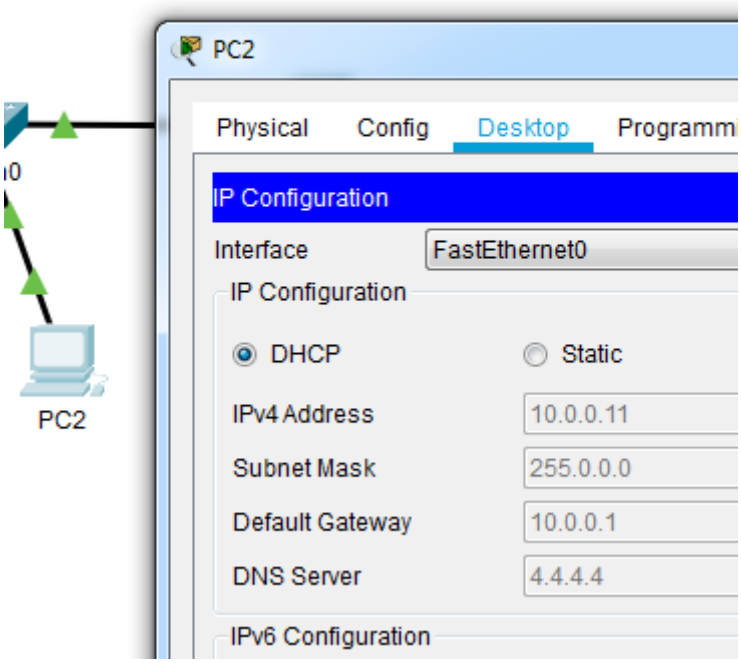
Configure DHCP clients

To configure PCs as DHCP clients, click the **PC** and click the **IP configuration** option from the **Desktop** menu item and select the **DHCP** option. The following image shows this procedure.



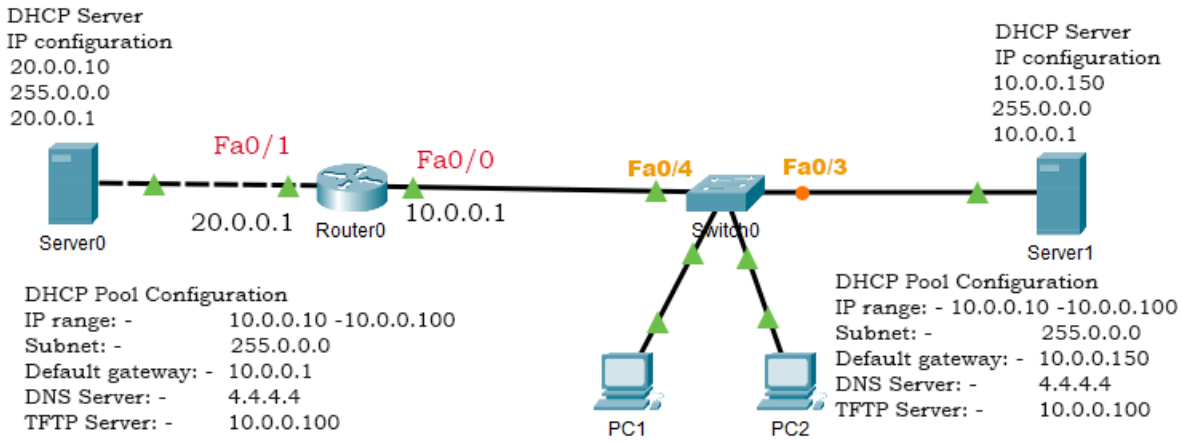
Verifying DHCP Server

If the DHCP server is configured properly, DHCP clients get IP addresses automatically as soon as they change their IP configuration to DHCP. The following image shows the IP configuration of the PC2 that it gets from the DHCP server.

