EXPERIMENT 1-KNOW YOUR DEVICES

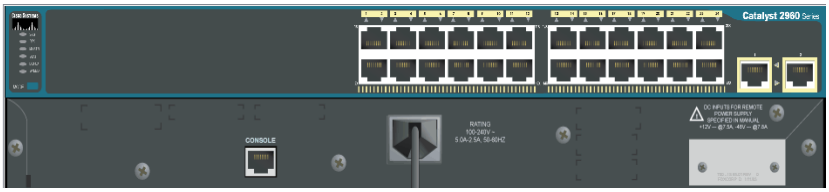
1) **Router**:
   - A router is a network device, which can be used to connect devices.
   - It can be used to send data over devices in the form of data packets.
   - Routers can be combined with other components and connected with devices to improve internet access.
   - Routers can be configured to define a set of IP addresses for incoming and outgoing data packets. The Cisco Packet Tracer allows us to configure a virtual Router as given in Fig ().

Device Name: Router1
Device Model: 1941
Hostname: Router

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Down	--	<not set>	<not set>	0090.0CD6.5201
GigabitEthernet0/1	Down	--	<not set>	<not set>	0090.0CD6.5202
Serial0/0/0	Down	--	<not set>	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
FastEthernet0/1/0	Down	1	--	<not set>	0060.5C1C.4501
FastEthernet0/1/1	Down	1	--	<not set>	0060.5C1C.4502
FastEthernet0/1/2	Down	1	--	<not set>	0060.5C1C.4503
FastEthernet0/1/3	Down	1	--	<not set>	0060.5C1C.4504
Vlan1	Down	1	<not set>	<not set>	000D.BD2B.4384

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1

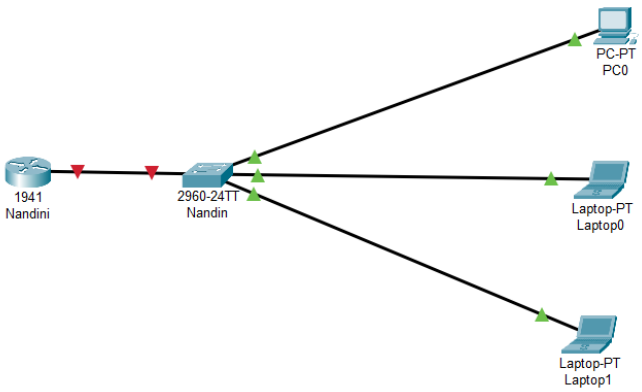
2) **Switches:**
   - A switch is a network device that can be used to connect multiple devices within a network, enabling them to communicate with each other.
   - These devices are generally used to design a network infrastructure.
   - A switch generally consists of a hub of ports to which devices can be connected. The Cisco Packet Tracer allows us to configure a virtual Switch as given in Fig ().




```
Device Name: Switch1
Custom Device Model: 2960 with IOS 12
Hostname: Switch

Port                Link   VLAN   IP Address          MAC Address
FastEthernet0/1     Down   1      --                  0050.0FAB.7901
FastEthernet0/2     Down   1      --                  0050.0FAB.7902
FastEthernet0/3     Down   1      --                  0050.0FAB.7903
FastEthernet0/4     Down   1      --                  0050.0FAB.7904
FastEthernet0/5     Down   1      --                  0050.0FAB.7905
FastEthernet0/6     Down   1      --                  0050.0FAB.7906
FastEthernet0/7     Down   1      --                  0050.0FAB.7907
FastEthernet0/8     Down   1      --                  0050.0FAB.7908
FastEthernet0/9     Down   1      --                  0050.0FAB.7909
FastEthernet0/10    Down   1      --                  0050.0FAB.790A
FastEthernet0/11    Down   1      --                  0050.0FAB.790B
FastEthernet0/12    Down   1      --                  0050.0FAB.790C
FastEthernet0/13    Down   1      --                  0050.0FAB.790D
FastEthernet0/14    Down   1      --                  0050.0FAB.790E
FastEthernet0/15    Down   1      --                  0050.0FAB.790F
FastEthernet0/16    Down   1      --                  0050.0FAB.7910
FastEthernet0/17    Down   1      --                  0050.0FAB.7911
```

3) **<u>Wires</u>**:

- In a network, common wires that can be used for connection are copper wires or Optic Fiber Cables.
- In a LAN environment, Copper Wires are generally used to connect devices as it offers a cheap alternative to Optic Fiber Cables.
- However, for long distances where the signal loss is to be kept minimum an Optical Fiber Cable is used. The Cisco Packet Tracer allows us to configure wires to connect devices, as given in Fig ().



EXPERIMENT 2-CONFIGURE INITIAL SWITCH SETTINGS

Aim- To configure initial switch settings.

Software Used-Cisco Packet Tracer

Commands Used-

1. **enable**: It allows the user to enter EXEC mode, the prompt will change as shown in the figure.

```
Switch> enable
Switch#
```

2. **show running config**: This allows the user to view the current configuration of the switch, it ranges from ethernet port to all the configurations of the switch. The execution of this command is shown in the figure.

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

Current configuration : 1259 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Raunaq
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 08221D0A0A49
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
 --More-- |
```

3. **configure terminal**: It allows the user to configure the parameters of the terminal such as hostname, password ,encryption etc. The execution of this command is shown in the figure.

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

4. **hostname:** It is used to configure the hostname parameter as shown in the figure.

5. **password**: It is used to set the password to the console as shown in the figure.

```
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#
```

6. **login:**It is used after password command, to set the password for User Access Verification as shown in the Figure.

```
User Access Verification
Password:
```

7. **exit:**This allows user to exit the EXEC mode or CLI .

8. **secret:** It is used to lock the EXEC mode of the terminal. The execution of the command is shown in Figure 6.

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

9. **service password-encryption:** It is used to encrypt the password. The execution of the command is shown in Fig 7.

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

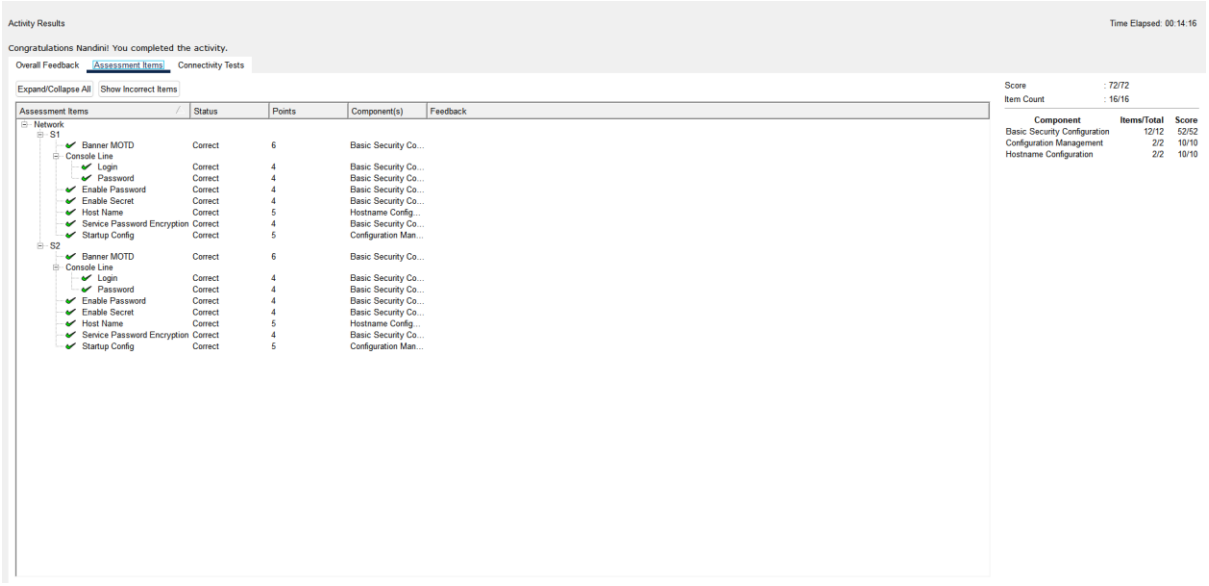
10. **banner motd**: It is a feature which allows the user to configure messages that anyone logging on the switch sees. These messages are known as Message of the Day. The execution of the command is shown in Figure 8 .

