INDEX

S.No	Experiment Name	Date of Allocation	Date of Submission	Signature
1.	Know your devices			
2.	To Configure initial Switch Settings			
3.	To implement basic connectivity			
4.	Basic switch and end device configuration			
5.	To connect the physical layer			
6.	To examine ARP Table.			
7.	To View Network Device MAC Addresses.			
8.	To View the Switch MAC Address Table.			
9.	To perform basic and initial router configuration			
10.	To connect a router to a LAN			

11	Understand Subnetting scenario			
12	Study VLSM design and implementation			
13	Implement subnetted IPv6 addressing scheme			

EXPERIMENT-1

Aim:
Know your devices.

Theory:

- **Cables: -**

- **Straight Cable:**
  A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal.

- **Crossover Cable:**
  The wire at pin 1 on one end of the cable connects to pin 3 at the other end of the cable. The wire at pin 2 connects to pin 6 on the other end of the cable. Remaining wires connect in the same positions at both ends.

- **Coaxial Cable:**
  A coaxial cable is an electrical cable with a copper conductor and an insulator shielding around it and a braided metal mesh that prevents signal interference and cross talk. Coaxial cable is also known as coax.

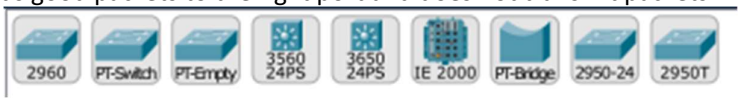
- **Data Terminal Equipment (DTE):**
  It is a device that is an information source or an information sink. It produces data and transfers them to a DCE, with essential control characters. Examples of DTE include computers, printers, and routers, etc.

- **Data Circuit Terminating Equipment (DCE):**
  It is a device used as an interface between a DTE. It converts signals to a format appropriate to transmission medium and introduces it onto network line. Examples of DCE include modem, ISDN adaptors, satellites, and network interface cards, etc.

- **Router:**
  A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

- **Switch:**

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (many ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it particularly effective because it only forwards good packets to the right port and does not transmit packets with problems.



- The Cisco® Catalyst® 2960 Series is a family of fixed- configuration, standalone switches that provide Fast Ethernet and Gigabit Ethernet connectivity and support enhanced switching services, advanced security, IP communications, wireless networking, and scalable management.
- The Cisco Catalyst 2950 Series is a line of fixed-configuration, stackable, and standalone switches that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity.

- The Cisco® Catalyst® 3560 Series is a line of fixed-configuration, enterprise-class switches that include IEEE 802.3af and Cisco prestandard Power over Ethernet (PoE) functionality in Fast Ethernet and Gigabit Ethernet configurations.

- **Hub:**

  In essence, a hub is a multi-port repeater. A hub joins several wires that come from several branches, like the connector in a star topology that joins various stations. Data packets are delivered to all connected devices since hubs are unable to filter data. In other words, all hosts connected by Hub continue to share a single collision domain. Additionally, they lack the intelligence to choose the best route for data packets, which results in waste and inefficiency.

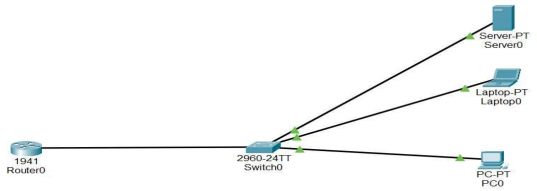
- **End Devices:**

  An end device is either the source or destination of a message transmitted over the network.
  - Computers (workstations, laptops, file servers, and web servers)
  - Network printers
  - VoIP phones
  - TelePresence endpoints
  - Security cameras
  - Mobile handheld devices

Result:

Successfully studied about all the devices.

Today's Lab Work:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT-2

AIM:

To Configure initial Switch Settings.

Devices Used:
Switches, PCs, and Cable**s**

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

Part 1: Verify the Default Switch Configuration
- Step 1: Enter privileged EXEC mode.
- Step 2: Examine the current switch configuration.

Part 2: Create a Basic Switch Configuration
- Step 1: Assign a name to a switch.
- Step 2: Secure access to the console line.
- Step 3: Verify that console access is secured.
- Step 4: Secure privileged mode access.
- Step 5: Verify that privileged mode access is secure.
- Step 6: Configure an encrypted password to secure access to privileged mode.
- Step 7: Verify that the enable secret password is added to the configuration file.
- Step 8: Encrypt the enable and console passwords.

Q.) What is Cisco Enable Secret Password (Encrypted Privileged Exec Password)?
Ans) The "enable secret" password in Cisco networking refers to the password used to protect access to privileged EXEC mode, which is a higher level of command-line access with more advanced configuration and management capabilities. This password is used to restrict unauthorized users from gaining elevated privileges on Cisco networking devices, such as routers and switches.

Q.) 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.
Ans) When we configure additional passwords on a Cisco switch or any other Cisco networking device, the passwords will be stored in the configuration file in encrypted form, not as plain text. This is a security measure to prevent unauthorized access to sensitive information, such as passwords, in case someone gains access to the configuration files.

Part 3: Configure a MOTD Banner
- Step 1: Configure a message of the day (MOTD) banner.

Part 4: Save and Verify Configuration Files to NVRAM
- Step 1: Verify that the configuration is accurate using the show run command.

Q.) Why should every switch have a MOTD banner?
Ans) A MOTD banner is a simple yet effective way to enhance the security, communication, and operational aspects of network device management.

Q.) **Which command will display the contents of NVRAM?**
Ans) show startup-config

Q.) When will this banner be displayed?
Ans) It's displayed at points where users are granted access to the device to ensure that they are aware of any relevant information before interacting with the system.

Part 5: Configure S2

Procedure:

Open the activity through the Cisco Packet Tracer (2.5.5)

