Experiment 6

Aim: To establish a connection among different network topology like star, mesh, bus etc and build a hybrid topology.

Theory:

1. Star Topology
In a star topology, all devices (nodes) are connected to a central hub or switch. The hub acts as a communication point, directing traffic between devices. If one device fails, it does not affect the rest of the network. However, if the central hub fails, the entire network goes down.

- Advantages: Easy to install, centralized management, easier fault identification.
- Disadvantages: The central hub is a single point of failure; additional costs for the hub or switch.

2. Bus Topology
In a bus topology, all devices share a single communication line (bus) to transmit data. This topology is relatively simple and inexpensive to implement. However, data collisions can occur, slowing down the network, and if the bus fails, the entire network is affected.

- Advantages: Simple layout, low cost.
- Disadvantages: Limited cable length, difficult to troubleshoot, performance degradation as more devices are added.

3. Mesh Topology
In a mesh topology, each device is connected to every other device in the network. This creates multiple paths for data to travel, ensuring redundancy and reliability. Even if one link fails, data can still reach its destination through another path.

- Advantages: High redundancy, no single point of failure, efficient data transmission.
- Disadvantages: High cost, complex setup, requires more cabling and configuration.

4. Hybrid Topology
A hybrid topology is a combination of two or more different types of topologies, such as star, bus, and mesh. This allows for more flexibility and efficiency in network design. For

example, the star topology might be used in one part of the network while the mesh topology is used in another, allowing for a mix of centralized and decentralized control.

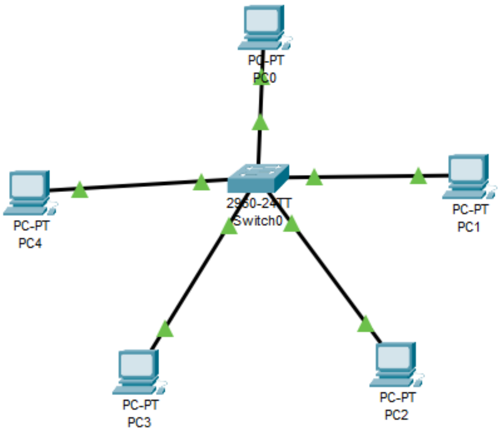
- Advantages: Flexible, scalable, and allows optimization of network performance.
- Disadvantages: Complex design and implementation, higher costs compared to simple topologies.

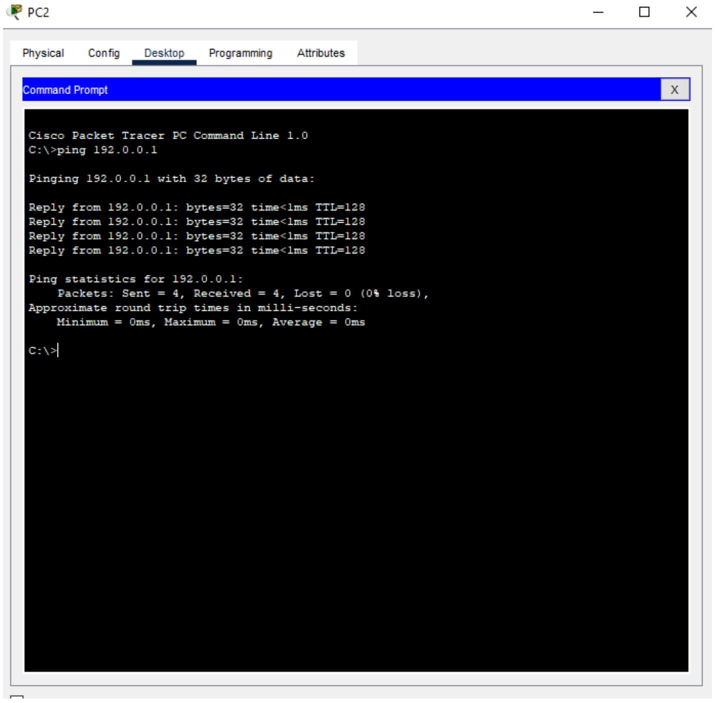
In practice, hybrid topologies are often used in larger networks, taking the best features of each topology and integrating them into a more complex but robust network.

Observations:

PC NAME	IP ADDRESS
PC0	192.0.0.1
PC1	192.0.0.2
PC2	192.0.0.3
PC3	192.0.0.4
PC4	192.0.0.5
PC5	192.0.0.6
PC6	192.0.0.7
PC7	192.0.0.8

