SHAHEED ZULFIKAR ALI BHUTTO
INSTITUTE OF SCIENCE AND TECHNOLOGY

Computer Networks and Data Communication

Laboratory Manual

CSCL-3205

Semester 6th
Spring-2023

Student’s Name: ____

Roll Number: ____

Lab Instructor: ***Engr. Ashar Tariq***

Department of Computing Sciences
Shaheed Zulfiqar Ali Bhutto Institute Of Science And Technology, Karachi,Pakistan
Tel:(021)111-922-478, Fax: (021)35830446, Email: info@szabist.edu.pk

Introduction

This laboratory course operates in co-ordination with the companion lecture course, CSC 3205, Computer Networks and Data Communications. This laboratory course presents 15 laboratory experiments on Computer Networks world. They provide hands on experience to the students on Interconnecting the Cisco Networks and Devices. Also over routing and switching essentials and techniques.

LAB OBJECTIVES

Upon successful completion of this Lab course, the student should be able to:

- Understand and explain Data Communications System and its components.
- Build an understanding of the fundamental concepts of computer networking.
- Identify the different types of network devices and their functions within a network
- Familiarize the student with the basic taxonomy and terminology of the computer networking area.
- Familiarity with the basic protocols of computer networks, and how they can be used to assist in network design and implementation.
- Independently understand basic computer network technology.
- Identify the different types of network topologies and protocols.
- Enumerate the layers of the OSI model and TCP/IP. Explain the function(s) of each layer.
- Understand and building the skills of subnetting and routing mechanisms.
- Introduce the student to advanced networking concepts, preparing the student for entry Advanced courses in computer networking.
- Allow the student to gain expertise in some specific areas of networking such as the design and maintenance of individual networks.

LIST OF EXPERIMENTS

SUBJECT: CSCL-3205 Lab: Computer Networks and Data Communications (BCS/BS)
Marks Evaluation Sheet

Sr. No.	Topics	Marks/Grade	Date Performed	Date Checked	Examiner Initial's
1	Introduction and network trouble shooting tools.				
2	Introduction to Cisco IOS. establishing console session Basic router configuration				
3	establishing remote session with cisco IOS Basic switch configuration				
4	Static IP Addressing				
5	DHCPv4				
6	VLANs, Trunking and VTP				
7	Security Features on switch (Switch Port Security)				
8	Inter VLAN routing (router on a Stick)				
9	static, default routes and VLSM				
10	OSPF				
11	EIGRP				
12	ACL (Standard)				
13	ACL (Extended)				
14	NAT				

Remarks			
Finalized Marks		Examiner Initial's	

Guidelines to Students

- Students must thoroughly read the assigned work. It will be assumed that they have studied the assigned work and have understood the majority of the material and technical terms before the start of the experiments.
- For safety reasons, students are requested not to leave their equipment unattended during the laboratory session. In the case of special circumstances, please seek the support of the class teachers/demonstrators.
- All practical contribute to the final results of the sessional course. Thus any absent laboratory session automatically means lost marks for the final grade. Under special circumstances (supported by documentary proof), e.g. illness and other reasonable causes a laboratory session may be re-scheduled upon approval of the head of the department.
- During the class, students will be continuously assessed by performance test on each and every experiment.
- To ensure your fellow students can proceed with their experiments in a degree of comfort and without undue noise and other disturbances, keep the noise level down and stay in your own laboratory bench area. Mobile phones should be switched off during the experiments.
- Equipment in the laboratory for the use of student community. Students need to maintain a proper decorum in the electronics and computer laboratories. Student must use the equipment with care. In case of any damage, students should be pay for it.
- Students are required to carry their report sheet, observation books or laboratory exercise manuals with complete exercises while entering the laboratory.
- CD burns with all Simulink task files and attach at the end of this manual.
- Laboratory records needs to be submitted on or before date of submission.

SHAHEED ZULFIKAR ALI BHUTTO
INSTITUTE OF SCIENCE AND TECHNOLOGY

Experiment#01

Introduction to Computer Networks and Windows Network Troubleshooting Tools

Part #1: Objectives:

- Introduction to Computer networks.
- Describe the functions and physical characteristics of the network device.
- Describe the functions and physical characteristics of the media.

Background / Scenario:

A computer network is a group of computer systems and other devices that are linked together through communication channels or media to facilitate communication and resource-sharing among a wide range of users.

Components of a computer network:

There are three categories of network components:

1. Devices
    - End devices (computer, printer, security cameras, etc.)
    - Intermediary devices (router, switch, hub, firewalls)
2. Media
    - Wired
        - Cooper (UTP, STP)
        - Fiber optic (multimode fiber , single mode fiber)
    - Wireless
3. Services

As a member of the networking support staff, you must be able to identify different networking equipment. You must also understand the function of equipment in the appropriate part of the network. In this lab, you will have access to network devices and media. You will identify the type and characteristics of the network equipment and media.

Identify Network Devices

Fill in the table below with the device tag ID number, manufacturer, device model, type (hub, switch, and router), functionality (wireless, router, switch, or combination), and other physical characteristics, such as number of interface types. The first line is filled out as a reference.

ID	Manufacturer	Model	Type	Functionality	Physical Characteristics
1	Cisco	1941	Router	Router	2 GigabitEthernet Ports 2 EHWIC slots 2 CompactFlash slots 1 ISM slot 2 Console ports: USB, RJ-45
2					
3					
4					
5					
6					

Identify Network Media:

You will name the network media, identify the media type (copper, fiber optic, or wireless), and provide a short media description including what device types it connects. Use the table below to record your findings. The first line in the table has been filled out as a reference.

ID	Network Media	Type	Description and to What It Connects
1	UTP	Copper	Connect wired NIC and Ethernet ports on network devices Cat 5 straight-through wired. Connects PCs and routers to switches and wiring panels.
2			
3			
4			
5			
6			

Reflection

After you have identified the network equipment, where would you find more information about the equipment?

____

____

____

____

Part#2: Objective:

- Windows Network Troubleshooting Tools

Back Ground Scenario:

If you call technical support about problems with your network or Internet connection, they will most likely have you use some or all of these utilities. You should check all of the hardware connections as well. Refer to the Network Connections handout for a detailed description of networking connections.

Some Useful Connectivity Utilities :

- **ipconfig – (IP configuration)**

Use ipconfig to find the IP address and configuration of your own computer and network. By default, ipconfig only displays the IP address, subnet mask, and default gateway. For more in depth information, add the text /all after ipconfig. You will be able to view all of the IP configuration information for the computer.

- **ping** – (**p**acket **i**nter**n**et **g**roper**)**

A utility to determine whether a specific IP address is accessible. It works by sending a packet of data to the specified address and waiting for a reply.
If you are having difficulty accessing the Internet, try using the ping command to connect to the different network nodes to narrow down where the problem could be coming from. For instance, if you are able to ping the network card, but not the router, the problem is most likely local. If you can ping everywhere except for a certain outside address, the problem is remote.

Syntax: **ping** ***IP address or domain***

- **tracert – (trace r**out**e)**

A utility that traces a packet from your computer to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. If you're visiting a Web site and pages are appearing slowly, you can use trace route to figure out where the longest delays are occurring.

Syntax: **tracert** ***IP address or domain***

- **nslookup – (n**ame server **lookup)**

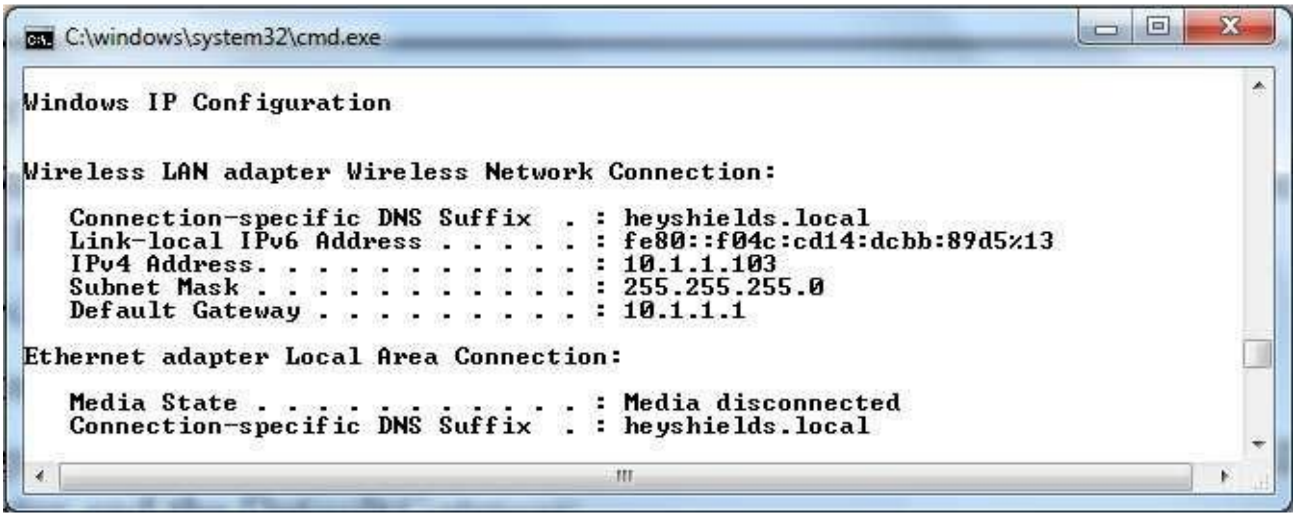
Nslookup is the name of a program that lets an Internet server administrator or user enter a host name (for example, www.yahoo.com) and find out the corresponding Internet address. It will also do reverse name lookup and find the host name for an IP address you specify.
Nslookup sends a domain name query packet to a designated (or defaulted) Domain Name System (DNS) server. Depending on the system you are using, the default may be the local DNS name server at your service provider, some intermediate name server, or the root name server (at InterNIC) for the entire domain name system hierarchy.

Syntax: **nslookup** ***IP address or domain***

Using Ipconfig:

1. Log on to the computer as a user with administrative rights.
2. Click **Start** and select **Run** (Windows Vista or Windows 7 Click the “Start” button and type in the “Search for Programs and Files” text box).
3. Type **cmd** and press ENTER. The black Command Prompt window will appear.

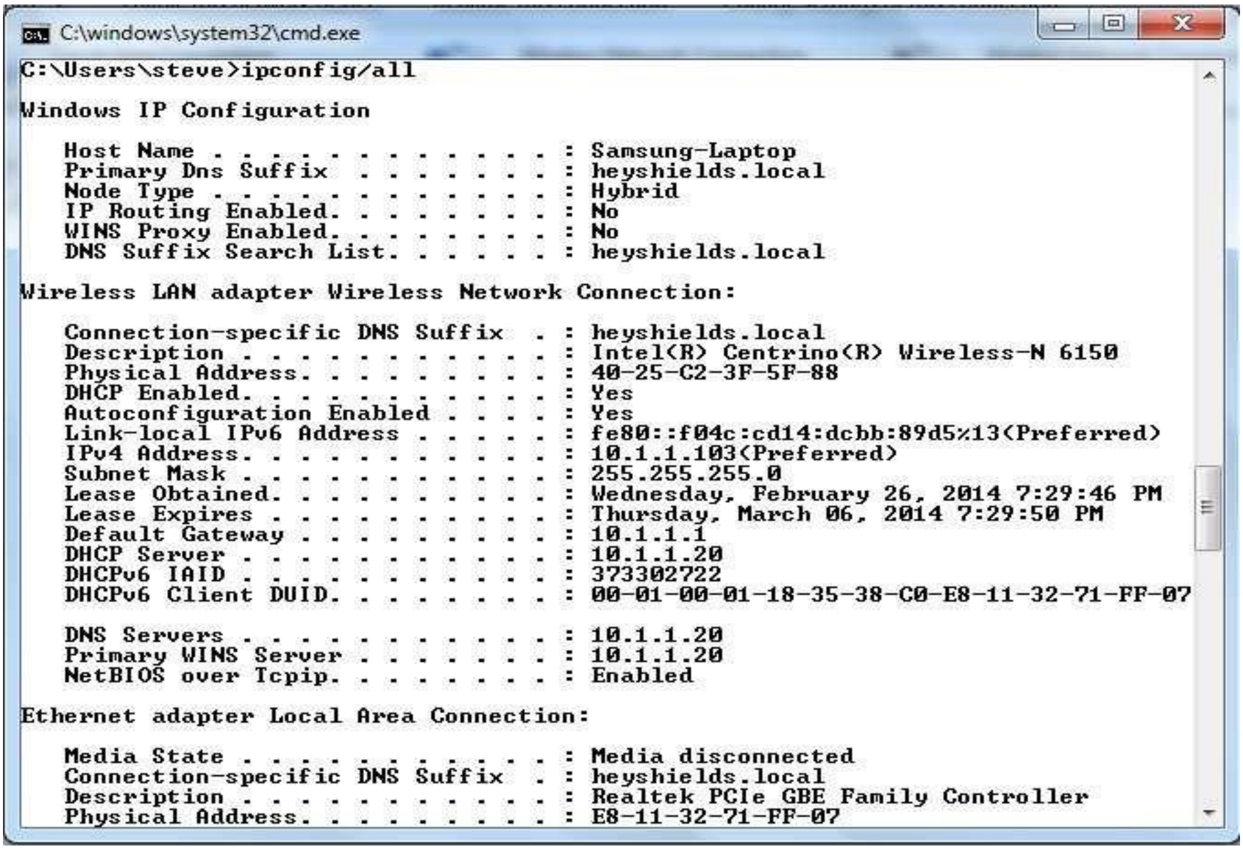
4. Type **ipconfig** at the command prompt and press ENTER. The following screenshot gives an example of the information shown when using “ipconfig”.



```
Windows IP Configuration


Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : heyshields.local
   Link-local IPv6 Address . . . . . : fe80::f04c:cd14:dcbb:89d5%13
   IPv4 Address. . . . . . . . . . . : 10.1.1.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.1.1

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : heyshields.local
```

5. Write down any configuration information you will need. At a minimum, it will be the IP address of your computer and the Default Gateway.

6. Sometimes you might need more information and you can add the “/all” to the above “ipconfig” command. This screenshot gives an example of the information shown when using “ipconfig /all”:

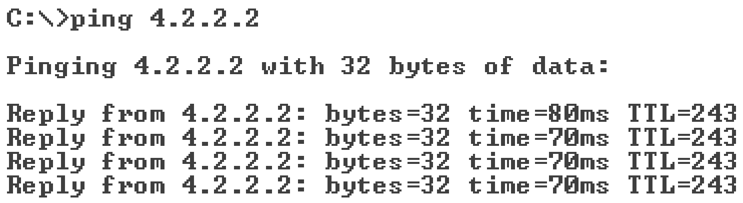


```
C:\Users\steve>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Samsung-Laptop
   Primary Dns Suffix  . . . . . . . : heyshields.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : heyshields.local

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : heyshields.local
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Wireless-N 6150
   Physical Address. . . . . . . . . : 40-25-C2-3F-5F-88
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f04c:cd14:dcbb:89d5%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.1.1.103(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, February 26, 2014 7:29:46 PM
   Lease Expires . . . . . . . . . . : Thursday, March 06, 2014 7:29:50 PM
   Default Gateway . . . . . . . . . : 10.1.1.1
   DHCP Server . . . . . . . . . . . : 10.1.1.20
   DHCPv6 IAID . . . . . . . . . . . : 373302722
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-35-38-C0-E8-11-32-71-FF-07

   DNS Servers . . . . . . . . . . . : 10.1.1.20
   Primary WINS Server . . . . . . . : 10.1.1.20
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : heyshields.local
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : E8-11-32-71-FF-07
```

Using Ping:

1. Log on to the computer as a user with administrative rights.
2. Click **Start** and select **Run** (Windows Vista or Windows 7 Click the “Start” button and type in the “Search for Programs and Files” text box).
3. Type **cmd** and press ENTER. The black Command Prompt window will appear.
4. Type **ping *IP address or domain*** and press ENTER. If you are unable to ping a destination, first check to see that there are no typing errors. If the address is correct, use the Troubleshooting Routing Errors table below to examine what the cause could be.

A successful ping looks similar to this:



```
C:\>ping 4.2.2.2

Pinging 4.2.2.2 with 32 bytes of data:

Reply from 4.2.2.2: bytes=32 time=80ms TTL=243
Reply from 4.2.2.2: bytes=32 time=70ms TTL=243
Reply from 4.2.2.2: bytes=32 time=70ms TTL=243
Reply from 4.2.2.2: bytes=32 time=70ms TTL=243
```

Use any or all of the following address options to determine where the connection is failing.
• **ping the Ethernet card (NIC) in your computer** — this will always be 127.0.0.1
• **ping your own computer** —use ipconfig to look up the IP address, if necessary.
• **ping the Default Gateway (router)** — you can find the Default Gateway on the computer in the same spot as the IP address.
• **ping an outside IP address** — for example the Level3 DNS Server 4.2.2.2.
• **ping a domain name to check DNS** — for example: ping www.google.com.

Troubleshooting Ping Errors

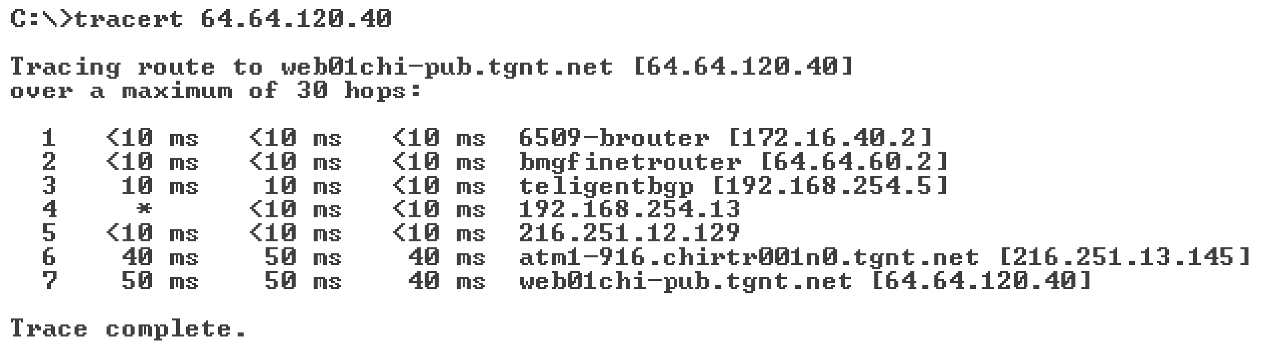
Once all of the hardware connections are checked and verified, any of the following could be the cause of your networking error(s).

Symptom	**Possible Causes**
Unable to ping the NIC.	The NIC is disabled or faulty.
Unable to ping your own computer.	The IP address is incorrect.
Unable to ping the Default Gateway.	The computer is disconnected from the network. The Default Gateway is down. The gateway address used in ping is incorrect. The gateway is not attached to the subnet.
Unable to ping an outside IP address.	The outside server is offline. The IP address was typed incorrectly. A packet is routed incorrectly between the source and destination networks.
Unable to ping a domain name.	The DNS server is not working. The destination server is offline.
Internet connections are slow and or intermittent.	Internet traffic is heavy. There are problems with the line. Contact the phone or cable company.

Using Tracert:

1. Log on to the computer as a user with administrative rights.
2. Click **Start** and select **Run** (Windows Vista or Windows 7 → Click the "Start" button and type in the "Search for Programs and Files" text box).
3. Type **cmd** and press ENTER. The black Command Prompt window will appear.
4. Type **tracert *IP address or domain*** and press ENTER.

The following screenshot shows an example using nslookup.



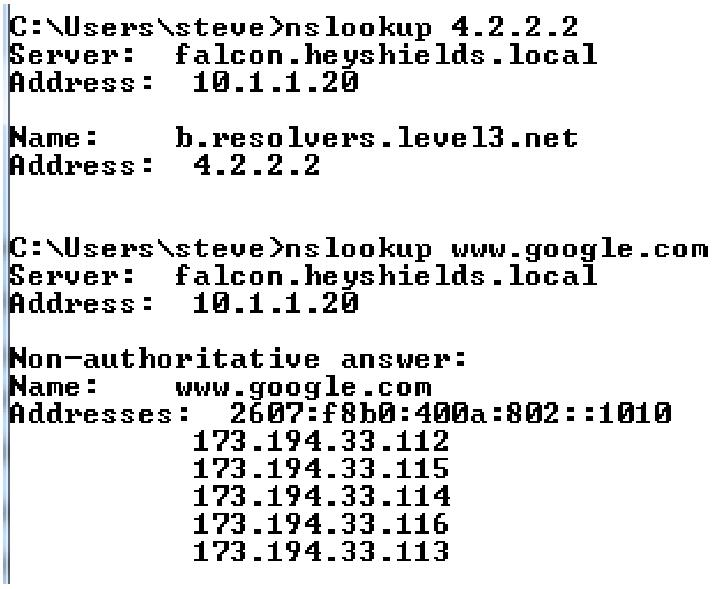
```
C:\>tracert 64.64.120.40

Tracing route to web01chi-pub.tgnt.net [64.64.120.40]
over a maximum of 30 hops:

  1    <10 ms    <10 ms    <10 ms   6509-brouter [172.16.40.2]
  2    <10 ms    <10 ms    <10 ms   bmgfinetrouter [64.64.60.2]
  3     10 ms     10 ms    <10 ms   teligentbgp [192.168.254.5]
  4      *       <10 ms    <10 ms   192.168.254.13
  5    <10 ms    <10 ms    <10 ms   216.251.12.129
  6     40 ms     50 ms     40 ms   atm1-916.chirtr001n0.tgnt.net [216.251.13.145]
  7     50 ms     50 ms     40 ms   web01chi-pub.tgnt.net [64.64.120.40]

Trace complete.
```

Tracert returns results in milliseconds (ms). Ideally, every hop should give an IP address and time. After requesting information from the DNS server, the first hop is to the default gateway. The hop to the default gateway should take 10-20 ms. After that, hops should take anywhere from 80-120ms. Errors indicated by ***** on the route can show where there is a lot of network traffic or possible line problems

Using Nslookup:

1. Log on to the computer as a user with administrative rights.
2. Click **Start** and select **Run** (Windows Vista or Windows 7 □ Click the "Start" button and type in the "Search for Programs and Files" text box).
3. Type **cmd** and press ENTER. The black Command Prompt window will appear.
4. Type **nslookup *IP address or domain*** and press ENTER.

The following screenshot shows two examples using nslookup. The first looks up an IP address (4.2.2.2) while the second looks up a domain name (www.yahoo.com).



```
C:\Users\steve>nslookup 4.2.2.2
Server:  falcon.heyshields.local
Address:  10.1.1.20

Name:    b.resolvers.level3.net
Address:  4.2.2.2


C:\Users\steve>nslookup www.google.com
Server:  falcon.heyshields.local
Address:  10.1.1.20

Non-authoritative answer:
Name:    www.google.com
Addresses:  2607:f8b0:400a:802::1010
          173.194.33.112
          173.194.33.115
          173.194.33.114
          173.194.33.116
          173.194.33.113
```

- **Server:** the local DNS server used to look up the information.
- **Address:** the IP address of the local DNS server.
- **Name:** The domain name of the server hosting the remote domain or IP.
- **Address(s)**: The IP address(s) of the remote server.
- **Aliases:** The common name(s) used to identify multiple IP addresses or domain names.

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

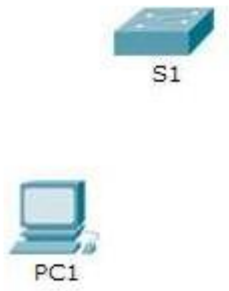
Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#02

Lab# 2.1:- Packet Tracer - Navigating the IOS

Topology



Objectives

Part 1: Basic Connections, Accessing the CLI and Exploring Help

Part 2: Exploring EXEC Modes

Part 3: Setting the Clock

Background

In this activity, you will practice skills necessary for navigating the Cisco IOS, including different user access modes, various configuration modes, and common commands you use on a regular basis. You also practice accessing the context-sensitive Help by configuring the **clock** command.

Part 1: Basic Connections, Accessing the CLI and Exploring Help

In Part 1 of this activity, you connect a PC to a switch using a console connection and explore various command modes and Help features.

Step 1: Connect PC1 to S1 using a console cable.

a. Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.

b. Select the light blue Console cable by clicking it. The mouse pointer will change to what appears to be a connector with a cable dangling off of it.

c. Click **PC1**; a window displays an option for an RS-232 connection.

d. Drag the other end of the console connection to the S1 switch and click the switch to bring up the connection list.

e. Select the Console port to complete the connection.