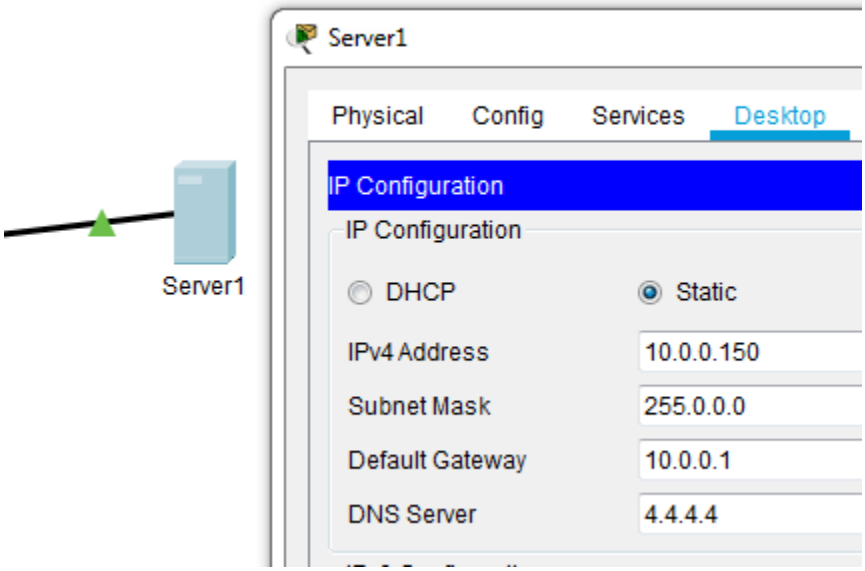


Adding the attacker's DHCP server

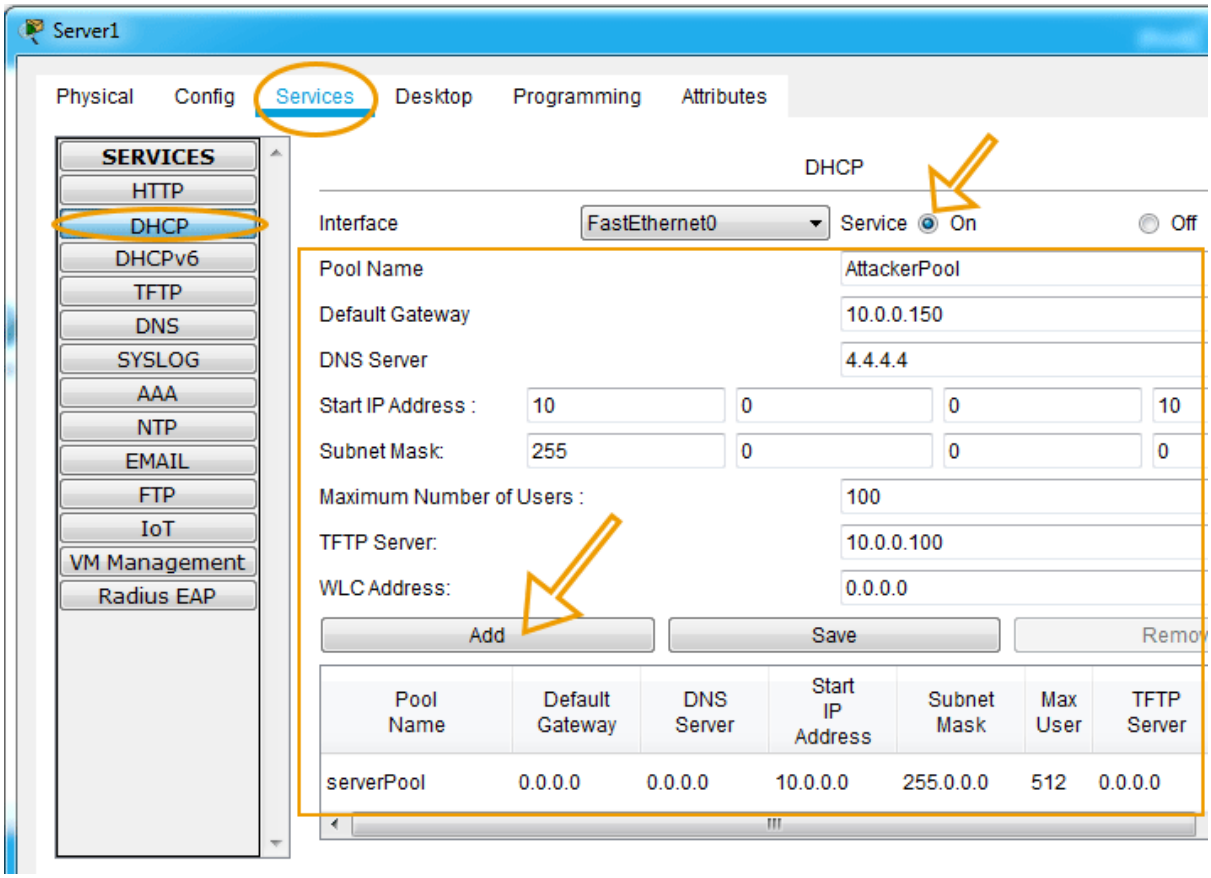
To understand how DHCP snooping protects the network from a rogue DHCP server, let's add an attacker's DHCP server to our network. The following image shows our example network after adding the attacker's DHCP server.



The following image shows the static IP configuration of the attacker DHCP server.



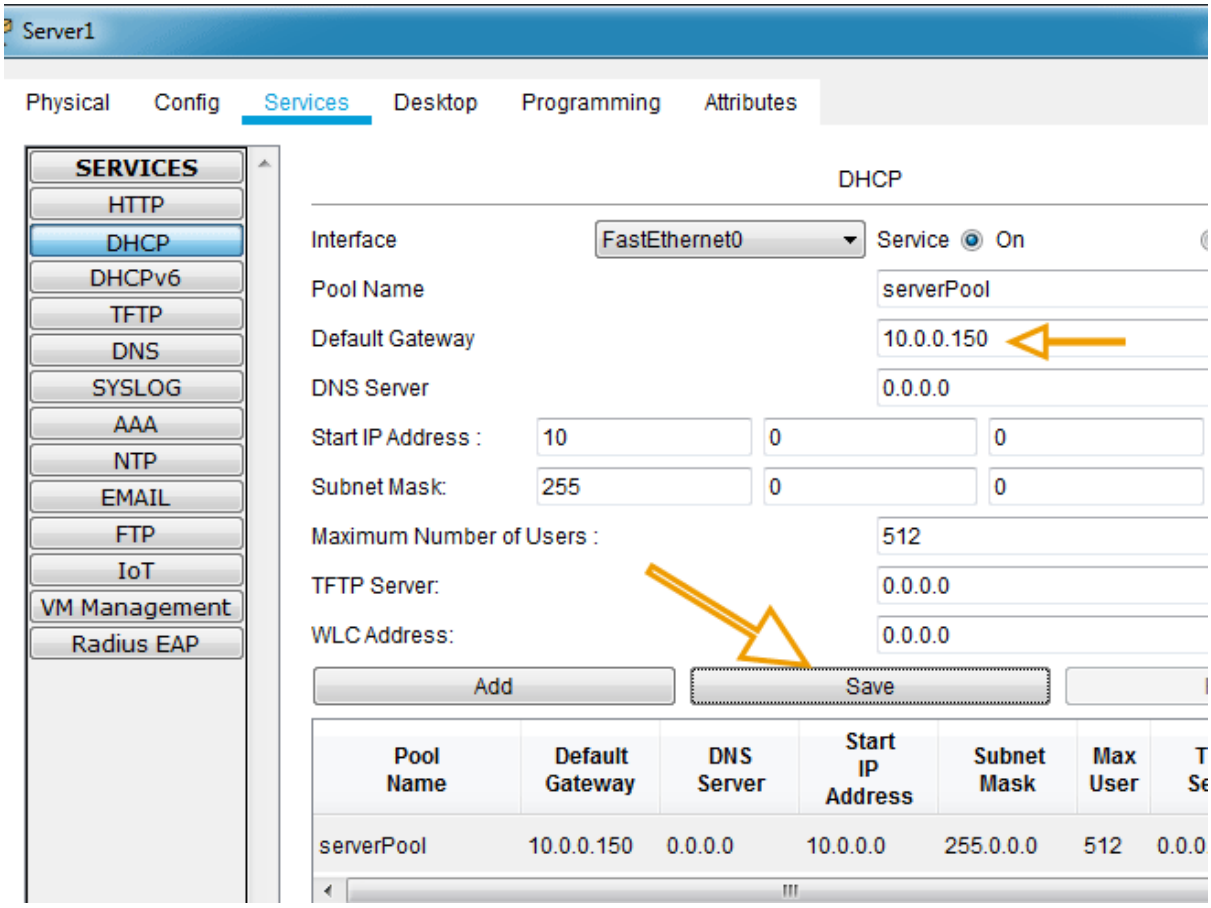
Add a DHCP pool that replicates the DHCP pool of the original DHCP server. In this pool, change the default gateway IP to the IP address that you assigned to this server. The following image shows how to do this.



By default, the server contains a default pool and the packet tracer does not allow us to delete it. If multiple pools are configured, DHCP uses the source address to determine the correct pool. Since DHCP clients use the 0.0.0.0

address as the source address and the default pool also uses this address as the default gateway and DNS server addresses, DHCP provides the IP configuration from the default pool instead of our pool. To force DHCP to use our pool, change the default gateway IP to the IP address of the server in the default pool.

The following image shows this step.