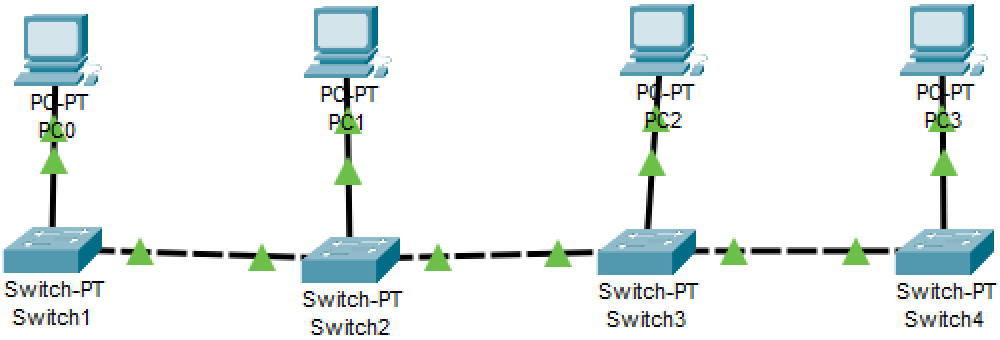
1. Star Topology

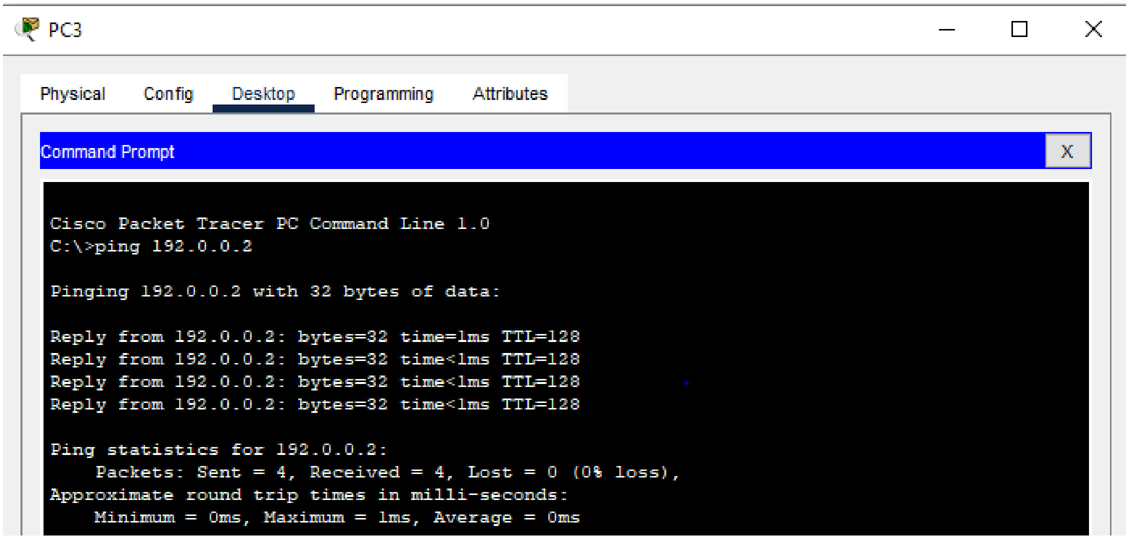




```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.0.0.1

Pinging 192.0.0.1 with 32 bytes of data:

Reply from 192.0.0.1: bytes=32 time<1ms TTL=128
Reply from 192.0.0.1: bytes=32 time<1ms TTL=128
Reply from 192.0.0.1: bytes=32 time<1ms TTL=128
Reply from 192.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

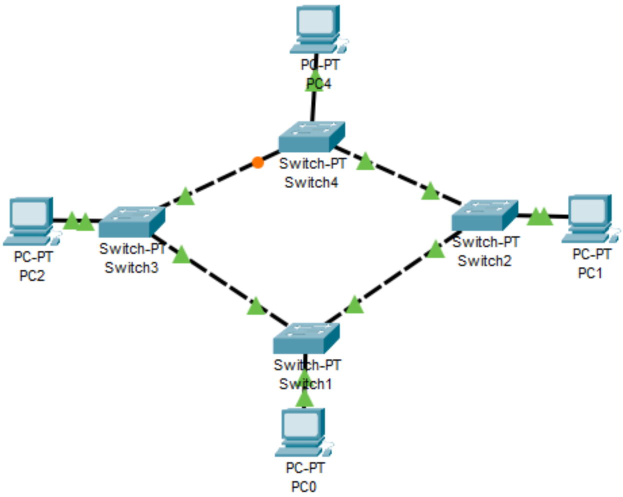
2. Bus Topology

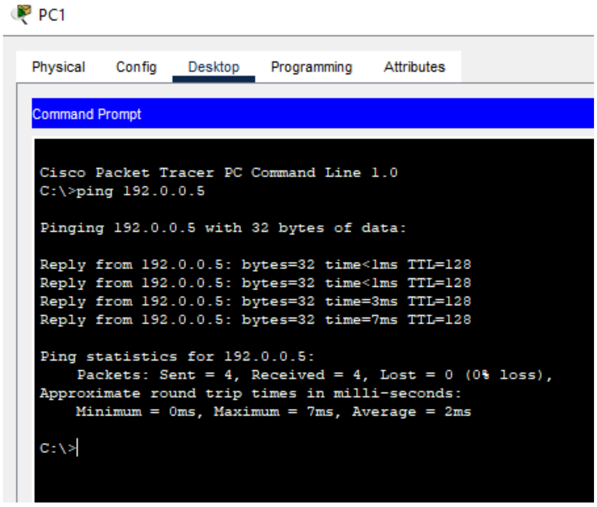




```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.0.0.2

Pinging 192.0.0.2 with 32 bytes of data:

Reply from 192.0.0.2: bytes=32 time=1ms TTL=128
Reply from 192.0.0.2: bytes=32 time<1ms TTL=128
Reply from 192.0.0.2: bytes=32 time<1ms TTL=128
Reply from 192.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