Step 2: Establish a terminal session with S1.

a. Click **PC1** and then select the **Desktop** tab.

b. Click the **Terminal** application icon; verify that the Port Configuration default settings are correct.

What is the setting for bits per second? ________

c. Click **OK**.

d. The screen that appears may have several messages displayed. Somewhere on the display there should be a Press RETURN to get started! message. Press **ENTER**.

What is the prompt displayed on the screen? __________

Step 3: Explore the IOS Help.

a. The IOS can provide help for commands depending on the level being accessed. The prompt currently being displayed is called **User EXEC** and the device is waiting for a command. The most basic form of help is to type a question mark (?) at the prompt to display a list of commands.

```
S1> ?
```

Which command begins with the letter 'C'? ____________________

b. At the prompt, type **t**, followed by a question mark (**?**).

```
S1> t?
```

Which commands are displayed? ____________________________

c. At the prompt, type **te**, followed by a question mark (**?**).

```
S1> te?
```

Which commands are displayed? ____________________

This type of help is known as **context-sensitive** Help, providing more information as the commands are expanded.

Part 2: Exploring EXEC Modes

In Part 2 of this activity, you switch to privileged EXEC mode and issue additional commands.

Step 1: Enter privileged EXEC mode.

a. At the prompt, type the question mark (**?**).

```
S1> ?
```

What information is displayed that describes the **enable** command? ______________________________

b. Type **en** and press the **Tab** key.

```
S1> en<Tab>
```

What displays after pressing the **Tab** key? __________

This is called command completion or tab completion. When part of a command is typed, the **Tab** key can be used to complete the partial command. If the characters typed are enough to make the command unique, as in the case with the **enable** command, the remaining portion is displayed.

What would happen if you were to type **te<Tab>** at the prompt?

____

____

____

c. Enter the **enable** command and press **ENTER**. How does the prompt change?

____

d. When prompted, type the question mark (**?**).

```
S1# ?
```

Previously there was one command that started with the letter 'C' in user EXEC mode. How many commands are displayed now that privileged EXEC mode is active? (**Hint**: you could type c? to list just the commands beginning with 'C'.)

____

Step 2: Enter Global Configuration mode.

a. One of the commands starting with the letter ‘C’ is **configure** when in Privileged EXEC mode. Type either the full command or enough of the command to make it unique along with the <**Tab**> key to issue the command and press **<ENTER>**.

```
S1# configure
```

What is the message that is displayed?

____

b. Press the **<ENTER>** key to accept the default parameter enclosed in brackets **[terminal]**.

How does the prompt change? ____

c. This is called global configuration mode. This mode will be explored further in upcoming activities and labs. For now exit back to Privileged EXEC mode by typing **end**, **exit** or **Ctrl-Z**.

```
S1(config)# exit
S1#
```

Part 3: Setting the Clock

Step 1: Use the clock command.

a. Use the **clock** command to further explore Help and command syntax. Type **show clock** at the privileged EXEC prompt.

```
S1# show clock
```

What information is displayed? What is the year that is displayed?

____

b. Use the context-sensitive Help and the **clock** command to set the time on the switch to the current time. Enter the command **clock** and press **ENTER**.

```
S1# clock<ENTER>
```

What information is displayed? ____

c. The % Incomplete command message is returned by the IOS indicating that the **clock** command needs further parameters. Any time more information is needed help can be provided by typing a space after the command and the question mark (?).

```
S1# clock ?
```

What information is displayed? ____

d. Set the clock using the **clock set** command. Continue proceeding through the command one step at a time.

```
S1# clock set ?
```

What information is being requested? ____

What would have been displayed if only the **clock set** command had been entered and no request for help was made by using the question mark? ____

e. Based on the information requested by issuing the **clock set ?** command, enter a time of 3:00 p.m. by using the 24-hour format of 15:00:00. Check to see if further parameters are needed.

```
S1# clock set 15:00:00 ?
```

The output returns the request for more information:

```
<1-31> Day of the month
MONTH  Month of the year
```

f. Attempt to set the date to 01/31/2035 using the format requested. It may be necessary to request additional help using the context-sensitive Help to complete the process. When finished, issue the **show clock** command to display the clock setting. The resulting command output should display as:

```
S1# show clock
*15:0:4.869 UTC Tue Jan 31 2035
```

g. If you were not successful, try the following command to obtain the output above:

```
S1# clock set 15:00:00 31 Jan 2035
```

Step 2: Explore additional command messages.

a. The IOS provides various outputs for incorrect or incomplete commands as experienced in earlier sections. Continue to use the **clock** command to explore additional messages that may be encountered as you learn to use the IOS.

b. Issue the following command and record the messages:

```
S1# cl
```

What information was returned? ____

```
S1# clock
```

What information was returned? ____

```
S1# clock set 25:00:00
```

What information was returned?

____

____

____

```
S1# clock set 15:00:00 32
```

What information was returned?

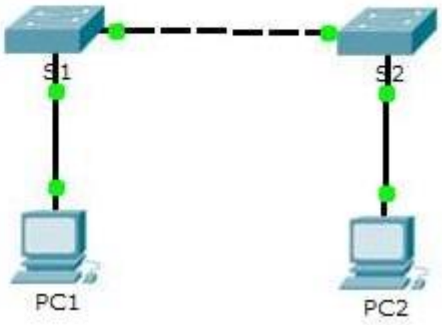
____

____

____

Lab# 2.2:- Configuring Initial Switch Settings

Topology



Objectives

Part 1: Verify the Default Switch Configuration

Part 2: Configure a Basic Switch Configuration

Part 3: Configure a MOTD Banner

Part 4: Save Configuration Files to NVRAM

Part 5: Configure S2

Background

In this activity, you will perform basic switch configurations. You will secure access to the command-line interface (CLI) and console ports using encrypted and plain text passwords. You will also learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited.

Part 4: Verify the Default Switch Configuration

Step 1: Enter privileged mode.

You can access all switch commands from privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.

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.

a. Click **S1** and then the **CLI** tab. Press **<Enter>**.

b. 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.

a. Enter the **show running-config** command.

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

b. Answer the following questions:

How many FastEthernet 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? _______________

Which command will display the current contents of non-volatile random-access memory (NVRAM)?

____

Why does the switch respond with startup-config is not present?

____

____

Part 5: Create a Basic Switch Configuration

Step 1: Assign a name to a switch.

To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

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

Step 2: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **letmein**.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Why is the **login** command required?

____

Step 3: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

Step 4: Secure privileged mode access.

Set the **enable** password to **c1$c0**. This password protects access to privileged mode.

Note: The **0** in **c1$c0** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

```
S1> enable
S1# configure  terminal
S1(config)# enable password c1$c0
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Step 5: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.

b. Press **<Enter>** and you will now be asked for a password:

```
User Access Verification
Password:
```

c. The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.

d. Enter the command to access privileged mode.

e. Enter the second password you configured to protect privileged EXEC mode.

f. Verify your configurations by examining the contents of the running-configuration file:

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

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 6: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enable secret password to **itsasecret**.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.

Step 7: Verify that the enable secret password is added to the configuration file.

a. Enter the **show running-config** command again to verify the new **enable secret** password is configured.

Note: You can abbreviate **show running-config** as

```
S1# show run
```

b. What is displayed for the **enable secret** password? ____

c. Why is the **enable secret** password displayed differently from what we configured?

____

Step 8: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

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

If you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain why?

____

Part 6: Configure a MOTD Banner

Step 1: Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

```
S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

When will this banner be displayed?

____

Why should every switch have a MOTD banner?

____

____

____

Part 7: Save Configuration Files to NVRAM

Step 1: Verify that the configuration is accurate using the show run command.

Step 2: Save the configuration file.

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

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

What is the shortest, abbreviated version of the **copy running-config startup-config** command? __________

Step 3: Examine the startup configuration file.

Which command will display the contents of NVRAM? ____

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

Part 8: Configure S2

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.

Configure S2 with the following parameters:

a. Name device: **S2**

b. Protect access to the console using the **letmein** password.

c. Configure an enable password of **c1$c0** and an enable secret password of **itsasecret**.

d. Configure a message to those logging into the switch with the following message:

Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

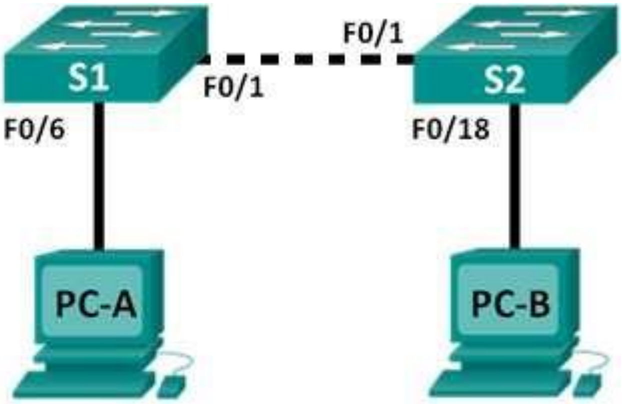
e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

Lab# 2.3: - Implement Basic Connectivity

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC-A	NIC	192.168.1.1	255.255.255.0
PC-**B**	NIC	192.168.1.2	255.255.255.0

Objectives

Part 1: Perform a Basic Configuration on S1 and S2

Part 2: Configure the PCs

Part 3: Configure the Switch Management Interface

Background

In this activity you will first perform basic switch configurations. Then you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various **show** commands to verify configurations and use the **ping** command to verify basic connectivity between devices.

Part 9: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 with a hostname.

a. Click **S1**, and then click the **CLI** tab.

b. Enter the correct command to configure the hostname as **S1**.

Step 2: Configure the console and privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

____

____

____

Step 4: Configure a message of the day (MOTD) banner.

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 5: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

____

____

Step 6: Repeat Steps 1 to 5 for S2.

Part 10: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Step 1: Configure both PCs with IP addresses.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **IP Configuration**. In the **Addressing Table** above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the **IP Configuration** window.

c. Repeat steps 1a and 1b for PC-B.

Step 2: Test connectivity to switches.

a. Click **PC1**. Close the **IP Configuration** window if it is still open. In the **Desktop** tab, click **Command Prompt**. .

b. Type the **ping** command and the IP address for S1, and press **Enter**.

```
Packet Tracer PC Command Line 1.0
PC> ping 192.168.1.253
```

Were you successful? Why or why not?

____.

Part 11: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 1: Configure S1 with an IP address. Also configure Virtual Terminal Line (VTY):

Switches can be used as a plug-and-play device, meaning they do not need to be configured for them to work. Switches forward information from one port to another based on Media Access Control (MAC) addresses. If this is the case, why would we configure it with an IP address?

____

____

a. Use the following commands to configure S1 with an IP address.

```
S1 #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

Why do you need to enter the **no shutdown** command?

____

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

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

Step 2: Configure S2 with an IP addresses.

Use the information in the addressing table to configure S2 with an IP address.

Step 3: Verify the IP address configuration on S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of the all the switch ports and interfaces. Alternatively, you can also use the **show running-config** command.

Step 4: Save configurations for S1 and S2 to NVRAM.

Which command is used to save the configuration file in RAM to NVRAM? ____________________________

Step 5: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1's and S2's IP address from PC1 and PC2.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC-B.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

Note: You can also use the same **ping** command on the switch CLI and on PC-B.

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

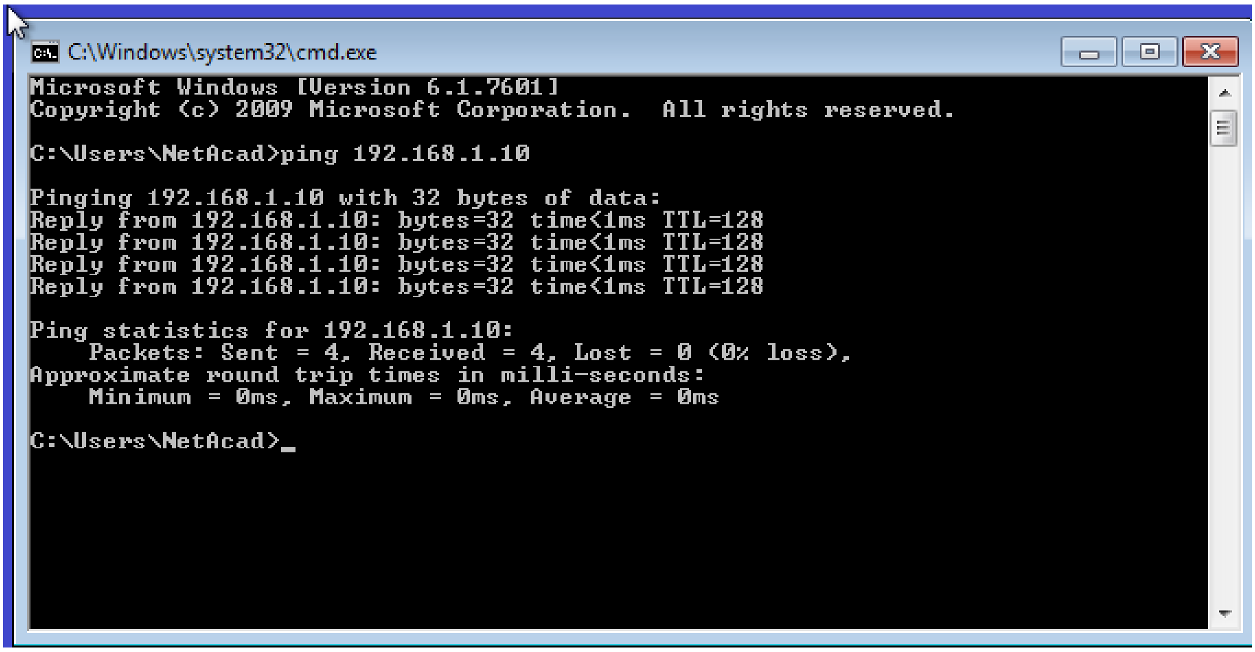
Step 6: Test end-to-end connectivity.

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

a. Ping your own PC-A address first.

C:\Users\NetAcad> **ping 192.168.1.1**

Your output should be similar to the following screen:

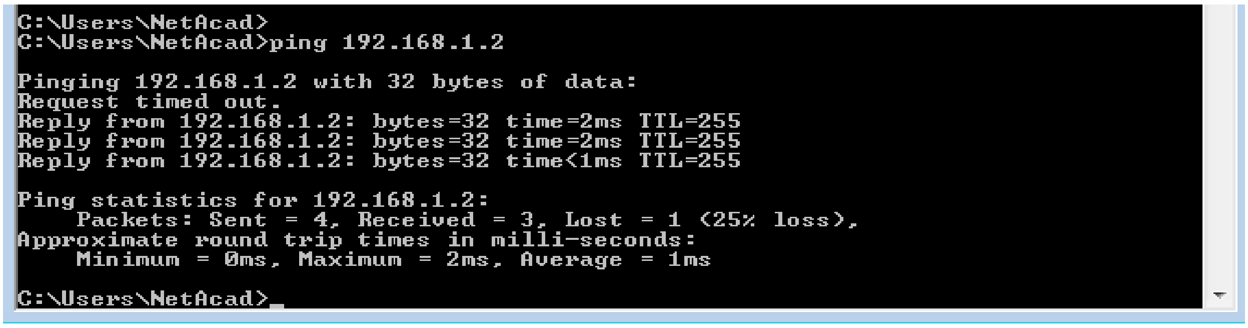


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\NetAcad>ping 192.168.1.10

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

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

C:\Users\NetAcad>_
```

b. Ping the SVI management address of S1.

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

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



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

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

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

C:\Users\NetAcad>_
```

Step 7: Test and verify remote management of S1.

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

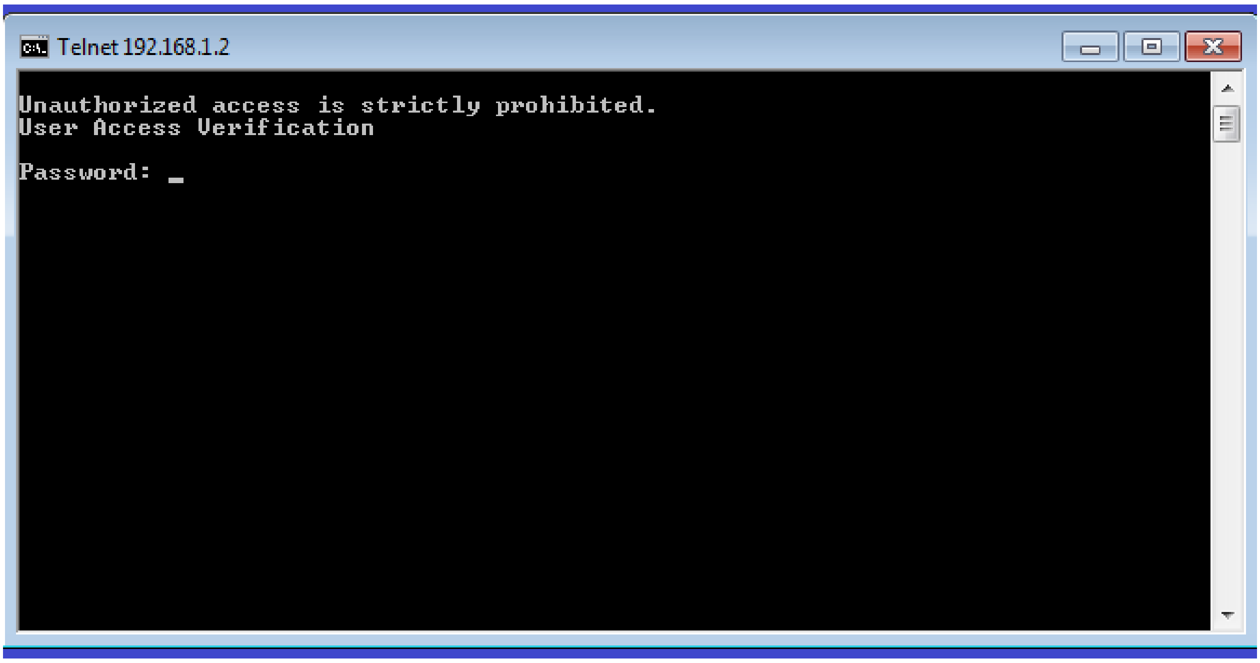
Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type **pkgmgr /iu:"TelnetClient"**.

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

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

```
C:\Users\NetAcad> telnet 192.168.1.253
```

Your output should be similar to the following screen:



```
Unauthorized access is strictly prohibited.
User Access Verification

Password: _
```

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

Reflection

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

____

____

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#03

Lab# 2.1:- Packet Tracer - Navigating the two different networks.

Topology

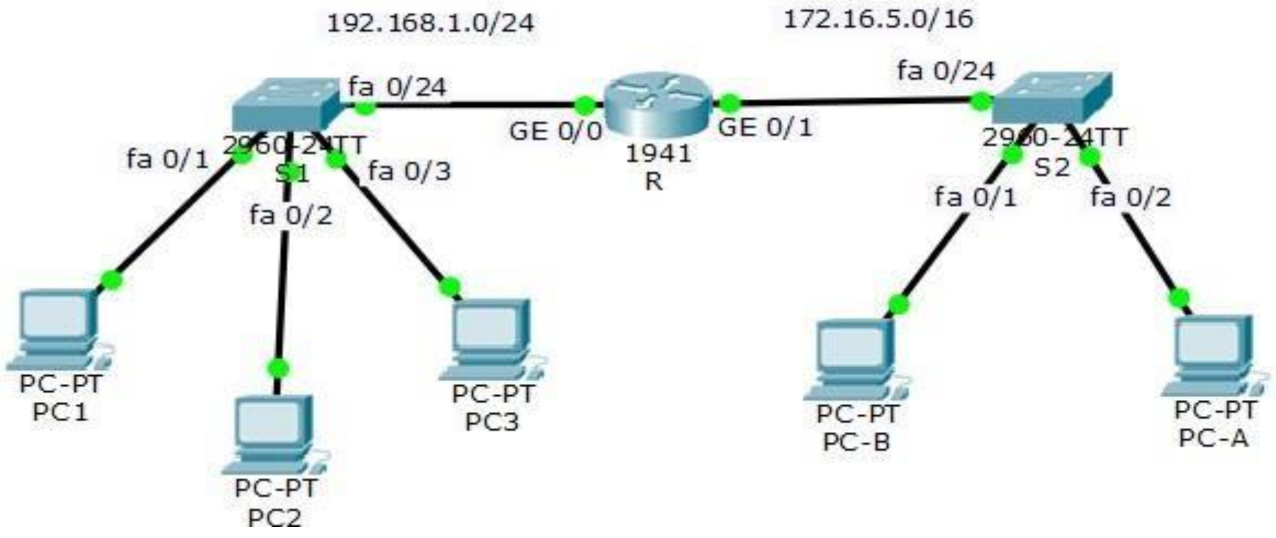


Figure 3.1

Objectives

Part 1: Connections using copper straight through wires.

Part 2: Accessing the CLI of each network device to do basic configuration.

Part 3: Assign IP address to each device and router's interfaces.

Part 4: Configure telnet on each network device.

Part 5: Set default gateways.

Part 6: Verify Network Connectivity by using PING.

Part 7: Establish telnet session to each network device via command prompt of different PCs.

Part 8: Home activity.

Part 1: Basic Connections, Accessing the CLI and Exploring Help

In Part 1 of this activity, you connect the all the devices together using copper straight through connection as mentioned in figure 3.1.

Connect PC1 to S1 using a console cable.

a. Click the **Connections** icon (the one that looks like a lightning bolt) in the lower left corner of the Packet Tracer window.

b. Select the black copper straight through cable by clicking it. The mouse pointer will change to what appears to be a connector with a cable dangling off of it.

c. Click on **PC1**; a window displays an option for a fast Ethernet connection.

d. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

e. Select the Fast Ethernet 0/1 port to complete the connection.

f. Click on **PC2**; a window displays an option for a fast Ethernet connection.

g. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

h. Select the Fast Ethernet 0/2 port to complete the connection.

i. Click on **PC3**; a window displays an option for a fast Ethernet connection.

j. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

k. Select the Fast Ethernet 0/3 port to complete the connection.

l. Click on **PC-A**; a window displays an option for a fast Ethernet connection.

m. Drag the other end of the copper straight through connection to the S2 switch and click the switch to bring up the connection list.

n. Select the Fast Ethernet 0/1 port to complete the connection.

o. Click on **PC-B**; a window displays an option for a fast Ethernet connection.

p. Drag the other end of the copper straight through connection to the S2 switch and click the switch to bring up the connection list.

q. Select the Fast Ethernet 0/2 port to complete the connection.

r. Click on **R router**; a window displays some option for Gigabit Ethernet or fast Ethernet ports. Select the Fast Ethernet 0/0 or Gigabit Ethernet 0/0.

s. Drag the other end of the copper straight through connection to the S1 switch and click the switch to bring up the connection list.

t. Select the Fast Ethernet 0/24 port to complete the connection.

u. Again Click on **R router**; a window displays some option for Gigabit Ethernet or fast Ethernet ports. Select the Fast Ethernet 0/1 or Gigabit Ethernet 0/1.

v. Drag the other end of the copper straight through connection to the S2 switch and click the switch to bring up the connection list.

w. Select the Fast Ethernet 0/24 port to complete the connection.

Part 2: Accessing the CLI of each network device to do basic configuration.

- Click on S**1switch** and then select the CLI tab to access the CISCO IOS.
- Do some basic configurations like setting the clock, assign name to each network device, set banner, console password, privilege mode password or enable secret and encrypt them.

Step 1: Assign a name to a switch.

To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

```
Switch# clock set 15:00:00 31 Jan 2035
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

Step 2: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **letmein**.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
```

```
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Step 3: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>
```

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

Step 4: Secure privileged mode access.

Set the **enable** password to **c1$c0**. This password protects access to privileged mode.

Note: The **0** in **c1$c0** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

```
S1> enable
S1# configure  terminal
S1(config)# enable password c1$c0
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Step 5: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.

b. Press **<Enter>** and you will now be asked for a password:

```
User Access Verification
Password:
```

c. The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.

d. Enter the command to access privileged mode.

e. Enter the second password you configured to protect privileged EXEC mode.

f. Verify your configurations by examining the contents of the running-configuration file:

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

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 6: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enable secret password to **itsasecret**.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.