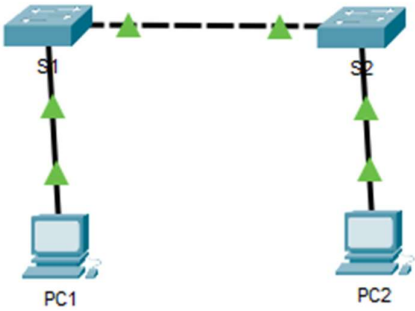
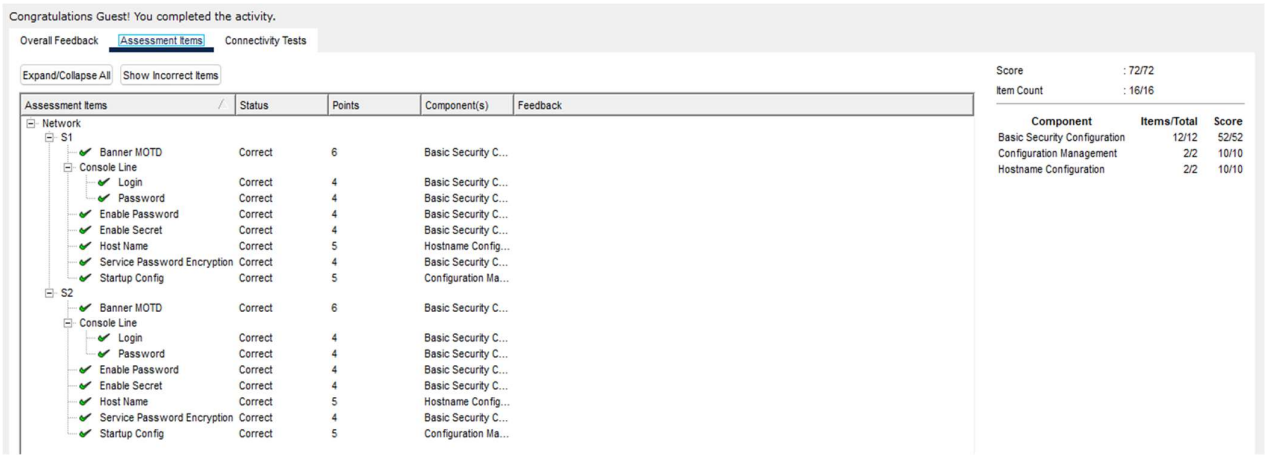


Fig. Diagram Representing connection between devices.

```
Switch>enable
Switch#
Switch#show run
Building configuration...

Current configuration : 1086 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
interface FastEthernet0/2
!

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

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
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

```
User Access Verification

Password:

S1>enable
Password:
S1#show running-config
Building configuration...

Current configuration : 1131 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
enable password c1$c0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable secret itsasecret
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
show run
Building configuration...

Current configuration : 1178 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password c1$c0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd "This is a secure system. Authorized Access Only!"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

Result:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT-3

AIM:

To implement basic connectivity.

Devices Used:
Switches, PCs, and Cable**s**

Objectives
Part 1: Perform a Basic Configuration on S1 and S2
Part 2: Configure the PCs
Part 3: Configure the Switch Management Interface

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
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

Fig. Addressing Table

Part 1: Perform a Basic Configuration on S1 and S2
- Step 1: Configure S1 with a hostname.
- Step 2: Configure the console and encrypted privileged EXEC mode passwords.
- Step 3: Verify the password configurations for S1.
- Step 4: Configure an MOTD banner.
- Step 5: Save the configuration file to NVRAM.
- Step 6: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs
- Step 1: Configure both PCs with IP addresses.
- Step 2: Test connectivity to switches.

Part 3: Configure the Switch Management Interface
- Step 1: Configure S1 with an IP address.
- Step 2: Configure S2 with an IP address.
- Step 3: Verify the IP address configuration on S1 and S2.
- Step 4: Save configurations for S1 and S2 to NVRAM.
- Step 5: Verify network connectivity.

Q.) Which command do you issue to accomplish this step?
Ans) copy running-config startup-config

Q.) Why do you enter the no shutdown command?
Ans) The no shutdown command is used within the interface configuration mode to enable the interface "GigabitEthernet0/1".

Procedure:
Open the activity through the Cisco Packet Tracer (2.7.6)

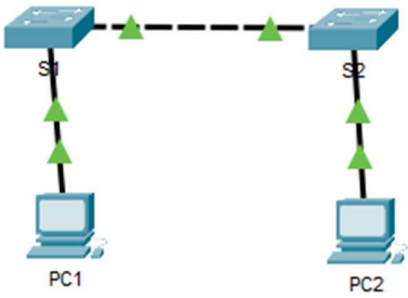
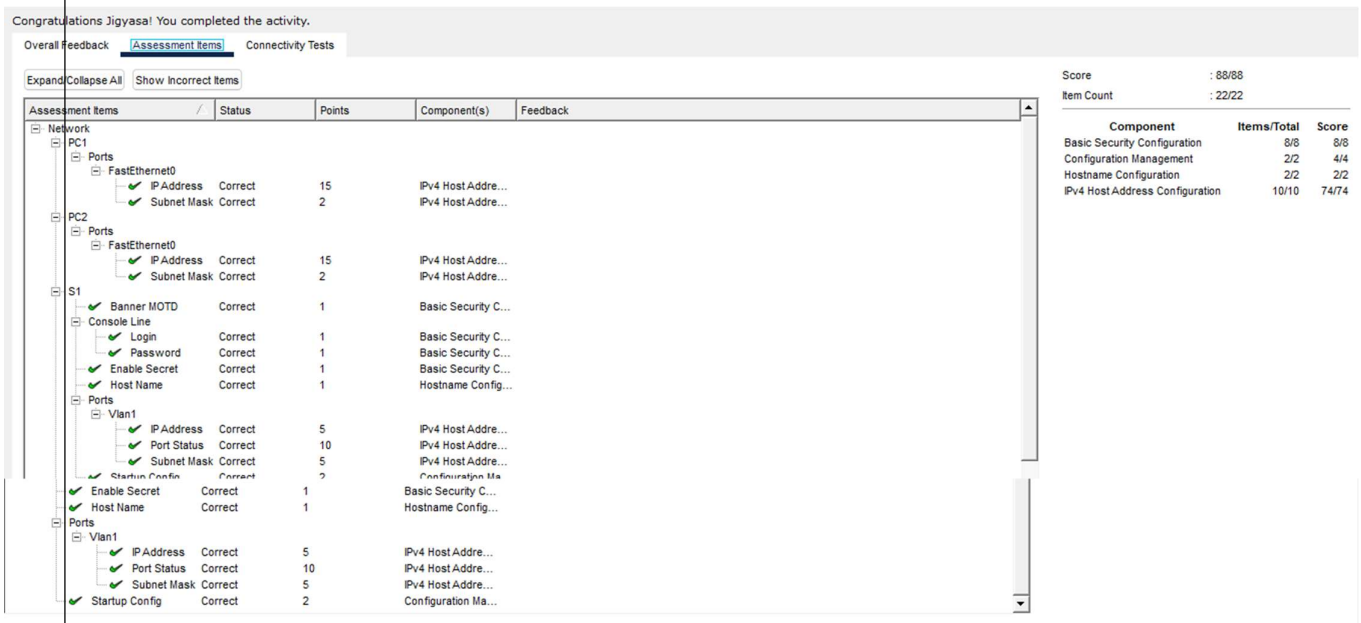


Fig. Diagram Representing Connection Between Devices

```
Switch>enable
Switch#
Switch#show run
Building configuration...

Current configuration : 1086 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/2
!

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

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
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

```
Password:

S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#enable password cl$c0
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit




S1 con0 is now available



Press RETURN to get started.
Building configuration...