```
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#
```

11. **<u>copy running-config startup-config:</u>** It allows the user to save the configuration file to NVRAM of the switch, which can be used when the switch is rebooted. It creates a startup script which ensures that changes made are not lost.

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

Conclusion: The switch was configured successfully.



EXPERIMENT 3- IMPLEMENT BASIC CONNECTIVITY

Aim- To implement basic connectivity by configuring IP addressing on switches and PCs.

Software Used- Cisco Packet Tracer

Background- In this activity, you will first create a basic switch configuration. 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 the configuration and use the ping command to verify basic connectivity between devices.

Procedure-

1. Perform a Basic Configuration on S1 and S2 Complete the following steps on S1 and S2.-
   a. Configure S1 with a hostname.
   b. Click S1 and then click the CLI tab.
   c. Enter the correct command to configure the hostname as S1.
   d: Configure the console and encrypted privileged EXEC mode password.
   e. Use cisco for the console password.
   f. Use class for the privileged EXEC mode password.
   g. Verify the password configurations for S1.
   h. Configure an MOTD banner. Use an appropriate banner text to warn unauthorized access.
   i. Save the configuration file to NVRAM.
   j. Repeat Steps 1 to 5 for S2.

2. Configure the PCs
   a. Configure both PCs with IP addresses.
   b. Click PC1 and then click the Desktop tab.
   c. 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.
   d. Repeat steps 1a and 1b for PC2.
   e. Test connectivity to switches.
   f. Click PC1. Close the IP Configuration window if it is still open. In the Desktop tab, click Command Prompt.
   g. 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
```

3. Configure the Switch Management Interface
   a. Configure S1 and S2 with an IP address.
   b. Configure S1 with an IP address. Switches can be used as plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses.
   c. 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#
```

   d. Configure S2 with an IP address. Use the information in the Addressing Table to configure S2 with an IP address.
   e. Verify the IP address configuration on S1 and S2. Use the show ip interface brief command to display the IP address and status of all the switch ports and interfaces. You can also use the show running-config command.
   f. Save configurations for S1 and S2 to NVRAM.
   g. 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.
   h. Ping S1 and S2 from PC1 and PC2.
   i. Click PC1 and then click the Desktop tab.
   j. Click Command Prompt.
   k. Ping the IP address for PC2.
   l. Ping the IP address for S1.
   m. Ping the IP address for S2.

Result-

Answering the Questions-

1. Which command do you issue to save the configuration file to NVRAM?

Ans, We use the **copy running-config startup-config command** to save the file configuration file to NVRAM.

2. Were you successful in running the ping command?

Ans Yes, here is a screenshot of the execution of the command-

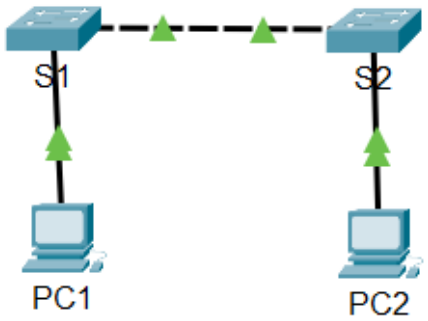
```
Pinging 192.168.1.253 with 32 bytes of data:
Reply from 192.168.1.77: Destination host unreachable.
Reply from 192.168.1.77: Destination host unreachable.
Reply from 192.168.1.77: Destination host unreachable.
Reply from 192.168.1.77: Destination host unreachable.

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

3. Why do we configure a switch with an IP address?

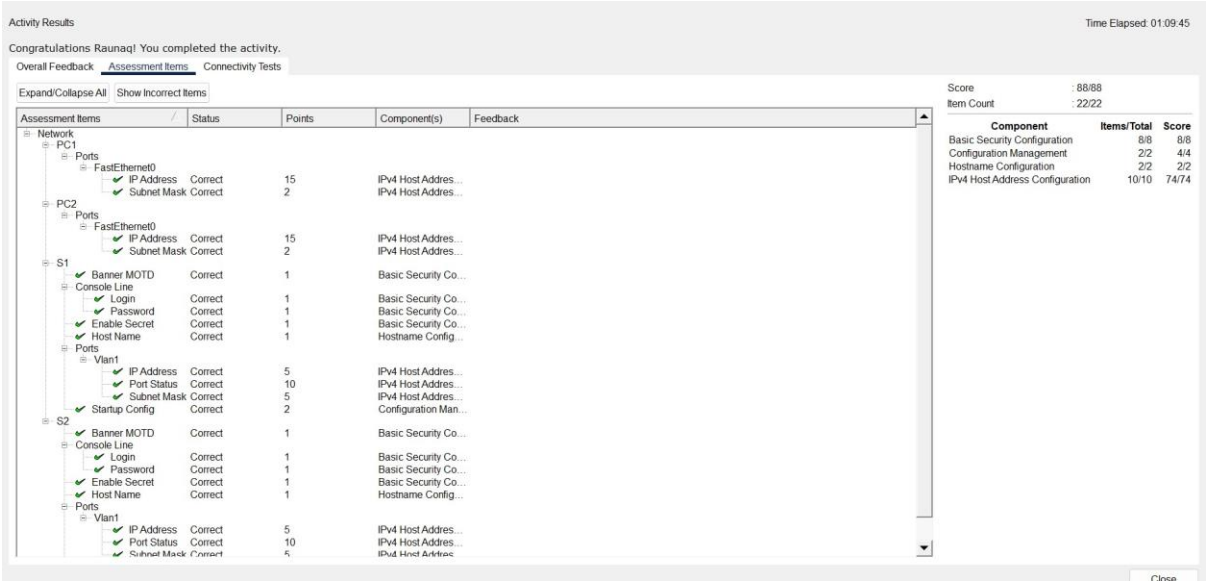
Ans. To perform switch management over the network the switch will need to have an IP address.

4. Why do you enter the no shutdown command?

Ans. The no shutdown command enables an interface This command must be used in interface configuration mode. It is useful for new interfaces and for troubleshooting.



After the completion is shown 100%, the result shown will be like this:



Conclusion- The aim is achieved, and the experiment is completed successfully.

EXPERIMENT 4- BASIC SWITCH AND END DEVICE CONFIGURATION

Aim- To perform basic switch and end device configuration.

Software Used- Cisco Packet Tracer

Background-Tasks include configuring initial settings on two switches using the Cisco IOS and configuring IP address parameters on host devices to provide end-to-end connectivity. Use two switches and two hosts/PCs on a cabled and powered network.

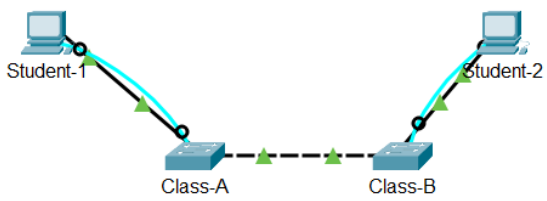
Addressing Table -

Device	Interface	IP Address	Subnet Mask
Class-A	VLAN 1	172.16.5.35	255.255.255.0
Class-B	VLAN 1	172.16.5.40	255.255.255.0
Student-1	NIC	172.16.5.50	255.255.255.0
Student-2	NIC	172.16.5.60	255.255.255.0

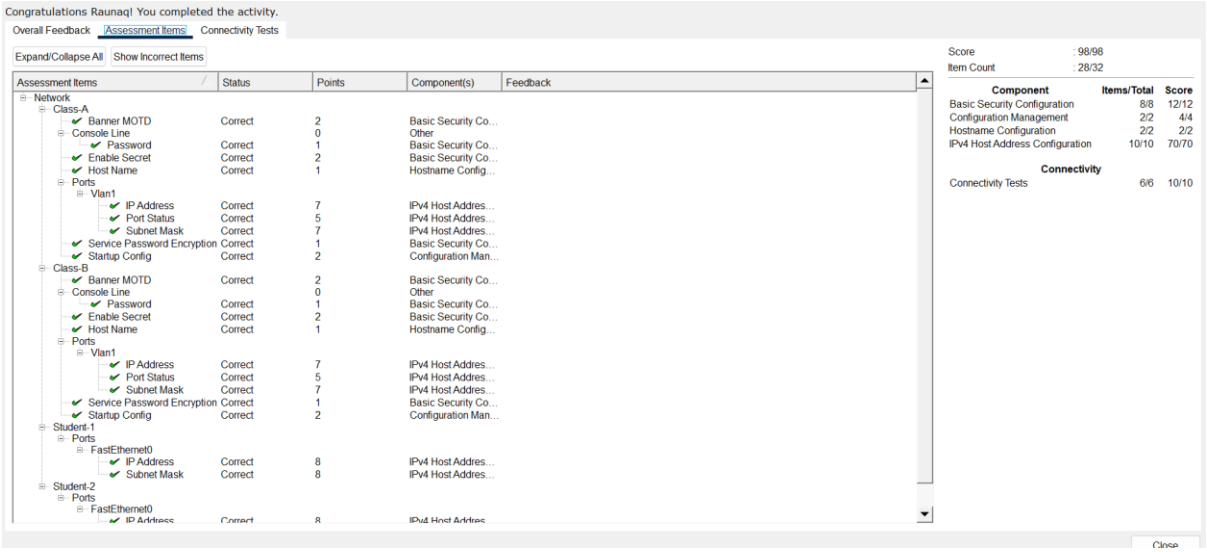
Procedure-

1. Use a console connection to access each switch.
2. Name **Class -A** and **Class -B** switches.
3. Use the **8ubRu** password for all lines.
4. Use the secret password **C9WrE.**
5. Encrypt all clear text passwords.
6. Configure an appropriate message-of-the-day (MOTD) banner.
7. Configure addressing for all devices according to the Addressing Table.
8. Save your configurations.
9. Verify connectivity between all devices