Step 7: Verify that the enable secret password is added to the configuration file.

a. Enter the **show running-config** command again to verify the new **enable secret** password is configured.

Note: You can abbreviate **show running-config** as

```
S1# show run
```

Step 8: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

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

Configure a MOTD Banner

Step 9: Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

```
S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Step 10: Save Configuration Files to NVRAM

- **Verify that the configuration is accurate using the show run command.**
- **Save the configuration file.**

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

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

Configure Router (R) and Switch2 (S2):

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Step 1 to 10 for assistance.

Configure S2 with the following parameters:

a. Name device: **S2**

b. Protect access to the console using the **letmein** password.

c. Configure an enable password of **c1$c0** and an enable secret password of **itsasecret**.

d. Configure a message to those logging into the switch with the following message:

Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

Part 3 and 4: - Implement Basic Addressing and Connectivity

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R	Gi 0/0	192.168.1.1	255.255.255.0	---
R	Gi 0/1	172.16.5.1	255.255.0.0	---
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	172.16.5.2	255.255.0.0	172.16.5.1
PC-A	NIC	172.16.5.3	255.255.0.0	172.16.5.1
PC-**B**	NIC	172.16.5.4	255.255.0.0	172.16.5.1
PC1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.4	255.255.255.0	192.168.1.1

table 3.1

Configure the PCs

Configure PC1, PC2 and PC3 with IP addresses, subnet mask and default gateway.

Step 1: Configure both PCs with IP addresses.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **IP Configuration**. In the **Addressing Table** above, you can see that the IP address for PC1 is 172.16.5.3, the subnet mask is 255.255.0.0 and the default gateway is 172.16.5.1. Enter these information for PC-A in the **IP Configuration** window.

c. Repeat steps 1a and 1b for PC-B, PC1, PC2 and PC3.

Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 2: Configure S1 with an IP address. Also configure Virtual Terminal Line (VTY):

a. Use the following commands to configure S1 with an IP address.

```
S1 #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

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

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

Step 2: Configure S2 with an IP addresses.

Use the information in the addressing table to configure S2 with an IP address.

Step 3: Configure Router's (R) Interfaces with IP addresses.

```
R> enable
R # configure terminal
R (config) # interface gigabitEthernet 0/0
R(config-if)# ip address 192.168.1.2 255.255.255.0
R(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
R(config-if)#
R(config-if)# exit
R (config) # interface gigabitEthernet 0/1
R(config-if)# ip address 172.16.5.1 255.255.0.0
R(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
R(config-if)#
R(config-if)# end
R# copy run start
R#exit
```

Step 4: Verify the IP address configuration on R, S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of the all the switch ports and interfaces. Alternatively, you can also use the **show running-config** command.

Part 5: - Configure default gateway on both Switches (S1 and S2):

On switch, following command is used to configure default gateway

```
S1 >en
S1 # configure terminal
S1 (config)# ip default-gateway 192.168.1.1
S1 (config)#exit
S1 # copy run start
```

Likewise on S2:

```
S2 >en
S2 # configure terminal
S2 (config)# ip default-gateway 172.16.5.1
S2 (config)#exit
S2 # copy run start
```

Part 6: Verify Network Connectivity by using PING .

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1's and S2's IP address from PC1, PC2, PC3,PC-A and PC-B.

a. Click **PC-A**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC-B.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

f. Ping the IP address of default gateway.

g. Ping the IP address for PC1.

h. Ping the IP address for PC2.

i. Ping the IP address for PC3.

Note: You can also use the same **ping** command on the switch CLI and on PCs.

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

Part 7: Test and verify remote management of S1.

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

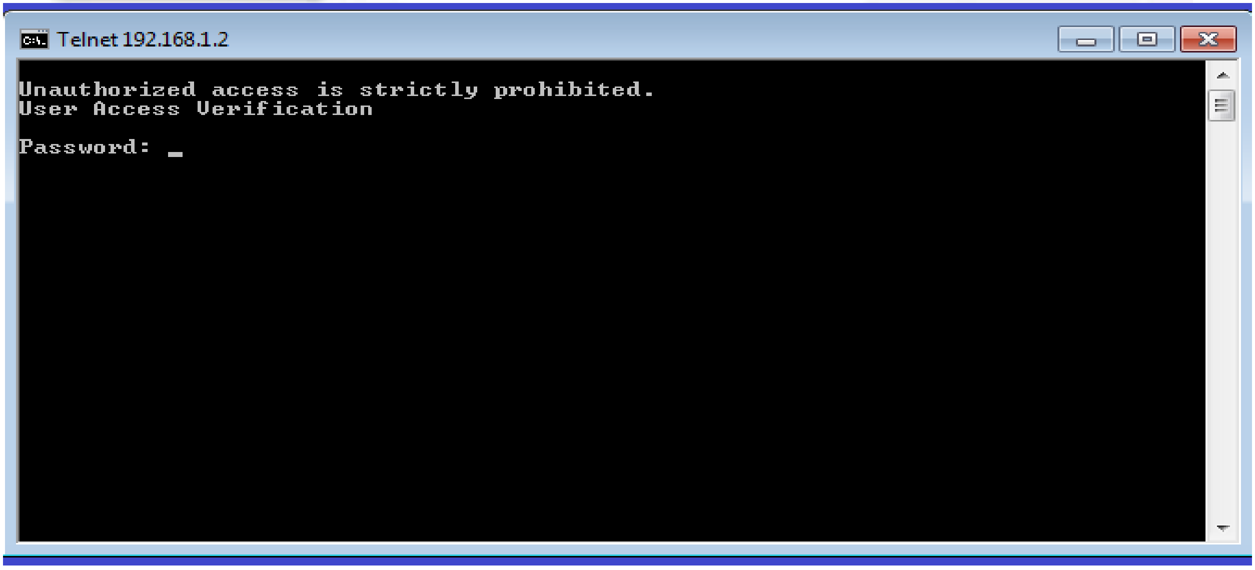
Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type **pkgmgr /iu:"TelnetClient"**.

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

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

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

Your output should be similar to the following screen:

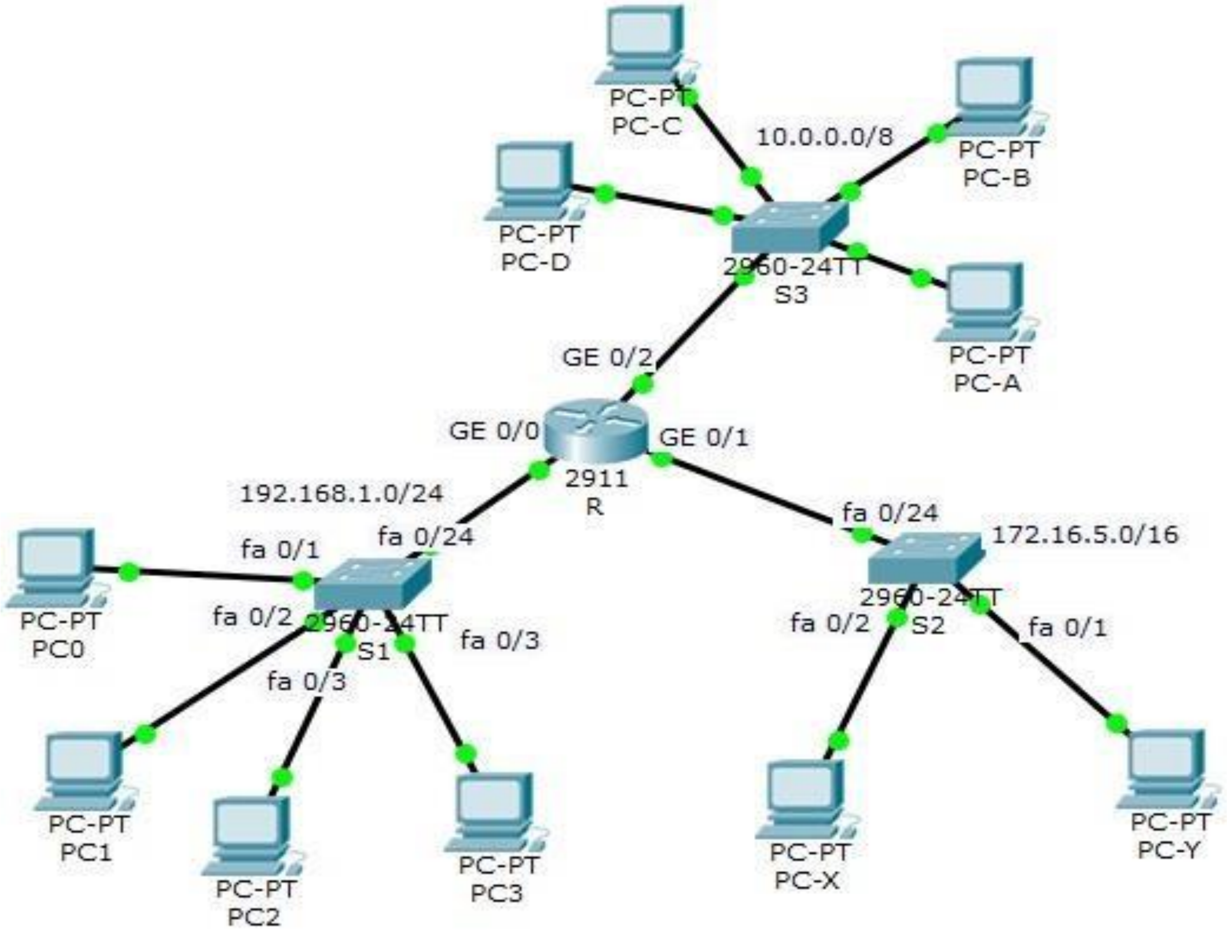


```
Unauthorized access is strictly prohibited.
User Access Verification

Password: _
```

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

Part 8: Home Activity:

Complete the addressing table of the given topology. Configure a following topology in the light of experiment#3 by using c2911(router). Attach the screen shots of the **topology**, **addressing table** and **startup configuration of each intermediary device** at end of this experiment.



Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#04

Lab# 4.1:- Packet Tracer – Router as DHCP server.

Topology

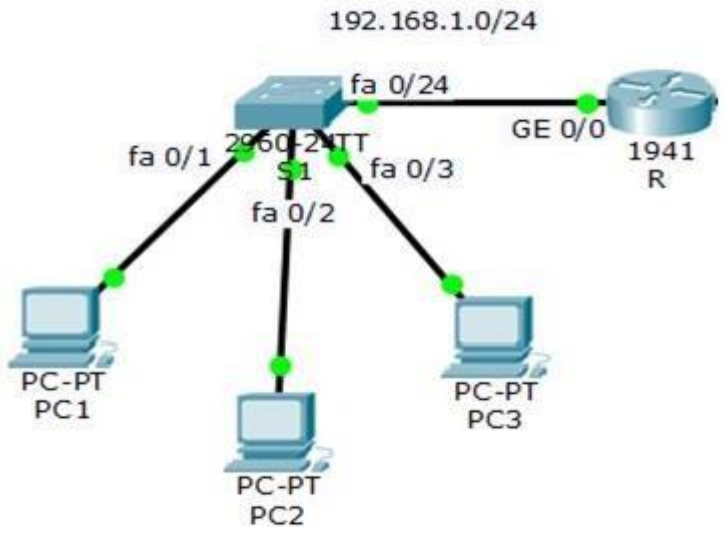


Figure 4.1

Objectives

Part 1: Connections using copper straight through wires.

Part 2: Accessing the CLI of each network device to do basic configuration.

Part 3: Assign IP Addresses to each network devices manually.

Part 4: Configure telnet on each network device.

Part 5: Configure a DHCPv4 server on a Router.

Part 6: Enable DHCP Services in PCs.

Part 7: Verify DHCP services

Part 8 Verify Network Connectivity by using PING.

Part 9: Test and verify remote management of S1 and R.

Part 10: Class activity.

Part 11: Home ativity.

Part 1: Basic Connections, Accessing the CLI and Exploring Help

In Part 1 of this activity, you connect the all the devices together using copper straight through connection as mentioned in figure 4.1.

Part 2: Accessing the CLI of each network device to do basic configuration.

- Click on S1 **switch** and then select the CLI tab to access the CISCO IOS.
- Do some basic configurations like setting the clock, assign host name to each network device, set banner, console password, privilege mode password or enable secret, virtual terminal line password and encrypt them.

<u>Part 3 and 4:</u> - Implement Basic Addressing on network devices manually.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R	Gi 0/0	192.168.1.1	255.255.255.0	---
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1

table 4.1

Configure the Switch Management Interface

Configure S1 with an IP address.

Step 1: Configure S1 with an IP address. Also configure Virtual Terminal Line (VTY):

a. Use the following commands to configure S1 with an IP address.

```
S #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S(config)# interface vlan 1
S(config-if)# ip address 192.168.1.2 255.255.255.0
S(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S(config-if)#
S(config-if)# exit
S (config)# ip default-gateway 192.168.1.1
S (config)#exit
S # copy run start
S# exit
```

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

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
```

Step 2: Configure Router’s (R) Interfaces with IP addresses.

a. Use the following commands to configure S1 with an IP address

```
R> enable
R # configure terminal
R (config) # interface gigabitEthernet 0/0
R(config-if)# ip address 192.168.1.1 255.255.255.0
R(config-if)# description connected to ACCOUNTS
R(config-if)# no shutdown
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
R(config-if)#
R(config-if)# end
R# copy run start
R#exit
```

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

```
R(config)# line vty 0 15
R(config-line)# password cisco
R(config-line)# login
R(config-line)# end
R# copy run start
R#exit
R#
```

Step 3: Verify the IP address configuration on Router (R) and Switch (S)

Use the **show ip interface brief** command to display the IP address and status of the all the switch ports and interfaces. Alternatively, you can also use the **show running-config** command.

Part 5: - Configure a DHCPv4 on Router:

```
R (config)# service dhcp
R (config)# ip dhcp pool ACCONUTS
R (dhcp-config)# network 192.168.1.0 255.255.255.0
R (dhcp-config)# default-router 192.168.1.1
R (dhcp-config)# dns-server 8.8.8.8
R (dhcp-config)# exit
R (config)# ip dhcp excluded-address 192.168.1.1  192.168.1.2
R (config)# ex
R # write memory
R#ex
```

Part 6: Enable DHCP Services in PCs.

Click on any PC then goes on DESKTOP tab then move to IP configuration and then check on DHCP. PC acquire IP configuration from DHCP automatically after a few moments. Repeat this for each PC in the topology for IP configuration.

Part 7: Verify DHCP services on R.

a. On R, enter the **show ip dhcp binding** command to view DHCP address leases.

Along with the IP addresses that were leased, what other piece of useful client identification information is in the output?

____

b. On R, enter the **show ip dhcp server statistics** command to view the DHCP pool statistics and message activity.

How many types of DHCP messages are listed in the output?

____

c. On R, enter the **show ip dhcp pool** command to view the DHCP pool settings.

In the output of the **show ip dhcp pool** command, what does the Current index refer to?

____

d. On R, enter the **show run | section dhcp** command to view the DHCP configuration in the running configuration.

Reflection

What do you think is the benefit of using DHCP relay agents instead of multiple routers acting as DHCP servers?

____

____

____

____

Part 8: Verify network connectivity:

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1's and R IP address from each PCs.

a. Click **PC-1**, and then click the **Desktop** tab.

b. Click **Command Prompt**.

c. Ping the IP address for PC-2.

d. Ping the IP address for S1.

e. Ping the IP address for R.

f. Ping the IP address of default gateway.

g. Ping the IP address for PC2.

h. Ping the IP address for PC3.

Note: You can also use the same **ping** command on the switch CLI and on PCs.

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

Part 9: Test and verify remote management of S1 and R.

You will now use Telnet to remotely access the operating system of switch S1and router R.

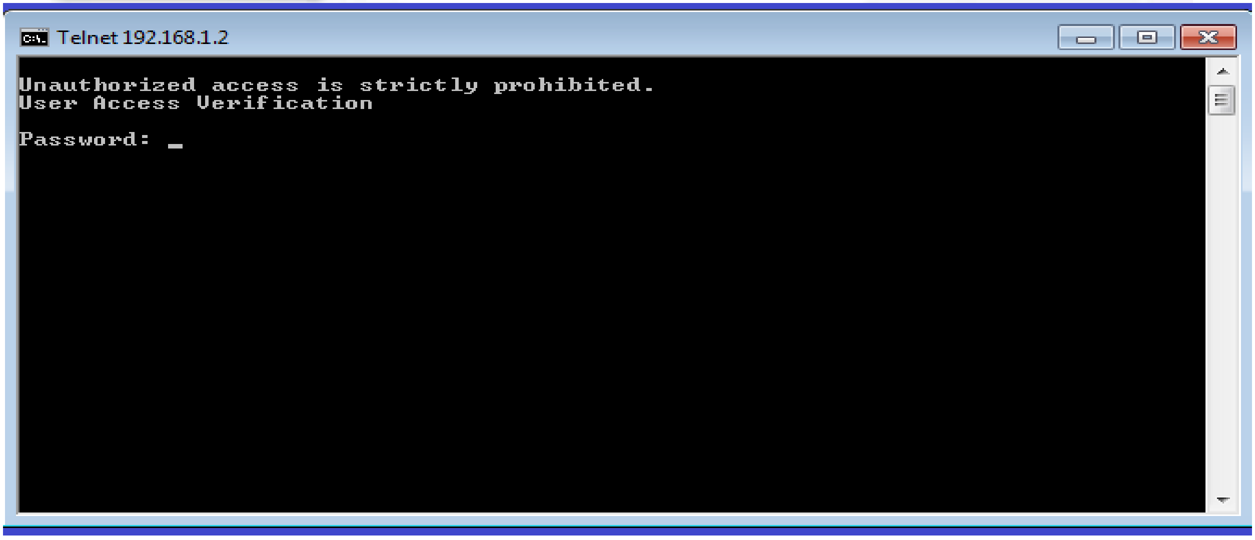
Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type **pkgmgr /iu:"TelnetClient"**.

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

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

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

Your output should be similar to the following screen:

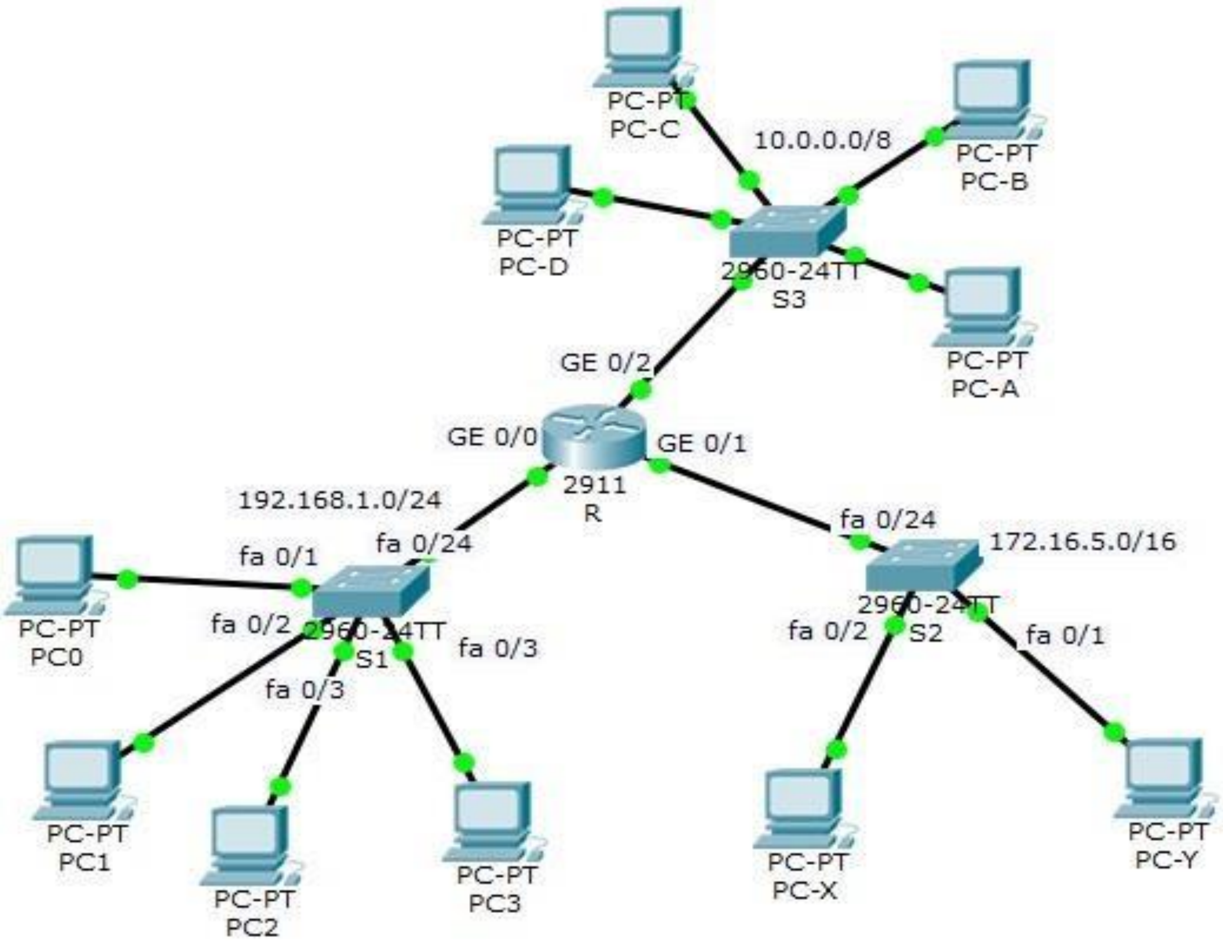


```
Unauthorized access is strictly prohibited.
User Access Verification

Password: _
```

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

Part 10: Class Activity

Configure the following topology in the light of above configuration by using Router 2911.



Step 1. **Configure Router (R):**

```
Router >en
Router# configure terminal
Router (config)# interface gi 0/0
Router (config-if)# ip address 192.168.1.1 255.255.255.0
Router (config-if)# description connected to FINANCE
Router (config-if)# no shutdown
Router (config-if)#exit
Router (config)# interface gi 0/1
Router (config-if)# ip address 172.16.0.1 255.255.0.0
Router (config-if)# description connected to ENGINEERING
Router (config-if)# no shutdown
Router (config-if)#exit
Router (config)# interface gi 0/2
Router (config-if)# ip address 10.0.0.1 255.0.0.0
Router (config-if)# description connected to IT
Router (config-if)# no shutdown
Router (config-if)#exit

Router (config)#service DHCP
Router (config)# ip dhcp pool FINANCE
Router (dhcp-config)# network 192.168.1.0 255.255.255.0
Router (dhcp-config)# default-router 192.168.1.1
Router (dhcp-config)#dns-server 64.6.64.6
Router (dhcp-config)# exit
Router (config)#ip dhcp excluded-address 192.168.1.1 192.168.1.2

Router (config)# ip dhcp pool ENGINEERING
Router (dhcp-config)# network 172.16.0.0 255.255.0.0
Router (dhcp-config)# default-router 172.16.0.1
Router (dhcp-config)#dns-server 8.8.8.8
Router (dhcp-config)# exit
Router (config)#ip dhcp excluded-address 172.16.0.1 172.16.0.2

Router (config)# ip dhcp pool IT
Router (dhcp-config)# network 10.0.0.0 255.0.0.0
Router (dhcp-config)# default-router 10.0.0.1
Router (dhcp-config)#dns-server 64.6.65.6
Router (dhcp-config)# exit
Router (config)#ip dhcp excluded-address 10.0.0.1 10.0.0.2

Router (config)# hostname R
R (config)# banner motd " Warning !!! This is a secure system. Authorized Access Only!"
R(config)# line console 0
R(config-line)# password 123
R(config-line)#login
R(config-line)#exit
R(config)# line vty 0 15
R(config-line)# password 12345
R(config-line)#login
R(config-line)# exit
```

```
R(config)#enable secret 1234
R(config)# service password-encryption
R(config)#exit
R# clock set 12:00:00 14 March 2017
R# write memory
```

Step 2. Configure Switch (S1):

```
Switch >en
Switch# configure terminal
Switch (config)# interface vlan 1
Switch (config-if)# ip address 192.168.1.2 255.255.255.0
Switch (config-if)# description connected to FINANCE
Switch (config-if)# no shutdown
Switch (config-if)#exit