Current configuration : 1178 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password cl$c0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd "This is a secure system. Authorized Access Only!"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

Result:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT-4

AIM:
Basic switch and end device configuration.

Devices Used:
Switches, PCs, and Cable**s.**

Objectives
Part 1: Set Up the Network Topology
Part 2: Configure PC Hosts
Part 3: Configure and Verify Basic Switch Settings

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Fig. Addressing Table

Q.) Why are some FastEthernet ports on the switches up while others are down?
Ans) The state of a port depends on various factors, and here are some common reasons why some FastEthernet ports might be up while others are down:

- Administrative Shutdown: If a FastEthernet port is in a "down" state, it might have been intentionally administratively shut down using the shutdown command in the interface configuration.
- Configuration Errors: Configuration errors, such as incorrect IP addressing, VLAN assignment, or security settings, can result in an interface being down. Misconfigured interfaces might not be able to establish a valid link, leading to the "down" state.
- Cable or Hardware Issues: Physical problems, such as faulty cables, damaged connectors, or hardware issues, can prevent an interface from establishing a link with the connected device. This can cause the port to remain in a "down" state.
- Link Status: The link status of an interface depends on whether a valid link has been established with the connected device. If the connected device (like another switch, router, or computer) is powered off, its interface might not be able to establish a link, resulting in the "down" state.
- Speed and Duplex Mismatch: If the speed and duplex settings of two connected interfaces do not match, it can lead to connectivity issues and cause the interface to remain down.
- STP (Spanning Tree Protocol) Blocking: In a redundant network topology, STP might temporarily block certain interfaces to prevent loops. These blocked interfaces will be in a "down" state until they are unblocked by the STP protocol.
- Auto-negotiation Issues: Auto-negotiation, which allows devices to automatically determine the best link settings, can sometimes fail. This can result in an interface being down if the auto-negotiation process is not successful.

Q.) What could prevent a ping from being sent between the PCs?
Ans) Given below are few reasons that could prevent a ping from being sent between the two PCs :

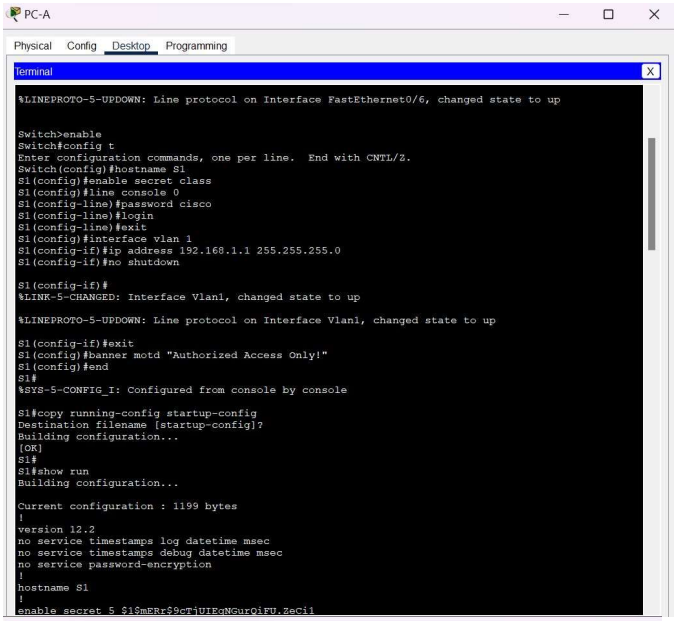
- Network Connectivity Issues

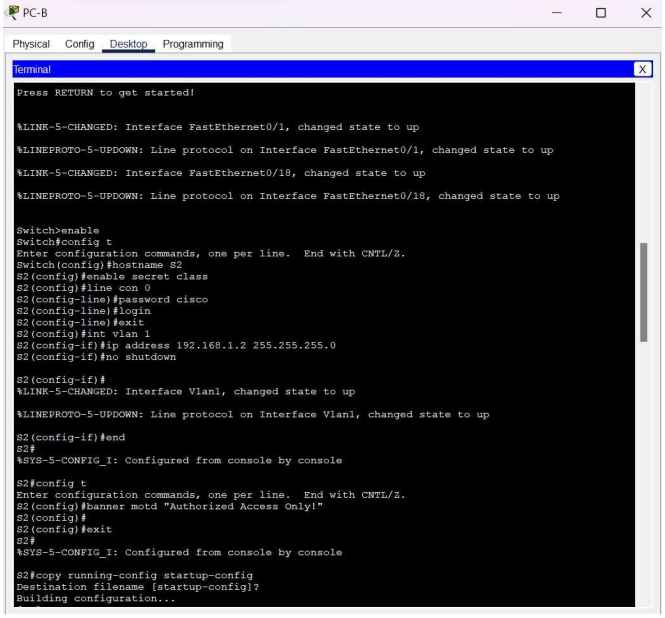
- IP Address Conflicts
- Incorrect Subnet Mask
- Firewall Settings
- Switch or Router Configuration
- Routing and Gateway Issues
- Network Load or Congestion
- Remote PC Settings

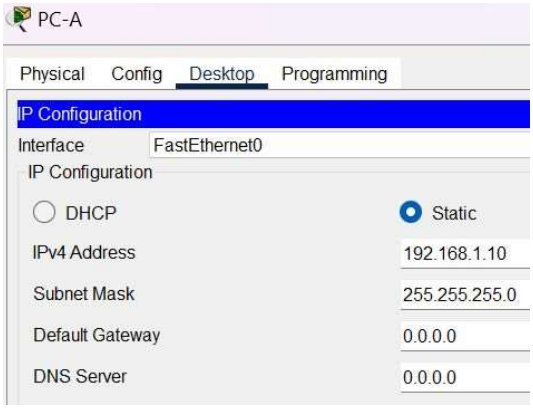
Procedure:

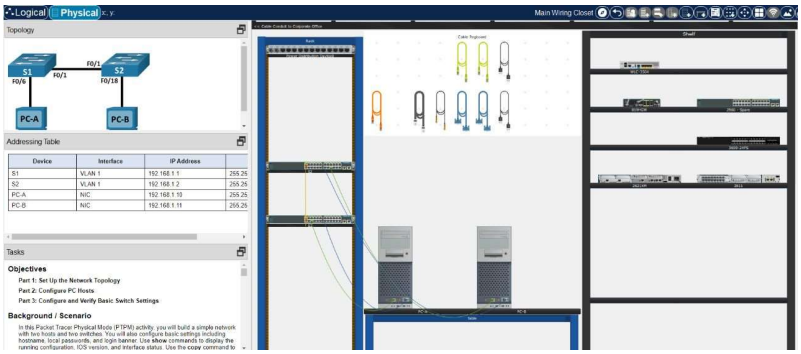
Open the activity through the Cisco Packet Tracer (2.9.2)

Fig. Diagram representing connection between devices.