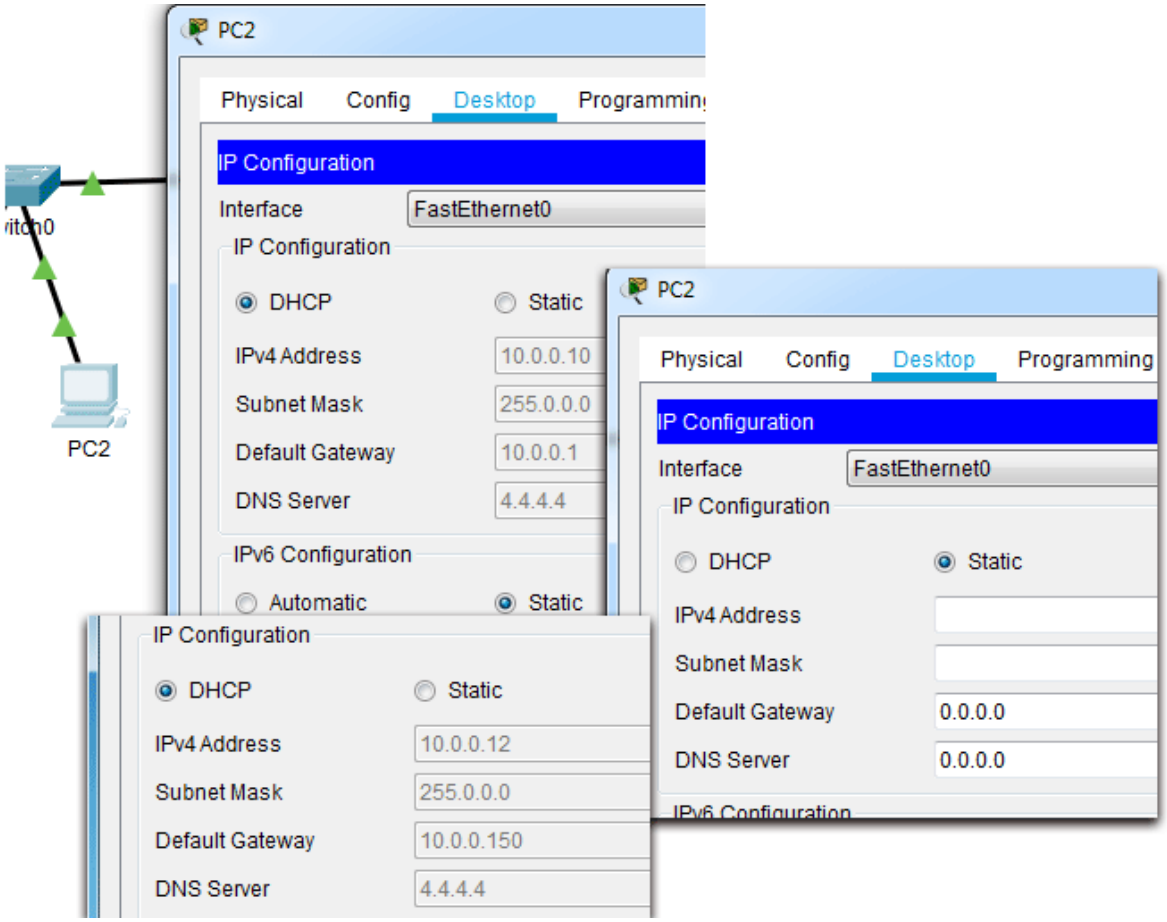


Verifying attacker's DHCP server

The attacker's DHCP server is available in the local network. It receives DHCP requests from clients before the original DHCP server. Since the attacker's DHCP server receives the request first, it also reacts first and the client gets an IP configuration from the attacker's DHCP server.

To verify this, click a PC from the local network and change its IP configuration to **Static** and back to **DHCP**.

The following image shows how PC2 obtains a new IP configuration from the attacker's DHCP server instead of the original DHCP server upon requesting a new IP configuration.



If DHCP clients use the IP configuration provided by the attacker's DHCP server, the attacker can misuse their data without knowing them. This is known as the **man-in-middle** attack.

To learn this attack in more detail, please check the previous part of this tutorial. The previous part of this tutorial explains the man-in-middle attack in detail with an example.

Configuring DHCP snooping on the switch

Configuring DHCP snooping on the switch involves the following steps.

- By default, DHCP snooping is disabled on Cisco switches. To use this feature, first, we have to enable it.
- DHCP snooping works a per-VLAN basic. Once DHCP snooping is enabled, we have to specify the VLAN on which we want to apply this. You can specify a single VLAN or multiple VLANs. To configure a single VLAN, enter a single VLAN number. To configure a range of VLANs, enter a beginning and an ending VLAN number or a dash and range of VLANs.

- DHCP snooping treats all ports of the specified VLAN as the untrusted ports. An untrusted port is a port that does not accept DHCP server messages. In other words, if a device is connected to an untrusted port, it can obtain IP configuration from the DHCP server but it cannot offer an IP configuration.
- If a DHCP server is connected to the port, we have to configure that port as the trusted port. A trusted port is a port that accepts DHCP server messages. In other words, a DHCP server can provide IP configuration only if it is connected to a trusted port.

The following table lists the commands that are used to configure and verify DHCP snooping on Cisco switches.

Command	**Description**
Switch(config)# ip dhcp snooping	To enable DHCP snooping globally.
Switch(config)# ip dhcp snooping vlan number [*number*]	To enable DHCP snooping on the specified VLAN.
Switch(config-if)# ip dhcp snooping trust	To configure the interface as a trusted interface.
Switch(config-if)# ip dhcp snooping limit rate [*rate*]	To limit the number of DHCP packets that the interface can receive in a second.
Switch# show ip dhcp snooping	To view DHCP snooping configuration and status
Switch# debug ip dhcp snooping event	To debug DHCP snooping events.
Switch# debug ip dhcp snooping packet	To view DHCP messages and packets.

The following commands configure DHCP snooping on the switch of our example network.

Switch>enable

Switch#configure terminal

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 1

Switch(config)#interface fa0/4

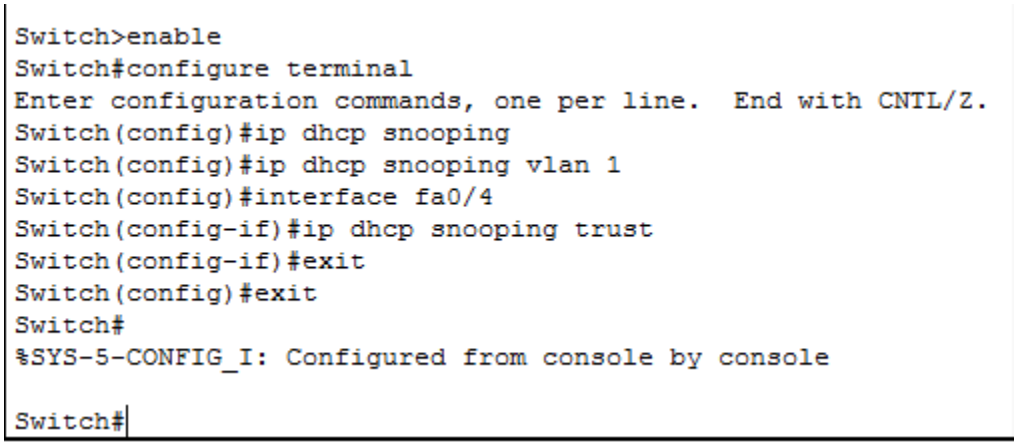
Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#exit

Switch(config)#exit

Switch#

The following image shows the above commands on the packet tracer.