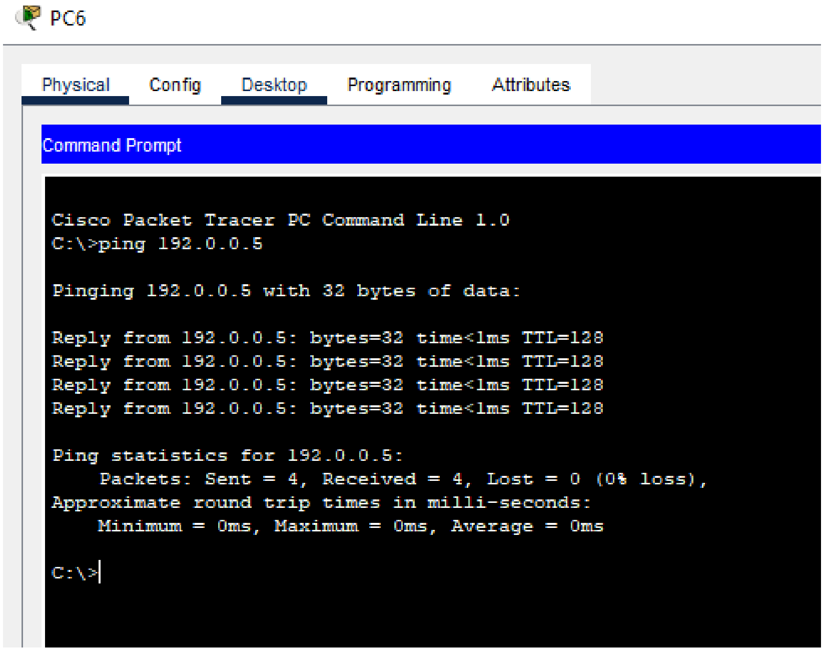
3. Mesh Topology



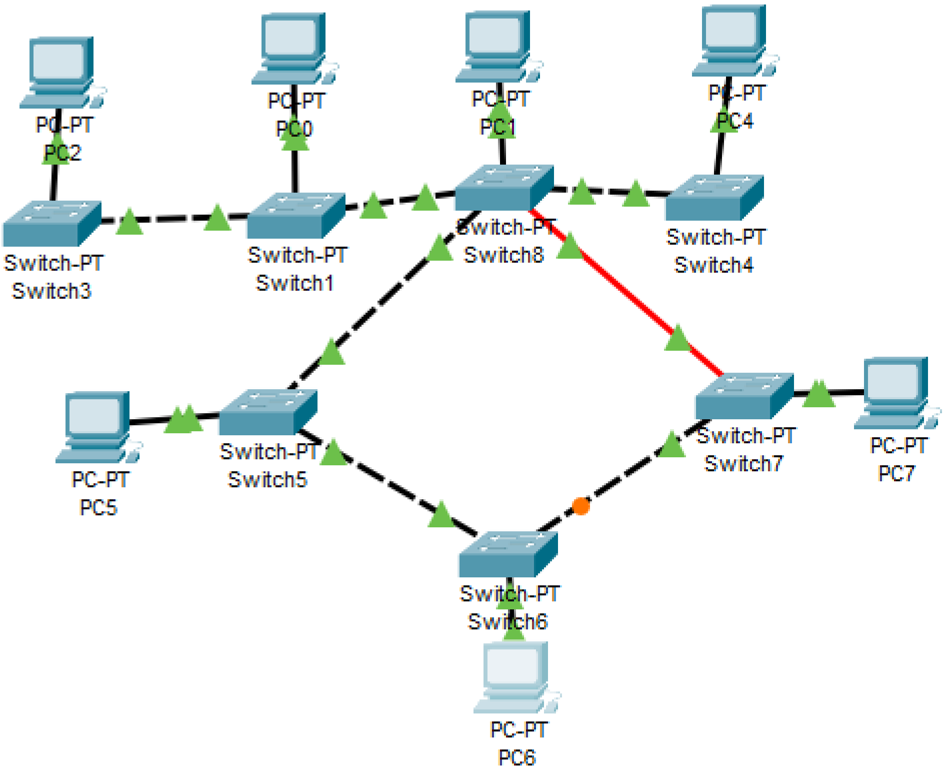


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.0.0.5

Pinging 192.0.0.5 with 32 bytes of data:

Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time=3ms TTL=128
Reply from 192.0.0.5: bytes=32 time=7ms TTL=128