Switch (config)# hostname S1
S1(config)# banner motd " Warning !!! This is a secure system. Authorized Access Only!"
S1(config)# line console 0
S1(config-line)# password 123
S1(config-line)#login
S1(config-line)#exit
S1(config)# line vty 0 15
S1(config-line)# password 12345
S1(config-line)#login
S1(config-line)# exit
S1(config)#enable secret 1234
S1(config)# service password-encryption
S1(config)#exit
S1# clock set 12:00:00 14 March 2017
S1# write memory
```

Step 3. Configure Switch (S2):

```
Switch >en
Switch# configure terminal
Switch (config)# interface vlan 1
Switch (config-if)# ip address 172.16.0.2 255.255.0.0
Switch (config-if)# description connected to ENGINEERING
Switch (config-if)# no shutdown
Switch (config-if)#exit

Switch (config)# hostname S2
S2(config)# banner motd " Warning !!! This is a secure system. Authorized Access Only!"
S2(config)# line console 0
S2(config-line)# password 123
S2(config-line)#login
S2(config-line)#exit
S2(config)# line vty 0 15
S2(config-line)# password 12345
S2(config-line)#login
S2(config-line)# exit
```

```
S2(config)#enable secret 1234
S2(config)# service password-encryption
S2(config)#exit
S2# clock set 12:00:00 14 March 2017
S2# write memory
```

Step 4. Configure Switch (S3):

```
Switch >en
Switch# configure terminal
Switch (config)# interface vlan 1
Switch (config-if)# ip address 10.0.0.2 255.0.0.0
Switch (config-if)# description connected to IT
Switch (config-if)# no shutdown
Switch (config-if)#exit

Switch (config)# hostname S3
S3(config)# banner motd " Warning !!! This is a secure system. Authorized Access Only!"
S3(config)# line console 0
S3(config-line)# password 123
S3(config-line)#login
S3(config-line)#exit
S3(config)# line vty 0 15
S3(config-line)# password 12345
S3(config-line)#login
S3(config-line)# exit
S3(config)#enable secret 1234
S3(config)# service password-encryption
S3(config)#exit
S3# clock set 12:00:00 14 March 2017
S3# write memory
```

Step 5. Verify the above configuration

Click on any PC then goes on DESKTOP tab then move to IP configuration and then check on DHCP. PC acquire IP configuration from DHCP automatically after a few moments. Repeat this for each PC in the topology for IP configuration

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1's, S2's, and R's IP address from each PCs.

Verify DHCP services by using:

a. On R, enter the **show ip dhcp binding** command to view DHCP address leases.

b. On R, enter the **show ip dhcp server statistics** command to view the DHCP pool statistics and message activity.

c. On R, enter the **show ip dhcp pool** command to view the DHCP pool settings.

d. On R, enter the **show run | section dhcp** command to view the DHCP configuration in the running configuration.

You will now use Telnet to remotely access the operating system of switch S1 S2, S3 and router R.

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

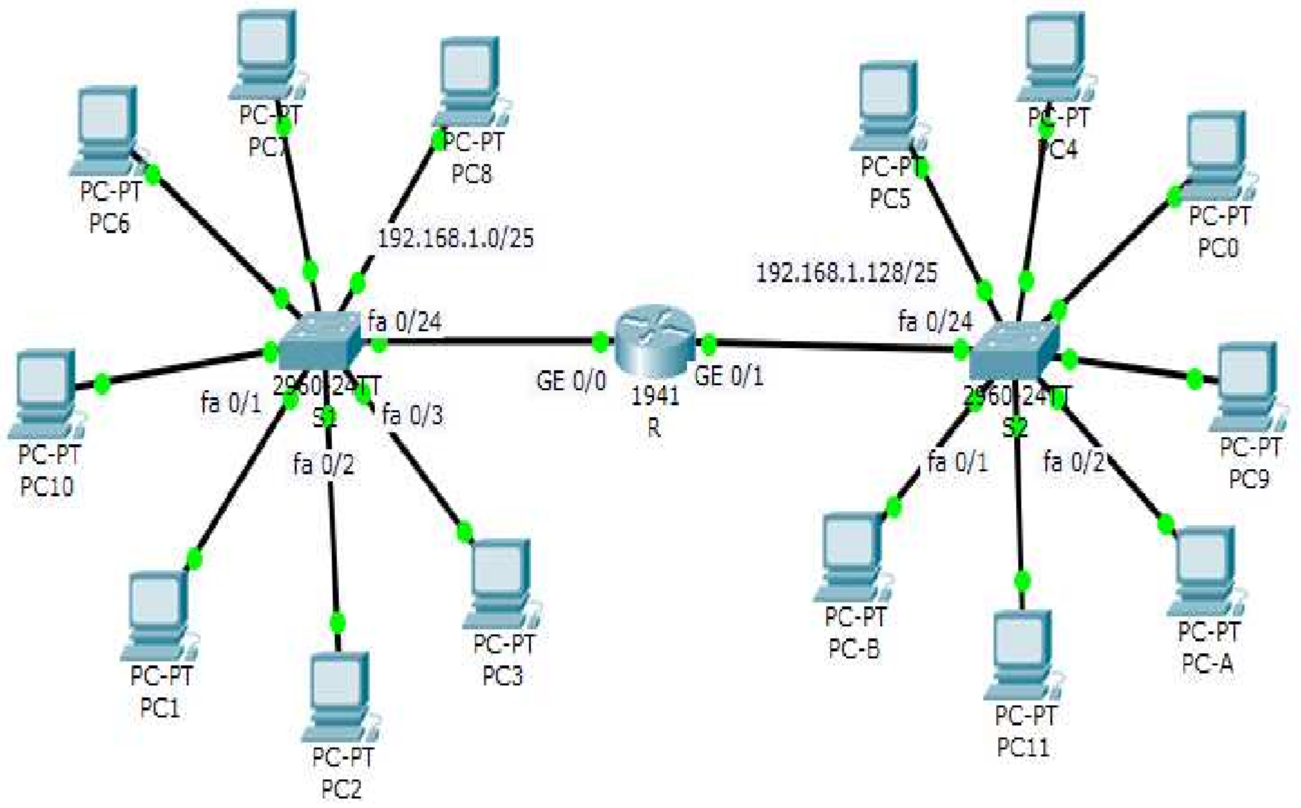
C:\Users\NetAcad> **pkgmgr /iu:"TelnetClient"**

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

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

Part 11: **<u>Home Activity</u>**

Suppose there are two different departments which are connected together throw a router. Configure a following topology in the light of above experiment. Attach screen shot of the topology and printout of startup configuration of each intermediary device in the end of this lab manual.



Lab's Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student's Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor's Name & Initial's)

Date

Experiment# 05

Lab 5.1 - Configuring VLANs and Trunking

Topology

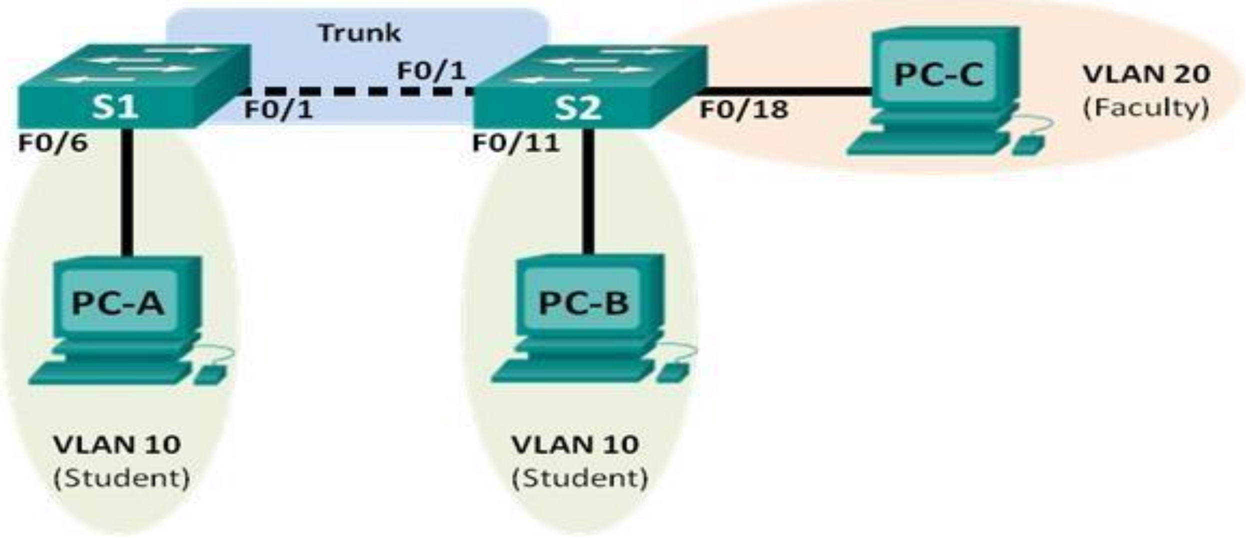


Figure:5.1.1

Addressing Table

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

table: 5.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Maintain VLAN Port Assignments and the VLAN Database

Part 4: Configure an 802.1Q Trunk between the Switches

Part 5: Delete the VLAN Database

Background / Scenario

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

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

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

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

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

Required Resources

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

Part 1: Build the Network and Configure Basic Device Settings

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

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

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

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure device name as shown in the topology.

c. Assign **class** as the privileged EXEC password.

d. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.

e. Configure **logging synchronous** for the console line.

f. Configure a MOTD banner to warn users that unauthorized access is prohibited.

g. Configure the IP address listed in the Addressing Table for VLAN 1 on both switches.

h. Administratively deactivate all unused ports on the switch.

i. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

Verify that the PC hosts can ping one another.

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

Can PC-A ping PC-B? ______________

Can PC-A ping PC-C? ______________

Can PC-A ping S1? ______________

Can PC-B ping PC-C? ______________

Can PC-B ping S2? ______________

Can PC-C ping S2? ______________

Can S1 ping S2? ________________

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

____

____

Part 2: Create VLANs and Assign Switch Ports

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

Step 1: Create VLANs on the switches.

a. Create the VLANs on S1.

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

b. Create the same VLANs on S2.

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

```
S1# show vlan

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

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
```

```
1004 fdnet 101004    1500 -      -    -      ieee -      0     0
1005 trnet 101005    1500 -      -    -      ibm  -      0     0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

What is the default VLAN? _______________

What ports are assigned to the default VLAN?

____

Step 2: Assign VLANs to the correct switch interfaces.

a. Assign VLANs to the interfaces on S1.

1) Assign PC-A to the Student VLAN.

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

2) Move the switch IP address VLAN 99.

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

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

```
S1# show vlan brief

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

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

What is the status of VLAN 99? Why?

____

d. Use the Topology to assign VLANs to the appropriate ports on S2.

e. Remove the IP address for VLAN 1 on S2.

f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.

g. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

S2# **show vlan brief**

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

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

____

Is S1 able to ping S2? Why?

____

____

Part 3: Maintain VLAN Port Assignments and the VLAN Database

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

Step 1: Assign a VLAN to multiple interfaces.

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

S1(config)# **interface range f0/11-24**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 10**

S1(config-if-range)# **end**

b. Issue the **show vlan brief** command to verify VLAN assignments.

c. Reassign F0/11 and F0/21 to VLAN 20.

d. Verify that VLAN assignments are correct.

Step 2: Remove a VLAN assignment from an interface.

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

S1(config)# **interface f0/24**

S1(config-if)# **no switchport access vlan**

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

b. Verify that the VLAN change was made.

Which VLAN is F0/24 is now associated with? ______________

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

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

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

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

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

```
S1# show vlan brief

VLAN Name                             Status    Ports
---------------------------------------------------------------
1    default                          active Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                             Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                             Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                          active  Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                             Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                             Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active Fa0/11, Fa0/21
30   VLAN0030                         active  Fa0/24
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

What is the default name of VLAN 30? _______________

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

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

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

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

____

```
S1# show vlan brief

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

e. Issue the **no switchport access vlan** command on interface F0/24.

f. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24. To which VLAN is F0/24 assigned?

____

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

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

____

____

____

Part 4: Configure an 802.1Q Trunk Between the Switches

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

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

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

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

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

You should also receive link status messages on S2.

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

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

```
S1# show vlan brief

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

```
99   Management                    active
1002 fddi-default                  act/unsup
1003 token-ring-default            act/unsup
1004 fddinet-default               act/unsup
1005 trnet-default                 act/unsup
```

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

S1# **show interfaces trunk**

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

Port      Vlans allowed on trunk
Fa0/1     1-4094

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

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

S2# **show interfaces trunk**

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

Port      Vlans allowed on trunk
Fa0/1     1-4094

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

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

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

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

Can S1 ping S2? ____________

Can PC-A ping PC-B? ____________

Can PC-A ping PC-C? ____________

Can PC-B ping PC-C? ____________

Can PC-A ping S1? ____________

Can PC-B ping S2? ____________

Can PC-C ping S2? ____________

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

____

____

Step 2: Manually configure trunk interface F0/1.

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

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

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

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

```
S2# show interfaces trunk

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

Port      Vlans allowed on trunk
Fa0/1       1-4094

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

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

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

____

____

Part 5: Delete the VLAN Database

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

Step 1: Determine if the VLAN database exists.

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

```
S1# show flash
Directory of flash:/
   2  -rwx       1285  Mar 1 1993 00:01:24 +00:00  config.text
   3  -rwx      43032  Mar 1 1993 00:01:24 +00:00  multiple-fs
   4  -rwx          5  Mar 1 1993 00:01:24 +00:00  private-config.text
   5  -rwx   11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
   6  -rwx        736  Mar 1 1993 00:19:41 +00:00  vlan.dat

32514048 bytes total (20858880 bytes free)
```

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

Step 2: Delete the VLAN database.

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

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

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

```
S1# show flash

Directory of flash:/

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

32514048 bytes total (20859904 bytes free)
```

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

____

____

Reflection

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

____

____

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

____

____

____

____

Lab 5.2:- Class Activity

Topology

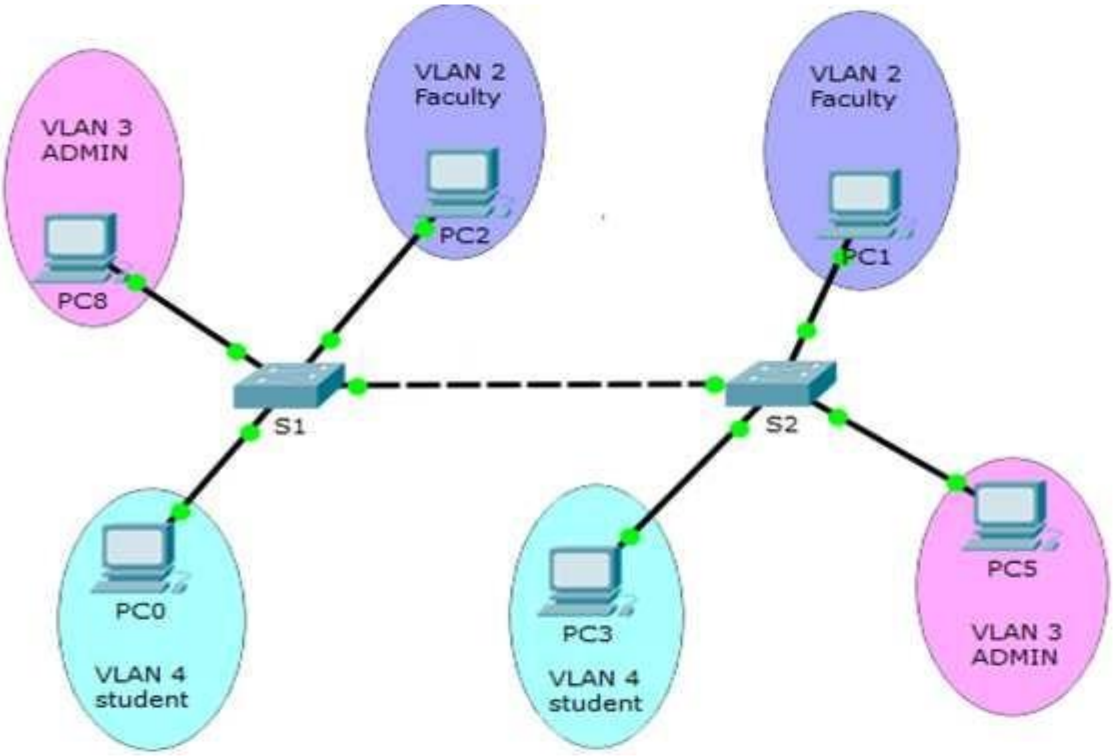


Fig:5.2.1

Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC3	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC1	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC2	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC5	NIC	192.168.3.2	255.255.255.0	192.168.3.1
PC8	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Table:5.2.1

VLANs Table:

VLAN	Name
2	Faculty
3	ADMIN
4	Students

Table:5.2.2

VLANs Ports Assigning Table:

VLANs	Name	Switch port Number			
		device	Access Ports	device	Trunk Ports
2	Faculty	S1	fa 0/1 – fa 0/5	S1	Fast Ethernet 0/24
		S2	fa 0/1 – fa 0/4		
3	ADMIN	S1	fa 0/6 –fa 0/7	S2	Fast Ethernet 0/24
		S2	fa 0/5 – fa 0/9		
4	Students	S1	fa 0/8 – fa 0/23		
		S2	fa 0/10 – fa 0/23		

Table:5.2.3

Objectives

Part 1: Build the Network and Configure Basic Device Settings on both switches

Part 2: Create VLANs and Assign Switch Ports to VLANs

Part 3: Configure an 802.1Q Trunk between the Switches

Part 4: Verification

Part 1: Build the Network and Configure Basic Device Settings on both switches

Part 2: Create VLANs and Assign Switch Ports to VLANs.

Step 1: Creating VLANs on S1 by referring VLANs and ports assigning table [*Table:5*.2.3]

```
S1# configure terminal
S1(config) # vlan 2
S1(config-vlan) # name Faculty
S1(config) # exit

S1(config) # vlan 3
S1(config-vlan) # name ADMIN
S1(config) # exit

S1(config) # vlan 4
S1(config-vlan) # name Students
S1(config) # exit
```

Step 2: Assign a VLANs to multiple switch interfaces by referring VLANs and ports assigning table [*Table:5*.2.3]

a. On S1, assign interfaces F0/1 – fa 0/5 to VLAN 2.

```
S1(config)# interface range f0/1- fa 0/5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 2
S1(config-if-range)# exit
```

b. On S1, assign interfaces F0/6 – fa 0/7 to VLAN 3.

```
S1(config)# interface range f0/6- fa 0/7
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 3
S1(config-if-range)# exit
```

c. On S1, assign interfaces F0/8 – fa 0/23 to VLAN 4.

```
S1(config)# interface range f0/8- fa 0/23
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 4
S1(config-if-range)# end
```

Step 3: Creating VLANs on S2 by using VLANs assigning table

```
S2# configure terminal
S2(config) # vlan 2
S2(config-vlan) # name Faculty
S2(config) # exit

S2(config) # vlan 3
S2(config-vlan) # name ADMIN
S2(config) # exit

S2(config) # vlan 4
S2(config-vlan) # name Students
S2(config) # exit
```

Step 4: Assign VLANs to multiple switch interfaces by referring VLANs and ports assigning table [*Table:5*.2.3]

a. On S2, assign interfaces F0/1 – fa 0/4to VLAN 2.

```
S2(config)# interface range f0/1- fa 0/4
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 2
S2(config-if-range)# exit
```

b. On S2, assign interfaces F0/5 – fa 0/9 to VLAN 3.

```
S2(config)# interface range f0/5- fa 0/9
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 3
S2(config-if-range)# exit
```

c. On S2, assign interfaces F0/10 – fa 0/23to VLAN 4.

```
S2(config)# interface range f0/10- fa 0/23
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 4
S2(config-if-range)# end
```

Part 3: Configure an 802.1Q Trunk between the Switches

Step 1: configure trunk interface F0/24 on S1

```
S1 (config) # int fa 0/24
S1 (config-if) # Switchport mode trunk
S1 (config-if) # exit
```

Step 2: configure trunk interface F0/24 on S2

```
S2 (config) # int fa 0/24
S2 (config-if) # Switchport mode trunk
S2 (config-if) # exit
```

Part 4: Verifications

- Issue the **show vlan brief** command on S1 and S2. Interface F0/24 is no longer assigned to VLAN 1. Trunked interfaces are not listed in the VLAN table.

  ```
  S1# show vlan brief
  S2# show vlan brief
  ```

- Issue **show vlan brief** command on S1 and S2. It is used to verify how many VLAN exist on the switch and how many ports are assigned in different VLANs.

  ```
  S1# show vlan brief
  S2# show vlan brief
  ```

- Issue the **show interface switchport** command on both switches

Lab 5.3 – Home Activity

In the light of above experiments, Configure the following topology by using addressing table, VLAN and port assignment table.

Scenario

Suppose you are designing a small VLAN switched network for three floor of SZABIST 100 campus.

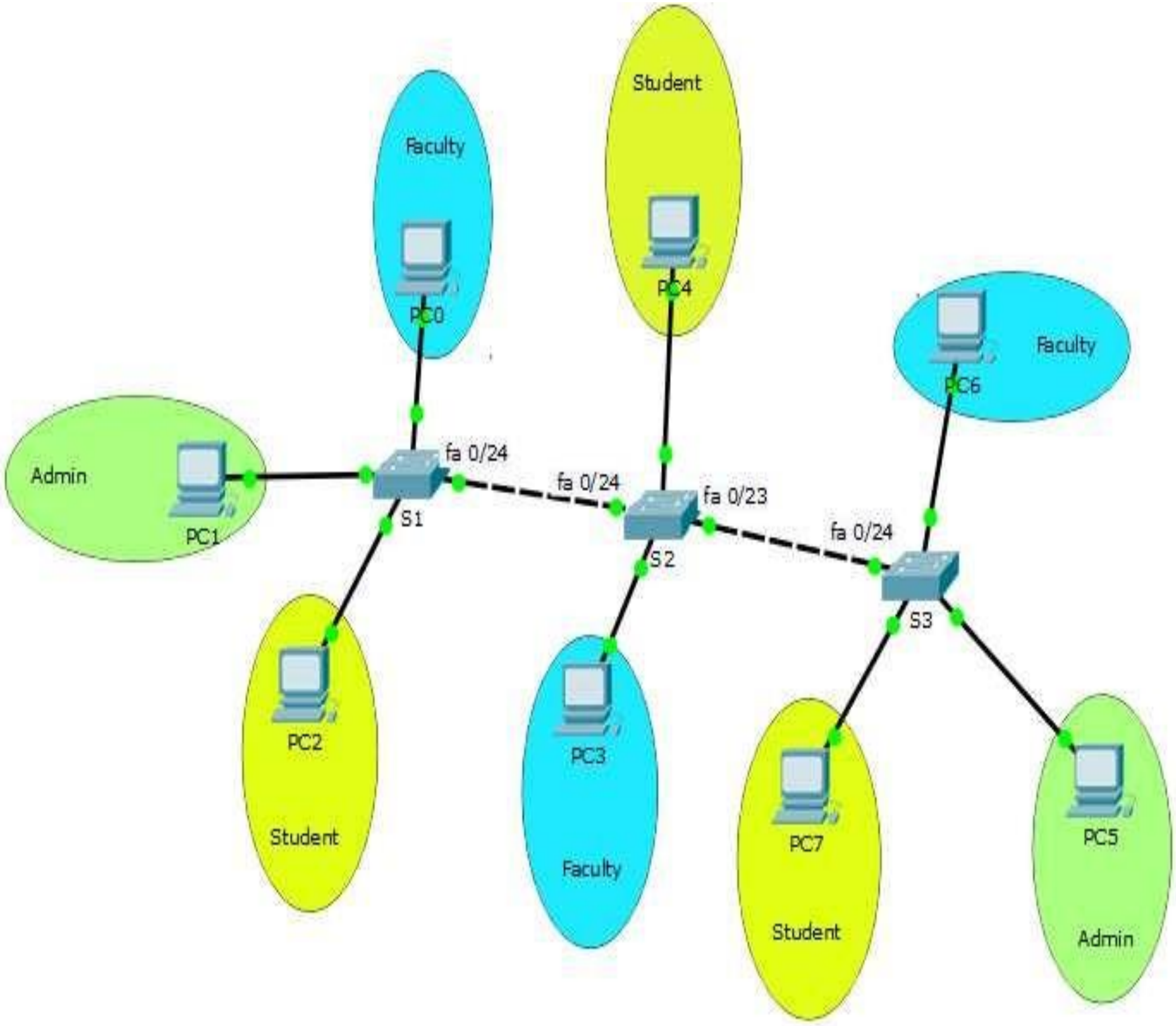


Fig:5.3.1

Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC3	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC6	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC1	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC5	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC2	NIC	192.168.3.3	255.255.255.0	192.168.3.1
PC4	NIC	192.168.3.3	255.255.255.0	192.168.3.1
PC7	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Table:5.3.1

VLANs and Ports Assigning Table:

VLANs	Name	Switchport Number			
		Access Ports		Trunk Ports	
2	Faculty	S1	fa 0/1 – fa 0/5	S1	Fast Ethernet 0/24
		S2	fa 0/18 – fa 0/22		
		S3	fa 0/18 – fa 0/23		
3	ADMIN	S1	fa 0/6 –fa 0/12	S2	Fast Ethernet 0/23 Fast Ethernet 0/24
		S2	——		
		S3	fa 0/14 – fa 0/17		
4	Students	S1	fa 0/13 – fa 0/23	S3	Fast Ethernet 0/24
		S2	fa 0/1 – fa 0/17		
		S3	fa 0/1 – fa 0/13		

Table:5.3.2

Note:

- Put the screen shot of your designed topology at the end of this experiment.
- Also attach the printout of startup configurations of each switch.

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

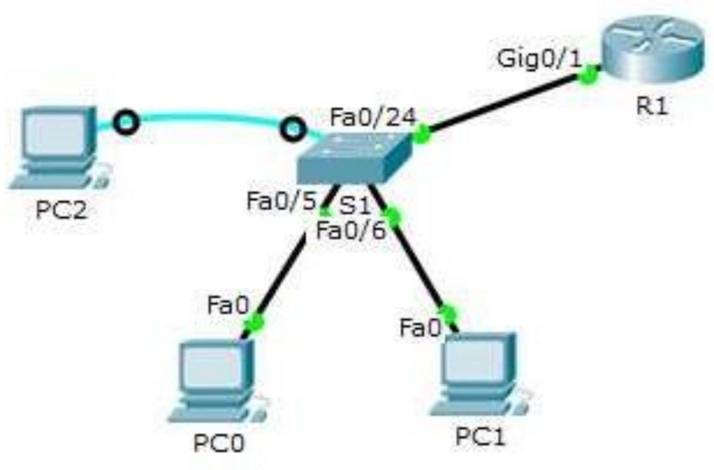
Examined By: (Instructor’s Name & Initial’s)

Date

Experiment# 06

Lab 6.1 - Security Features on Switch

Topology:



Objectives:

Part 1: Configure general security features on S1.

Part 2: Configure and verify port security on S1.

Configure and Verify Security Features on S1

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

Note: To implementing security features on S1, please make sure that you should be established a console session or configure security features through console cable.

Step 1: Configure general security features on S1.

a. Configure a message of the day (MOTD) banner on S1 with an appropriate security warning message.

b. Issue a **show ip interface brief** command on S1. What physical ports are up?

____

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

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

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

____

Step 2: Configure and verify port security on S1.

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

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

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

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

F0/5 MAC address: ____

F0/6 MAC address: ____

c. Configure basic port security.

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

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

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

2) Shut down the port.

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

3) Enable the switch port.

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

4) Enable port security on F0/5.