Result- After following all the requirements, the circuit looks like:



After the completion is shown 100%, the result shown will be like this:



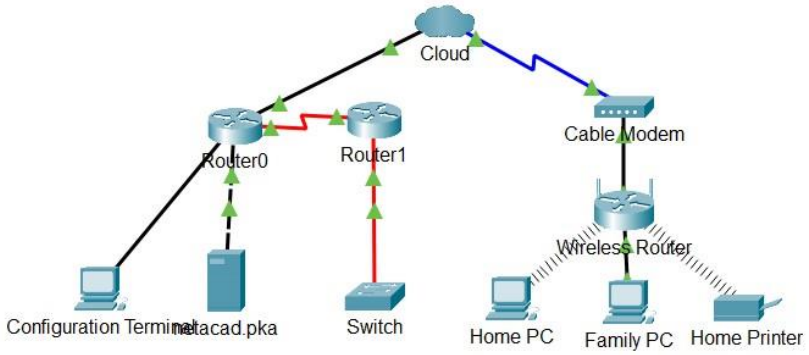
<u>Conclusion</u>- The aim is achieved, and the experiment is completed successfully.

EXPERIMENT 5-CONNECT A WIRED AND WIRELESS LAN

Aim- To connect a wired and wireless LAN.

Software Used- Cisco Packet Tracer

Topology-



Addressing Table-

Device	Interface	IP Address	Connects To
Cloud	Eth6	N/A	F0/0
	Coax7	N/A	Port0
Cable Modem	Port0	N/A	Coax7
	Port1	N/A	Internet
Router0	Console	N/A	RS232
	F0/0	192.168.2.1/24	Eth6
	F0/1	10.0.0.1/24	F0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	F1/0	172.16.0.1/24	F0/1
WirelessRouter	Internet	192.168.2.2/24	Port 1
	Eth1	192.168.1.1	F0
Family PC	F0	192.168.1.102	Eth1
Switch	F0/1	172.16.0.2	F1/0
Netacad.pka	F0	10.0.0.254	F0/1
Configuration Terminal	RS232	N/A	Console

Objectives-

1. Part 1: Connect to the Cloud
2. Part 2: Connect Router0
3. Part 3: Connect Remaining Devices
4. Part 4: Verify Connections
5. Part 5: Examine the Physical Topology

Part 1: Connect to the Cloud

Step 1: Connect the cloud to Router0.

Step 2: Connect the cloud to Cable Modem.

Part 2 : Connect Router0

Step 1: Connect Router0 to Router1

Step 2: Connect Router0 to netacad.pka

Step 3: Connect Router0 to Configuration Table

Part 3 : Connect Remaining Devices

Step 1 : Connect Router 1 to Switch

Step 2 : Connect Cable model to Wireless Router

Step 3 : Connect Wireless Router to Family PC.

Part 4: Verify Connections

Step 1: Test the connection from Family Pc to netacad.pka

Step 2: Ping the Switch from Home PC.

Step 3: Open Router0 from Configuration Terminal

Part 5 :Examine the Physical Topology

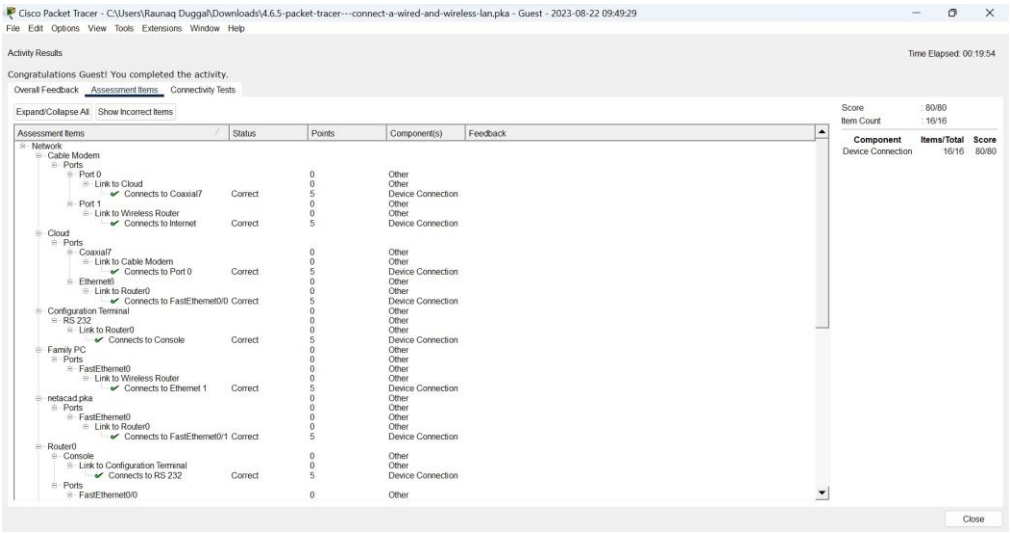
Step 1: Examine the Cloud

Step 2 : Examine the Primary Network

Step 3 : Examine the Secondary Network

Step 4: Examine the Home Network

Result- After the completion is shown 100%, the result shown will be like this:



Questions mentioned in the Experiment-

1. How many wires are connected to the switch in the blue rack?

   Ans: 2

2. What is located on the table to the right of the blue rack?

   Ans: Configuration Terminal

3. Why are there two orange cables connected to each device?

   Ans: Fibre cables come in pairs , one for transmit other for receive.

4. Why is there an oval mesh covering the home network?

   Ans: It represents the range of the wireless network.

5. Why is there no rack to hold the equipment?

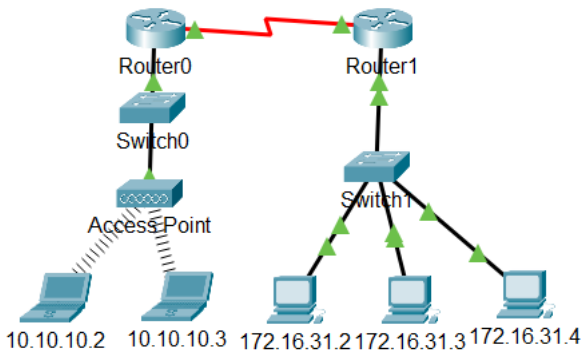
   Ans: Home networks typically do not have racks.

EXPERIMENT 6- TO EXAMINE ARP TABLE

Aim- To examine ARP Table.

Software Used- Cisco Packet Tracer

Topology –



Addressing Table-

Device	Interface	MAC Address	Switch Interface
Router0	Gg0/0	0001.6458.2501	G0/1
	S0/0/0	N/A	N/A
Router1	G0/0	00E0.F7B1.8901	G0/1
	S0/0/0	N/A	N/A
10.10.10.2	Wireless	0060.2F84.4AB6	F0/2
10.10.10.3	Wireless	0060.4706.572B	F0/2
172.16.31.2	F0	000C.85CC.1DA7	F0/1
172.16.31.3	F0	0060.7036.2849	F0/2
172.16.31.4	G0	0002.1640.8D75	F0/3

Objectives-

Part 1: Examine an ARP Request

Part 2: Examine a Switch MAC Address Table

Part 3: Examine the ARP Process in Remote Communications

Instructions-

Part 1: Examine an ARP Request

Step 1: Generate ARP requests by pinging 172.16.31.3 from 172.16.31.2. Open a command prompt a. Click 172.16.31.2 and open the Command Prompt.

b. Enter the arp -d command to clear the ARP table. Close a command prompt

c. Enter Simulation mode and enter the command ping 172.16.31.3. Two PDUs will be generated. The ping command cannot complete the ICMP packet without knowing the MAC address of the destination. So the computer sends an ARP broadcast frame to find the MAC address of the destination.

d. Click Capture/Forward once. The ARP PDU moves Switch1 while the ICMP PDU disappears, waiting for the ARP reply. Open the PDU and record the destination MAC address.

e. Click Capture/Forward to move the PDU to the next device.

f. Open the PDU and examine Layer 2.

g. Click Capture/Forward until the PDU returns to 172.16.31.2.