Ping statistics for 192.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\>
```

4. Hybrid Topology



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.0.0.5

Pinging 192.0.0.5 with 32 bytes of data:

Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128
Reply from 192.0.0.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



Result: Successfully establish a connection among different network topology like star, mesh, bus etc and build a hybrid topology.

Experiment 7

Aim: Establish a WAN network using 2 switches and routers

Theory: In modern networking, Wide Area Networks (WANs) are essential for connecting multiple Local Area Networks (LANs) across large geographical areas, such as cities, countries, or even globally. A WAN allows for the sharing of resources, data, and services between these distant networks.

To establish a WAN network, routers and switches play critical roles in directing and managing data traffic efficiently. This experiment involves using two routers and switches to create a WAN connection between two separate LANs, simulating how enterprises or organizations connect remote offices or data centers.

Components of a WAN**:**

1. Routers**:**
Routers operate at the network layer (Layer 3) of the OSI model. They are responsible for directing data packets between different networks, making decisions based on IP addresses and routing protocols. In this experiment, two routers will serve as the gateway between each LAN and the wider WAN, ensuring data can travel between the two distant networks.

2. Switches**:**
Switches operate at the data link layer (Layer 2) and are used to connect multiple devices within a LAN. They forward data based on MAC addresses, ensuring efficient communication within the local network. In this setup, switches connect individual devices (such as computers) within each LAN and then direct data to the routers for WAN transmission.

Establishing the WAN Connection**:**

To set up a WAN, each router connects to its respective LAN through a switch. The routers are then interconnected to establish a wide area link. This interconnection can occur over a physical medium (such as fiber optics or leased lines) or virtually via tunneling protocols (like VPNs). Routing protocols like OSPF or BGP are typically used to determine the best path for data transmission between networks.

Data Flow in the WAN:

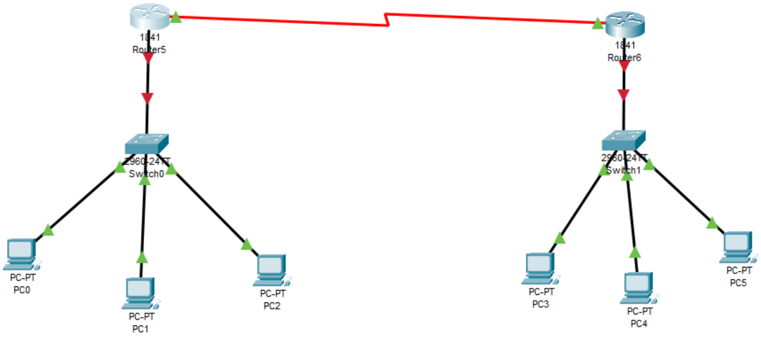
1. Local Communication**:**
   Within each LAN, devices communicate through the switch, which handles internal data flow. Data intended for a remote network is forwarded to the router.

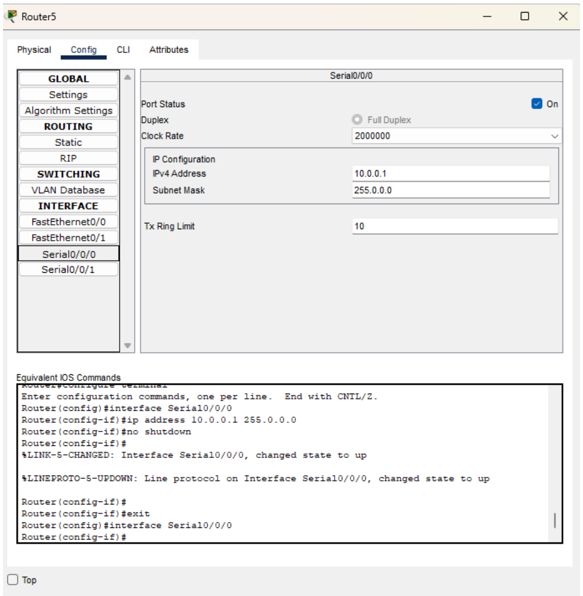
2. WAN Communication**:**
   When data needs to be sent across the WAN, the router takes responsibility. It analyzes the destination IP address, identifies the best path, and transmits the data over the WAN link to the other router.

3. Reception at Remote Network**:**
   The second router receives the data and passes it through to its connected switch, which forwards it to the appropriate device within the second LAN.

By using this combination of routers and switches, the experiment demonstrates how WANs are established, enabling communication between geographically separated networks while maintaining efficient data management at both the local and wide area levels.

Observations:





Serial0/0/0

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

IP Configuration

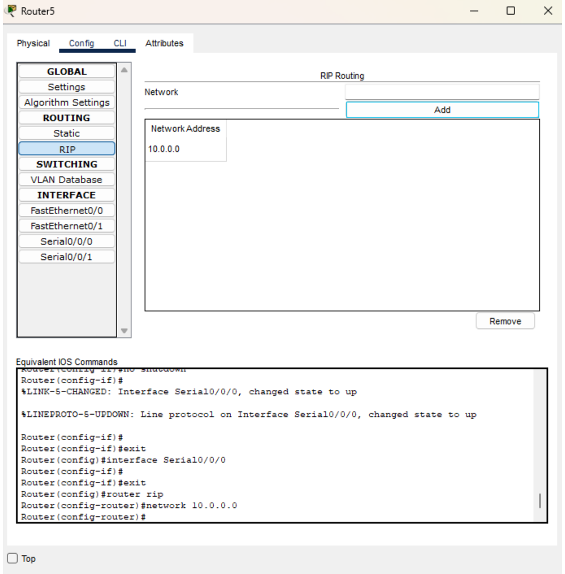
IPv4 Address 10.0.0.1

Subnet Mask 255.0.0.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(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

Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
```