```
S1 (config) # int fa 0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 1
S1(config-if)# switchport port-security mac-address 0060.47ed.4873
S1(config-if)# switchport port-security violation shut down
OR
S1(config-if)# switchport port-security violation protect
OR
S1(config-if)# switchport port-security violation Restrict
```

Note:

- Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.
- There are three different modes of violation in terms of switch port security
    1. **Shutdown:** port will be administratively shutdown because of security violation.
    2. **Protect:** Port remains active after security violation occur but ignore that rogue MAC-Address
    3. **Restrict:** Port remains active after security violation occur but ignore that rogue MAC-Address and copy the information to the network monitoring system.

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

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

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

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

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

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      1
Total MAC Addresses        1
Configured MAC Addresses   1
Sticky MAC Addresses       0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count   0
```

What is the port status of F0/5? ____________________________

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

```
R1# ping 172.16.99.3
```

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

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

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

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

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

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

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

____

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

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)       (Count)        (Count)
-------------------------------------------
     Fa0/5         1          1               1        Shutdown
---------------------------------------------
Total Addresses in System (excluding one mac per port)      :0
Max Addresses limit in System (excluding one mac per port) :8192
```

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
```

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

```
S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

```
S1# show port-security address
               Secure Mac Address Table
-----------------------------------------------
Vlan    Mac Address      Type              Ports    Remaining Age
                                                (mins)
---    --------      ---              ----  ---------
  99    30f7.0da3.1821   SecureConfigured    Fa0/5       -
-----------------------------------------------
Total Addresses in System (excluding one mac per port)      :0
Max Addresses limit in System (excluding one mac per port) :8192
```

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

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

l. From R1, ping PC-A again at 172.16.99.3. Was the ping successful? ___________________

m. On the Switch, issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

____

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

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

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

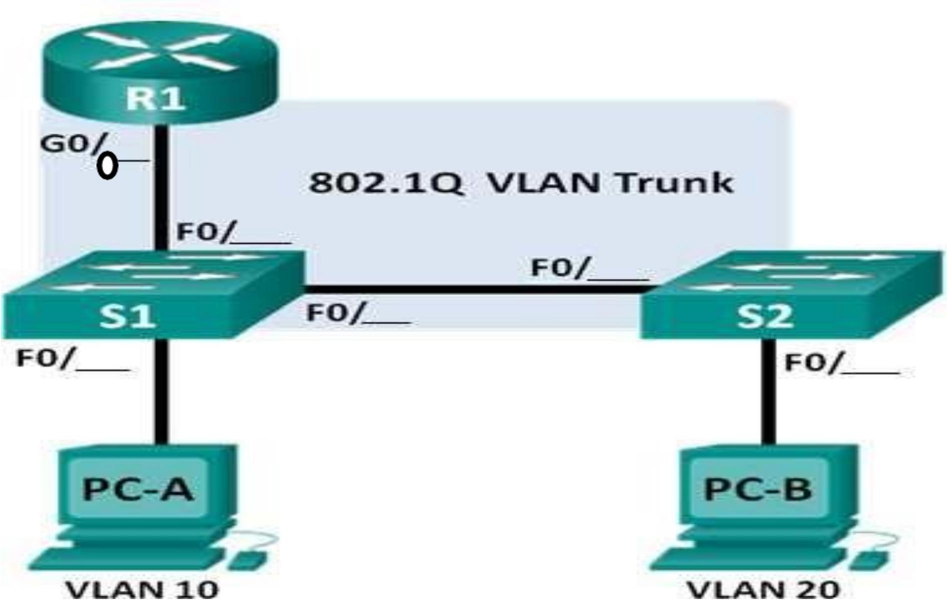
o. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

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

Lab 6.2– Configuring 802.1Q Trunk-Based Inter-VLAN Routing

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0.1	192.168.1.1	255.255.255.0	N/A
	G0/0.10	192.168.10.1	255.255.255.0	N/A
	G0/0.20	192.168.20.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Table: 6.2.1

Switch Port Assignment Specifications

Ports	Assignment	Network
S1 F0/_____	802.1Q Trunk	N/A
S2 F0/_____	802.1Q Trunk	N/A
S1 F0/_____	802.1Q Trunk	N/A
S1 F0/_____	VLAN 10 – Students	192.168.10.0/24
S2 F0/_____	VLAN 20 – Faculty	192.168.20.0/24

Table: 6.2.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Switches with VLANs and Trunking

Part 3: Configure Trunk-Based Inter-VLAN Routing

Background / Scenario

A second method of providing routing and connectivity for multiple VLANs is through the use of an 802.1Q trunk between one or more switches and a single router interface. This method is also known as router-on-a-stick inter-VLAN routing. In this method, the physical router interface is divided into multiple subinterfaces that provide logical pathways to all VLANs connected.

In this lab, you will configure trunk-based inter-VLAN routing and verify connectivity to hosts on different VLANs as well as with a loopback on the router.

Note: This lab provides minimal assistance with the actual commands necessary to configure trunk-based inter-VLAN routing. However, the required configuration commands are provided in Appendix A of this lab. Test your knowledge by trying to configure the devices without referring to the appendix.

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

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

Required Resources

- 1 Router
- 2 Switches
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

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

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the router and switches as necessary.

Step 4: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure device names as shown in the topology.

c. Assign **class** as the privileged EXEC password.

d. Assign **cisco** as the console and vty passwords.

e. Configure **logging synchronous** for the console line.

f. Configure the IP address listed in the Addressing Table for VLAN 1 on both switches.

g. Configure the default gateway on both switches.

h. Administratively deactivate all unused ports on the switch.

i. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for the router.

a. Disable DNS lookup.

b. Configure device names as shown in the topology.

c. Configure the Lo0 IP address as shown in the Address Table. Do not configure subinterfaces at this time as they will be configured in Part 3.

d. Assign **cisco** as the console and vty passwords.

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

f. Configure **logging synchronous** to prevent console messages from interrupting command entry.

g. Copy the running configuration to the startup configuration.

Part 2: Configure Switches with VLANs and Trunking

In Part 2, you will configure the switches with VLANs and trunking.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure S1 and S2 without referring to the appendix.

Step 1: Configure VLANs on S1.

a. On S1, configure the VLANs and names listed in the Switch Port Assignment Specifications table. Write the commands you used in the space provided.

____

____

____

____

____

b. On S1, configure the interface connected to R1 as a trunk. Also configure the interface connected to S2 as a trunk. Write the commands you used in the space provided.

____

____

____

____

c. On S1, assign the access port for PC-A to VLAN 10. Write the commands you used in the space provided.

____

____

____

Step 2: Configure VLANs on Switch 2.

a. On S2, configure the VLANs and names listed in the Switch Port Assignment Specifications table.

b. On S2, verify that the VLAN names and numbers match those on S1. Write the command you used in the space provided.

____

c. On S2, assign the access port for PC-B to VLAN 20.

d. On S2, configure the interface connected to S1 as a trunk.

Part 3: Configure Trunk-Based Inter-VLAN Routing

In Part 3, you will configure R1 to route to multiple VLANs by creating subinterfaces for each VLAN. This method of inter-VLAN routing is called router-on-a-stick.

Note: The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure trunk-based or router-on-a-stick inter-VLAN routing without referring to the appendix.

Step 1: Configure a subinterface for VLAN 1.

a. Create a subinterface on R1 G0/1 for VLAN 1 using 1 as the subinterface ID. Write the command you used in the space provided.

____

b. Configure the subinterface to operate on VLAN 1. Write the command you used in the space provided.

____

c. Configure the subinterface with the IP address from the Address Table. Write the command you used in the space provided.

____

Step 2: Configure a subinterface for VLAN 10.

a. Create a subinterface on R1 G0/1 for VLAN 10 using 10 as the subinterface ID.

b. Configure the subinterface to operate on VLAN 10.

c. Configure the subinterface with the address from the Address Table.

Step 3: Configure a subinterface for VLAN 20.

a. Create a subinterface on R1 G0/1 for VLAN 20 using 20 as the subinterface ID.

b. Configure the subinterface to operate on VLAN 20.

c. Configure the subinterface with the address from the Address Table.

Step 4: Enable the G0/0 interface.

Enable the G0/0 interface. Write the commands you used in the space provided.

____

____

Step 5: Verify connectivity.

Enter the command to view the routing table on R1. What networks are listed?

____

From PC-A, is it possible to ping the default gateway for VLAN 10? ______________

From PC-A, is it possible to ping PC-B? ______________

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

From PC-A, is it possible to ping S2? ______________

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

Reflection

What are the advantages of trunk-based or router-on-a-stick inter-VLAN routing?

____

____

Appendix A – Configuration Commands

Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
S1(config)# interface f0/___
S1(config-if)# switchport mode trunk
S1(config-if)# exit
S1(config)# interface f0/___
S1(config-if)# switchport mode trunk
S1(config-if)# exit
S1(config)# interface f0/___
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
```

Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name Students
S2(config-vlan)# vlan 20
S2(config-vlan)# name Faculty
S2(config-vlan)# exit
S2(config)# interface f0/____
S2(config-if)# switchport mode trunk
S2(config-if)# exit
S2(config)# interface f0/____
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# exit
```

Router R1

```
R1(config)# interface g0/0
R1(config-if)# no ip address
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/0.1
R1(config-subif)# encapsulation dot1Q 1
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
R1(config-subif)# exit
R1(config)#interface g0/0.2
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/0.3
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
```

Lab 6.3 – Home Activity

In the light of above experiments, Configure the following topology by using addressing table, VLAN and port assignment table. Also implement the port security features on all the switch ports.

Scenario

Suppose you are designing a small VLAN switched network with inter VLAN routing for three floors of SZABIST 100 campus.

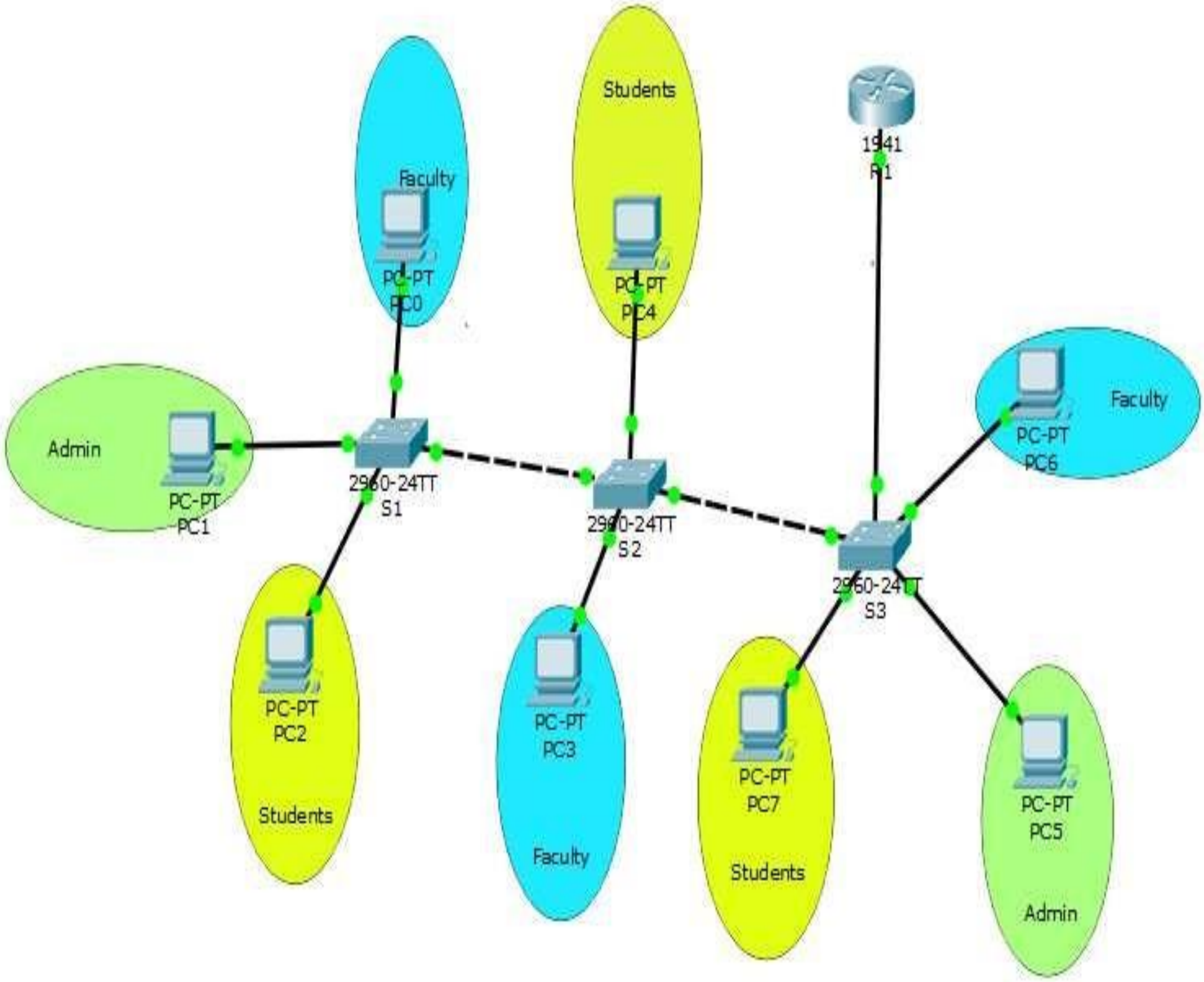


Fig:6.3.1

Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC3	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC6	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC1	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC5	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC2	NIC	192.168.3.3	255.255.255.0	192.168.3.1
PC4	NIC	192.168.3.3	255.255.255.0	192.168.3.1
PC7	NIC	192.168.3.3	255.255.255.0	192.168.3.1
R1	G0/0.1	192.168.1.1	255.255.255.0	N/A
	G0/0.2	192.168.2.1	255.255.255.0	N/A
	G0/0.3	192.168.3.1	255.255.255.0	N/A

Table:6.3.1

VLANs and Ports Assigning Table:

VLANs	Name	Switchport Number			
		Access Ports		Trunk Ports	
2	Faculty	S1	fa 0/1 – fa 0/5	S1	Fast Ethernet 0/24
		S2	fa 0/18 – fa 0/22		
		S3	fa 0/18 – fa 0/23		
3	ADMIN	S1	fa 0/6 –fa 0/12	S2	Fast Ethernet 0/23 Fast Ethernet 0/24
		S2	—		
		S3	fa 0/14 – fa 0/17		
4	Students	S1	fa 0/13 – fa 0/23	S3	Fast Ethernet 0/24
		S2	fa 0/1 – fa 0/17		
		S3	fa 0/1 – fa 0/13		

Table:6.3.2

Note:

- Put the screen shot of your designed topology at the end of this experiment.
- Also attach the screen shots of startup configurations of each network devices.

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	**Student’s Behavior**	**2.5**	
2	**Lab Performance**	**2.5**	
3	**On Time Submission**	**5**	
4	**Home Activity**	**10**	
	Net Result	**20**	

Examined By: (Instructor’s Name & Initial’s)

Date

Experiment# 07

Lab 7.1 - Configuring IPv4 Static and Default Routes

Topology

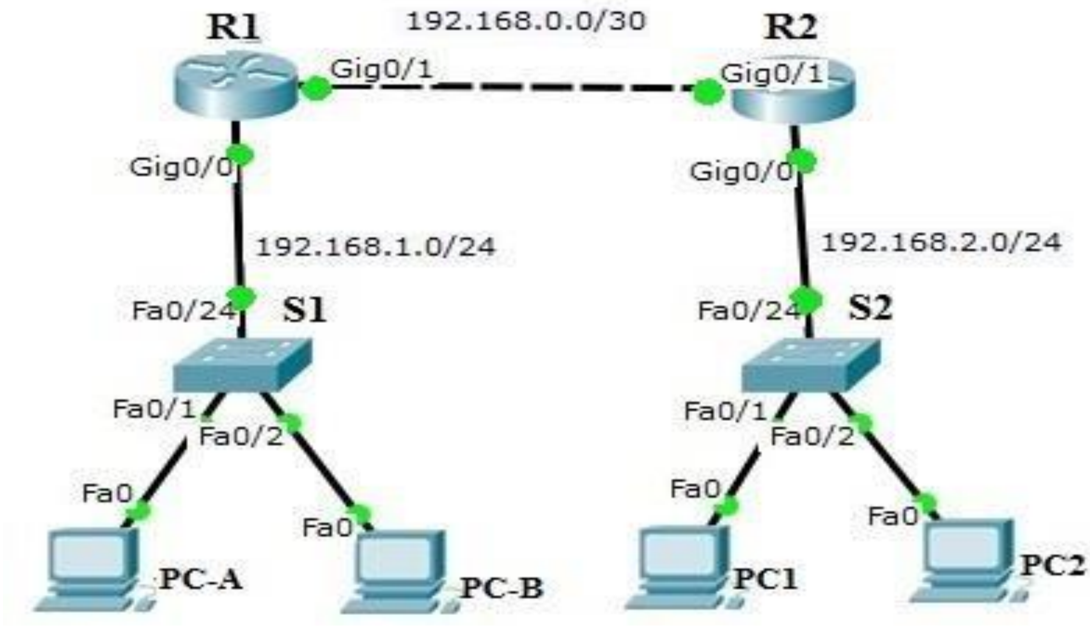


Figure: 7.1.1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.0.1	255.255.255.252	N/A
R1	G0/0	192.168.1.1	255.255.255.0	N/A
R2	G0/1	192.168.0.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.2.2	255.255.255.0	192.168.2.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC1	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC2	NIC	192.168.2.4	255.255.255.0	192.168.2.1

Table: 7.1.1

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

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

Required Resources

- 3 Routers (1914,1914 and 2911)
- 3 Switches (2960)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

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

Step 2: Initialize and reload the router and switch.

Part 2: 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.

Step 1: Configure the PC interfaces.

Step 2: Configure basic settings on the routers.

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

b. Disable DNS lookup.

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

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

Step 3: Configure IP settings on the routers.

a. Configure the R1, R2 and R3 interfaces with IP addresses according to the Addressing Table.

b. The R1 G0/0 configuration is displayed below.

```
R1(config)# interface G 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

c. The R2 G0/0 configuration is displayed below.

```
R2(config)# interface G 0/0
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

Step 4: 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 PC1, is it possible to ping the default gateway? ___________

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

From R1, is it possible to ping the G0/1 interface of R3? ___________

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

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

From PC-A, is it possible to ping PC1? ___________

Step 5: 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? ___________

b. Check the status of the interfaces on R2.

How many interfaces are activated on R2? ___________

c. 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?

____

d. View the routing table information for R2.

What networks are present in the Addressing Table in this lab, but not in the routing table for R2?

____

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

____

____

Part 3: 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.

Step 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*

Step 2: 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*

Step 3: Configure a static route.

a. On the R1 router, configure a static route to the 198.168.2.0 network using one of the static route configuration options from the previous steps. Write the command you used in the space provided.

____

b. On the R2 router, configure a static route to the 192.168.1.0 network using the other static route configuration option from the previous steps. Write the command you used in the space provided.

____

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

How is this new route listed in the routing table?

____

d. From host PC-A, is it possible to ping the R2 address 192.168.2.3? __________

This ping should be successful.

Part 4: 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.

Reflection

1. A new network 192.168.3.0/24 is connected to interface G0/2 on R1. What commands could be used to configure a static route to that network from R2?

____

____

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

____

____

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

____

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.

Basic Device Settings

Configure IP settings on the router.

a. The R1 G0/0 configuration is displayed below.

```
R1(config)# interface G 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

b. The R1 G0/1 configuration is displayed below.

```
R1(config)# interface G 0/1
R1(config-if)# ip address 192.168.0.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
```

c. The R2 G0/0 configuration is displayed below.

```
R2(config)# interface G 0/0
R2(config-if)# ip address 192.168.2.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

d. The R2 G0/1 configuration is displayed below.