Step 2: Examine the ARP table.

a. Note that the ICMP packet reappears. Open the PDU and examine the MAC addresses.
b. Switch back to Realtime and the ping completes. c. Click 172.16.31.2 and enter the arp –a command

Part 2: Examine a Switch MAC Address Table

Step 1: Generate additional traffic to populate the switch MAC address table. Open a command prompt .

a. From 172.16.31.2, enter the ping 172.16.31.4 command.

b. Click 10.10.10.2 and open the Command Prompt.

c. Enter the ping 10.10.10.3 command

Step 2: Examine the MAC address table on the switches

a. Click Switch1 and then the CLI tab. Enter the show mac-address-table command.
b. Click Switch0, then the CLI tab. Enter the show mac-address-table command.

Part 3: Examine the ARP Process in Remote Communications

Step 1: Generate traffic to produce ARP traffic. Open a command prompt

a. Click 172.16.31.2 and open the Command Prompt.

b. Enter the ping 10.10.10.1 command.

c. Type arp –a

d. Enter arp -d to clear the ARP table and switch to Simulation mode

e. Repeat the ping to 10.10.10.1.

f. Click Capture/Forward. Click the PDU that is now at Switch1.

g. The destination IP address is not 10.10.10.1.

Step 2: Examine the ARP table on Router1.

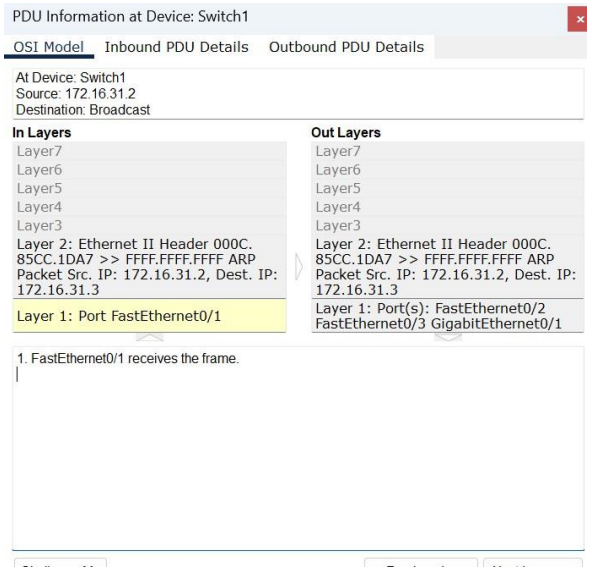
a. Switch to Realtime mode. Click Router1 and then the CLI tab.

b. Enter privileged EXEC mode and then the show mac-address-table command.

c. Enter the show arp command.

Result-

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -d
C:\>ping 172.16.31.3

Pinging 172.16.31.3 with 32 bytes of data:

Reply from 172.16.31.3: bytes=32 time<1ms TTL=128
Reply from 172.16.31.3: bytes=32 time<1ms TTL=128
Reply from 172.16.31.3: bytes=32 time<1ms TTL=128
Reply from 172.16.31.3: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.31.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



PDU Information at Device: 172.16.31.2

OSI Model | Outbound PDU Details

At Device: 172.16.31.2
Source: 172.16.31.2
Destination: 172.16.31.3

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer 2: Ethernet II Header 000C.85CC.1DA7 >> 0060.7036.2849
Layer1	Layer 1: Port(s): FastEthernet0

1. The ARP process takes out this packet from the buffer and resends it.
2. The device encapsulates the PDU into an Ethernet frame.

```
C:\>arp -a
  Internet Address      Physical Address      Type
  172.16.31.3           0060.7036.2849        dynamic
```

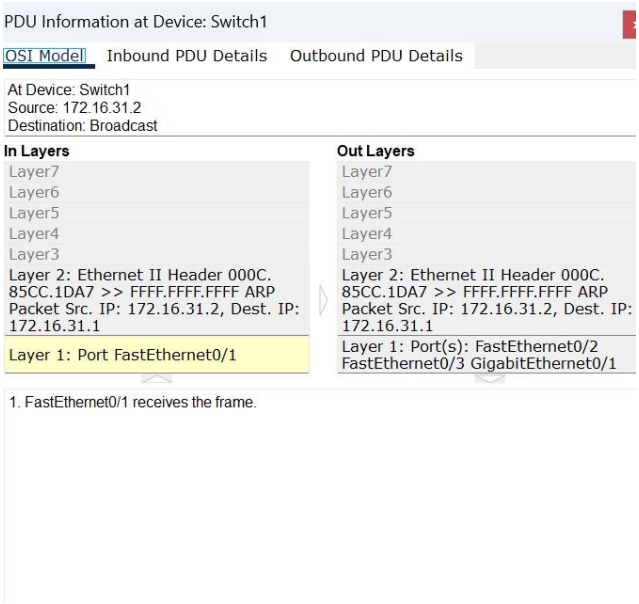
```
C:\>ping 172.16.31.4

Pinging 172.16.31.4 with 32 bytes of data:

Reply from 172.16.31.4: bytes=32 time<1ms TTL=128
Reply from 172.16.31.4: bytes=32 time<1ms TTL=128
Reply from 172.16.31.4: bytes=32 time<1ms TTL=128
Reply from 172.16.31.4: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.31.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Reply from 10.10.10.3: bytes=32 time=51ms TTL=128
Reply from 10.10.10.3: bytes=32 time=21ms TTL=128
Reply from 10.10.10.3: bytes=32 time=15ms TTL=128
Reply from 10.10.10.3: bytes=32 time=19ms TTL=128

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 51ms, Average = 26ms
```

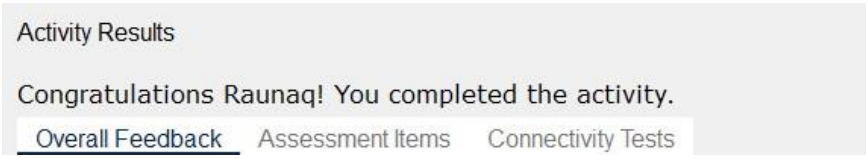
```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0002.1640.8d75    DYNAMIC     Fa0/3
   1    000c.85cc.1da7    DYNAMIC     Fa0/1
   1    00e0.f7b1.8901    DYNAMIC     Gig0/1
Switch#
```

```
Switch0>enable
Switch0#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.6458.2501    DYNAMIC     Gig0/1
   1    0060.2f84.4ab6    DYNAMIC     Fa0/2
   1    0060.4706.572b    DYNAMIC     Fa0/2
Switch0#S
```

```
C:\>arp -a
  Internet Address      Physical Address      Type
  172.16.31.1           00e0.f7b1.8901        dynamic
  172.16.31.3           0060.7036.2849        dynamic
  172.16.31.4           0002.1640.8d75        dynamic
```




```
Router>enable
Router#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.31.1             -   00E0.F7B1.8901  ARPA   GigabitEthernet0/0
Internet  172.16.31.2             1   000C.85CC.1DA7  ARPA   GigabitEthernet0/0
Router#
```



Questions mentioned in the experiment-

1. What is the IP address of the device that accepted the PDU?

Ans 172.16.31.3

2. What happened to the source and destination MAC addresses?

Ans Source became destination, FFFF.FFFF.FFFF turned into MAC address of 172.16.31.3

3. How many copies of the PDU did the switch make during the ARP reply?

Ans 1

4. Do the MAC addresses of the source and destination align with their IP addresses?

Ans Yes

5. To what IP address does the MAC address entry correspond?

Ans 172.16.31.3

6. In general, when does an end device issue an ARP request?

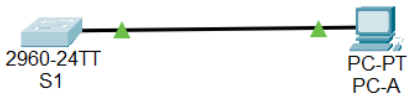
Ans When it does not know the receiver’s MAC address.

EXPERIMENT 7- TO VIEW NETWORK DEVICE MAC ADDRESSES

Aim- To View Network Device MAC Addresses.

Software Used- Cisco Packet Tracer

Topology-



Addressing Table-

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.3	255.255.255.0

Objectives –

Part 1: Configure Devices and Verify Connectivity.

Part 2: Display, Describe, and Analyse Ethernet MAC Addresses.

Instructions-

Part 1: Configure Devices and Verify Connectivity In this part, you will set up the network topology and configure basic settings, such as the interface IP addresses and device name. For device name and address information, refer to the Topology and Addressing Table.

Step 1: Cable the network as shown in the topology

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

b. Power on all the devices in the topology.

Step 2: Configure the IPv4 address for the PC

a. Configure the IPv4 address, subnet mask for PC-A.

b. From the command prompt on PC-A, ping the switch address.

Step 3: Configure basic settings for the switch. In this step, you will configure the device name and the IP address, and disable DNS lookup on the switch.

a. Console into the switch and enter global configuration mode.
b. Assign a hostname to the switch based on the Addressing Table.
c. Disable DNS lookup.
d. Configure and enable the SVI interface for VLAN 1.

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


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interface vlan1
S1(config-if)#ip address 192.168.1.2 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

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

Step 4: Verify network connectivity. Ping the switch from PC-A

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Step 1: Analyze the MAC address for the PC-A NIC.