RIP Routing

Network

Network Address

10.0.0.0

Equivalent IOS Commands

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

Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#
```

Result: Successfully established a WAN network.

Experiment 8

Aim: To use a router to connect two or more network topologies.

Theory: In network design, routers are critical for interconnecting multiple network topologies. These topologies could be of various types, such as star, mesh, or bus, and a router serves as a gateway that allows these networks to communicate with one another.

Role of the Router:

Routers operate at Layer 3 of the OSI model (Network Layer), using IP addresses to direct traffic between different networks. Unlike switches, which connect devices within a single local area network (LAN), routers allow communication between multiple LANs or between different network topologies.

Steps for Connecting Network Topologies:

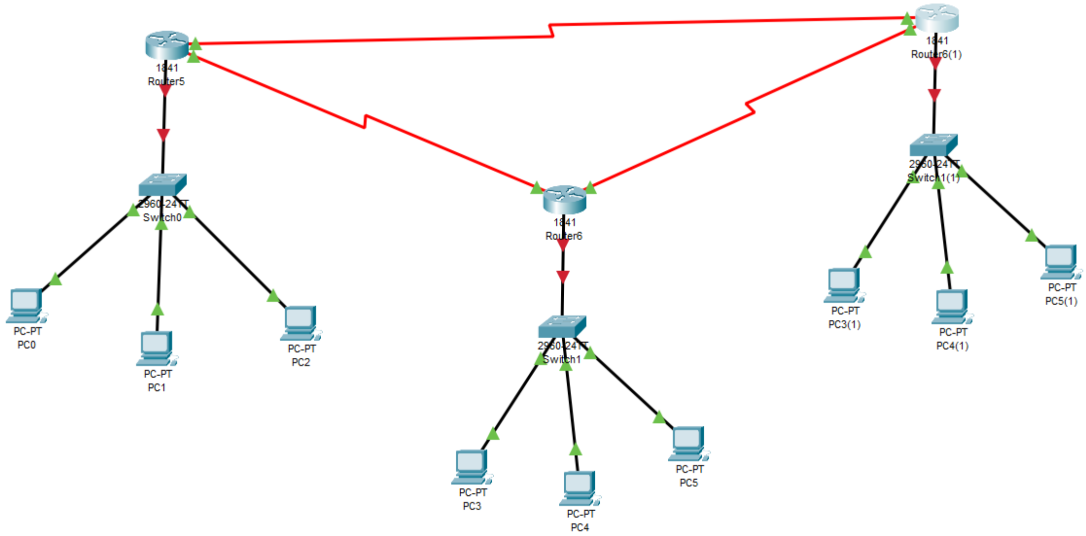
1. Identify Networks**:**
   Each network topology (such as star, bus, mesh) has its own set of devices, switches, and addressing scheme (IP subnet). In this experiment, the goal is to interconnect them through a router.

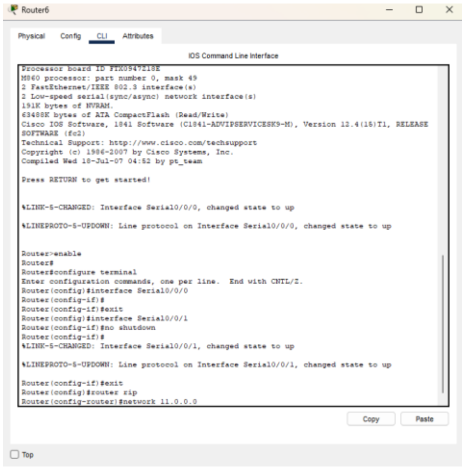
2. Router Configuration**:**
   The router's interfaces are configured with IP addresses for each network it connects to. These interfaces act as the entry and exit points for data traveling between the networks. Proper routing protocols such as RIP, OSPF, or static routes are configured to guide data packets to their destination.

3. Data Flow:
   When a device in one network (e.g., the star topology) needs to communicate with a device in another network (e.g., the mesh topology), the router takes the data, examines the destination IP, and forwards it to the appropriate network based on the routing table. The router ensures that different network topologies, which might otherwise be incompatible, can communicate seamlessly.

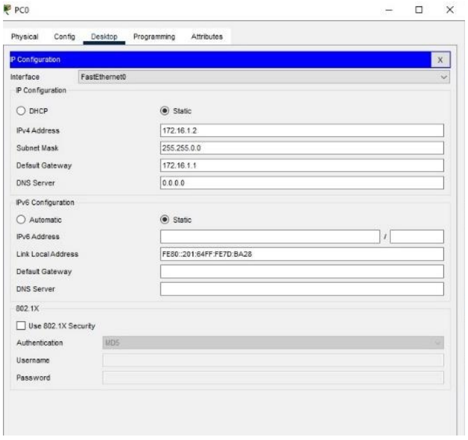
By using routers to interconnect different topologies, networks are scalable, and their performance can be optimized to meet different requirements. This setup is common in enterprise environments, where different departments or branches use distinct topologies but need to exchange data securely and efficiently.

Observations:





```
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!