```
R2(config)# interface G 0/1
R2(config-if)# ip address 192.168.0.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
```

Static Route Configurations

a. On Router 1

```
R1 (config) # ip route 192.168.2.0 255.255.255.0 192.168.0.2
```

b. On Router 2

```
R2 (config) # ip route 192.168.1.0 255.255.255.0 192.168.0.1
```

Lab 7.2 - Configuring IPv4 Static Routes

Topology

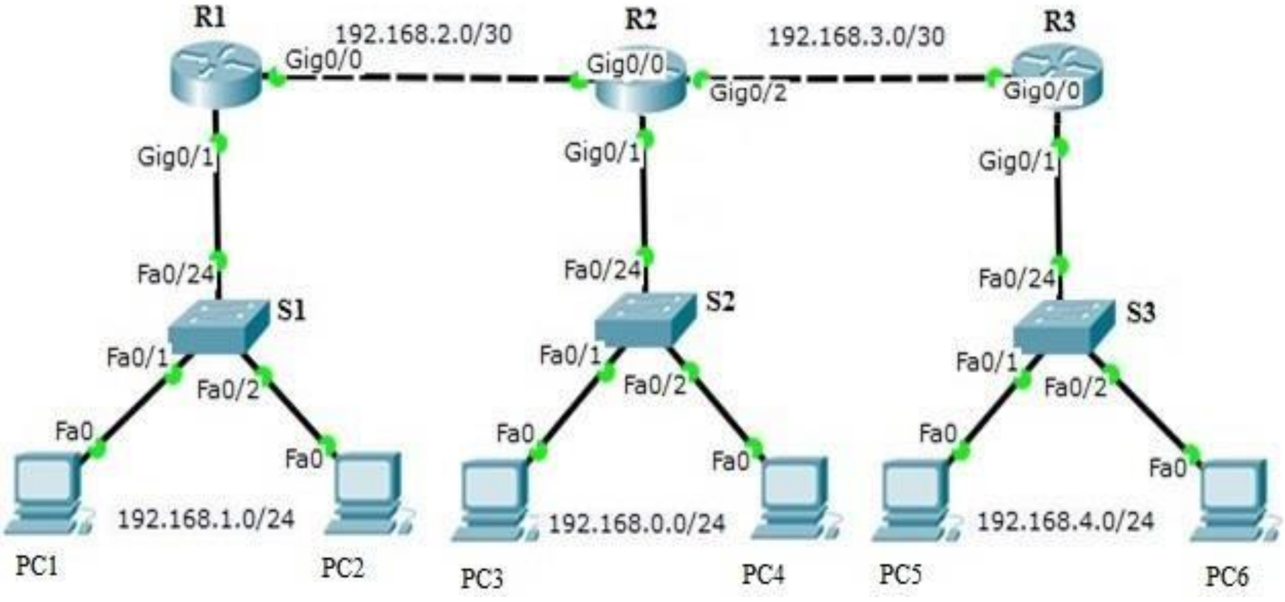


Figure: 7.2.1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.0.1	255.255.255.0	N/A
R1	G0/0	192.168.2.1	255.255.255.252	N/A
R2	G0/2	192.168.3.1	255.255.255.252	N/A
R2	G0/1	192.168.0.1	255.255.255.0	N/A
R2	G0/0	192.168.2.2	255.255.255.252	N/A
R3	G0/0	192.168.3.2	255.255.255.252	N/A
R3	G0/1	192.168.4.1	255.255.255.0	N/A
PC1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC3	NIC	192.168.0.3	255.255.255.0	192.168.0.1
PC4	NIC	192.168.0.4	255.255.255.0	192.168.0.1
PC5	NIC	192.168.4.3	255.255.255.0	192.168.4.1
PC6	NIC	192.168.4.4	255.255.255.0	192.168.4.1

Table: 7.2.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure Static Routes

Required Resources

- 3 Routers (1914,1914 and 2911)
- 3 Switches (2960)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

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

Step 2: Initialize and reload the router and switch.

Part 2: 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.

Step 1: Configure the PC interfaces.

Step 2: Configure basic settings on the routers.

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

b. Disable DNS lookup.

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

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

Step 3: Configure IP settings on the routers.

a. Configure the R1, R2 and R3 interfaces with IP addresses according to the Addressing Table.

Step 4: Verify connectivity of the LANs.

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

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

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

Step 5: Gather information.

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

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

c. View the routing table information for R2 and R3.

Part 3: Configure Static Routes

Appendix A: Configuration Commands

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

Basic Device Settings

Configure IP settings on the routers.

a. The R1 G0/0 configuration is displayed below.

```
R1(config)# interface G 0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
```

b. The R1 G0/1 configuration is displayed below.

```
R1(config)# interface G 0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

c. The R2 G0/0 configuration is displayed below.

```
R2(config)# interface G 0/0
R2(config-if)# ip address 192.168.2.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
```

d. The R2 G0/1 configuration is displayed below.

```
R2(config)# interface G 0/1
R2(config-if)# ip address 192.168.0.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
```

e. The R2 G0/2 configuration is displayed below.

```
R2(config)# interface G 0/2
R2(config-if)# ip address 192.168.3.1 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
```

f. The R3 G0/0 configuration is displayed below.

```
R3(config)# interface G 0/0
R3(config-if)# ip address 192.168.3.2 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
```

g. The R3 G0/1 configuration is displayed below.

```
R3(config)# interface G 0/1
R3(config-if)# ip address 192.168.4.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
```

Static Route Configurations

a. On Router 1

   R1 (config) # **ip route 192.168.0.0 255.255.255.0 192.168.2.2**

   R1 (config) # **ip route 192.168.3.0 255.255.255.252 192.168.2.2**

   R1 (config) # **ip route 192.168.4.0 255.255.255.0 192.168.2.2**

b. On Router 2

   R2 (config) # **ip route 192.168.1.0 255.255.255.0 192.168.2.1**

   R2 (config) # **ip route 192.168.4.0 255.255.255.0 192.168.3.2**

c. On Router 3

   R3 (config) # **ip route 192.168.0.0 255.255.255.0 192.168.3.1**

   R3 (config) # **ip route 192.168.2.0 255.255.255.252 192.168.3.1**

   R3 (config) # **ip route 192.168.1.0 255.255.255.0 192.168.3.1**

Lab 7.3: Home Activity

Topology:

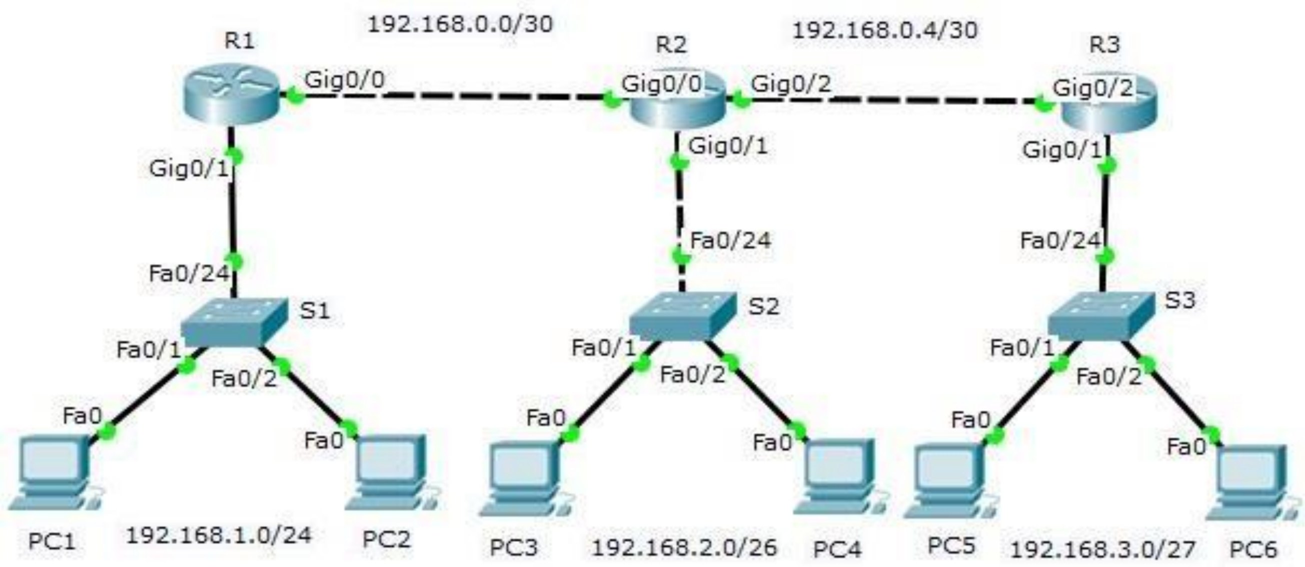


Figure:7.3.1

Addressing Table:

Fill the addressing table as shown in the topology

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1			N/A
R1	G0/0			N/A
R2	G0/2			N/A
R2	G0/1			N/A
R2	G0/0			N/A
R3	G0/0			N/A
R3	G0/1			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			
PC5	NIC			
PC6	NIC			

Table:7.3.1

Note:

- **Put the screen shot of your designed topology at the end of this experiment.**
- **Also attach the printout of startup configurations of each switch.**

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#8

Lab 8.1.1– Configuring Basic RIP

Topology:

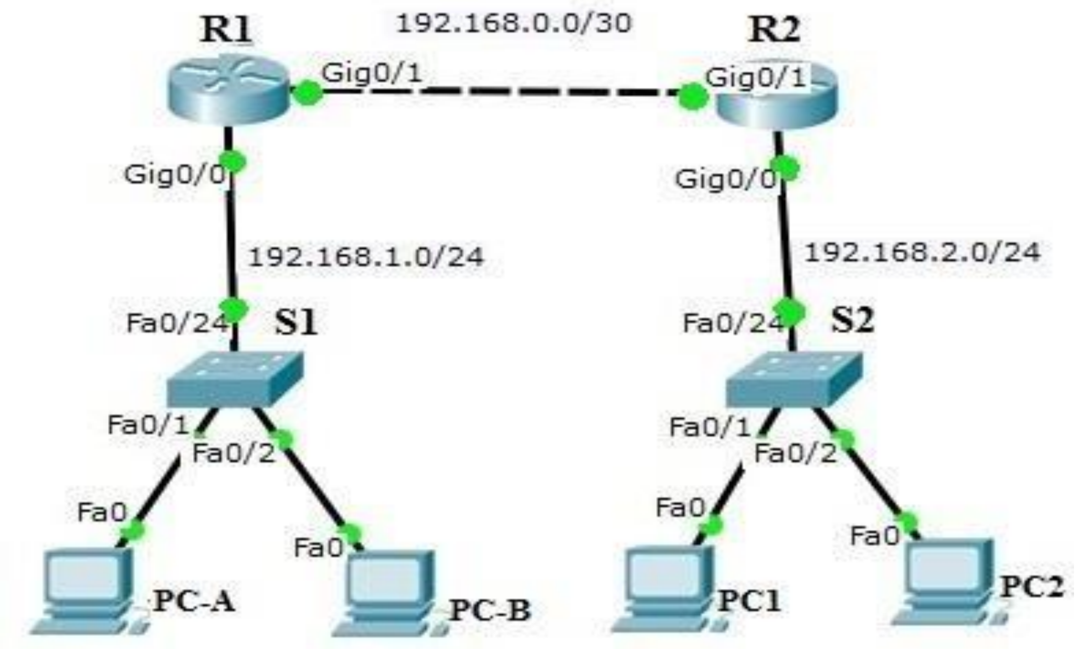


Figure: 8.1.1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.0.1	255.255.255.252	N/A
R1	G0/0	192.168.1.1	255.255.255.0	N/A
R2	G0/1	192.168.0.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC1	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC2	NIC	192.168.2.4	255.255.255.0	192.168.2.1

Table: 8.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify RIP Routing

- Configure and verify RIP is running on routers.
- Configure a passive interface.
- Examine routing tables.
- Disable automatic summarization.
- Configure a default route.
- Verify end-to-end connectivity.

Part 4: Configure and Verify RIPng Routing

- Configure and verify RIPng is running on routers.
- Examine routing tables.
- Configure a default route.
- Verify end-to-end connectivity.

Background / Scenario

RIP version 2 (RIPv2) is used for routing of IPv4 addresses in small networks. RIPv2 is a classless, distance-vector routing protocol, as defined by RFC 1723. Because RIPv2 is a classless routing protocol, subnet masks are included in the routing updates. By default, RIPv2 automatically summarizes networks at major network boundaries. When automatic summarization has been disabled, RIPv2 no longer summarizes networks to their classful address at boundary routers.

RIPng (RIP Next Generation) is a distance-vector routing protocol for routing IPv6 addresses, as defined by RFC 2080. RIPng is based on RIPv2 and has the same administrative distance and 15-hop limitation.

In this lab, you will configure the network topology with RIPv2 routing, disable automatic summarization, propagate a default route, and use CLI commands to display and verify RIP routing information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services. The switches used are Cisco Catalyst 2960s). 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.

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

Required Resources

- 2 Routers (Cisco 1941 or 2900)
- 2 Switches (Cisco 2960)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

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

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

Step 2: Initialize and reload the router and switch.

Step 3: Configure basic settings for each router and switch.

a. Disable DNS lookup.

b. Configure device names as shown in the topology.

c. Configure password encryption.

d. Assign **class** as the privileged EXEC password.

e. Assign **cisco** as the console and vty passwords.

f. Configure a MOTD banner to warn users that unauthorized access is prohibited.

g. Configure the IP address listed in the Addressing Table for all interfaces.

h. Configure a description to each interface with an IP address..

i. Copy the running-configuration to the startup-configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

At this point, the PCs are unable to ping each other.

a. Each workstation should be able to ping the attached router. Verify and troubleshoot if necessary.

b. The routers should be able to ping one another. Verify and troubleshoot if necessary.

Part 2: Configure and Verify RIP Routing

In Part 2, you will configure RIP routing on all routers in the network and then verify that routing tables are updated correctly. After RIP has been verified, you will disable automatic summarization, configure a default route, and verify end-to-end connectivity.

Step 1: Configure RIP routing.

a. On R1, configure RIP as the routing protocol and advertise the appropriate networks.

```
R1# config t
R1(config)# router rip
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.0.0
R1(config-router)# passive-interface g0/1
```

The **passive-interface** command stops routing updates out the specified interface. This process prevents unnecessary routing traffic on the LAN. However, the network that the specified interface belongs to is still advertised in routing updates that are sent out across other interfaces.

b. Configure RIP on R2 and use the **network** statement to add appropriate networks and prevent routing updates on the LAN interface.

Step 2: Examine current state of network.

a. The status of the two links can quickly be verified using the **show ip interface brief** command on R1.

R1# **show ip interface brief**

```
Interface            IP-Address      OK? Method Status            Protocol
GigabitEthernet0/0       192.168.0.1   YES manual up                 up
GigabitEthernet0/1       192.168.1.1   YES manual up                 up
```

b. Check connectivity between PCs.

From PC-A, is it possible to ping PC-B?__________Why?_______________________________________

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

From PC-C, is it possible to ping PC-B?__________Why?_______________________________________

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

c. Verify that RIP is running on the routers.

You can use the **debug ip rip**, **show ip protocols**, and **show run** commands to confirm that RIPv2 is running. The **show ip protocols** command output for R1 is shown below.

R1# **show ip protocols**

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 23 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface            Send Recv Triggered RIP Key-chain
  GigabitEthernet0/1    1     2 1
  GigabitEthernet0/0    1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
        192.168.0.0
        192.168.1.0
Passive Interface(s):
Routing Information Sources:
        Gateway        Distance     Last Update
        192.168.0.2         120      00:00:13
Distance: (default is 120)
```

When issuing the **debug ip rip** command on R2, what information is provided that confirms RIP is running?

____

When you are finished observing the debugging outputs, issue the **undebug all** command at the privileged EXEC prompt.

d. Examine the automatic summarization of routes.

The LANs connected to R1 and R2 are composed of discontiguous networks..

R1# **show ip route**

```
R   192.168.0.0/24 [120/1] via 192.168.2.2, 00:00:23, GigabitEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.0.1/24 is directly connected, GigabitEthernet0/1
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/30 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
R   192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:23, GigabitEthernet0/0R3 only displays its own subnets for the
172.30.0.0 network. R3 does not have any routes for the 172.30.0.0 subnets on R1.
```

R2# **show ip route**

<Output omitted>

R2# **show ip route**

```
Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/30 is directly connected, GigabitEthernet0/0
L       192.168.0.2/32 is directly connected, GigabitEthernet0/0
R   192.168.1.0/24 [120/1] via 192.168.0.1, 00:00:01, GigabitEthernet0/0
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.1/32 is directly connected, GigabitEthernet0/1R3# show ip route
```

e. Use the **debug ip rip** command on R2 to exam the RIP updates.

R2# debug ip rip

After 60 seconds, issue the **no debug ip rip** command.

What routes are in the RIP updates that are received from R3?

____

Are the subnet masks now included in the routing updates? _________

Appendix A – Configuration Commands

Router R1

```
R1(config)# interface g0/0
R1(config-if)#  ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-subif)# ip address 192.168.0.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-subif)# exit

R1(config)# router rip
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.0.0
```

Router R2

```
R1(config)# interface g0/0
R1(config-if)#  ip address 192.168.2. 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-subif)# ip address 192.168.0.2 255.255.255.252
R1(config-if)# no shutdown
R1(config-subif)# exit

R1(config)# router rip
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.2.0
```

Lab 8.2– Home Activity for Configuring Basic RIP

Topology:

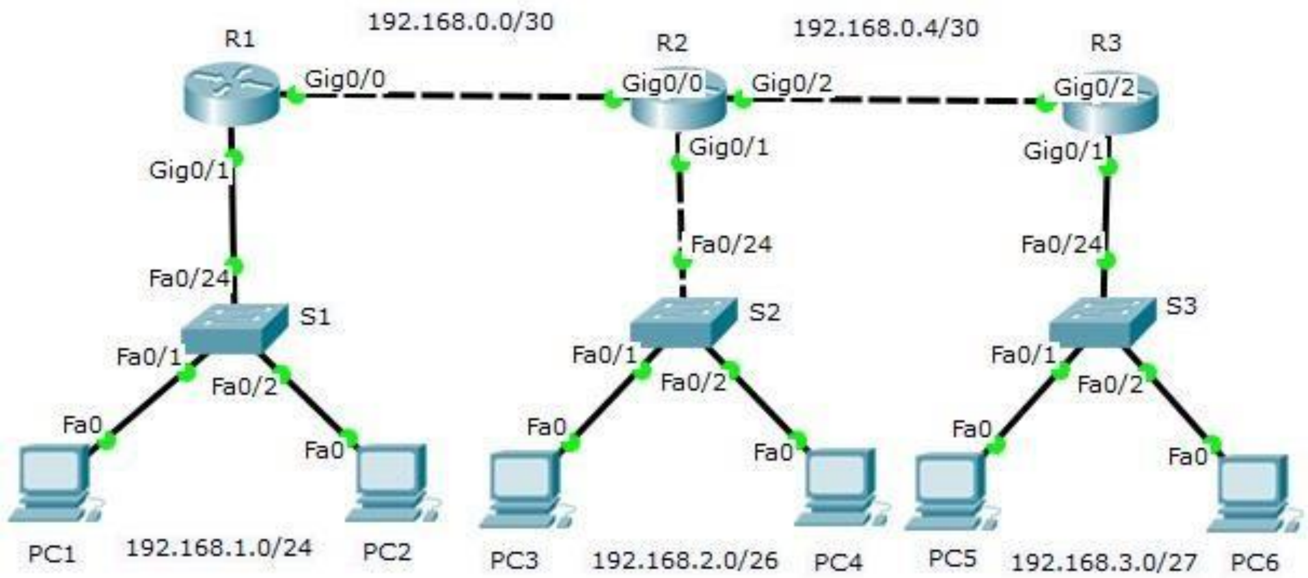


Figure:8.2.1

Addressing Table:

Fill the addressing table as shown in the topology

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1			N/A
R1	G0/0			N/A
R2	G0/2			N/A
R2	G0/1			N/A
R2	G0/0			N/A
R3	G0/2			N/A
R3	G0/1			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			
PC5	NIC			
PC6	NIC			

Table:8.2.1

Note:

- **Put the screen shot of your designed topology at the end of this experiment.**
- **Also attach the printout of startup configurations, protocol information (#show ip protocol) and routing table of each router.**

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#9

Lab 9.1- Configuring Single-Area OSPF

Topology

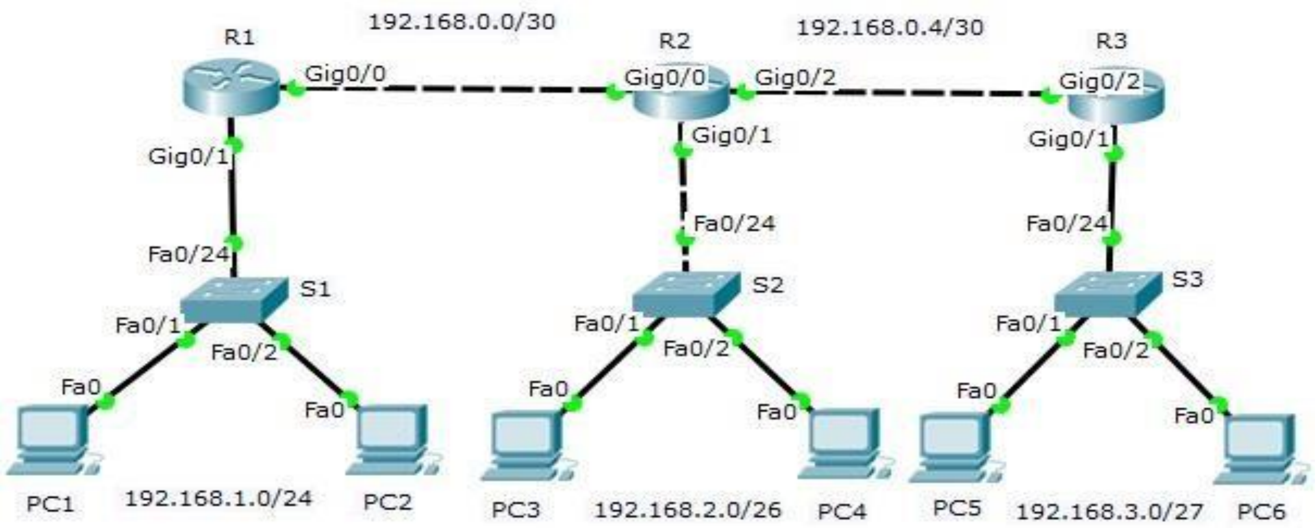


figure: 9.1.1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.252	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
R2	G0/0	192.168.1.2	255.255.255.252	N/A
	G0/1	192.168.2.1	255.255.255.0	N/A
	G0/2	192.168.0.5	255.255.255.252	N/A
R3	G0/2	192.168.0.6	255.255.255.252	N/A
	G0/1	192.168.3.1	255.255.255.252	N/A
PC1	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC3	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC4	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC5	NIC	192.168.3.2	255.255.255.0	192.168.3.1
PC6	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Table:9.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify OSPF Routing

Background / Scenario

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. OSPFv2 is defined for IPv4 networks. OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure very quickly. It computes each route using Dijkstra's algorithm, a shortest path first algorithm.

In this lab, you will configure the network topology with OSPFv2 routing and use a number of CLI commands to display and verify OSPF routing information.

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

Required Resources

- 3 Routers (Cisco 2911)
- 6 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you set up the network topology and configure basic settings on the PC hosts and routers.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure device name as shown in the topology.

c. Assign **class** as the privileged EXEC password.

d. Assign **cisco** as the console and vty passwords.

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

f. Configure the IP address listed in the Addressing Table for all interfaces.

g. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Step 5: Test connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs are unable to ping other PCs until OSPF routing is configured. Verify and troubleshoot if necessary.

Part 2: Configure and Verify OSPF Routing

In Part 2, you will configure OSPF routing on all routers in the network and then verify that routing tables are updated correctly. After OSPF has been verified, you will configure OSPF authentication on the links for added security.

Step 1: Configure OSPF on R1,R2 and R3.

a. Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1(config)# router ospf 1
```

Note: The OSPF process id is kept locally and has no meaning to other routers on the network.

b. Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0  0.0.0.255 area 0
R1(config-router)# network 192.168.0.0  0.0.0.3 area 0
```

c. Configure the **network** statements for the networks on R2. Use an area ID of 0.

```
R2(config)# router ospf 1
R2(config-router)# network 192.168.2.0  0.0.0.63 area 0
R2(config-router)# network 192.168.0.0  0.0.0.3 area 0
R2(config-router)# network 192.168.0.4  0.0.0.3 area 0
```

d. Configure the **network** statements for the networks on R3. Use an area ID of 0.

```
R3(config)# router ospf 1
R3(config-router)# network 192.168.3.0  0.0.0.31 area 0
R3(config-router)# network 192.168.0.4  0.0.0.3 area 0
```

Step 2: Verify OSPF neighbors and routing information.

a. Issue the **show ip ospf neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip ospf neighbor
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
```

Step 3: Verify OSPF protocol settings.

The **show ip protocols** command is a quick way to verify vital OSPF configuration information. This information includes the OSPF process ID, the router ID, networks the router is advertising, the neighbors the router is receiving updates from, and the default administrative distance, which is 110 for OSPF.

```
R1# show ip protocols
```

Step 4: Verify OSPF process information.

Use the **show ip ospf** command to examine the OSPF process ID and router ID. This command displays the OSPF area information, as well as the last time the SPF algorithm was calculated.

```
R1# show ip ospf
```

Step 5: Verify OSPF interface settings.

a. Issue the **show ip ospf interface brief** command to display a summary of OSPF-enabled interfaces.