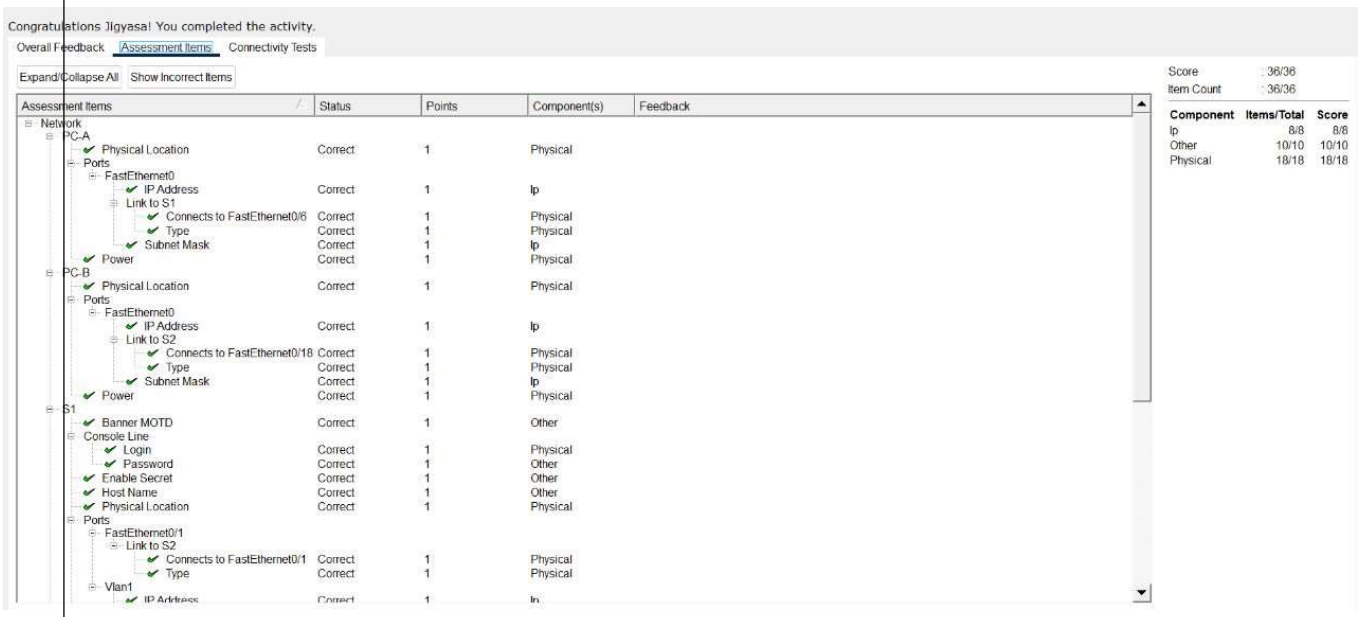

PC-A
Physical
Config
Desktop
Programming
Terminal
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
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)#banner motd "Authorized Access Only!"
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
S1#show run
Building configuration...
Current configuration : 1199 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 imERr$9cTjUIEqNGurQiFU.ZeCii


PC-B
Physical
Config
Desktop
Programming
Terminal
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#int vlan 1
S2(config-if)#ip address 192.168.1.2 255.255.255.0
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)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Authorized Access Only!"
S2(config)#
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...


PC-A
Physical
Config
Desktop
Programming
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.10
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0



Result:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT-5

AIM:
To connect the physical layer.

Devices Used:
Switches, PCs, and Cable**s**

Objectives
Part 1: Identify Physical Characteristics of Internetworking Devices
Part 2: Select Correct Modules for Connectivity
Part 3: Connect Devices
Part 4: Check Connectivity

Part 1: Identify Physical Characteristics of Internetworking Devices
- Step 1: Identify the management ports of a Cisco router.
- Step 2: Identify the LAN and WAN interfaces of a Cisco router.
- Step 3: Identify module expansion slots.

Part 2: Select Correct Modules for Connectivity
- Step 1: Determine which modules provide the required connectivity.
- Step 2: Add the correct modules and power up devices.

Part 3: Connect Devices

Device	Interface	Cable Type	Device	Interface
East	GigabitEthernet0/0	Copper Straight-Through	Switch1	GigabitEthernet0/1
East	GigabitEthernet0/1	Copper Straight-Through	Switch4	GigabitEthernet0/1
East	FastEthernet0/1/0	Copper Straight-Through	PC1	FastEthernet0
East	FastEthernet0/1/1	Copper Straight-Through	PC2	FastEthernet0
East	FastEthernet0/1/2	Copper Straight-Through	PC3	FastEthernet0
Switch1	FastEthernet0/1	Copper Straight-Through	PC4	FastEthernet0
Switch1	FastEthernet0/2	Copper Straight-Through	PC5	FastEthernet0
Switch1	FastEthernet0/3	Copper Straight-Through	PC6	FastEthernet0
Switch4	GigabitEthernet0/2	Copper Cross-Over	Switch3	GigabitEthernet3/1
Switch3	GigabitEthernet5/1	Fiber	Switch2	GigabitEthernet5/1
Switch2	FastEthernet0/1	Copper Straight-Through	PC7	FastEthernet0
Switch2	FastEthernet1/1	Copper Straight-Through	PC8	FastEthernet0
Switch2	FastEthernet2/1	Copper Straight-Through	PC9	FastEthernet0
Switch2	Gigabit3/1	Copper Straight-Through	AccessPoint	Port 0

Fig. Reference Table for connecting devices.

Part 4: Check Connectivity
- Step 1: Check the interface status on East.
- Step 2: Connect wireless devices, Laptop and TabletPC
- Step 3: Change the access method of the TabletPC.
- Step 4: Check connectivity of the other PCs.

Q.) Which management ports are available?
Ans) AUX and console ports are available.

Q.) Which LAN and WAN interfaces are available on the East router and how many are there?
Ans) There are 2 WAN interfaces and 2 Gigabit Ethernet interfaces.

Q.) How many physical interfaces are listed?
Ans) 4

Q.) What is the default bandwidth of this interface?
Ans) 1000000 Kbit

Q.) Click Switch2. How many expansion slots are available?
Ans) 5 slots are available.