Let's understand the above configuration in detail.

We used the first and second commands to enter global configuration mode. We used the third command to enable the DHCP snooping.

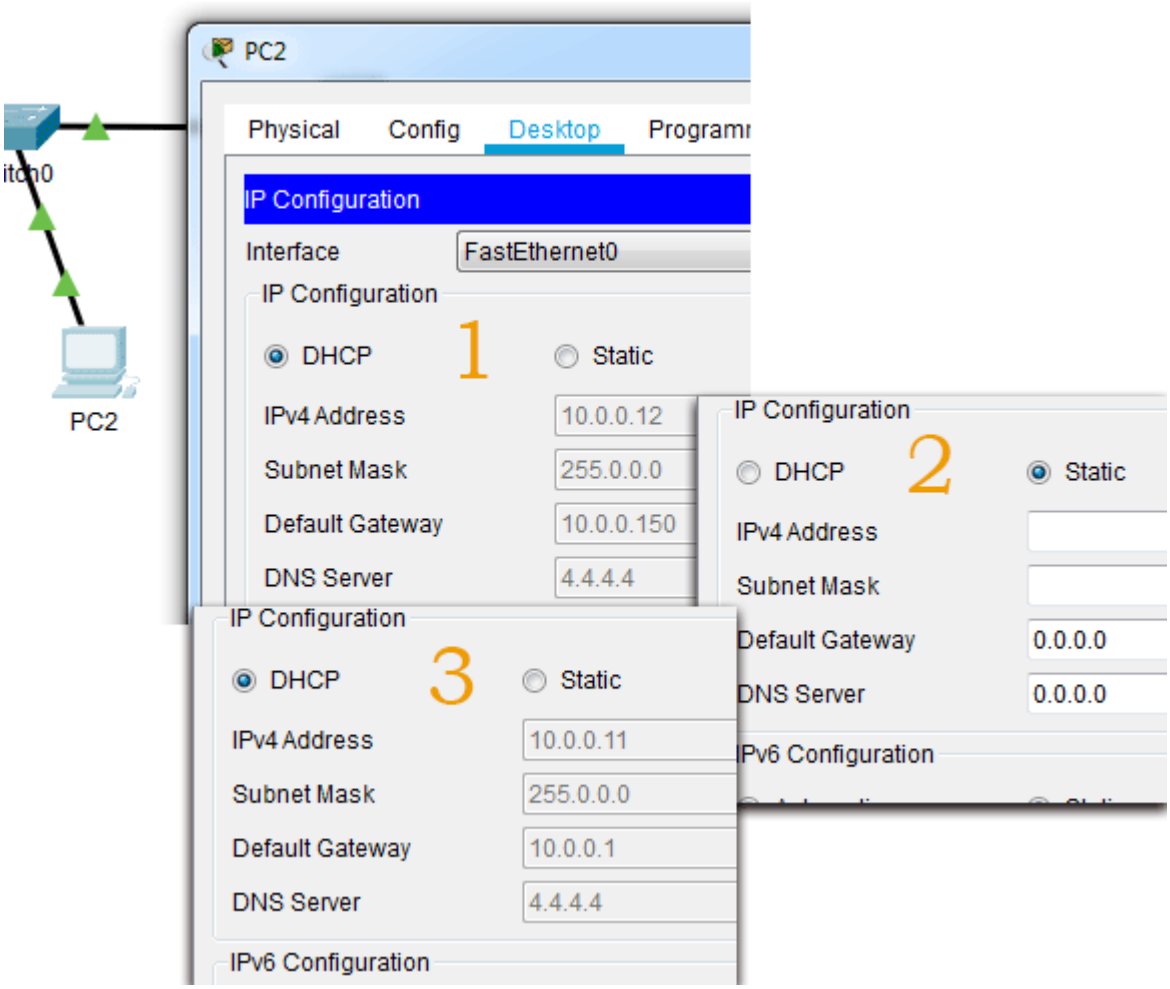
VLAN 1 is the default VLAN on Cisco switches. By default, all ports belong to this VLAN. Since DHCP snooping works on VLANs and we did not create any VLAN in our example, we implemented DHCP snooping on the default VLAN using the fourth command.

In our example, the original DHCP is connected to the interface **Fa0/4**. We used the fifth command to enter the interface configuration mode of the **Fa0/4** interface. In interface configuration mode, we used the sixth command to configure the interface as the trusted interface.

We used the last command to exit interface configuration mode.

Once DHCP snooping is enabled, only the DHCP server that is connected to the trusted interface can provide IP configuration. To verify this, let's obtain a new IP configuration on a PC of the local network.

The following image shows how PC2 obtains a new IP configuration from the original DHCP server.



Viewing DHCP snooping configuration

To view DHCP snooping configuration and statistics, use the '**show ip dhcp snooping**' command in privileged-exec mode.

The following image shows the output of this command.