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

b. For a more detailed list of every OSPF-enabled interface, issue the **show ip ospf interface** command.

```
R1# show ip ospf interface
```

Step 6: Verify end-to-end connectivity.

Each PC should be able to ping the other PCs in the topology. Verify and troubleshoot if necessary.

Lab 9.2– Home Activity for Configuring Single area OSPF

Topology:

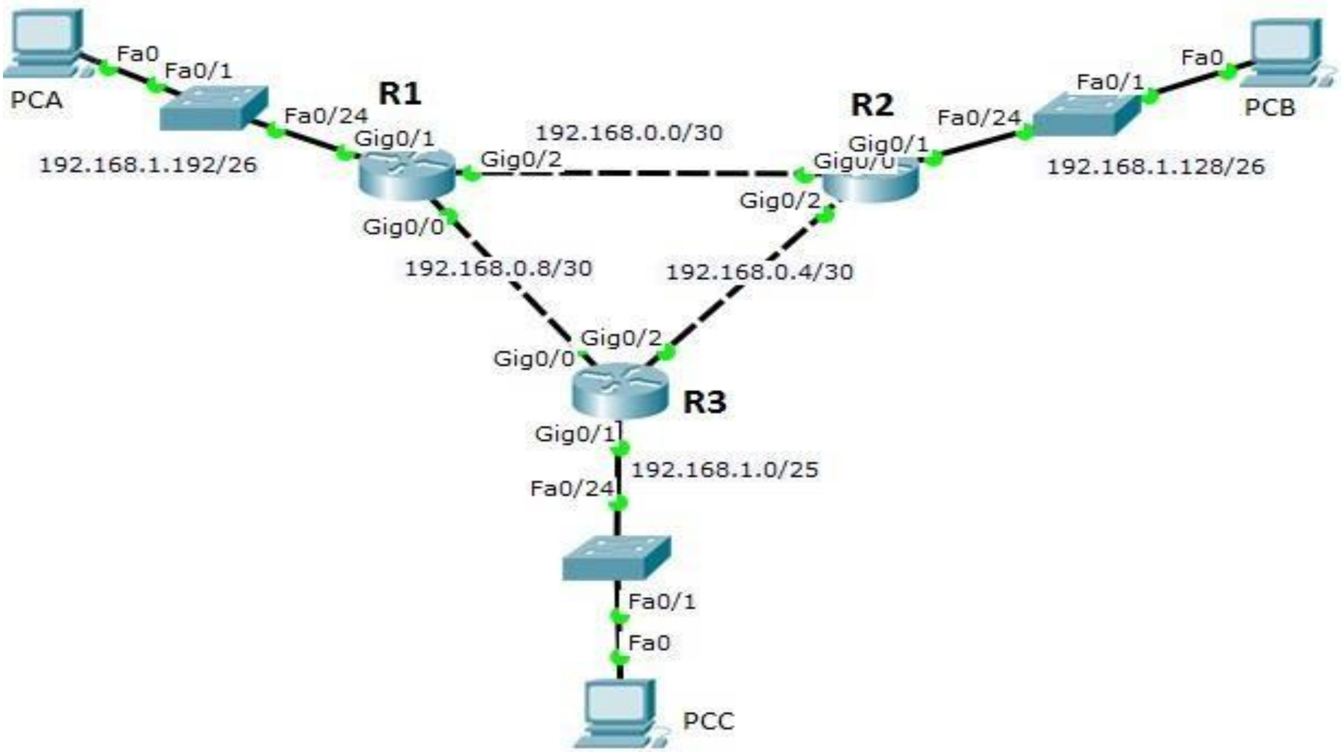


Figure: 9.2.1

Addressing Table:

Fill the addressing table as shown in the topology

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0			N/A
R1	G0/1			N/A
R1	G0/2			N/A
R2	G0/0			N/A
R2	G0/1			N/A
R2	G0/2			N/A
R3	G0/0			N/A
R3	G0/1			N/A
R3	G0/2			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			

Note:

- **Put the screen shot of your designed topology at the end of this experiment.**
- **Also attach the printout of startup configurations, protocol information (#show ip protocol), interface information (#show ip interface brief), neighboring information (show ip ospf neighbor) and routing table of each router.**

SHAHEED ZULFIKAR ALI BHUTTO
INSTITUTE OF SCIENCE AND TECHNOLOGY

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#10

Lab 10.1- Configuring Basic EIGRP

Topology

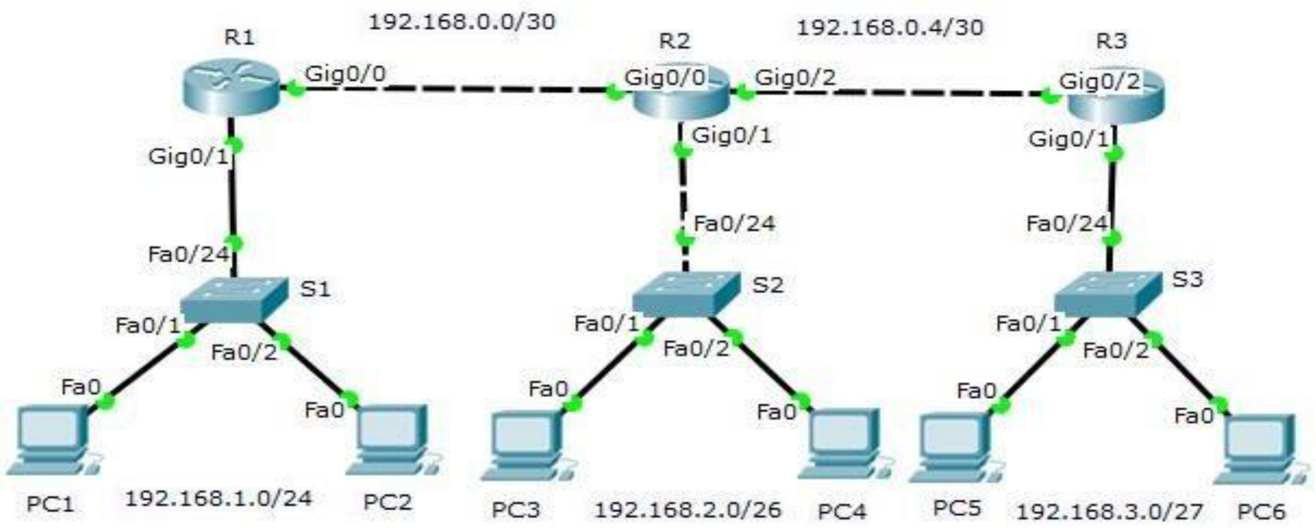


figure: 10.1.1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.252	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
R2	G0/0	192.168.1.2	255.255.255.252	N/A
	G0/1	192.168.2.1	255.255.255.0	N/A
	G0/2	192.168.0.5	255.255.255.252	N/A
R3	G0/2	192.168.0.6	255.255.255.252	N/A
	G0/1	192.168.3.1	255.255.255.252	N/A
PC1	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC3	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC4	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC5	NIC	192.168.3.2	255.255.255.0	192.168.3.1
PC6	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Table:10.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify EIGRP Routing

Background / Scenario

Enhanced Interior Gateway Routing Protocol (EIGRP) is is an advanced distance-vector routing protocol for IP networks. In this lab, you will configure the network topology with EIGRP routing, and use a number of CLI commands to display and verify EIGRP routing information.

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

Required Resources

- 3 Routers (Cisco 2911)
- 6 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you set up the network topology and configure basic settings on the PC hosts and routers.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure device name as shown in the topology.

c. Assign **class** as the privileged EXEC password.

d. Assign **cisco** as the console and vty passwords.

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

f. Configure the IP address listed in the Addressing Table for all interfaces.

g. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Step 5: Test connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs are unable to ping other PCs until EIGRP routing is configured. Verify and troubleshoot if necessary.

Part 2: Configure and Verify EIGRP Routing

In Part 2, you will configure EIGRPv2 routing on all routers in the network and then verify that routing tables are updated correctly. After EIGRP has been verified, you will configure EIGRP authentication on the links for added security.

Step 1: Configure EIGRP on R1,R2 and R3.

a. Use the **router EIGRP** command in global configuration mode to enable EIGRP on R1.

```
R1(config)# router EIGRP 1
```

Note: The EIGRP Autonomous System Number is kept locally and has no meaning to other routers on the network.

b. Configure the **network** statements for the networks on R1.

```
R1(config)# router EIGRP 1
R1(config-router)# network 192.168.1.0  0.0.0.255
R1(config-router)# network 192.168.0.0  0.0.0.3
```

c. Configure the **network** statements for the networks on R2.

```
R2(config)# router EIGRP 1
R2(config-router)# network 192.168.2.0  0.0.0.63
R2(config-router)# network 192.168.0.0  0.0.0.3
R2(config-router)# network 192.168.0.4  0.0.0.3
```

d. Configure the **network** statements for the networks on R3.

```
R3(config)# router EIGRP 1
R3(config-router)# network 192.168.3.0  0.0.0.31
R3(config-router)# network 192.168.0.4  0.0.0.3
```

Step 2: Verify EIGRP neighbors and routing information.

a. Issue the **show ip EIGRP neighbor** command to verify that each router lists the other routers in the network as neighbors.

```
R1# show ip EIGRP neighbor
```

b. Issue the **show ip route** command to verify that all networks display in the routing table on all routers.

```
R1# show ip route
```

Step 3: Verify EIGRP protocol settings.

The **show ip protocols** command is a quick way to verify vital EIGRP configuration information. This information includes the EIGRP process ID, the router ID, networks the router is advertising, the neighbors the router is receiving updates from, and the default administrative distance, which is 110 for EIGRP.

```
R1# show ip protocols
```

Step 4: Verify EIGRP process information.

Use the **show ip EIGRP** command to examine the EIGRP process ID and router ID. This command displays the EIGRP area information, as well as the last time the SPF algorithm was calculated.

```
R1# show ip EIGRP
```

Step 5: Verify EIGRP interface settings.

a. Issue the **show ip EIGRP interface brief** command to display a summary of EIGRP-enabled interfaces.

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

b. For a more detailed list of every EIGRP-enabled interface, issue the **show ip EIGRP interface** command.

```
R1# show ip EIGRP interface
```

Step 6: Verify end-to-end connectivity.

Each PC should be able to ping the other PCs in the topology. Verify and troubleshoot if necessary.

Lab 10.2– Home Activity for Configuring Basic EIGRP

Topology:

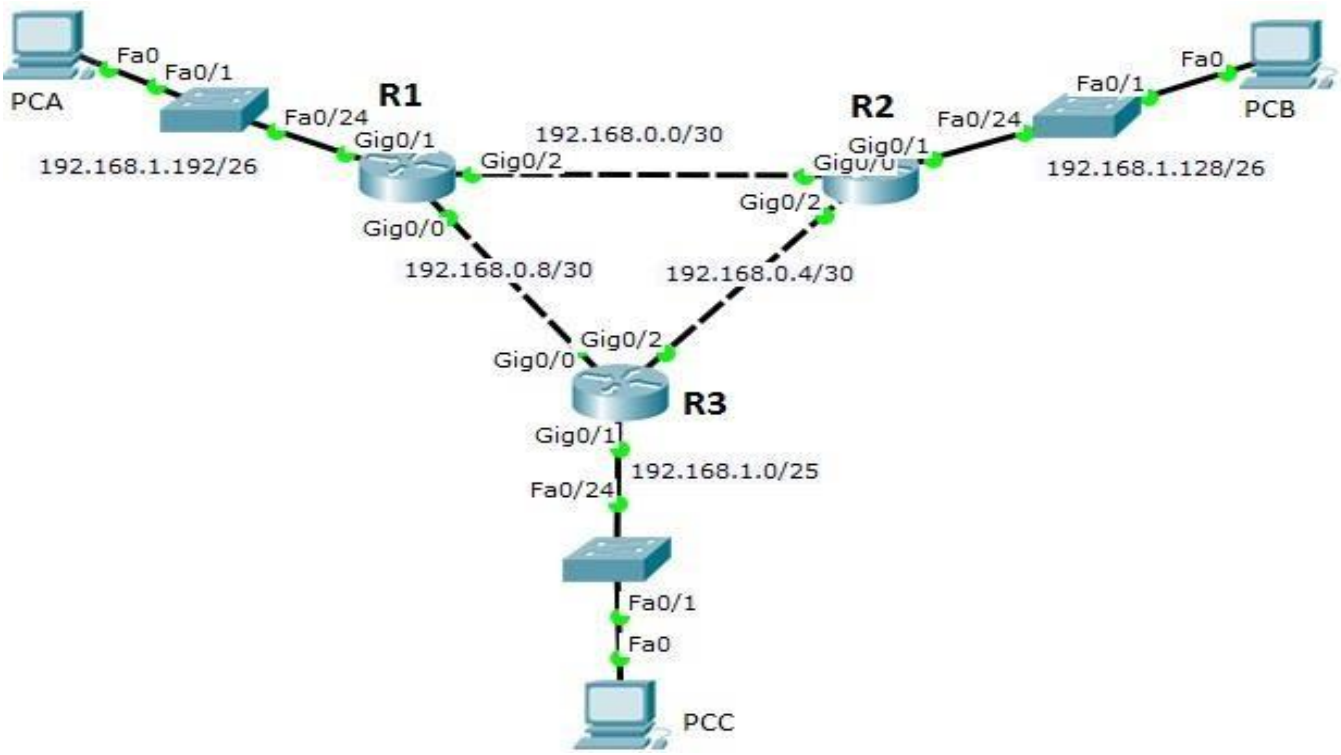


Figure: 10.2.1

Addressing Table:

Fill the addressing table as shown in the topology

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0			N/A
R1	G0/1			N/A
R1	G0/2			N/A
R2	G0/0			N/A
R2	G0/1			N/A
R2	G0/2			N/A
R3	G0/0			N/A
R3	G0/1			N/A
R3	G0/2			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			

Note:

- **Put the screen shot of your designed topology at the end of this experiment.**
- **Also attach the printout of startup configurations, protocol information (#show ip protocol), interface information (#show ip interface brief), neighboring information (show ip EIGRP neighbor) and routing table of each router.**

SHAHEED ZULFIKAR ALI BHUTTO
INSTITUTE OF SCIENCE AND TECHNOLOGY

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#11

Lab 11.1 – Configuring and Verifying Standard ACLs

Topology:

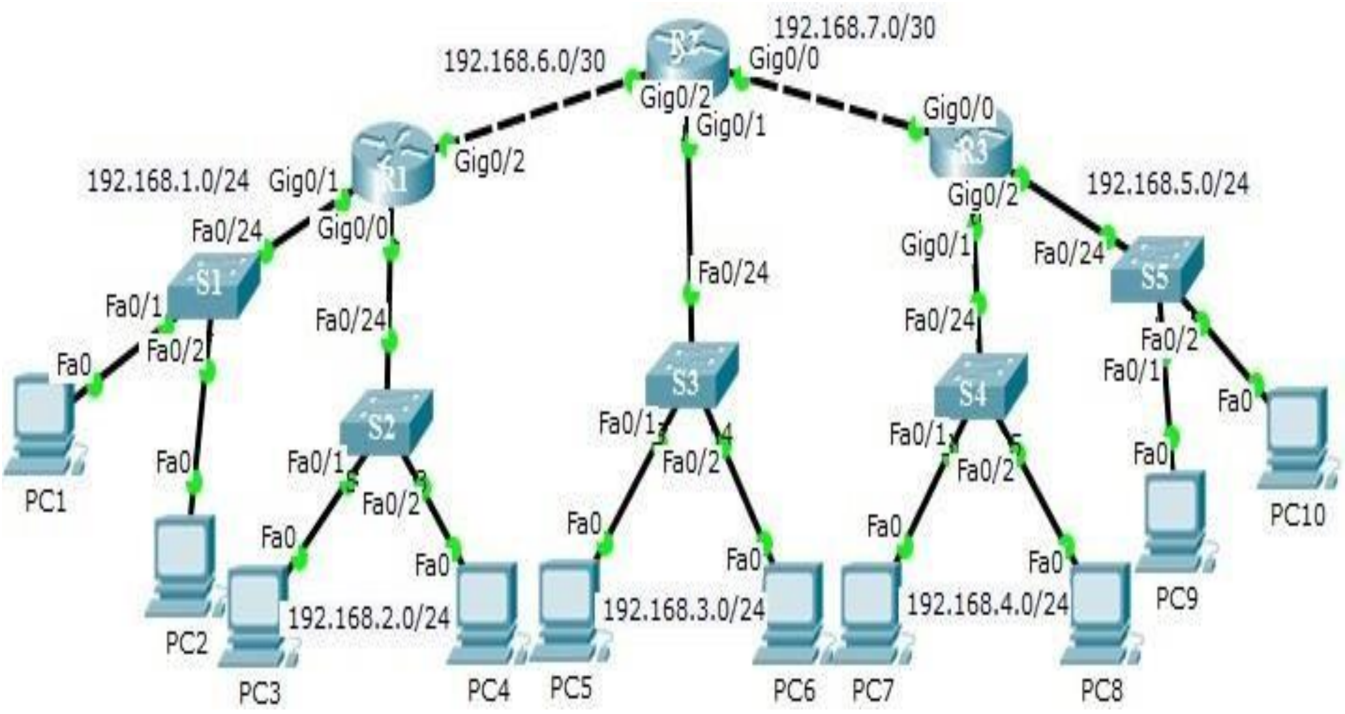


Figure: 11.1.1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.2.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	G0/2	192.168.6.1	255.255.255.252	N/A
R2	G0/0	192.168.7.1	255.255.255.252	N/A
	G0/1	192.168.3.1	255.255.255.0	N/A
	G0/2	192.168.6.2	255.255.255.252	N/A
R3	G0/0	192.168.7.	255.255.255.252	N/A
	G0/1	192.168.4.1	255.255.255.0	N/A
	G0/2	192.168.5.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.2.2	255.255.255.0	192.168.2.1
S3	VLAN 1	192.168.3.2	255.255.255.0	192.168.3.1
S4	VLAN 1	192.168.4.2	255.255.255.0	192.168.4.1
S5	VLAN 1	192.168.5.2	255.255.255.0	192.168.5.1
PC1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC2	NIC	192.168.1.4	255.255.255.0	192.168.1.1
PC3	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC4	NIC	192.168.2.4	255.255.255.0	192.168.2.1
PC5	NIC	192.168.3.3	255.255.255.0	192.168.3.1
PC6	NIC	192.168.3.4	255.255.255.0	192.168.3.1
PC7	NIC	192.168.4.3	255.255.255.0	192.168.4.1
PC8	NIC	192.168.4.4	255.255.255.0	192.168.4.1
PC9	NIC	192.168.5.3	255.255.255.0	192.168.5.1
PC10	NIC	192.168.5.4	255.255.255.0	192.168.5.1

Table: 11.1.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

- Set up equipment to match the network topology.
- Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity

- Assign a static IP address to PCs.
- Configure basic settings on routers.
- Configure basic settings on switches.
- Configure OSPF routing on R1, R2, and R3.

- Verify connectivity between devices.

Part 3: Configure and Verify Standard Numbered and Named ACLs

- Configure, apply, and verify a numbered standard ACL.
- Configure, apply, and verify a named ACL.

Part 4: Modify a Standard ACL

- Modify and verify a named standard ACL.
- Test the ACL.

Background / Scenario

Network security is an important issue when designing and managing IP networks. The ability to configure proper rules to filter packets, based on established security policies, is a valuable skill.

In this lab, you will set up filtering rules for three offices represented by R1, R2 and R3. Management has established some access policies between the LANs located at R1, R2 and R3, which you must implement.

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

Required Resources

- 3 Routers (Cisco 2911)
- 5 Switches (Cisco 2960)
- 10 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

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

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

Step 2: Initialize and reload the routers and switches.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you configure basic settings on the routers, switches, and PCs. Refer to the Topology and Addressing Table for device names and address information.

Step 1: Configure IP addresses on PC-A and PC-C.

Step 2: Configure basic settings for the routers.

a. Disable DNS lookup.

b. Configure the device names as shown in the topology.

c. Configure interface IP addresses as shown in the Topology and Addressing Table.

d. Configure a privileged EXEC mode password of **class**.

e. Assign **cisco** as the console password.

f. Assign **cisco** as the vty password and enable Telnet access.

Step 3: (Optional) Configure basic settings on the switches.

a. Disable DNS lookup.

b. Configure the device names as shown in the topology.

c. Configure the management interface IP address as shown in the Topology and Addressing Table.

d. Configure a privileged EXEC mode password of **class**.

e. Configure a default gateway.

f. Assign **cisco** as the console password.

g. Assign **cisco** as the vty password and enable Telnet access.

Step 4: Configure OSPF routing on R1, R2, and R3.

a. Assign 1 as the OSPF process ID and advertise all networks on R1, R2, and R3. The OSPF configuration for R1 and R2 is included for reference.

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
R1(config-router)# network 192.168.6.0 0.0.0.3 area 0

R2(config)# router ospf 1
R2(config-router)# network 192.168.3.0 0.0.0.255 area 0
R2(config-router)# network 192.168.6.0 0.0.0.3 area 0
R2(config-router)# network 192.168.7.0 0.0.0.3 area 0

R3(config)# router ospf 1
R3(config-router)# network 192.168.4.0 0.0.0.255 area 0
R3(config-router)# network 192.168.5.0 0.0.0.255 area 0
R3(config-router)# network 192.168.7.0 0.0.0.3 area 0
```

b. After configuring OSPF on R1, R2, and R3, verify that all routers have complete routing tables listing all networks. Troubleshoot if this is not the case.

Step 5: Verify connectivity between devices.

Note: It is very important to test whether connectivity is working **before** you configure and apply access lists! You want to ensure that your network is properly functioning before you start to filter traffic.

a. From PC-A, ping PC-C and the loopback interface on R3. Were your pings successful? ________

b. From R1, ping PC-C and the loopback interface on R3. Were your pings successful? ________

c. From PC-C, ping PC-A and the loopback interface on R1. Were your pings successful? ________

d. From R3, ping PC-A and the loopback interface on R1. Were your pings successful? ________

Part 3: Configure and Verify Standard Numbered and Named ACLs

Step 1: Configure a numbered standard ACL.

Standard ACLs filter traffic based on the source IP address only. A typical best practice for standard ACLs is to configure and apply it as close to the destination as possible. For the first access list, create a standard numbered ACL that allows traffic from all hosts on the 192.168.1.0/24 network and all hosts on the 192.168.2.0/24 network to access all hosts on the 192.168.4.0/24 network. The security policy also states that a **deny any** access control entry (ACE), also referred to as an ACL statement, should be present at the end of all ACLs.

What wildcard mask would you use to allow all hosts on the 192.168.1.0/24 network to access the 192.168.3.0/24 network?

____

Following Cisco's recommended best practices, on which router would you place this ACL? ____________

On which interface would you place this ACL? In what direction would you apply it?

____

____

a. Configure the ACL on R3. Use 1 for the access list number.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.1.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.2.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Apply the ACL to the appropriate interface in the proper direction.

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

c. Verify a numbered ACL.

The use of various **show** commands can aid you in verifying both the syntax and placement of your ACLs in your router.

To see access list 1 in its entirety with all ACEs, which command would you use?

____

What command would you use to see where the access list was applied and in what direction?

____

1) On R3, issue the **show access-lists 1** command.

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.1.0, wildcard bits 0.0.0.255
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    30 deny   any
```

2) On R3, issue the **show ip interface g0/1** command.

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.4.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Output omitted
```

3) Test the ACL to see if it allows traffic from the 192.168.1.0/24 network access to the 192.168.4.0/24 network. From the PC1 command prompt, ping the PC7 IP address. Were the pings successful? ________

4) Test the ACL to see if it allows traffic from the 192.168.2.0/24 network access to the 192.168.4.0/24 network. You must do an extended ping and use the loopback 0 address on R1 as your source. Ping PC7's IP address. Were the pings successful? ________

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.4.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.2.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

Step 2: Configure a named standard ACL.

Create a named standard ACL that conforms to the following policy: allow traffic from all hosts on the 192.168.5.0/24 network access to all hosts on the 192.168.1.0/24 network. Also, only allow host PC8 access to the 192.168.1.0/24 network. The name of this access list should be called BRANCH-OFFICE-POLICY.

Following Cisco's recommended best practices, on which router would you place this ACL? ____________

On which interface would you place this ACL? In what direction would you apply it?

____

a. Create the standard named ACL BRANCH-OFFICE-POLICY on R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.4.4
R1(config-std-nacl)# permit 192.168.5.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Looking at the first permit ACE in the access list, what is another way to write this?

____

b. Apply the ACL to the appropriate interface in the proper direction.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. Verify a named ACL.

1) On R1, issue the **show access-lists** command.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Is there any difference between this ACL on R1 with the ACL on R3? If so, what is it?

____

____

____

____

____

2) On R1, issue the **show ip interface g0/1** command.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Output omitted>
```

3) Test the ACL. From the command prompt on PC-C, ping PC-A's IP address. Were the pings successful? ________

4) Test the ACL to ensure that only the PC-C host is allowed access to the 192.168.1.0/24 network. You must do an extended ping and use the G0/1 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? ________

Part 4: Modify a Standard ACL

It is common in business for security policies to change. For this reason, ACLs may need to be modified. In Part 4, you will change one of the previous ACLs you configured, to match a new management policy being put in place.