Before you analyze the MAC address on PC-A, look at an example from a different PC NIC. You can issue the ipconfig /all command to view the MAC address of your NIC.

Step 2: Analyze the MAC address for the S1 F0/6 interface. You can use a variety of commands to display MAC addresses on the switch. a. Console into S1 and use the show interfaces vlan 1 command to find the MAC address information. A sample is shown below. Use output generated by your switch to answer the questions.

b. Another way to display the MAC address on the switch is to use the show arp command. Use the show arp command to display MAC address information. This command maps the Layer 2 address to its corresponding Layer 3 address. A sample is shown below. Use output generated by your switch to answer the questions.

Step 3: View the MAC addresses on the switch. Issue the show mac address-table command on S1. A sample is shown below. Use output generated by your switch to answer the questions.

```
S1#show interface vlan1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0007.ec40.2899 (bia 0007.ec40.2899)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out

S1#
```

```
S1#
S1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.2             -   0007.EC40.2899  ARPA   Vlan1
Internet  192.168.1.3             2   0001.64AD.17A2  ARPA   Vlan1
S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.64ad.17a2    DYNAMIC     Fa0/1
S1#
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=5ms TTL=128
Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms

C:\>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<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms 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 = 0ms, Average = 0ms

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0001.64AD.17A2
   Link-local IPv6 Address.........: FE80::201:64FF:FEAD:17A2
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-D3-13-C6-0D-00-01-64-AD-17-A2
```

Questions mentioned in the experiment-

1. What is the OUI portion of the MAC address for this device?

   Ans 5C-26-0A

2. What is the serial number portion of the MAC address for this device?

   Ans 24-2A-60

3. What is the MAC address for VLAN 1 on S1?

Ans 001b.0c6d.8f40

4. What is the MAC serial number for VLAN 1?

Ans 6d-8f-40

5. What is the OUI for VLAN 1?

Ans 00-1b-0c

6. Based on this OUI, what is the name of the vendor?

Ans Cisco Systems

7. What does bia stand for?

Ans Burned in address

8. Why does the output show the same MAC address twice?

Ans The MAC address can be changed via a software command. The actual address (bia) will still be there. It is shown in the parenthesis.

9. What Layer 2 addresses are displayed on S1?

Ans S1 VLAN 1 and PC-A MAC addresses.

10. What Layer 3 addresses are displayed on S1?

Ans S1 and PC-A IP addresses.

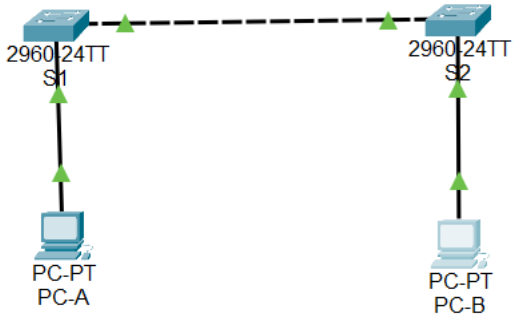
Result- Hence, we viewed the Network Device MAC Address.

EXPERIMENT 8- TO VIEW THE SWITCH MAC ADDRESS TABLE

Aim- To View the Switch MAC Address Table.

Software Used- Cisco Packet Tracer

Topology-



Addressing Table-

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	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: Build and Configure the Network

Part 2: Examine the Switch MAC Address Table

Instructions-

Part 1: Build and Configure the Network

Step 1: Cable the network according to the topology.

Step 2: Configure PC hosts.

Step 3: Initialize and reload switches as necessary.

Step 4: Configure basic settings for each switch.

a. Configure device name as shown in the topology.

b. Configure IP address as listed in Addressing Table.

c. Assign cisco as the console and vty passwords.

d. Assign class as the privileged EXEC password.

Part 2: Examine the Switch MAC Address Table. A switch learns MAC addresses and builds the MAC address table, as network devices initiate communication on the network.

Step 1: Record network device MAC addresses.

a. Open a command prompt on PC-A and PC-B and type ipconfig /all.

b. Console into switch S1 and S2 and type the show interface F0/1 command on each switch.

Step 2: Display the switch MAC address table. Console into switch S2 and view the MAC address table, both before and after running network communication tests with ping.

a. Establish a console connection to S2 and enter privileged EXEC mode. Open a configuration window.

b. In privileged EXEC mode, type the show mac address-table command and press Enter.

Step 3: Clear the S2 MAC address table and display the MAC address table again

a. In privileged EXEC mode, type the clear mac address-table dynamic command and press Enter. S2# clear mac address-table dynamic

b. Quickly type the show mac address-table command again.

Step 4: From PC-B, ping the devices on the network and observe the switch MAC address table. a. From PC-B, open a command prompt and type arp -a.

b. From the PC-B command prompt, ping PC-A, S1, and S2.

c. From a console connection to S2, enter the show mac address-table command.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>PING 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 3ms
```

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=5ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 2ms
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#interfave vlan1
                  ^
% Invalid input detected at '^' marker.

S1(config)#interface vlan1
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

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

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#interface vlan1
S2(config-if)#ip address 192.168.1.12 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S2(config-if)#exit
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 15
S2(config-line)#pass cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#enable secret class
S2(config)#
```

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0000.0CA0.DB41
   Link-local IPv6 Address.........: FE80::200:CFF:FEA0:DB41
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.1
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-BD-31-EA-BC-00-00-0C-A0-DB-41
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.................: 0001.9716.51AE
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-BD-31-EA-BC-00-00-0C-A0-DB-41
   DNS Servers.....................: ::
                                     0.0.0.0
```

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 00E0.A330.3080
   Link-local IPv6 Address.........: FE80::2E0:A3FF:FE30:3080
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-C0-1D-67-53-00-E0-A3-30-30-80
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.................: 0060.2F1B.A2D5
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-C0-1D-67-53-00-E0-A3-30-30-80
   DNS Servers.....................: ::
                                     0.0.0.0
```

Questions mentioned in the experiment-

1. What are the Ethernet adapter physical addresses?

Ans PC-A MAC Address- 00-50-56-B3-27-D6

PC-B MAC Address- 00-50-56-B3-FF-54

2. Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed?

Ans No, it is discovered that the MAC address for the other switch's F0/1 switch port has been quickly reinserted in the MAC address table.

3. Are there new addresses in the MAC address table?

Ans Answers will vary.

Result- Hence, we viewed the Switch MAC Address Table.

EXPERIMENT 9- TO CONFIGURE INITIAL ROUTER SETTINGS

Aim: To perform basic and initial router configuration

Devices Used: Router, PCs, and Console Cable.

Objectives:

Part 1: Verify the Default Router Configuration

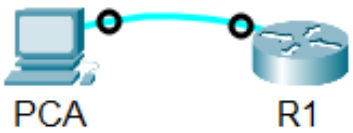
Part 2: Configure and Verify the Initial Router Configuration

Part 3: Save the Running Configuration File

Background:

In this activity, you will perform basic router configuration tasks. You will secure access to the CLI and console port using encrypted and plain-text passwords. You will also configure messages for users who are logging into the router. These banners warn unauthorized users that access is prohibited. Finally, you will verify and save your running configuration.

Figure:



Procedure:

Part 1: Verify the Default Router Configuration

Step 1: Establish a console connection to R1.

a) Choose a Console cable from the available connections.

b) Click PCA and select RS 232.

c) Click R1 and select Console.

d) Click PCA > Desktop tab > Terminal.

e) Click OK and press ENTER. You are now able to configure R1.

Part 2: Configure and Verify the Initial Router Configuration Step 1: Perform initial router configuration

Router> enable

Router# show running-config Router# show startup-config Router# configure terminal Router(config) hostname R1

R1(config)# banner motd #Unauthorized access is strictly prohibited# R1(config)#enable password cisco

R1(config)#enable secret itsasecret R1(config)#line console 0 R1(config)#password letmein R1(config)#login

R1(config)#service password-encyrption R1(config)#exit

R1#show running-config

R1#copy running-config startup-config R1# exit

Step 2:Verify the initial router configuration

a. Verify the initial settings by viewing the configuration for R1. Type your answers here.

b. Exit the current console session until you see the following message:

R1 con0 is now available Press RETURN to get started.

c. Press ENTER; you should see the following message:

Unauthorized access is strictly prohibited. User Access Verification

Password:

Part 3: Save Running Configuration to NVRAM file

You have configured the initial settings for R1. 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.

Questions:

Q.1) What is the router's hostname?

Ans) Router

Q.2) How many Fast Ethernet interfaces does the Router have?

Ans) none

Q.3) How many Gigabit Ethernet interfaces does the Router have?

Ans) 2

Q.4) How many Serial interfaces does the router have?