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/2            no         unlimited
FastEthernet0/3            no         unlimited
FastEthernet0/4            yes        unlimited
Switch#
```

DHCP rate limit

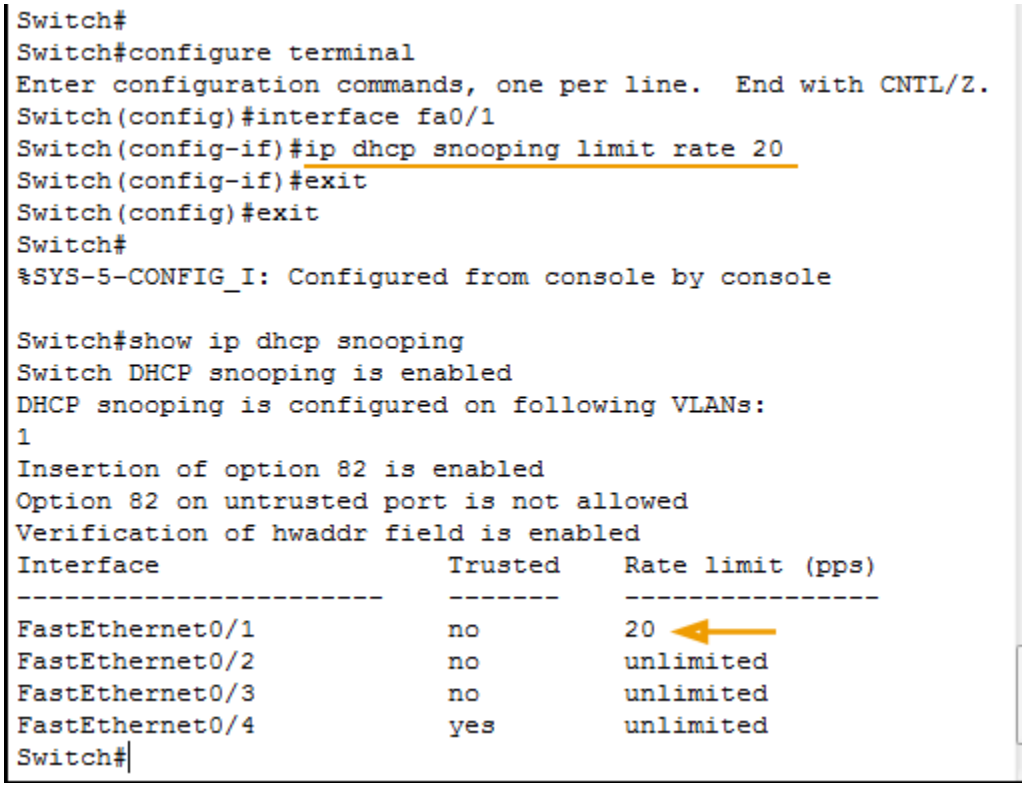
By default, DHCP snooping does not limit the number of DHCP packets that an interface can receive. Since untrusted interfaces connect to DHCP clients, to

enhance the security you can limit the number of DHCP packets on these interfaces.

The recommended rate limit for each untrusted port is 15 packets per second. Generally, the rate limit is applied to untrusted interfaces. But if required, you can also configure it on a trusted interface.

To configure DHCP snooping rate limit on an interface, use the **'ip dhcp snooping limit rate [number]'** command in interface configuration mode of the interface.

The following image shows how to set the rate limit on the Fa0/1 interface and verifies the same.

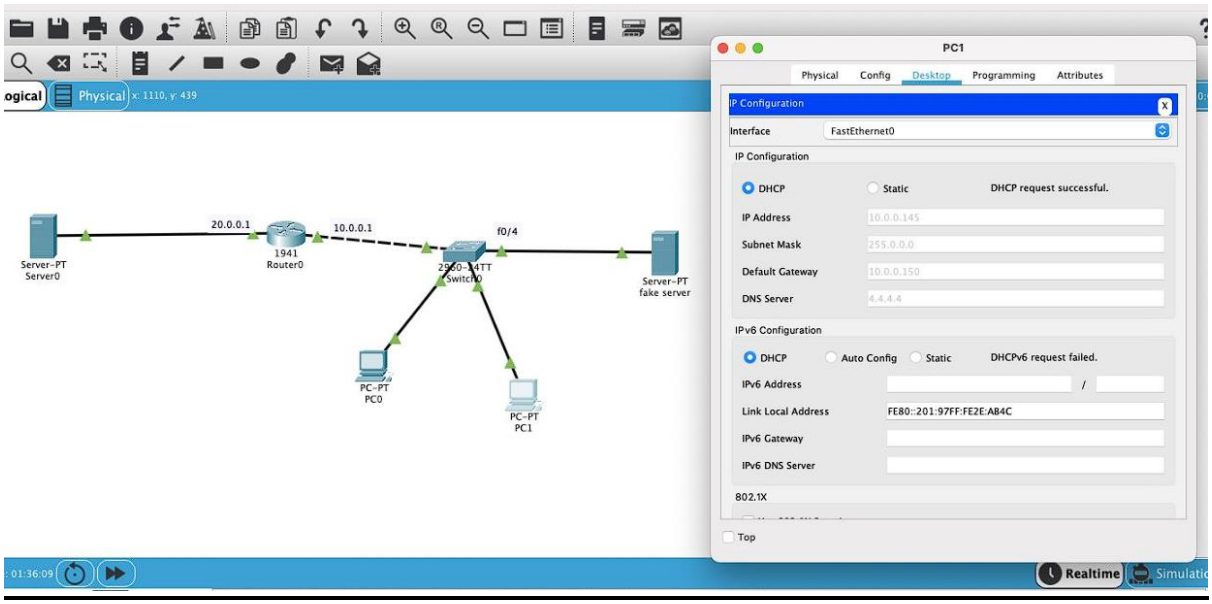


Debugging DHCP snooping

To debug DHCP snooping events and packets, use the **'debug ip dhcp snooping event'** and **'debug ip dhcp snooping packet'** commands in privileged-exec mode. To disable debugging, use the keyword **'no'** before the same commands.

The following image shows how to enable and disable the debugging of DHCP snooping.

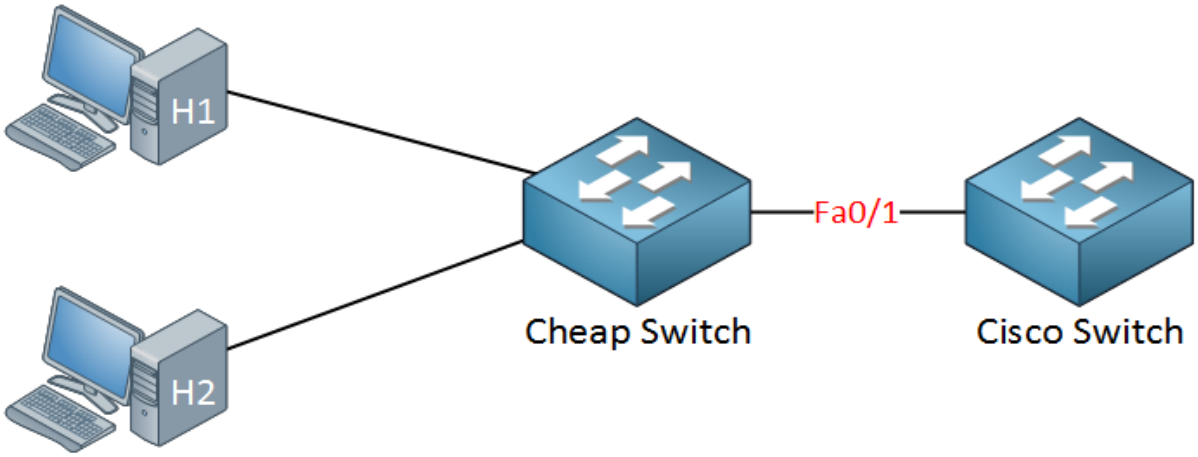
```
Switch#debug ip dhcp snooping event
Switch#debug ip dhcp snooping packet
Switch#00:31:47: DHCP_SNOOPING: received new DHCP packet from input interface
(FastEthernet0/2)
00:31:47: DHCP_SNOOPING: process new DHCP packet, message type: DHCP REQUEST, input
interface: Fa0/2, MAC da: FFFF.FFFF.FFFF, MAC sa: 0006.2A9D.D077, IP da: 255.255.255.255, IP
sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.0.0.10, DHCP siaddr: 20.0.0.10, DHCP
giaddr: 10.0.0.1, DHCP chaddr: 0006.2A9D.D077
00:31:47: %DHCP_SNOOPING: add binding on port FastEthernet0/2
00:31:47: DHCP_SNOOPING: add relay information option.
00:31:47: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
00:31:47: DHCP_SNOOPING: binary dump of relay info option, length: 20  data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x0 0x2 0x2 0x8 0x0 0x6 0x00 0x09 0x7C 0x75 0x22 0x45
00:31:47: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/2
00:31:47: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/3)
00:31:47: DHCP_SNOOPING: process new DHCP packet, message type: DHCP ACK, input interface:
Fa0/3, MAC da: FFFF.FFFF.FFFF, MAC sa: 0030.F296.C6C2, IP da: 255.255.255.255, IP sa:
10.0.0.150, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.0.0.10, DHCP siaddr: 10.0.0.150, DHCP
giaddr: 10.0.0.150, DHCP chaddr: 0006.2A9D.D077
00:31:47: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/4)
00:31:47: DHCP_SNOOPING: process new DHCP packet, message type: DHCP ACK, input interface:
Fa0/4, MAC da: FFFF.FFFF.FFFF, MAC sa: 000A.4182.2501, IP da: 255.255.255.255, IP sa:
10.0.0.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.0.0.10, DHCP siaddr: 20.0.0.10, DHCP giaddr:
10.0.0.1, DHCP chaddr: 0006.2A9D.D077
00:31:47: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/4

