

# Indian Institute of Information Technology Bhopal



**Session:2024-25**

**Computer Network**

**Course Code: CSE 223**

**Submitted By:**

Kunal Koshta  
22U02025

**Submitted To:**

Dr. Sonal Chandel

## INDEX

S.No	Name of Assignment	Date of Performance	Page No.	Remarks
1	Study of Network Devices in Detail.	18-07-2024	1	
2	Study of basic network command and Network configuration commands.	18-07-2024	4	
3	Basic of CPT Downloading CPT and getting familiar with it?	18-07-2024	7	
4	a).Establish a peer-to-peer connection and showthat delivery of packets is successful, also checkfor the MAC or Physical Address of the systems being communicating. Simulate LAN using HUB using the start topology (Minimum 5 machines)	25-07-2024	9	
5	a).Demonstrate the use of SWITCH and show through simulation that the switch is able to communicate often in LAN only. b).Demonstrate the use of static routing with theuse of a router and Switch simultaneously to establish communication in different LANs	08-08-2024	13	
6	Interpreting Ping and Traceroute Output	08-08-2024	17	
7	a).Configure the static routing using 4 switches 4 routes and at least 8 machines. b).Build a basic network using static routing,use a server in each network and connect each router to one another (at least 2 routers)	22-08-2023	20	
8	a).Demonstrate use of dynamic routing with use of router and switch simultaneously to establish communication in different LAN. b).Build a basic network using dynamic routing, use a server in each network and connect each router to one another.	17-10-2023	24	

## **ASSIGNMENT-1**

### **Study of Network Devices in Detail.**

Some common devices used to establish networks are:

#### **1. Router:**

Routers are devices that route or forward data packets across networks, often connecting different network segments or types (such as local area networks, or LANs, and wide area networks, or WANs). They operate at Layer 3 (the **Network Layer**) of the OSI model.

- **Function:** Routers analyze the destination IP address of each packet, determine the best path for data transfer, and forward packets to their destination.
- **Types:**
  - **Core Routers:** Handle large amounts of data at the core of the network.
  - **Edge Routers:** Located at the boundaries of the network, they connect internal networks to external ones.
  - **Wireless Routers:** Provide wireless connectivity and often include integrated switches and firewalls for home or small office use.
- **Protocols Used:** Routing protocols like OSPF, BGP, and RIP determine the best route for data packets across networks.

#### **2. Switch:**

Switches are devices that connect devices within a single network, typically within a LAN, and manage data traffic to optimize data transfer efficiency. They operate at Layer 2 (the **Data Link Layer**) of the OSI model, although some switches (Layer 3 switches) also have routing capabilities.

- **Function:** Switches receive incoming data packets, examine the destination MAC address, and forward the packets only to the intended recipient device, enhancing bandwidth efficiency.
- **Types:**
  - **Unmanaged Switches:** Basic switches with no configuration options, used primarily in small networks.
  - **Managed Switches:** Allow configuration, monitoring, and control over LAN traffic and often include VLAN support, quality of service (QoS) settings, and port mirroring.
  - **Layer 3 Switches:** Combine the functions of switches and routers, operating at both Layer 2 and Layer 3 to route data between VLANs.

### 3. Hub:

Hubs are simple devices that connect multiple computers in a network. Unlike switches, hubs do not filter or direct data packets. They operate at Layer 1 (the **Physical Layer**) of the OSI model.

- **Function:** Hubs transmit incoming data packets to all ports, regardless of the destination. This approach is inefficient compared to switches as it increases network congestion.
- **Types:**
  - **Active Hub:** Amplifies signals before broadcasting to all devices.
  - **Passive Hub:** Simply broadcasts incoming data without amplifying it.
  - **Intelligent Hub:** Adds basic management features and network monitoring.

### 4. Access Point (AP):

An Access Point (AP) is a device that allows wireless devices to connect to a wired network. They operate primarily at Layer 2 (the **Data Link Layer**) of the OSI model.

- **Function:** Access points receive and transmit wireless signals, enabling devices to communicate with a network without cables. They also facilitate roaming between different APs in larger networks, allowing seamless connectivity.
- **Types:**
  - **Standalone Access Points:** Basic APs for single, smaller areas.
  - **Controller-Based Access Points:** Part of a centrally managed wireless network, often found in enterprises.
  - **Mesh APs:** Used in mesh networks to extend coverage by relaying data through multiple access points.

### 5. Modem:

Modems are devices that modulate and demodulate signals, enabling digital data transmission over telephone lines or cable systems. They operate at Layer 1 (the **Physical Layer**) and Layer 2 (the **Data Link Layer**) of the OSI model.