Ans) 2

Q.5) What is the range of values shown for the vty lines?

Ans) 0-4

Q.6) What command do you use to verify initial configuration on router?

Ans) show running-config

Q.7) Why should every router have a message-of-the-day (MOTD) banner?

Ans) Every router should have a banner to warn unauthorized users that access is prohibited. MOTD Banners can also be used to send messages to network personnel (such as impending system shutdowns or who to contact for access).

Q.8) f you are not prompted for a password before reaching the user EXEC prompt, what console line command did you forget to configure?

Ans) R1(config-line)# login

Q.9) If you configure any more passwords on the router, are they displayed in the configuration file as plain text or in encrypted form? Explain.

Ans) The service password-encryption command encrypts all current and future passwords.

Q.10) What command did you enter to save the configuration to NVRAM?

Ans) copy running-config startup-config

Q.11) Which command displays the contents of the NVRAM?

Ans) show startup-configuration or show start

Result:

```
Router>enable
Router#show running-config
Building configuration...

Current configuration : 1110 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX152459PZ
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
```

```
Router#show startup-config
startup-config is not present
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#banner motd #Unautorised access is strictly prohibited.#
R1(config)#enable password cisco
R1(config)#ensable secret itsasecret
          ^
% Invalid input detected at '^' marker.

R1(config)#enable secret itsasecret
R1(config)#line console 0
R1(config-line)#password letmein
R1(config-line)#login
R1(config-line)#exit
```

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Congratulations Raunaq! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All | Show Incorrect Items

Assessment Items	Status	Points
Network		
PCA		0
RS 232		0
Link to R1		0
✔ Connects to Console	Correct	8
R1		
✔ Banner MOTD	Correct	8
Console		0
Link to PCA		0
✔ Connects to RS 232	Correct	8
Console Line		
✔ Login	Correct	8
✔ Password	Correct	8
✔ Enable Password	Correct	8
✔ Enable Secret	Correct	8
✔ Host Name	Correct	8
✔ Service Password Encryption	Correct	8
✔ Startup Config	Correct	8

Score : 80/80
Item Count : 10/10

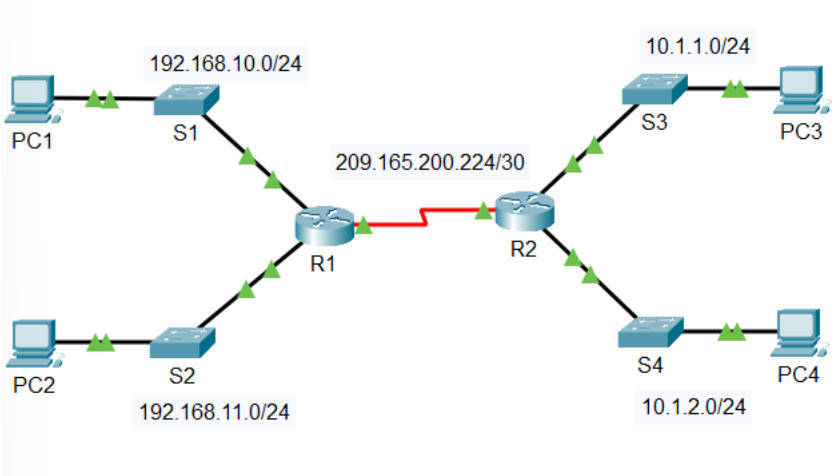
Component	Items/Total	Score
Basic Security Configuration	6/6	48/48
Configuration Management	1/1	8/8
Device Connection	2/2	16/16
Hostname Configuration	1/1	8/8

EXPERIMENT 10-TO CONNECT A ROUTER TO A LAN

Aim- To connect a router to a LAN.

Software Used- Cisco Packet Tracer

Topology-



Addressing Table-

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0 (DCE)	209.165.200.225	255.255.255.252	N/A
R2	G0/0	10.1.1.1	255.255.255.0	N/A
	G0/1	10.1.2.1	255.255.255.0	N/A
	S0/0/0	209.165.200.226	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	10.1.1.10	255.255.255.0	10.1.1.1
PC4	NIC	10.1.2.10	255.255.255.0	10.1.2.1

Objectives –
Part 1: Display Router Information
Part 2: Configure Router Interfaces
Part 3: Verify the Configuration

Part 1: Display Router Information

Step 1: Display interface information on R1.

Note: Click a device and then click the CLI tab to access the command line directly. The console password is cisco. The privileged EXEC password is class.

a. Enter the command to display the statistics for the Serial 0/0/0 interface on R1 .

b. Enter the command to display the statistics for the Gigabit Ethernet 0/0 interface

Step 2: Display a summary list of the interfaces on R1.

Step 3: Display the routing table on R1.

Part 2: Configure Router Interfaces

Step 1: Configure the GigabitEthernet 0/0 interface on R1.

a. Enter the following commands to address and activate the GigabitEthernet 0/0 interface on R1:

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config-if)#description LAN connection to S1
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#ping 192.168.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

b. It is good practice to configure a description for each interface to help document the network. Configure an interface description that indicates the device to which it is connected.

c. R1 should now be able to ping PC1

Step 2: Configure the remaining Gigabit Ethernet Interfaces on R1 and R2.

a. Use the information in the Addressing Table to finish the interface configurations for R1 and R2. For each interface, do the following:

1) Enter the IP address and activate the interface.

2) Configure an appropriate description.

b. Verify interface configurations.

Step 3: Back up the configurations to NVRAM. Question: Save the configuration files on both routers to NVRAM.

Part 3: Verify the Configuration

Step 1: Use verification commands to check your interface configurations.

a. Use the show ip interface brief command on both R1 and R2 to quickly verify that the interfaces are configured with the correct IP address and are active.

b. Use the show ip route command on both R1 and R2 to view the current routing tables.

Step 2: Test end-to-end connectivity across the network.

You should now be able to ping from any PC to any other PC on the network. In addition, you should be able to ping the active interfaces on the routers. For example, the following tests should be successful:

• From the command line on PC1, ping PC4.

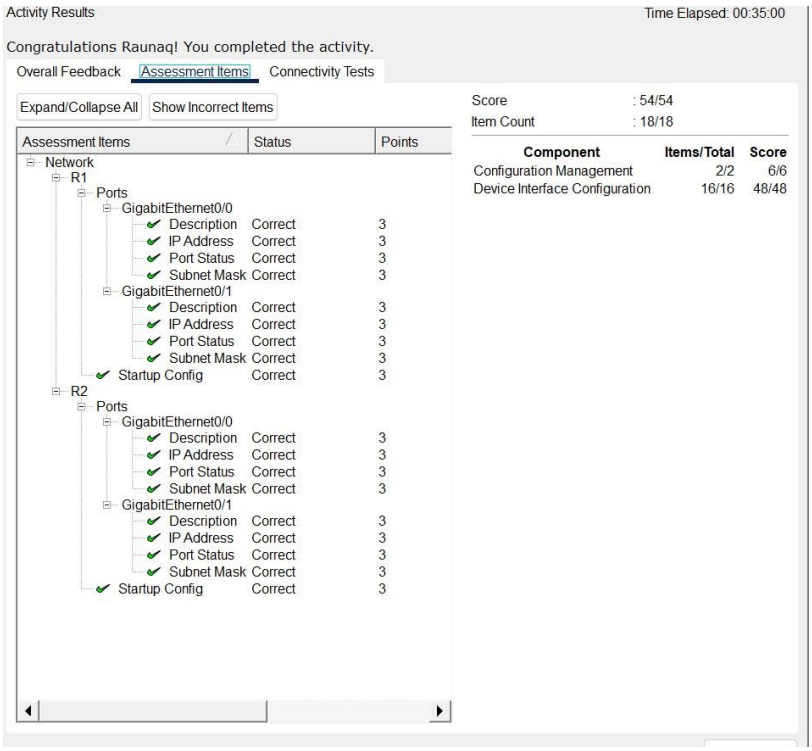
• From the command line on R2, ping PC2.

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config-if)#description LAN connection to S2
R1(config-if)#
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface gig 0/1
R2(config-if)#ip addrss 10.1.2.1 255.255.255.0
                 ^
% Invalid input detected at '^' marker.

R2(config-if)#ip address 10.1.2.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to u

R2(config-if)#description LAN connection to S4
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.1.1.1        YES manual up                    up
GigabitEthernet0/1     10.1.2.1        YES manual up                    up
Serial0/0/0            209.165.200.226 YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.1.1.1        YES manual up                    up
GigabitEthernet0/1     10.1.2.1        YES manual up                    up
Serial0/0/0            209.165.200.226 YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R2#show interfaces gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 0002.16cb.1d01 (bia 0002.16cb.1d01
  Description: LAN connection to S3
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 93 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 1017 multicast, 0 pause input
```

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

```
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```



Questions Mentioned in the Experiment-

1. What is the IP address configured on R1?

Ans 209.165.200.225/30

2. What is the bandwidth on the Serial 0/0/0 interface?

Ans 1544 kbits

3. What is the IP address on R1?

Ans There is no IP address configured on the GigabitEthernet 0/0 interface.