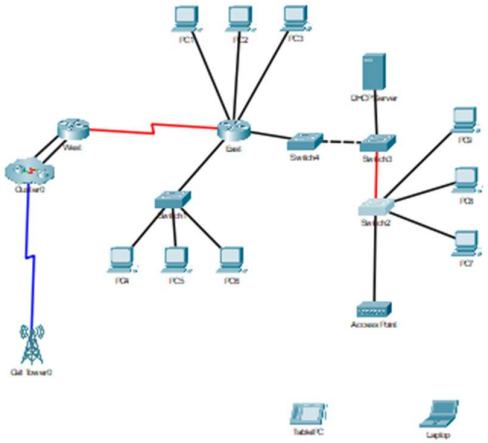
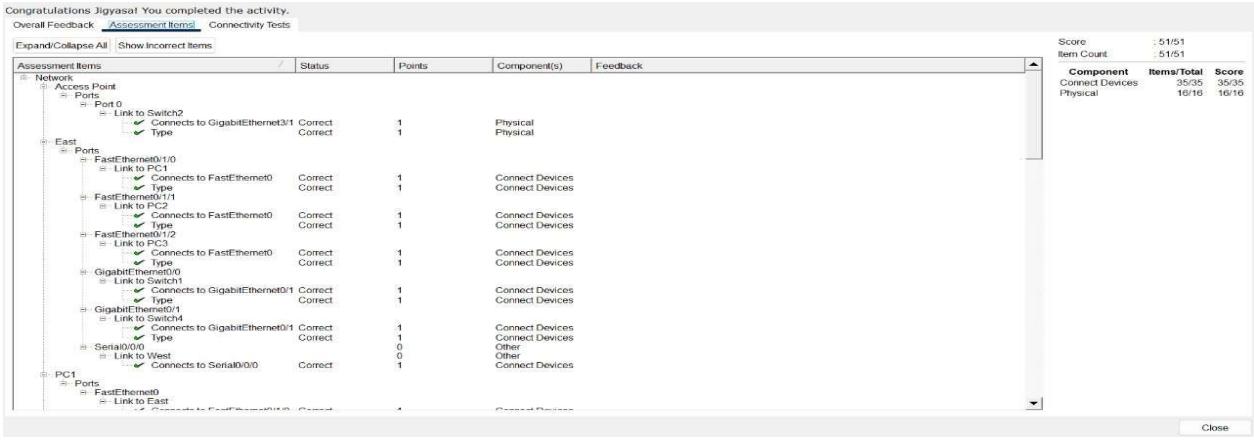


Fig. Diagram with all the connections

Result:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		

Total	6

EXPERIMENT 6

AIM:

To examine ARP Table.

Software Used:

Cisco Packet Tracer

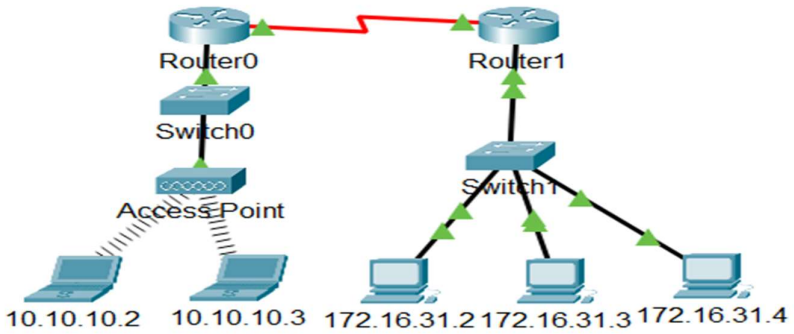
Objectives:

Part 1: Examine an ARP Request

Part 2: Examine a Switch MAC Address Table

Part 3: Examine the ARP Process in Remote Communications

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

Questions:

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.

Procedure:

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.

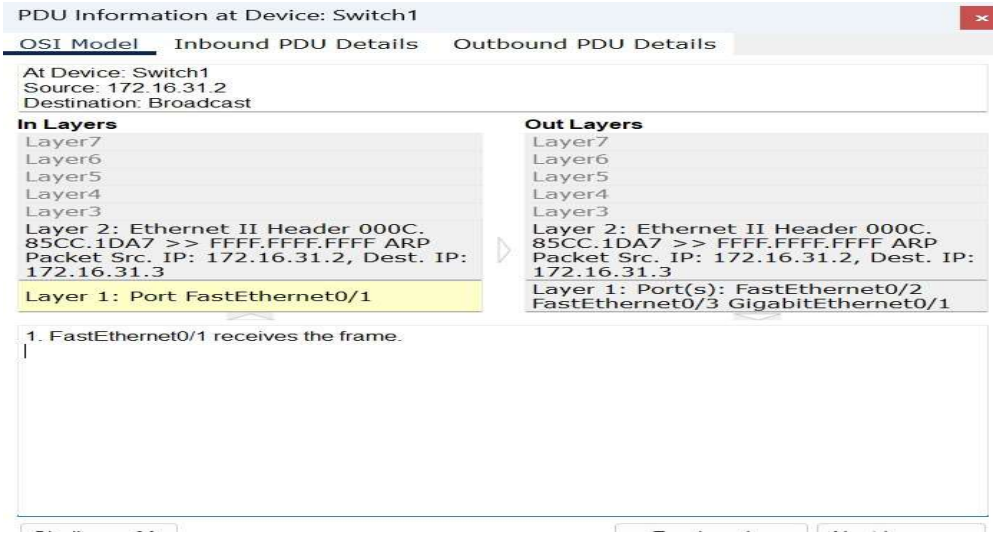
a. Switch to Realtime mode. Click Router1 and then the CLI tab.

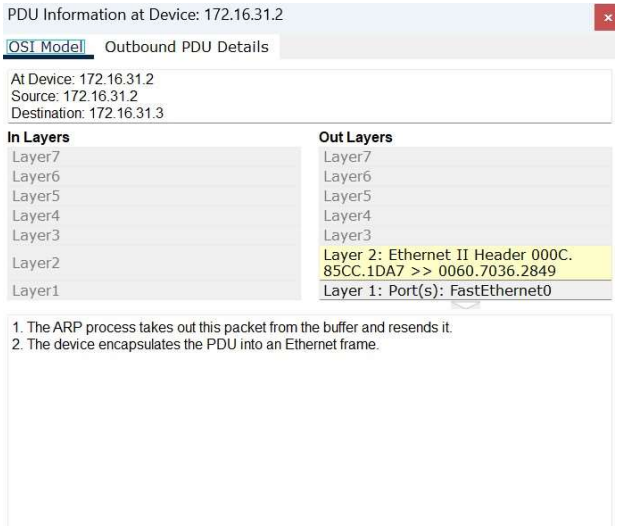
b. Enter privileged EXEC mode and then the show mac-address-table command.