Switch#no debug ip dhcp snooping event
Switch#no debug ip dhcp snooping packet
Switch#
```



Experiment-4

Objective: How to configure port-security on Cisco Switch

By default there is no limit to the number of MAC addresses a switch can learn on an interface and all MAC addresses are allowed. If we want we can change this behavior with **port-security**. Let's take a look at the following situation:



In the topology above someone connected a cheap (unmanaged) switch that they brought from home to the FastEthernet 0/1 interface of our Cisco switch. Sometimes people like to bring an extra switch from home to the office. As a result our Cisco switch will learn the MAC address of H1 and H2 on its FastEthernet 0/1 interface.

Of course we don't want people to bring their own switches and connect it to our network so we want to prevent this from happening. This is how we can do it:

Switch(config)#**interface fa0/1**

Switch(config-if)#**switchport port-security**

Switch(config-if)#**switchport port-security maximum 1**

Use the **switchport port-security** command to enable port-security. I have configured port-security so only one MAC address is allowed. Once the switch sees another MAC address on the interface it will be in **violation** and something will happen. I'll show you what happens in a bit…

Besides setting a maximum on the number of MAC addresses we can also use port security to **filter** MAC addresses. You can use this to only allow certain MAC addresses. In the example above I configured port security so it only

allows MAC address aaaa.bbbb.cccc. This is not the MAC address of my computer so it's perfect to demonstrate a violation.

Switch(config)#**interface fa0/1**

Switch(config-if)#**switchport port-security mac-address aaaa.bbbb.cccc**

Use the **switchport port-security mac-address** command to define the MAC address that you want to allow. Now we'll generate some traffic to cause a violation:

C:\Documents and Settings\H1>**ping 1.2.3.4**

I'm pinging to some bogus IP address…there is nothing that has IP address 1.2.3.4; I just want to generate some traffic. Here's what you will see:

SwitchA#

%PM-4-ERR_DISABLE: **psecure-violation error detected on Fa0/1**, putting Fa0/1 in **err-disable state**

%PORT_SECURITY-2-PSECURE_VIOLATION: **Security violation occurred, caused by MAC address 0090.cc0e.5023 on port FastEthernet0/1.**

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

We have a security violation and as a result the port goes in **err-disable state**. As you can see it is now down. Let's take a closer look at port-security:

Switch#**show port-security interface fa0/1**

Port Security : Enabled

Port Status : Secure-shutdown

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 1

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0090.cc0e.5023:1

Security Violation Count : 1

Here is a useful command to check your port security configuration. Use **show port-security interface** to see the port security details per interface. You can see the violation mode is shutdown and that the last violation was caused by MAC address 0090.cc0e.5023 (H1).