4. What is the MAC address of the GigabitEthernet 0/0 interface?

Ans 000d.bd6c.7d01

5. What is the bandwidth on the GigabitEthernet 0/0 interface?

Ans 1000000 kbits

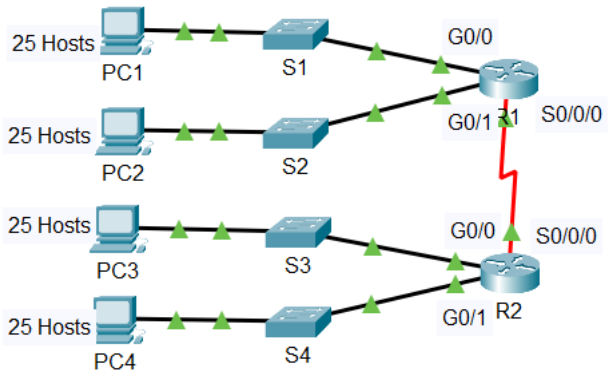
Result- Hence, we have connected a Router to LAN.

EXPERIMENT 11-SUBNETTING SCENARIO

Aim- To understand the Subnetting Scenario.

Software Used- Cisco Packet Tracer

Topology-



Objectives-

Part 1: Design an IP Addressing Scheme

Part 2: Assign IP Addresses to Network Devices and Verify Connectivity

Addressing Table-

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.100.1	255.255.255.224	N/A
	G0/1	192.168.100.33	255.255.255.224	N/A
	S0/0/0	192.168.100.129	255.255.255.224	N/A
R2	G0/0	192.168.100.65	255.255.255.224	N/A
	G0/1	192.168.100.97	255.255.255.224	N/A
	S0/0/0	192.168.100.158	255.255.255.224	N/A
S1	VLAN 1	192.168.100.2	255.255.255.224	192.168.100.1
S2	VLAN 1	192.168.100.34	255.255.255.224	192.168.100.33
S3	VLAN 1	192.168.100.66	255.255.255.224	192.168.100.65
S4	VLAN 1	192.168.100.98	255.255.255.224	192.168.100.97
PC1	NIC	192.168.100.30	255.255.255.224	192.168.100.1
PC2	NIC	192.168.100.62	255.255.255.224	192.168.100.33
PC3	NIC	192.168.100.94	255.255.255.224	192.168.100.65
PC4	NIC	192.168.100.126	255.255.255.224	192.168.100.97

Part 1: Design an IP Addressing Scheme

Step 1: Subnet the 192.168.100.0/24 network into the appropriate number of subnets.

Subnet Table -

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	192.168.100.0	192.168.100.1	192.168.100.30	192.168.100.31
1	192.168.100.32	192.168.100.33	192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.65	192.168.100.94	192.168.100.95
3	192.168.100.96	192.168.100.97	192.168.100.126	192.168.100.127
4	192.168.100.128	192.168.100.129	192.168.100.158	192.168.100.159
5	192.168.100.160	192.168.100.161	192.168.100.190	192.168.100.191
6	192.168.100.192	192.168.100.193	192.168.100.222	192.168.100.223
7	192.168.100.224	192.168.100.225	192.168.100.254	192.168.100.255

Step 2: Assign the subnets to the network shown in the topology.

Step 3: Document the addressing scheme.

Part 2: Assign IP Addresses to Network Devices and Verify Connectivity

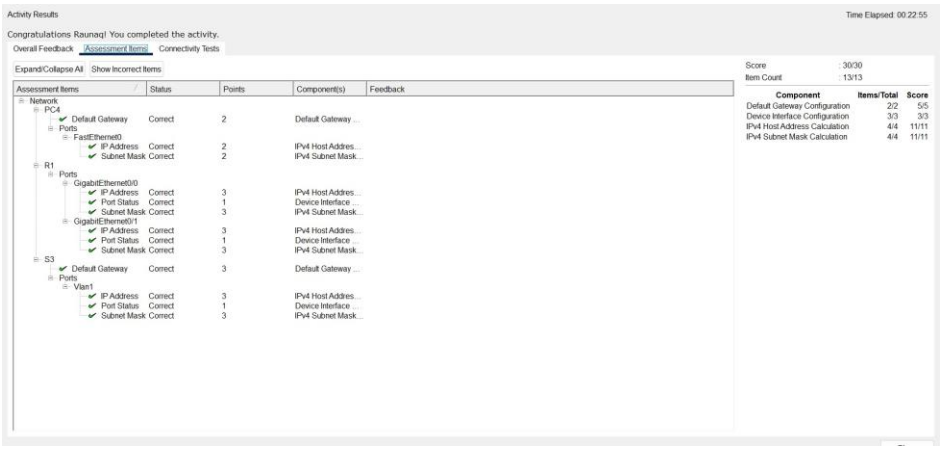
Step 1: Configure R1 LAN interfaces.

Step 2: Configure IP addressing on S3.

Step 3: Configure PC4.

Step 4: Verify connectivity.

Result-

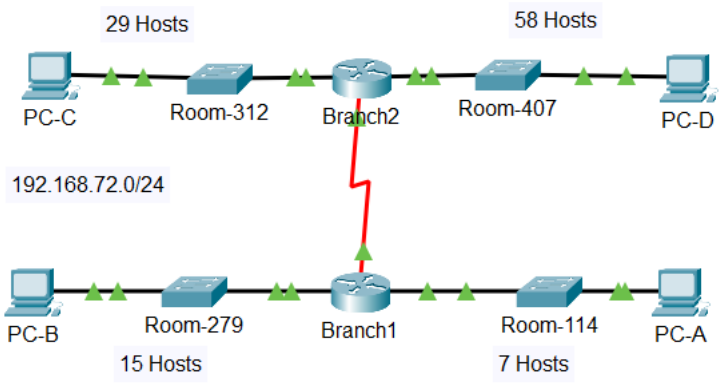


EXPERIMENT 12-VLSM DESIGN AND IMPLEMENTATION

Aim- To study VLSM Design and Implementation.

Software Used- Cisco Packet Tracer

Topology-



Objectives-

Part 1: Examine the Network Requirements

Part 2: Design the VLSM Addressing Scheme

Part 3: Assign IP Addresses to Devices and Verify Connectivity

Addressing Table

Device	Interface	Address	Subnet Mask	Default Gateway
Branch 1	G0/0	192.168.72.129	255.255.255.240	N/A
	G0/1	192.168.72.97	255.255.255.224	N/A
	S0/0/0	192.162.72.145	255.255.255.252	N/A
Branch2	G0/0	192.168.72.65	255.255.255.248	N/A
	G0/1	192.168.72.1	255.255.255.192	N/A
	S0/0/0	192.168.72.146	255.255.255.252	N/A
Room-114	VLAN 1	192.168.72.130	255.255.255.240	192.168.72.129

Device	Interface	Address	Subnet Mask	Default Gateway
Room-279	VLAN 1	192.168.72.96	255.255.255.224	192.168.72.97
Room-312	VLAN 1	192.168.72.66	255.255.255.248	192.168.72.65
Room-407	VLAN 1	192.168.72.2	255.255.255.192	192.168.72.1
PC-A	NIC	192.168.72.142	255.255.255.240	192.168.72.129
PC-B	NIC	192.168.72.126	255.255.255.224	192.168.72.97
PC-C	NIC	192.168.72.94	255.255.255.248	192.168.72.65
PC-D	NIC	192.168.72.62	255.255.255.192	192.168l.72.1

Instructions

Part 1: Examine the Network Requirements

Step 1: Determine the number of subnets needed.

You will subnet the network address **192.168.72.0/24**. The network has the following requirements:

- **Room-114** LAN will require **7** host IP addresses
- **Room-279** LAN will require **15** host IP addresses
- **Room-312** LAN will require **29** host IP addresses
- **Room-407** LAN will require **58** host IP addresses

Step 2: Determine the subnet mask information for each subnet.

Part 2: Design the VLSM Addressing Scheme

Step 1: Divide the 192.168.72.0/24 network based on the number of hosts per subnet.

a. Use the first subnet to accommodate the largest LAN.

b. Use the second subnet to accommodate the second largest LAN.

c. Use the third subnet to accommodate the third largest LAN.

d. Use the fourth subnet to accommodate the fourth largest LAN.

e. Use the fifth subnet to accommodate the connection between **Branch1** and **Branch2**.

Step 2: Document the VLSM subnets.