Management has decided that users from the 192.168.2.0/24 network should be allowed full access to the 192.168.1.0/24 network. Management also wants ACLs on all of their routers to follow consistent rules. A **deny any** ACE should be placed at the end of all ACLs. You must modify the BRANCH-OFFICE-POLICY ACL.

You will add two additional lines to this ACL. There are two ways you could do this:

OPTION 1: Issue a **no ip access-list standard BRANCH-OFFICE-POLICY** command in global configuration mode. This would effectively take the whole ACL out of the router. Depending upon the router IOS, one of the following scenarios would occur: all filtering of packets would be cancelled and all packets would be allowed through the router; or, because you did not take off the **ip access-group** command on the G0/1 interface, filtering is still in place. Regardless, when the ACL is gone, you could retype the whole ACL, or cut and paste it in from a text editor.

OPTION 2: You can modify ACLs in place by adding or deleting specific lines within the ACL itself. This can come in handy, especially with ACLs that have many lines of code. The retyping of the whole ACL or cutting and pasting can easily lead to errors. Modifying specific lines within the ACL is easily accomplished.

Note: For this lab, use Option 2.

Step 1: Modify a named standard ACL.

a. From R1 privileged EXEC mode, issue a **show access-lists** command.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.4.3 (8 matches)
    20 permit 192.168.5.0, wildcard bits 0.0.0.255 (5 matches)
```

b. Add two additional lines at the end of the ACL. From global config mode, modify the ACL, BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 192.168.2.0 0.0.0.255
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c. Verify the ACL.

1) On R1, issue the **show access-lists** command.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 192.168.2.0, wildcard bits 0.0.0.255
    40 deny   any
```

Do you have to apply the BRANCH-OFFICE-POLICY to the G0/1 interface on R1?

____

____

2) From the R2 command prompt, issue an extended ping. Test the ACL to see if it allows traffic from the 192.168.2.0/24 network access to the 192.168.1.0/24 network. You must do an extended ping and use the loopback 0 address on R2 as your source. Ping PC-A's IP address. Were the pings successful? ________

Reflection

1. As you can see, standard ACLs are very powerful and work quite well. Why would you ever have the need for using extended ACLs?

____

____

____

____

2. Typically, more typing is required when using a named ACL as opposed to a numbered ACL. Why would you choose named ACLs over numbered?

____

____

____

____

Lab 11.2– Home Activity for Configuring Single area OSPF

Topology:

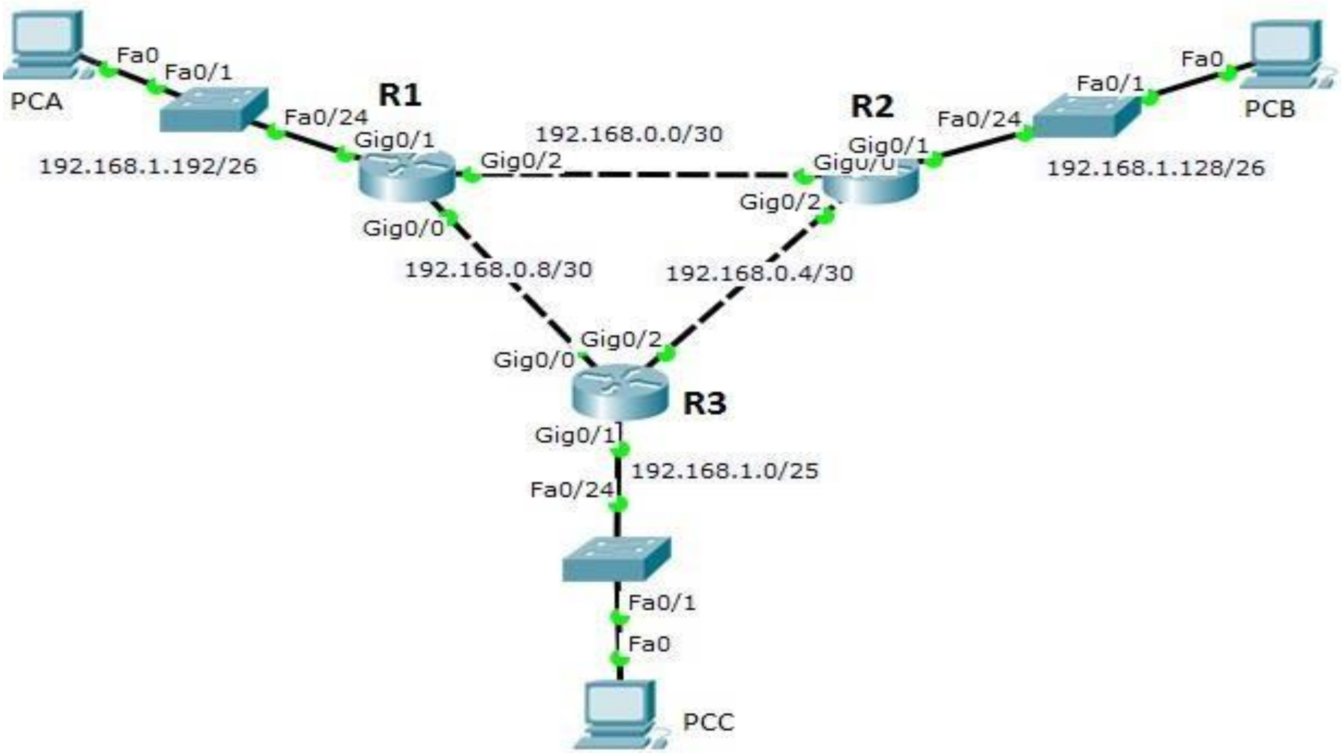


Figure: 9.2.1

Addressing Table:

Fill the addressing table as shown in the topology

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0			N/A
R1	G0/1			N/A
R1	G0/2			N/A
R2	G0/0			N/A
R2	G0/1			N/A
R2	G0/2			N/A
R3	G0/0			N/A
R3	G0/1			N/A
R3	G0/2			N/A
PC1	NIC			
PC2	NIC			
PC3	NIC			

Table: 11.2.1

Scenarios:

- **PCB** will not be allowed to access 192.168.1.192/26 network.
- **PCC** will be allowed to access 192.168.1.192/26 network only

Note:

- **Put the screen shot of your designed topology at the end of this experiment.**
- **Also attach the printout of protocol information (#show ip protocol), interface information (#show ip interface brief), neighboring information (show ip ospf neighbor), routing table and Access lists (#show ip access-lists) of each router.**

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	Student’s Behavior	2.5	
2	Lab Performance	2.5	
3	On Time Submission	5	
4	Home Activity	10	
	Net Result	20	

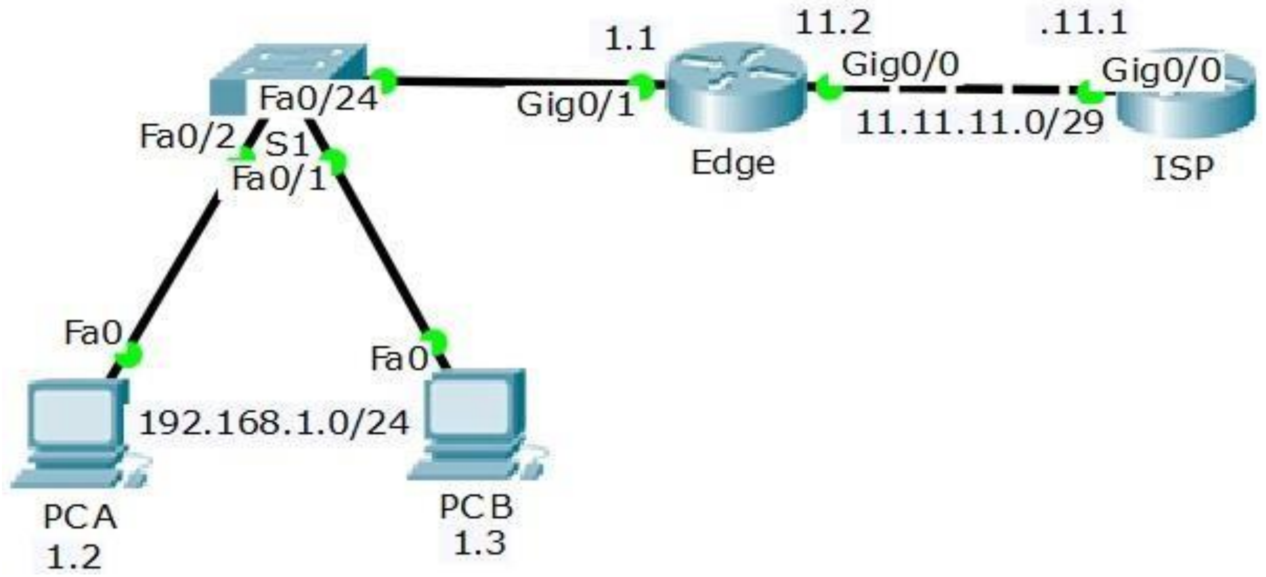
Examined By: (Instructor’s Name & Initial’s)

Date

Experiment#12

Lab 12.1 – Configuring Dynamic and Static NAT

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default EDGE
EDGE	G0/1	192.168.1.1	255.255.255.0	N/A
	G0/0	11.11.11.2	255.255.255.248	N/A
ISP	G0/0	11.11.11.1	255.255.255.248	N/A
	G0/1	192.168.2.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify Static NAT

Part 3: Configure and Verify Dynamic NAT

Background / Scenario

Network Address Translation (NAT) is the process where a network device, such as a Cisco router, assigns a public address to host devices inside a private network. The main reason to use NAT is to reduce the number of public IP addresses that an organization uses because the number of available IPv4 public addresses is limited.

In this lab, an ISP has allocated the public IP address space of 11.11.11.0/29 to a company. This provides the company with 6 public IP addresses. The addresses, 11.11.11.1 to 11.11.11.6, are for static allocation. A static route is used from the ISP to the EDGE router, and a default route is used from the EDGE to the ISP router.

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

Required Resources

- 2 Routers (Cisco 1941)
- 1 Switch (Cisco 2960)
- 2 PCs
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

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

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

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

Step 2: Configure PC hosts.

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

Step 4: Configure basic settings for each router.

Step 5: Configure static routing.

a. Create a static route from the ISP router to the EDGE router using the assigned public network address range 209.165.200.224/27.

```
ISP(config)# ip route 192.168.1.0  255.255.255.0  11.11.11.2
```

b. Create a default route from the EDGE router to the ISP router.

```
EDGE(config)# ip route 0.0.0.0 0.0.0.0  11.11.11.1
```

Step 6: Save the running configuration to the startup configuration.

Step 7: Verify network connectivity.

a. From the PC hosts, ping the G0/1 interface on the EDGE router. Troubleshoot if the pings are unsuccessful.

b. Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

Part 2: Configure and Verify Static NAT

Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant. Static NAT is particularly useful for web servers or devices that must have static addresses that are accessible from the Internet.

Step 1: Configure a static mapping.

A static map is configured to tell the router to translate between the private inside address 192.168.1.2 and the public address 11.11.11.3. This allows a user from the Internet to access PC-A.

```
EDGE(config)# ip nat inside source static 192.168.1.2  11.11.11.3
```

Step 2: Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

```
EDGE(config)# interface g0/1
EDGE(config-if)# ip nat inside
EDGE(config-if)# interface g0/0
EDGE(config-if)# ip nat outside
```

Step 3: Test the configuration.

a. Display the static NAT table by issuing the **show ip nat translations** command.

```
EDGE# show ip nat translations
Pro Inside global     Inside local     Outside local     Outside global
---     11.11.11.3     192.168.1.2          ---                    ---
```

What is the translation of the Inside local host address?

192.168.1.2 = ______________________________

The Inside global address is assigned by? ____

The Inside local address is assigned by?

____

b. Verify NAT statistics by using the **show ip nat statistics** command on the EDGE router.

```
EDGE# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Note: This is only a sample output. Your output may not match exactly.

Part 3: Configure and Verify Dynamic NAT

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Dynamic NAT results in a many-to-many address mapping between local and global addresses.

Step 1: Clear NATs.

Before proceeding to add dynamic NATs, clear the NATs and statistics from Part 2.

```
EDGE# clear ip nat translation *
EDGE# clear ip nat statistics
```

Step 2: Define an access control list (ACL) that matches the LAN private IP address range.

ACL 1 is used to allow 192.168.1.0/24 network to be translated.

```
EDGE(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 3: Verify that the NAT interface configurations are still valid.

Issue the **show ip nat statistics** command on the EDGE router to verify the NAT configurations.

Step 4: Define the pool of usable public IP addresses.

```
EDGE(config)# ip nat pool public_access 11.11.11.3 11.11.11.6 netmask 255.255.255.248
```

Step 5: Define the NAT from the inside source list to the outside pool.

Note: Remember that NAT pool names are case-sensitive and the pool name entered here must match that used in the previous step.

```
EDGE(config)# ip nat inside source list 1 pool public_access
```

Step 6: Remove the static NAT entry.

In Step 7, the static NAT entry is removed and you can observe the NAT entry.

a. Remove the static NAT from Part 2. Enter **yes** when prompted to delete child entries.

```
EDGE(config)# no ip nat inside source static 192.168.1.2 11.11.11.3

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Clear the NATs and statistics.

c. Ping the ISP (192.31.7.1) from both hosts.

d. Display the NAT table and statistics.

```
EDGE# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
```

```
 pool public_access: netmask 255.255.255.224
       start 209.165.200.242 end 209.165.200.254
       type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Note: This is only a sample output. Your output may not match exactly.

Reflection

1. Why would NAT be used in a network?

____

____

____

2. What are the limitations of NAT?

____

____

____

Lab 12.2 – Configuring NAT Pool Overload and PAT

Topology

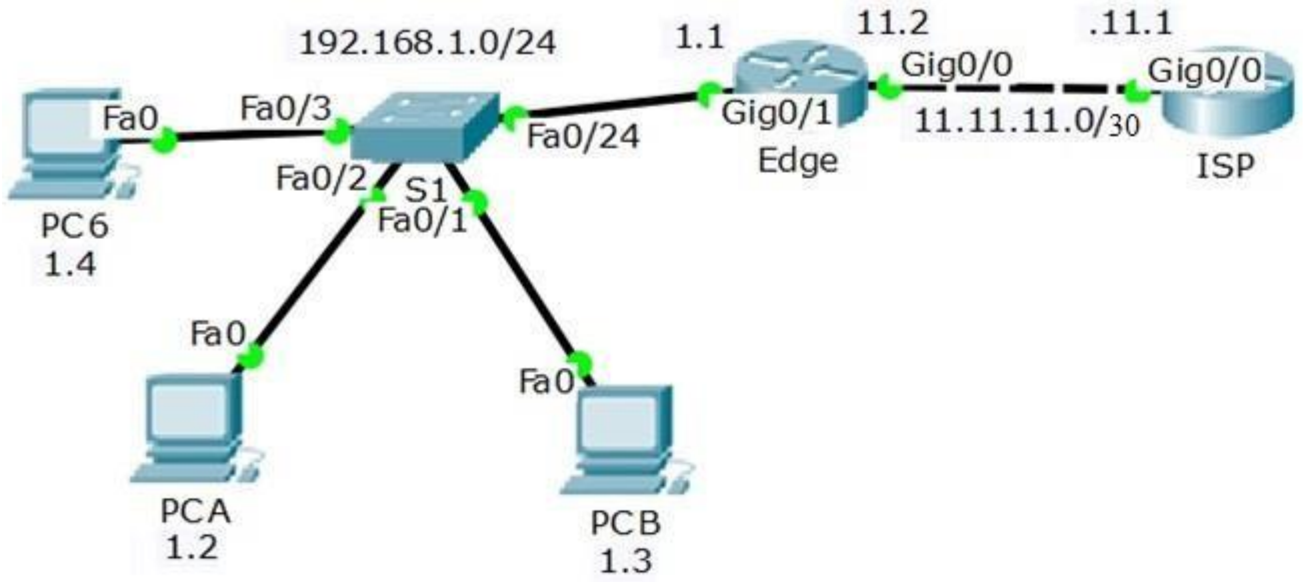


Figure:12.2.1

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default EDGE
EDGE	G0/1	192.168.1.1	255.255.255.0	N/A
	G0/0	11.11.11.2	255.255.255.252	N/A
ISP	G0/0	11.11.11.1	255.255.255.252	N/A
	G0/1	192.168.2.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC6	NIC	192.168.1.4	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 3: Configure and Verify PAT

Background / Scenario

In Part 2, the ISP has allocated a single IP address, 11.11.11.2, to your company for use on the Internet connection from the company EDGE router to the ISP. You will use the Port Address Translation (PAT) to convert multiple internal addresses into the one usable public address. You will test, view, and verify that the translations are taking place, and you will interpret the NAT/PAT statistics to monitor the process.

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

Required Resources

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

Part 1: Build the Network and Verify Connectivity

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

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches.

Step 4: Configure basic settings for each router.

Step 5: Configure static routing.

a. Create a static route from the ISP router to the EDGE router.

```
ISP(config)# ip route 192.168.1.0  255.255.255.0  11.11.11.2
```

b. Create a default route from the EDGE router to the ISP router.

```
EDGE(config)# ip route 0.0.0.0 0.0.0.0  11.11.11.1
```

Step 6: Verify network connectivity.

a. From the PC hosts, ping the G0/0 interface on the EDGE router. Troubleshoot if the pings are unsuccessful.

b. Verify that the static routes are configured correctly on both routers.

Part 2: Configure and Verify PAT

In Part 3, you will configure PAT by using an interface instead of a pool of addresses to define the outside address. Not all of the commands in Part 2 will be reused in Part 3.

Step 1: Clear NATs and statistics on the EDGE router.

Step 2: Define an access control list (ACL) that matches the LAN private IP address range.

ACL 1 is used to allow 192.168.1.0/24 network to be translated.

```
EDGE(config)# access-list 1 permit 192.168.1.0  0.0.0.255
```

Step 3: Associate the source list with the outside interface.

```
EDGE(config)# ip nat inside source list 1 interface GigabitEthernet 0/0 overload
```

Step 4: Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

```
EDGE(config)# interface g0/1
EDGE(config-if)# ip nat inside
EDGE(config-if)# interface g0/0
EDGE(config-if)# ip nat outside
```

Step 5: Test the PAT configuration.

a. From each PC, ping the 11.11.11.1 address on the ISP router.

b. Display NAT statistics on the EDGE router.

```
EDGE# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface gigabitethernet 0/0 refcount 3

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

c. Display NAT translations on EDGE.

```
EDGE# show ip nat translations
```

Reflection

What advantages does PAT provide?

____

____

Lab 12.3 – Home Activity

In the light of above experiments, configure the following topology (for **Static NAT, Dynamic NAT** and **PAT)**, Fill the addressing tables and use your SZABIST ID for public IP ADDRESSING.

Topology:

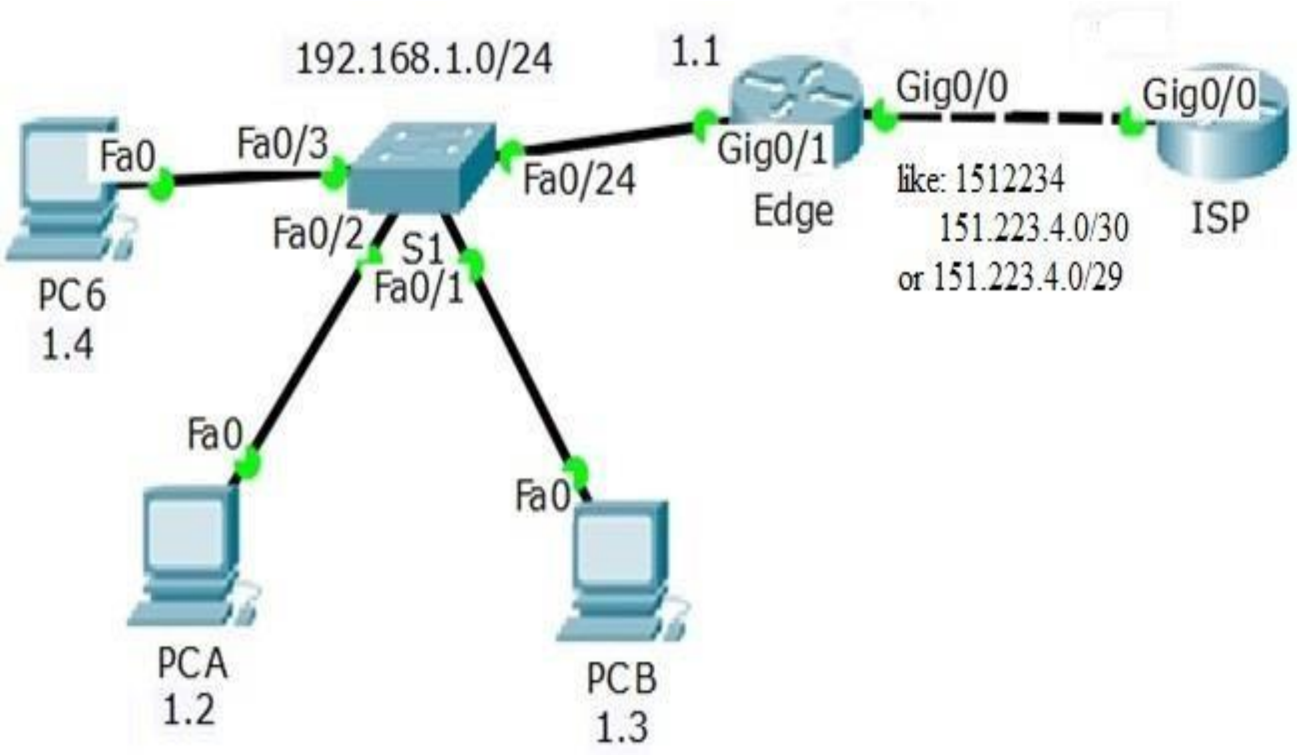


Figure: 12.3.1

Addressing Table for STATIC NAT:

Device	Interface	IP Address	Subnet Mask	Default EDGE
EDGE				N/A
				N/A
ISP				N/A
				N/A
PC-A	NIC			
PC-B	NIC			
PC6	NIC			

Table: 12.3.1

Addressing Table for Dynamic NAT:

Device	Interface	IP Address	Subnet Mask	Default EDGE
EDGE				N/A
				N/A
ISP				N/A
				N/A
PC-A	NIC			
PC-B	NIC			
PC6	NIC			

Table: 12.3.2

Addressing Table for Dynamic NAT:

Device	Interface	IP Address	Subnet Mask	Default EDGE
EDGE				N/A
				N/A
ISP				N/A
				N/A
PC-A	NIC			
PC-B	NIC			
PC6	NIC			

Table: 12.3.3

Note:

- **Put the screen shot of your all designed topologies (static, Dynamic and PAT) at the end of this experiment.**
- **Also attach the printout of startup configurations, interfaces information (#show ip interface brief), routing table of each router, NAT translation Table (EDGE# show ip nat translation) and NAT statistics (EDGE# show ip nat statistics).**
- **Above mentioned information are required for each type of NAT.**

Lab’s Evaluation Sheet

Students Registration No:	
Date Performed:	
Group No:	
Date of Submission:	

Sr. No.	Categories	Total Marks/Grade	Marks /Grade Obtained
1	**Student’s Behavior**	**2.5**	
2	**Lab Performance**	**2.5**	
3	**On Time Submission**	**5**	
4	**Home Activity**	**10**	
	Net Result	**20**	

Examined By: (Instructor’s Name & Initial’s)

Date