%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


Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 11.0.0.0
```



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 172.16.1.2

Subnet Mask: 255.255.0.0

Default Gateway: 172.16.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:64FF:FE7D:BA28

Default Gateway:

DNS Server:

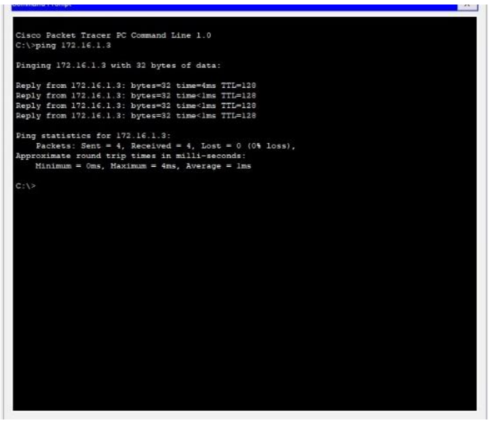
802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.3

Pinging 172.16.1.3 with 32 bytes of data:

Reply from 172.16.1.3: bytes=32 time=4ms TTL=128
Reply from 172.16.1.3: bytes=32 time<1ms TTL=128
Reply from 172.16.1.3: bytes=32 time<1ms TTL=128
Reply from 172.16.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

Result: Successfully used routers to connect two or more topologies

Experiment 9

Aim: Connect two or more routers and verify ICMP

Theory: In this experiment, we will connect two or more routers to establish communication between multiple networks. The aim is to create a routed network where each router connects separate LANs (Local Area Networks), and connectivity between these LANs will be verified using the ICMP (Internet Control Message Protocol), commonly tested with the ping command.

Components:

1. Routers**:**
   Routers play a critical role in connecting multiple networks by routing data packets based on IP addresses. In this experiment, we connect two or more routers, each with its own connected network (or subnet), creating a larger interconnected system.
2. ICMP (Internet Control Message Protocol):
   ICMP is a diagnostic protocol used by network devices to send control messages and error reports. It plays a significant role in network troubleshooting and communication testing. The ping command, which uses ICMP, helps to verify the connection by sending echo request packets to a target device and awaiting an echo reply.

Process:

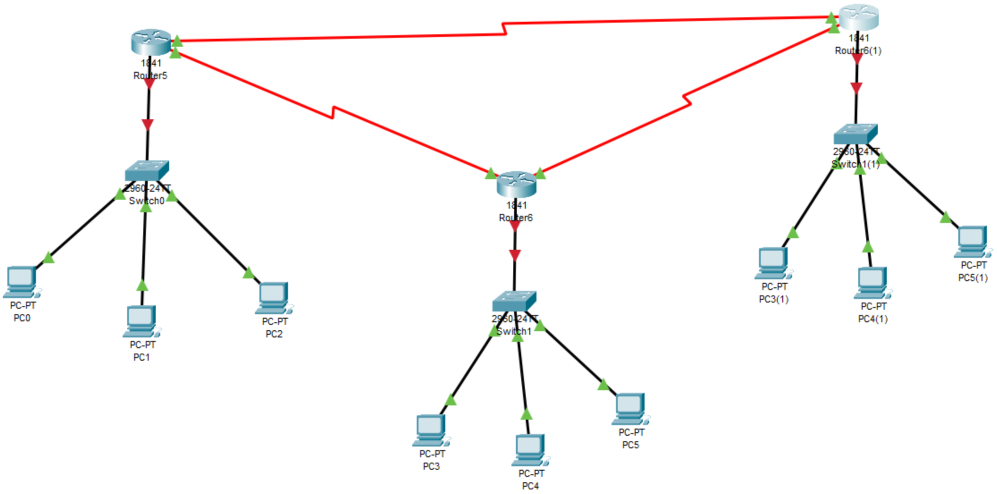
1. Router Configuration:
   - Each router will have its own LAN connected through one of its interfaces. The interfaces are configured with distinct IP addresses corresponding to the subnet they are part of.
   - The routers are interconnected via their WAN (Wide Area Network) interfaces, using either a direct connection (Ethernet or serial) or a switch.
   - Static routes or dynamic routing protocols (such as OSPF or RIP) are configured to allow the routers to share information about the networks they are connected to, enabling them to forward packets between their respective LANs.
2. Connecting Routers:

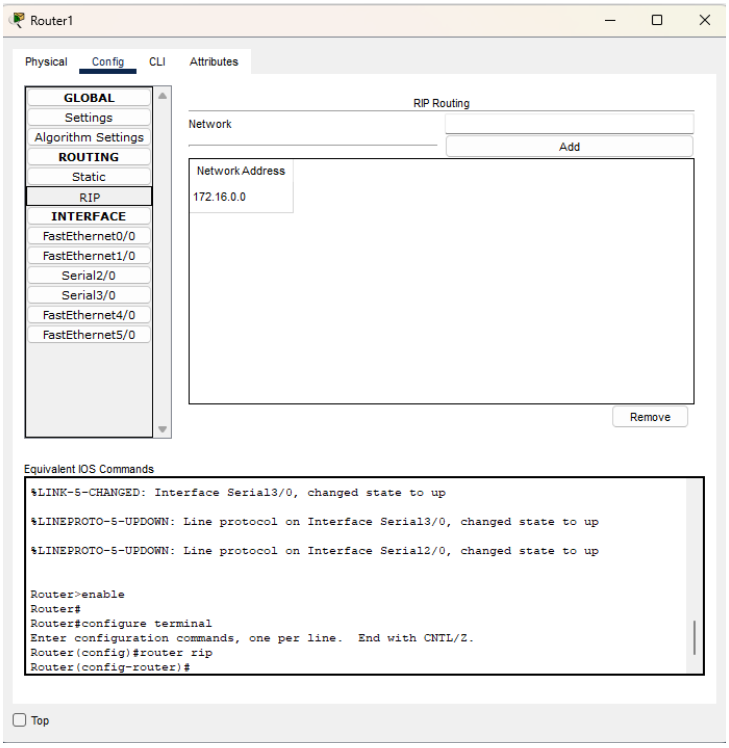
    - In the case of two routers, the two devices will be directly connected, and static or dynamic routes are added to ensure data transmission between the networks.
    - For three or more routers, you create a more complex topology where each router is connected to at least one other router, forming a mesh of connections that allows data to flow between all connected networks.

3. Verification using ICMP:
    - Once the routers are connected and configured, ICMP verification is done using the ping command. From a device in one network, you send a ping request to a device in another network (connected via the routers).
    - If the routers are correctly configured, they will route the ICMP request packets to the target network, and an echo reply will be received, confirming connectivity.
    - This process can be repeated for all connected routers and networks, ensuring that data can flow seamlessly across all networks in the setup.

By interconnecting multiple routers and using ICMP for verification, this experiment demonstrates how routers facilitate communication between different subnets and how multiple networks can be integrated to form a wide-reaching and robust routed system.

Observations:

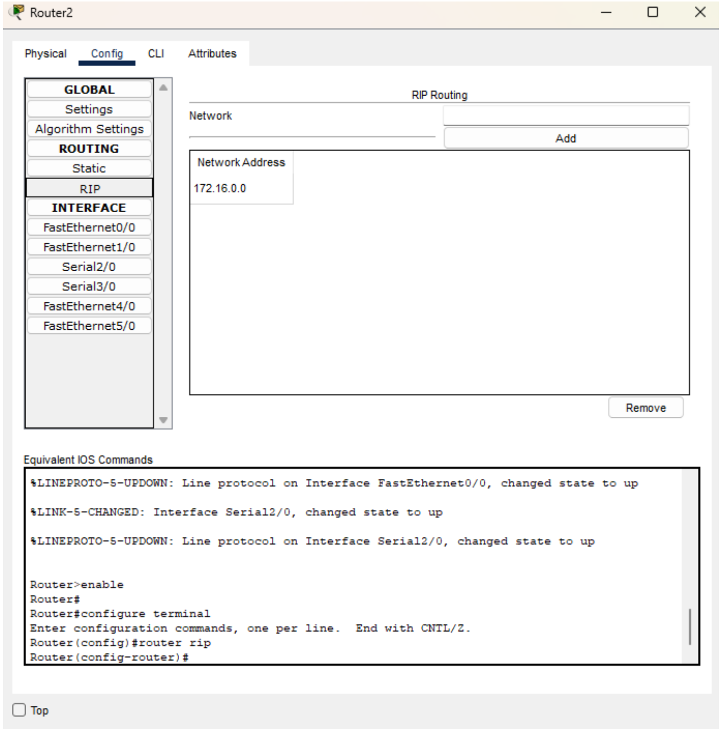




Network Address
172.16.0.0

Equivalent IOS Commands

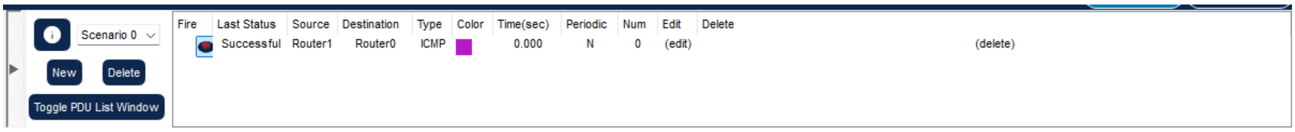
```
%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up


Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```



Network Address
172.16.0.0

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up


Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Router1	Router0	ICMP	🟪	0.000	N	0	(edit)	(delete)

Result: Successfully connected two routers and verified ICMP.

Experiment 10

Aim: To simulate the process of subnetting using a router.

Theory: Subnetting is the process of dividing a larger network (IP address space) into smaller, more manageable sub-networks, called subnets. Each subnet functions as an independent network, allowing for more efficient IP address allocation, improved network performance, and enhanced security.

In this experiment, we simulate subnetting using a router to create multiple subnets within a single network. The router will be used to route traffic between the subnets and demonstrate how IP addressing and subnet masks are applied to segment a network.

Key Concepts**:**

1. IP Addressing and Subnet Masks:
    - Every device in a network is assigned an IP address. An IP address consists of two parts: the network portion and the host portion.
    - Subnetting is achieved by extending the network portion of the IP address, allowing for the creation of smaller subnets. This is done by adjusting the subnet mask, which determines how much of the IP address is used for the network and how much is left for hosts.
2. Router and Subnetting:
    - The router acts as an intermediary device that routes traffic between different subnets. It maintains routing tables to direct data between devices in separate subnets.
    - Each interface of the router is assigned an IP address from a different subnet. This ensures that the router can communicate with all the subnets and can forward traffic appropriately.

Process:

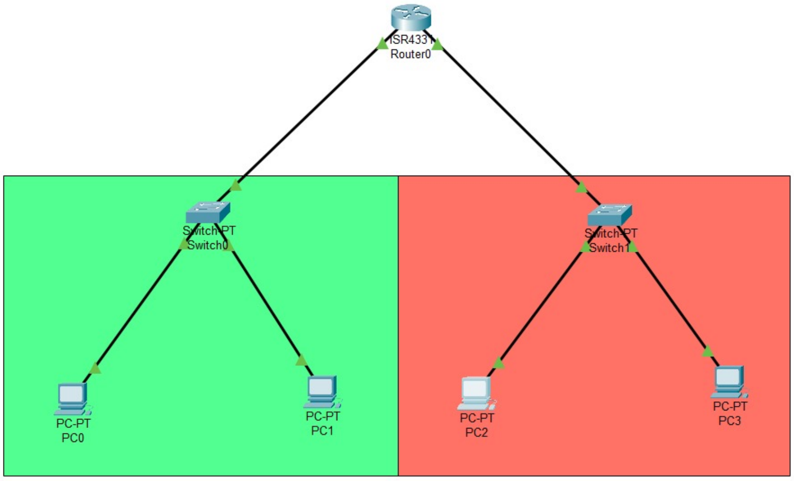
1. Subnet Design:
    - The larger network, for instance, 192.168.1.0/24, is divided into two subnets:
        - Subnet 1 (Green): 192.168.1.0/25 (hosts PC0 and PC1)
        - Subnet 2 (Red): 192.168.1.128/25 (hosts PC2 and PC3)