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
```






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

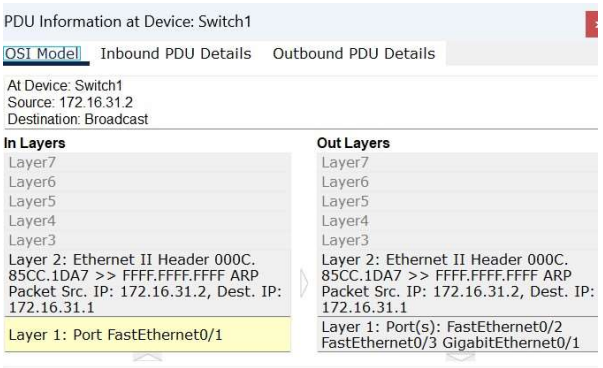
```
C:\>ping 172.16.31.4

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#
```

Evaluation Table:

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT 7

AIM:

To View Network Device MAC Addresses.

Software Used:

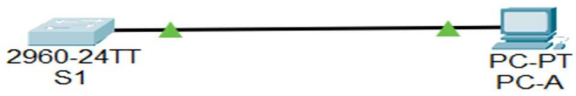
Cisco Packet Tracer

Objectives:

Part 1: Configure Devices and Verify Connectivity.

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

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

Questions:

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

Ans 24-2A-60

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

Ans 001b.0c6d.8f40

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

Ans 6d-8f-40

4. What is the OUI for VLAN 1?

Ans 00-1b-0c

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

Ans Cisco Systems

6. What does bia stand for?

Ans Burned in address

7. 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.

8. What Layer 2 addresses are displayed on S1?

Ans S1 VLAN 1 and PC-A MAC addresses.

9. What Layer 3 addresses are displayed on S1?

Ans S1 and PC-A IP addresses.

Procedure:

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.

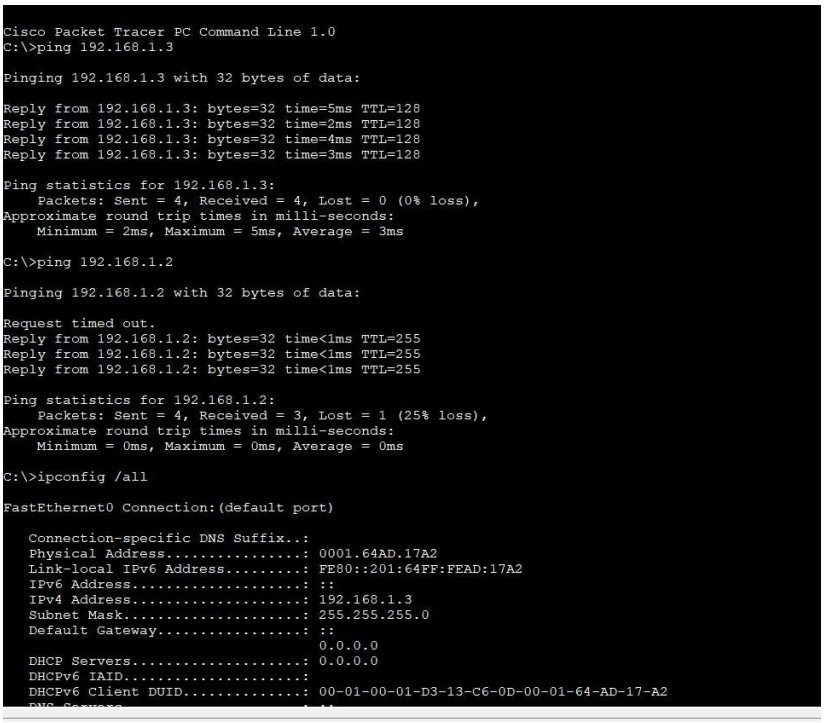
Before you analyze the MAC address on PC-A, look at an example from a different PC NIC. You can issue the ipconfig /all command to view the MAC address of your NIC.

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#
```



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

Evaluation Table:

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT 8

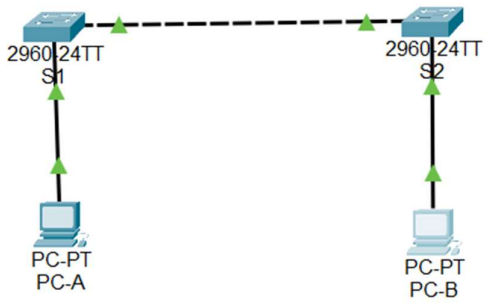
AIM:

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

Questions :

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 .

Procedure:

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
```

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

Evaluation Table: -

Criteria	**Total Marks**	**Marks Obtained**	**Comments**
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT 9

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 ConfigurationPart 3:

Save the Running Configuration File

Questions:
Q) What is the router's hostname?

Ans) Router
Q) How many Fast Ethernet interfaces does the Router have?
Ans) none
Q) How many Gigabit Ethernet interfaces does the Router have?
Ans) 2
Q) How many Serial interfaces does the router have?
Ans) 2
Q) What is the range of values shown for the vty lines?
Ans) 0-4
Q) What command do you use to verify initial configuration on router?
Ans) show running-config
Q) 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 beused to send messages to network personnel (such as impending system shutdowns or who to contact for access).
Q) f you are not prompted for a password before reaching the user EXEC prompt, what console line command did youforget to configure?
Ans) R1(config-line)# login
Q) If you configure any more passwords on the router, are they displayed in the configuration file as plain text or inencrypted form? Explain.
Ans) The service password-encryption command encrypts all current and future passwords.
Q) What command did you enter to save the configuration to NVRAM?
Ans) copy running-config startup-config
Q) Which command displays the contents of the NVRAM?
Ans) show startup-configuration or show start
In this activity, you will perform basic router configuration tasks. You will secure access to the CLI and console port usingencrypted 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.

Topology:

Procedure:

Part 1: Verify the Default Router Configuration

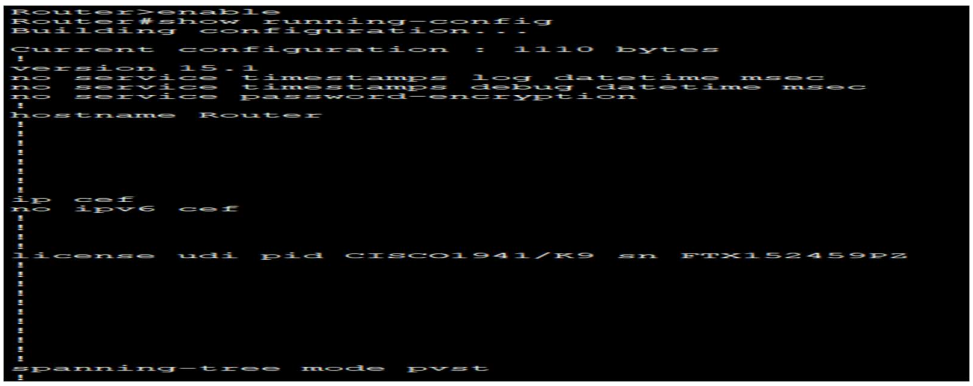
Step 1: Establish a console connection to R1.

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
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

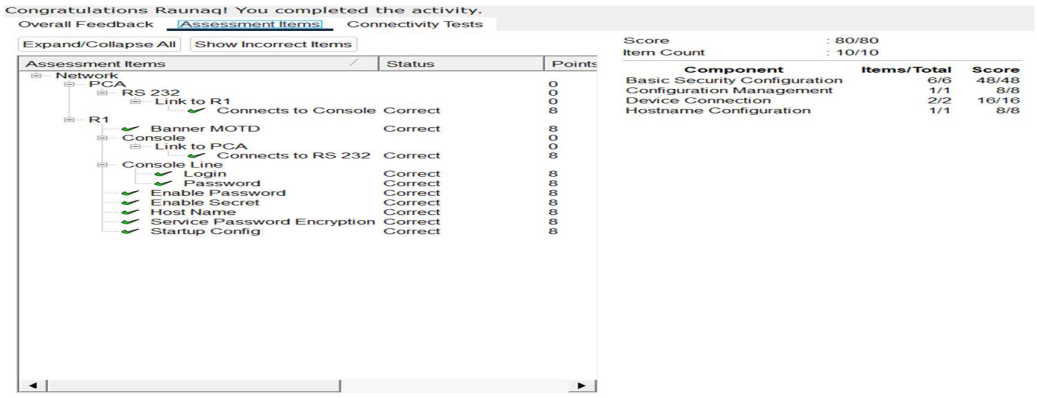
You have configured the initial settings for R1. Now back up the running configuration file to NVRAM toensure that the changes made are not lost if the system is rebooted or loses power.