Step 3: Document the addressing scheme.

a. Assign the first usable IP addresses to **Branch1** for the two LAN links and the WAN link.

b. Assign the first usable IP addresses to **Branch2** for the two LAN links. Assign the last usable IP address for the WAN link.

c. Assign the second usable IP addresses to the switches.

d. Assign the last usable IP addresses to the hosts.

Part 3: Assign IP Addresses to Devices and Verify Connectivity

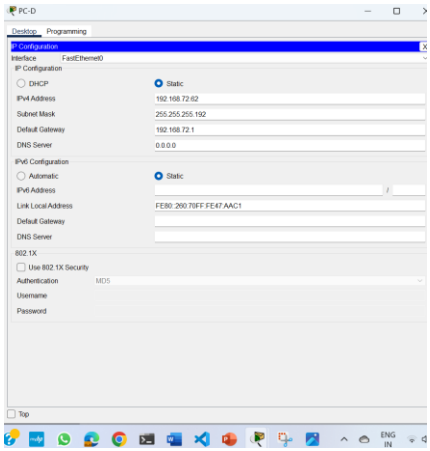
Most of the IP addressing is already configured on this network. Implement the following steps to complete the addressing configuration.

Step 1: Configure IP addressing on the Branch1 router LAN interfaces.

Step 2: Configure IP addressing on the Room-312, switch including the default gateway.

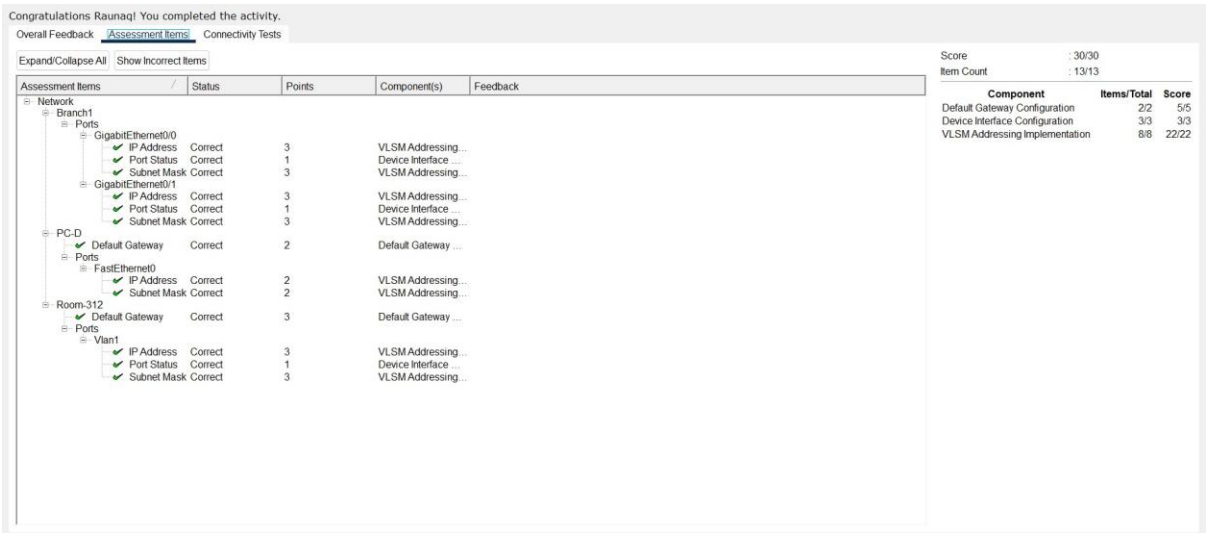
Step 3: Configure IP addressing on PC-D, including the default gateway.

Step 4: Verify connectivity.




```
C:\>ping 192.168.72.97

Pinging 192.168.72.97 with 32 bytes of data:

Reply from 192.168.72.97: bytes=32 time=1ms TTL=254
Reply from 192.168.72.97: bytes=32 time=1ms TTL=254
Reply from 192.168.72.97: bytes=32 time=1ms TTL=254
Reply from 192.168.72.97: bytes=32 time=25ms TTL=254

Ping statistics for 192.168.72.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 25ms, Average = 7ms

C:\>ping 192.168.72.98

Pinging 192.168.72.98 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.72.98: bytes=32 time=25ms TTL=253
Reply from 192.168.72.98: bytes=32 time=40ms TTL=253

Ping statistics for 192.168.72.98:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 40ms, Average = 32ms

C:\>ping 192.168.72.142

Pinging 192.168.72.142 with 32 bytes of data:

Request timed out.
Reply from 192.168.72.142: bytes=32 time=1ms TTL=126
Reply from 192.168.72.142: bytes=32 time=60ms TTL=126
Reply from 192.168.72.142: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.72.142:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 60ms, Average = 20ms
```

Result- Hence we have studied the VLSM Design and Implementation.



Congratulations Raunaq! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Expand/Collapse All | Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
Branch1				
Ports				
GigabitEthernet0/0				
IP Address	Correct	3	VLSM Addressing...	
Port Status	Correct	1	Device Interface ...	
Subnet Mask	Correct	3	VLSM Addressing...	
GigabitEthernet0/1				
IP Address	Correct	3	VLSM Addressing...	
Port Status	Correct	1	Device Interface ...	
Subnet Mask	Correct	3	VLSM Addressing...	
PC-D				
Default Gateway	Correct	2	Default Gateway ...	
Ports				
FastEthernet0				
IP Address	Correct	2	VLSM Addressing...	
Subnet Mask	Correct	2	VLSM Addressing...	
Room-312				
Default Gateway	Correct	3	Default Gateway ...	
Ports				
Vlan1				
IP Address	Correct	3	VLSM Addressing...	
Port Status	Correct	1	Device Interface ...	
Subnet Mask	Correct	3	VLSM Addressing...	

Score : 30/30
Item Count : 13/13

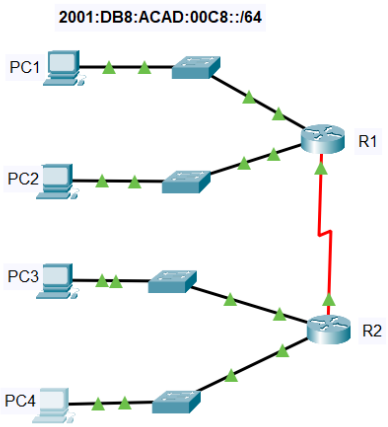
Component	Items/Total	Score
Default Gateway Configuration	2/2	5/5
Device Interface Configuration	3/3	3/3
VLSM Addressing Implementation	8/8	22/22

EXPERIMENT 13- IMPLEMENT A SUBNETTED IPV6 ADDRESSING SCHEME

Aim- To implement a subnetted IPv6 addressing scheme.

Software Used- Cisco Packet Tracer

Topology-



Addressing Table-

Device	Interface	IPv6 Address	Link-local Address
R1	G0/0	2001:db8:acad:00c8::1/64	fe80::1
R1	G0/1	2001:db8:acad:00c9::1/64	fe80::1
R1	S0/0/0	2001:db8:acad:00cc::1/64	fe80::1
R2	G0/0	2001:db8:acad:00ca::1/64	fe80::2
R2	G0/1	2001:db8:acad:00cb::1/64	fe80::2
R2	S0/0/0	2001:db8:acad:00cc::2/64	fe80::2
PC1	NIC	Auto Config	
PC2	NIC	Auto Config	
PC3	NIC	Auto Config	
PC4	NIC	Auto Config	

Objectives-

Step 1: Determine IPv6 subnets and addressing scheme.

Step 2: Configure IPv6 addressing on routers and PCs.

Step 3: Verify IPv6 connectivity

Instructions -

Step 1: Determine IPv6 subnets and addressing scheme.

Step 2: Configure IPv6 addressing on routers and PCs.

Step 3: Verify IPv6 connectivity.

CLI Mode of R1-

```
R1(config)#interface gigabit ethernet 0/1
                                     ^
% Invalid input detected at '^' marker.

R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:00c9::1/64
R1(config-if)#ipv6 address fe 80::1 link-local
                              ^
% Invalid input detected at '^' marker.

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config-if)#interface serial 0/0/0/0
                 ^
% Invalid input detected at '^' marker.

R1(config-if)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:00cc::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R1(config-if)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:00c8::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

```
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#
```

CLI Mode Of R2-

```
R2>enable
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ipv6 address 2001:db8:acad:00ca::1/64
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2(config-if)#exit
R2(config)#interface gigabitethernet 0/1
R2(config-if)#ipv6 address 2001:db8:acad:00cb::1/64
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R2(config-if)#exit
R2(config)#interface serial 0/0/0
R2(config-if)#ipv6 address 2001:db8:acad:00cc::2/64
R2(config-if)#ipv6 address fe80::2 link-local
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#
```

```
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#
```

Result- Hence we have implemented a subnetted IPv6 Addressing Scheme .