- **Function:** Modems convert digital signals from a computer into analog signals for transmission over phone lines (DSL modem) or coaxial cables (cable modem). They also convert received analog signals back into digital form.
- **Types:**
  - **DSL Modems:** Used with digital subscriber lines for high-speed internet over phone lines.
  - **Cable Modems:** Provide internet connectivity over cable TV infrastructure.
  - **Fiber Optic Modems:** Convert optical signals for transmission over fiber networks, often paired with routers for IP packet handling.

## **6. Firewall:**

Firewalls are security devices that monitor and control incoming and outgoing network traffic based on predefined security rules. They operate primarily at Layer 3 (the **Network Layer**) and Layer 4 (the **Transport Layer**), though some advanced firewalls work up to Layer 7 (the **Application Layer**) of the OSI model.

- **Function:** Firewalls block or allow traffic based on security policies, filtering traffic by IP address, protocol, port number, or application. They protect networks from unauthorized access and cyber threats.
- **Types:**
  - **Network Firewalls:** Standalone hardware or software firewalls that protect entire networks.
  - **Host-Based Firewalls:** Installed on individual devices to filter traffic to and from that device.
  - **Next-Generation Firewalls (NGFW):** Incorporate advanced features such as deep packet inspection (DPI), intrusion prevention, and application-layer filtering.

## **7. Gateway**

Gateways are devices that connect networks using different protocols and formats. They operate across multiple OSI layers, typically from Layer 4 (the **Transport Layer**) to Layer 7 (the **Application Layer**).

- **Function:** Gateways translate data between different networks, enabling communication between incompatible networks by performing protocol conversion.
- **Types:**
  - **Protocol Gateways:** Convert data between different network protocols.
  - **Email Gateways:** Filter and monitor email traffic to prevent spam and malware.
  - **Voice over IP (VoIP) Gateways:** Convert voice data between digital VoIP and traditional analog telephony networks.

## **8. Bridge:**

A bridge connects two or more network segments within the same network. It operates at Layer 2 (the **Data Link Layer**) of the OSI model.

- **Function:** Bridges filter and forward data between network segments, reducing collisions and improving performance by creating separate collision domains.
- **Types:**
  - **Local Bridges:** Connect devices within the same physical location.
  - **Remote Bridges:** Connect network segments over longer distances, often using dedicated links or VPNs.

- **Wireless Bridges:** Extend network connectivity wirelessly, often used to connect two buildings.

### **9. Repeater:**

Repeaters are simple devices that regenerate and amplify signals across network segments. They operate at Layer 1 (the **Physical Layer**) of the OSI model.

- **Function:** Repeaters extend network range by regenerating signals to overcome signal degradation over long distances.
- **Types:**
  - **Standard Repeaters:** Used in wired networks to extend the reach of Ethernet cables.
  - **Wi-Fi Repeaters:** Extend wireless network coverage by retransmitting Wi-Fi signals.

### **10. Network Interface Card (NIC):**

A NIC is a hardware component that connects a device to a network. It operates at Layer 1 (the **Physical Layer**) and Layer 2 (the **Data Link Layer**) of the OSI model.

- **Function:** NICs provide a physical connection to the network and manage data transmission over the network, often embedding a unique MAC address for network identification.
- **Types:**
  - **Wired NICs:** Connect devices using Ethernet cables.
  - **Wireless NICs:** Connect devices to wireless networks, using Wi-Fi standards such as 802.11ac or 802.11ax.

## ASSIGNMENT-2

### Study of basic network command and Network configuration commands.

Some diagnostic and config commands are as follows:

#### Basic Network Diagnostic Commands:

1. **ping:**
  - **Purpose:** Tests the connectivity to a host by sending ICMP (Internet Control Message Protocol) echo requests.
  - **Syntax:** ping [hostname or IP address]
  - **Example:** ping google.com
  - **Usage:** If you can ping an IP but not a hostname, there may be DNS issues. Continuous pings can show packet loss or network quality.
2. **tracert (Windows) / traceroute (Linux):**
  - **Purpose:** Shows the route packets take to reach a destination, displaying each hop along the path.
  - **Syntax:** tracert [hostname or IP address] (Windows) / traceroute [hostname or IP address] (Linux)
  - **Example:** tracert google.com
  - **Usage:** Identify where delays occur in the network path.
3. **nslookup:**
  - **Purpose:** Looks up DNS records for a given domain or IP address.
  - **Syntax:** nslookup [hostname or IP address]
  - **Example:** nslookup google.com
  - **Usage:** Useful for troubleshooting DNS issues or verifying domain-to-IP mappings.
4. **ipconfig (Windows) / ifconfig (Linux):**
  - **Purpose:** Displays the IP configuration of the system, including IP address, subnet mask, and default gateway.
  - **Syntax:** ipconfig (Windows) / ifconfig (Linux)
  - **Example:** ipconfig /all (detailed view)
  - **Usage:** Check your IP address, subnet, and gateway information; release or renew IP on Windows with ipconfig /release and ipconfig /renew.
5. **netstat:**
  - **Purpose:** Displays network connections, routing tables, and network interface statistics.
  - **Syntax:** netstat [options]
  - **Example:** netstat -a (shows all connections and listening ports)
  - **Usage:** See open ports, active connections, and identify potential unwanted connections.
6. **arp:**
  - **Purpose:** Shows the Address Resolution Protocol (ARP) cache, which maps IP addresses to physical (MAC) addresses.