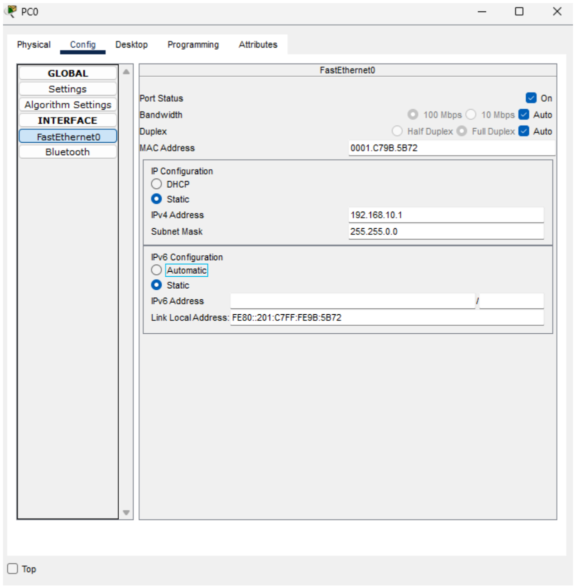
- The subnet mask for both subnets is 255.255.255.128, which allows for 128 IP addresses in each subnet.

2. Router Configuration:
    - The router has two interfaces, each assigned an IP address from the corresponding subnet:
        - Interface 0 (Subnet 1 - Green): 192.168.1.1/25 (connected to Switch 0)
        - Interface 1 (Subnet 2 - Red): 192.168.1.129/25 (connected to Switch 1)
    - Each interface acts as the gateway for the devices in its subnet.
3. Switch and PC Configuration:
    - Switch 0 connects PC0 and PC1 to Subnet 1 (192.168.1.0/25), with IP addresses like 192.168.1.2 and 192.168.1.3 respectively.
    - Switch 1 connects PC2 and PC3 to Subnet 2 (192.168.1.128/25), with IP addresses like 192.168.1.130 and 192.168.1.131 respectively.
    - Each PC is configured with its corresponding IP address and uses the router's interface IP as its default gateway.
4. Routing Between Subnets:
    - The router will automatically route traffic between Subnet 1 and Subnet 2.
    - If a PC in Subnet 1 (e.g., PC0) wants to communicate with a PC in Subnet 2 (e.g., PC2), the data is sent to the router, which forwards it through the appropriate interface to the destination subnet.
5. Verification of Subnetting and Routing:
    - Use the ping command from one subnet to another to verify connectivity. For example:
        - From PC0 (192.168.1.2/25), ping PC2 (192.168.1.130/25). The router should successfully route the traffic from Subnet 1 to Subnet 2.
    - This verifies that subnetting is correctly implemented and the router is facilitating inter-subnet communication.

By segmenting the network into two subnets and using the router for routing, this experiment demonstrates the practical implementation of subnetting and how routers enable communication between different subnets.

Observations:





FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0001.C79B.5B72

IP Configuration

○ DHCP

● Static

IPv4 Address 192.168.10.1

Subnet Mask 255.255.0.0

IPv6 Configuration

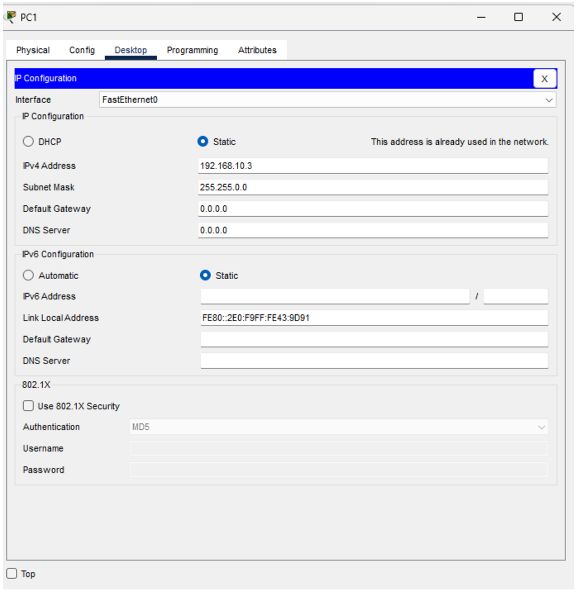
○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::201:C7FF:FE9B:5B72

□ Top



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static This address is already used in the network.

IPv4 Address 192.168.10.3

Subnet Mask 255.255.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::2E0:F9FF:FE43:9D91

Default Gateway

DNS Server

802.1X

□ Use 802.1X Security

Authentication MD5

Username

Password

□ Top

Results: Successfully simulated the process of subnetting using a router.