Switch#**show interfaces fa0/1**

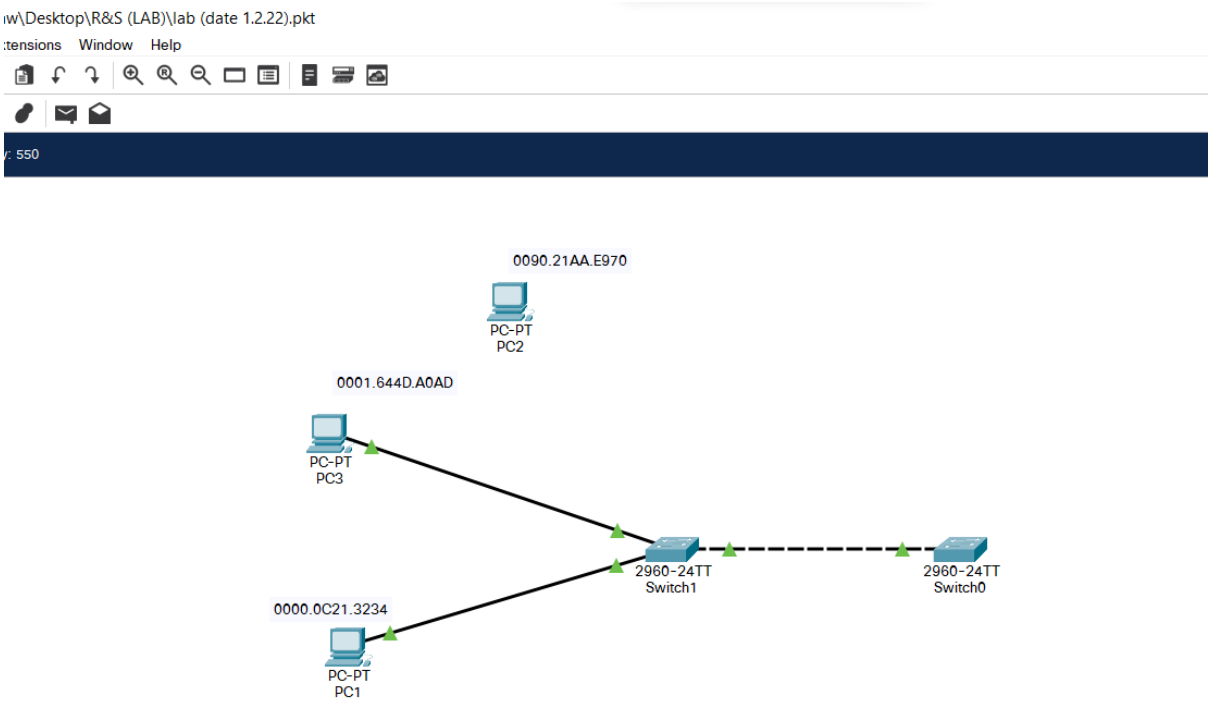
FastEthernet0/1 is down, line protocol is down (err-disabled)

Shutting the interface after a security violation is a good idea (security-wise) but the problem is that the interface will **stay in err-disable state**. This probably means another call to the helpdesk and *you* bringing the interface back to the land of the living! Let's activate it again:

Switch(config)#**interface fa0/1**

Switch(config-if)#**shutdown**

Switch(config-if)#**no shutdown**



Experiment-5

Objective:

1. To create a basic switch configuration and verify it

2. To create 2 VLANS

3. Name the VLANS and assign multiple ports to them.

4. Connect 2 connections between Switch 1 and Switch 2 for each VLAN 5. Understand why it is not possible to delete VLAN1.

Step1: Display the VLAN interface information: Swach1>enable

Switch1# show VLAN

Troubleshoot Configuration

PC1 C ping 15.0.0.12

Sucessfuly Ping

PC1 C ping 15.0.0.11 Sucessfuly Ping

PC1 C/>ping 15.0.0.13 Sucessfuly Ping

Step 2 Create and name two VLANS:

Switch1>enable

Switch 1# configuration terminal.

Swach1(config)# vian 2

Switch(config-vian)#name VLANZ Switch1(config-vian)#ext

Switch1(config)#vian 3

Switch1(config-vian)#name VLAN3 Switch1(config-vian)#ext

Step 3 Assign ports to VLANs on both the switch

Switch 1#configure terminal

Switch(config)#interface fastEthernet 0/2

Switch 1(config-if)#switchport mode access

Switch1(config-if)#switchport access vian 3

Switch 1(config-if)#exit

Switch1(config)#interface fastEthernet 0/1

Switch1(config-if)#switchport mode access

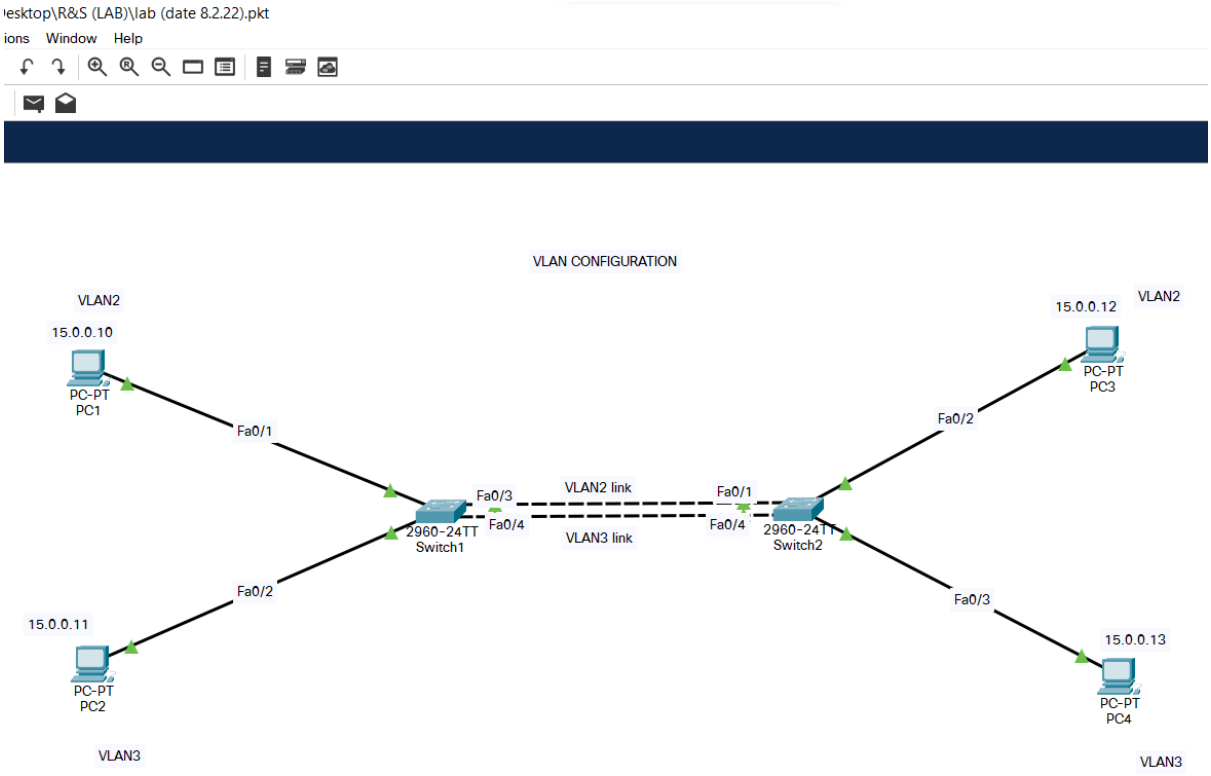
Switch1(config-if)#switchport access vian 2

Questions:

Is PC1 to PC4 access is possible?

Is PC1 to PC3 access is possible?

Is PC1 to PC2 access is possible?



Experiment-6

Objective: Router on a stick or inter-VLAN routing configuration

Router on a stick configuration on Packet Tracer

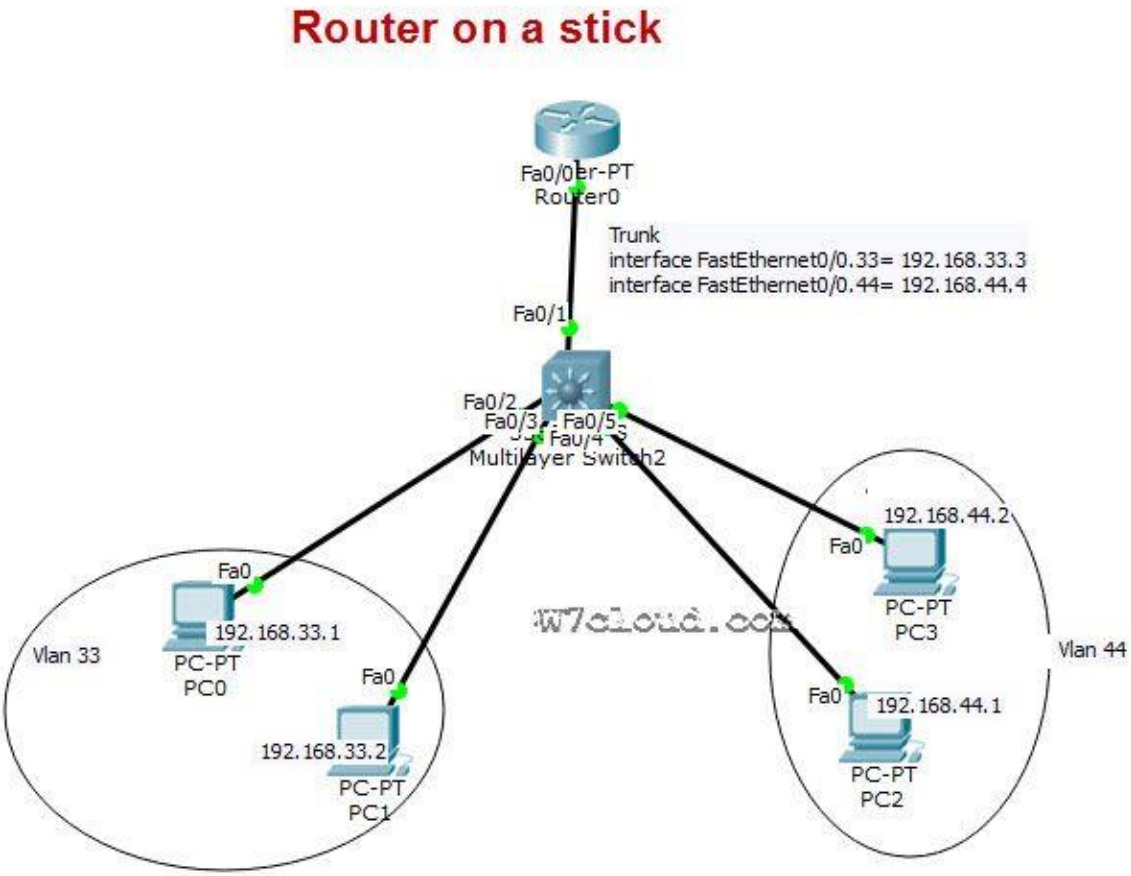
By default the nodes associated to same vlans can communicate with each other in switching environment. You require a router if you want to interconnect VLANs with each other. In this lesson I will show you how you can use a router connecting different Vlans with each other with single switch & this is known as “router on a stick” or “inter-vlan routing”.

For inter clan routing you are required to create the **sub-interfaces** for each vlan on a router. We can configure an IP address on each sub-interface in order to make communication possible between different Vlans.

For this lab you will need:

- 2 Subnets (VLANs)
    - VLAN 33 – 192.168.33.0/24
    - VLAN 44 – 192.168.44.0/24
- 1 Routers
- 1 switch
- 4 PC/Host

Design the lab according to following figure and we have four PC/host PC0 & PC1 are belongs to vlan 33 and PC2 & PC3 are belong to vlan 44. Configure the each device according to following configuration.



Switch configuration:

Four ports are required to be configured as access ports because these ports are connected with the PCs. We will assign the vlan 33 to port2 and port3 as it is in vlan 33, while other ports will be assign with vlan 44.