```
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)#enable 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#
```

Result:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

EXPERIMENT 10

AIM:

To connect a router to a LAN.

Software Used:

Cisco Packet Tracer

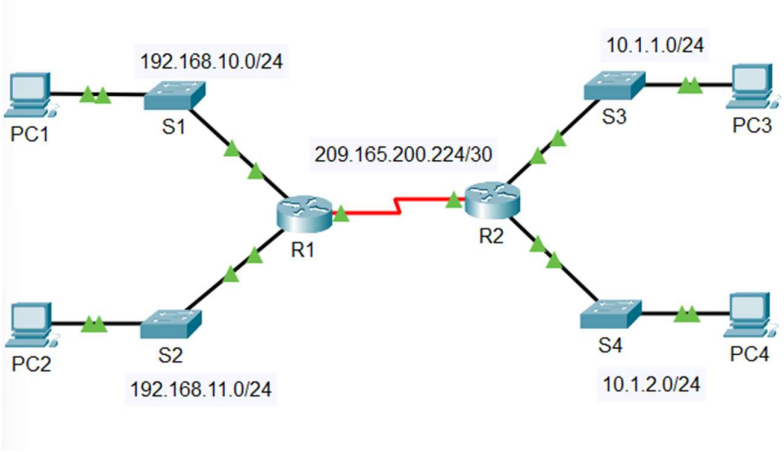
Objectives –

Part 1: Display Router Information

Part 2: Configure Router Interfaces

Part 3: Verify the Configuration

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

Questions:

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

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.

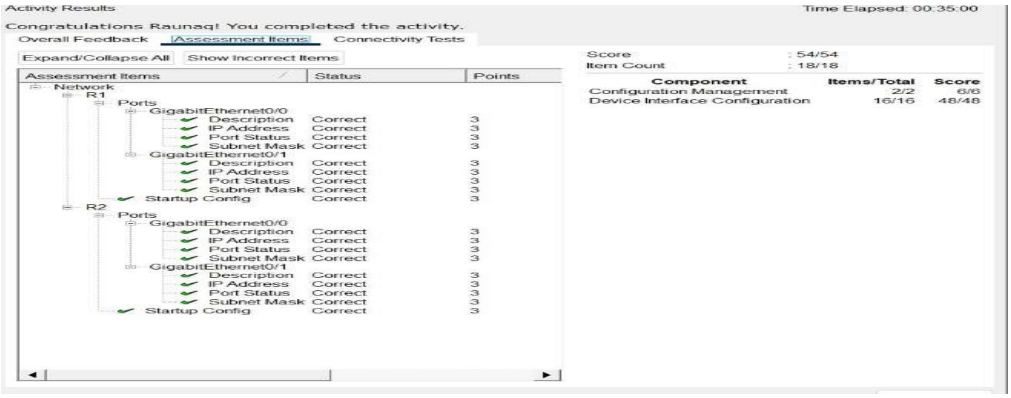
```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown

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#
```

Result:



Evaluation Table: -

Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

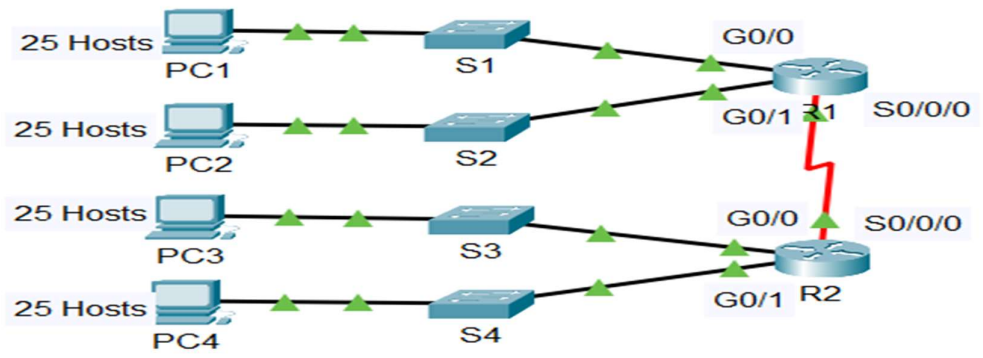
EXPERIMENT 11

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

Questions based on this activity are:

Q1: Based on the topology, how many subnets are needed?

Ans: 5 Four for the LANS, and one for the link between the routers.

Q2: How many bits must be borrowed to support the number of subnets in the topology table?

Ans: 3

Q3: How many subnets does this create?

Ans: 8

Q4: How many usable hosts does this create per subnet?

Ans: 30

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

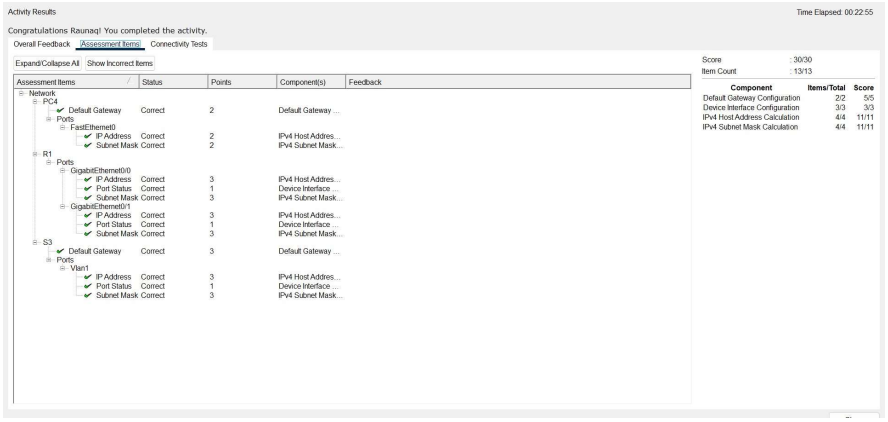
Step 1: Configure R1 LAN interfaces.

Step 2: Configure IP addressing on S3.

Step 3: Configure PC4.

Step 4: Verify connectivity.

Result-



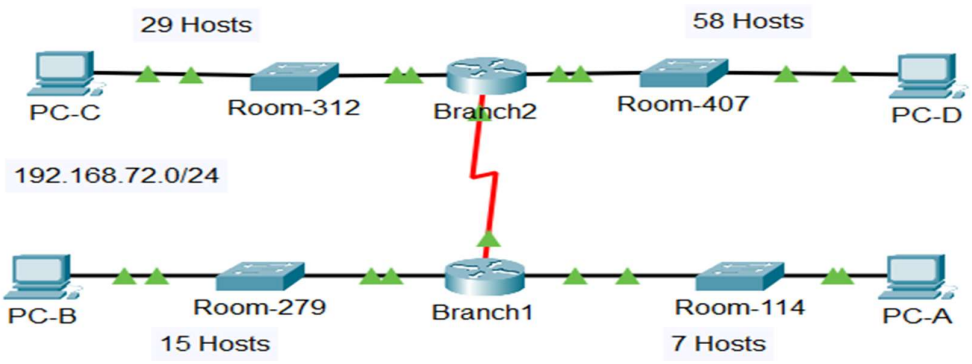
EXPERIMENT 12

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

Questions related to this activity are:

Q1: How many subnets are needed in the network topology?

Ans: 5

Q2: Which subnet mask will accommodate the number of IP addresses required for ASW-1?

Ans: 255.255.255.240/24

Q3: How many usable host addresses will this subnet support?

Ans: 14 (10.11.48.97-10.11.48.110)

Q4: Which subnet mask will accommodate the number of IP addresses required for ASW-2?

Ans: 255.255.255.224 /27

Q5: How many usable host addresses will this subnet support?

Ans: 30 (10.11.48.65-10.11.48.94)

Q6: Which subnet mask will accommodate the number of IP addresses required for ASW-3?

Ans: 255.255.255.248/29

Q7: How many usable host addresses will this subnet support?

Ans: 6 (10.11.48.113-10.11.48.118)

Q8: Which subnet mask will accommodate the number of IP addresses required for ASW-4?

Ans: 255.255.255.192/26

Q9: How many usable host addresses will this subnet support?

Ans: 62 (10.11.48.1-10.11.48.62)

Q10: Which subnet mask will accommodate the number of IP addresses required for the connection between Building I and Building??

Ans: 255.255.255.252/30

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
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

Device	Interface	Address	Subnet Mask	Default Gateway
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

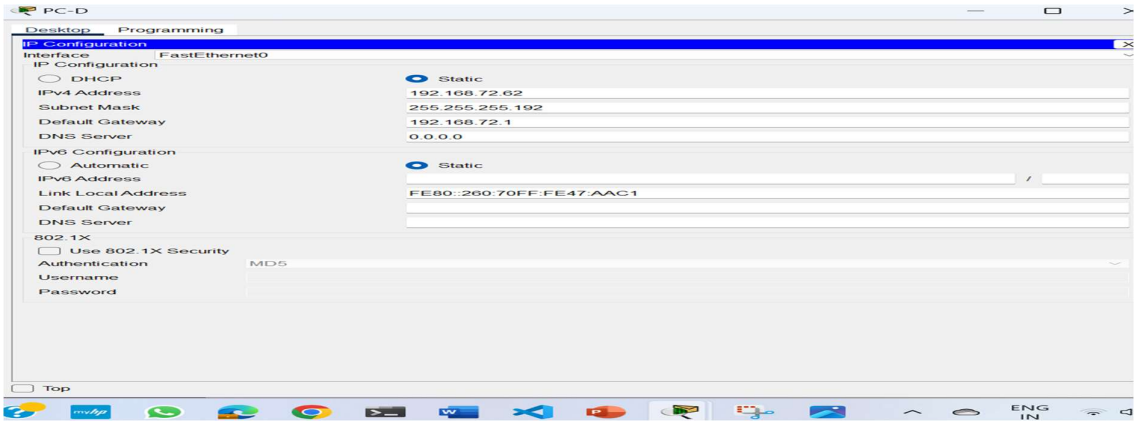
Most of the IP addressing is already configured on this network. Implement the following steps to complete the addressing configuration.

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

```
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
```

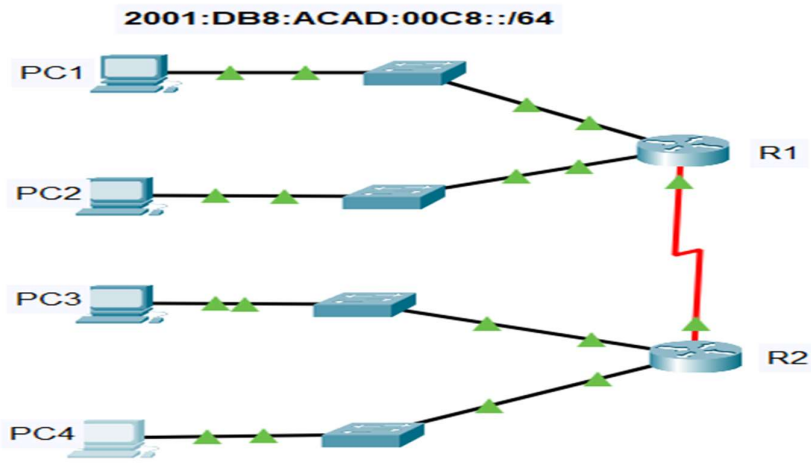
EXPERIMENT 13

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 .