Switch(config)#interface range fastEthernet 0/2 – 3

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 33

% Access VLAN does not exist. Creating vlan 33

Above Command will create the vlan 33 automatically on switch.

Switch(config-if-range)#exit

Switch(config)#interface range fastEthernet 0/4 – 5

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 44

% Access VLAN does not exist. Creating vlan 44

Switch(config-if-range)#exit

Switch(config)#exit

There are five ports of switch which are involve in this lab, port fastEthernet 0/1 is connected to swich therefore we configure this port as trunk with encapsulation dot1q for inter-vlan routing. Host ports associated with the proper VLANs, we now need to allow this VLAN traffic to be brought up to the router to be "routed". We will accomplish this by setting up a link called a trunk. A trunk will allow for multiple VLANs to traverse the connection to the other device so that it can be processed.

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#**switchport trunk encapsulation dot1q**

Switch(config-if)#**switchport mode trunk**

Switch(config-if)#exit

We will also set the layer 2 trunking encapsulation type, there are 2 for these switches, ISL (Cisco) and

Dot1Q, Dot1Q being an open standard. We will use Dot1Q. Use the "**switchport mode trunk**" and "switchport trunk" commands to accomplish this task.

Router configuration:

We will need to configure our router to accept frames over our trunk for both VLANs 33 and 44. Identify the interface on the router you used for the trunk to the switch. The first command you should do is a no shutdown and then you need to use "'Sub-Interfaces" in order to use one physical interface to represent two virtual interfaces. we will create two sub interfaces in this lab i.e. interface fastEthernet 0/0.33 & interface fastEthernet 0/0.44

Router>enable

Router#conf t

Router(config)#interface f0/0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0.33

Router(config-subif)#ip address 192.168.33.3 255.255.255.0

Router(config-subif)#encapsulation dot1Q 33

Router(config-subif)#no shut

Router(config-subif)#exit

Router(config)#interface fastEthernet 0/0.44

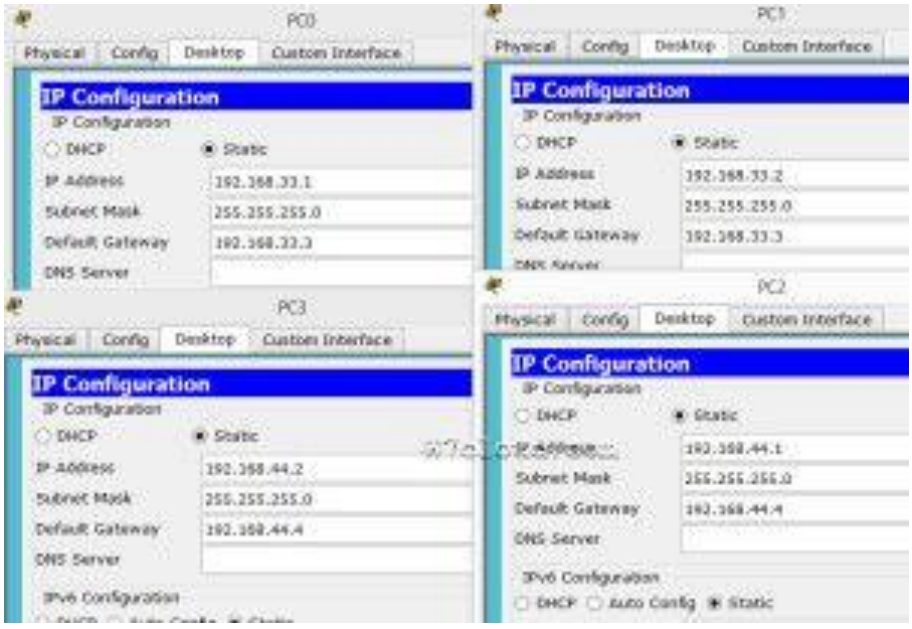
Router(config-subif)#ip address 192.168.44.4 255.255.255.0

Router(config-subif)#no shu

Router(config-subif)#encapsulation dot1Q 44

PC or Host configurations:

Assign the IPs as per diagram and set the default **gateway IP address** for hosts. For vlan 33 hosts have the gatway 192.168.33.3 because we have configured a sub interhace on router for this vlan with IP 192.168.33.3 and 192.168.33.4 will be gateway for vlan 44. See the following figure to verifying this configurations:



Lab connectivity verification:

Once you have done the above configurations you can now begin the process of verifying our configurations. Let’s check our hosts. First, ping their gateway to see if they can reach the router and then ping the PC3 from PC0 or PC1. In case of correct configuration this ping will be successful.