- **Syntax:** arp -a
- **Usage:** Troubleshoot local network issues, especially when IPs don't resolve to correct MAC addresses.

### **Network Configuration Command:**

1. **ip (Linux):**
  - **Purpose:** Used for configuring network interfaces.
  - **Syntax:** ip [option] [action] [arguments]
  - **Example:** ip addr show (displays IP addresses), ip route (shows routing table)
  - **Usage:** Manage IP addresses, routes, and network devices.
2. **route:**
  - **Purpose:** Displays or modifies the routing table.
  - **Syntax:** route [add|del] [destination]
  - **Example:** route add default gw [gateway IP]
  - **Usage:** Set or view the default gateway or configure static routes.
3. **hostname:**
  - **Purpose:** Displays or sets the hostname of the system.
  - **Syntax:** hostname [new-hostname]
  - **Example:** hostname server01
  - **Usage:** Identify or set the machine's name on the network, helpful for DNS and identifying devices.
4. **dhclient (Linux):**
  - **Purpose:** Requests an IP address from a DHCP server.
  - **Syntax:** dhclient [interface]
  - **Example:** dhclient eth0
  - **Usage:** Useful if you lose network connectivity and need to renew your IP from DHCP.
5. **netsh (Windows):**
  - **Purpose:** Configures network interfaces and other networking-related configurations.
  - **Syntax:** netsh [context] [commands]
  - **Example:** netsh interface ip set address "Local Area Connection" static [IP Address] [Subnet Mask] [Gateway]
  - **Usage:** Manages IP configurations, firewall settings, and more.
6. **systemctl (Linux) (for managing network services):**
  - **Purpose:** Manages services, like enabling or restarting network services.
  - **Syntax:** systemctl [action] [service]
  - **Example:** systemctl restart networking
  - **Usage:** Useful for restarting network services after configuration changes.

### **Practical Use Cases:**

1. **Troubleshooting Connectivity:**



- Use ping to check if the host is reachable.
- Follow up with tracert/traceroute to find where the connection may be failing.
- 2. **Resolving DNS Issues:**
  - Use nslookup to verify DNS server responses.
  - Check with ipconfig /displaydns (Windows) to see local DNS cache.
- 3. **Resetting Network Configuration:**
  - In Windows, use ipconfig /release followed by ipconfig /renew to refresh your IP.
  - In Linux, use dhclient -r followed by dhclient for similar effect.
- 4. **Configuring Static Routes:**
  - Use the route command to add persistent routes if specific networks should go through different gateways.
- 5. **Identifying Network Congestion or Unauthorized Connections:**
  - netstat helps in reviewing all active connections, so you can spot unexpected or excessive usage patterns.

## **ASSIGNMENT – 3**

### **Basic of CPT, Downloading CPT and Getting familiar with it.**

#### **Introduction:**

Cisco Packet Tracer is a network simulator tool that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

#### **Features:**

- **Create network topologies:** Packet Tracer allows users to create network topologies with a variety of devices, including routers, switches, hosts, and firewalls.
- **Configure devices:** Packet Tracer allows users to configure Cisco devices using a simulated command line interface.
- **Simulate network traffic:** Packet Tracer allows users to simulate network traffic between devices.
- **Visualize network traffic:** Packet Tracer allows users to visualize network traffic using a variety of tools, such as packet captures and traceroutes.
- **Create and share labs:** Packet Tracer allows users to create and share labs with other users.

#### **Uses:**

- Learning about networking concepts
- Practicing network troubleshooting
- Instructing networking courses
- Researching new networking technologies

#### **Installing Packet Tracer:**

Follow the below steps to install Packet Tracer on Windows:

**Step 1:** Visit the official website of NetAcad using any web browser

**Step 2:** Press the login button and select log in option.

**Step 3:** Next screen will appear, click on the sign-up option and then will ask for email and password and other simple details, fill them and click on Register.

**Step 4:** After successfully sign-up Dashboard will initialize, now click on Resources and choose Download Packet Tracer Option.

**Step 5:** On the next web page choose the operating system to download the packet tracer. Downloading will start automatically.

**Step 6:** Open the downloaded file and setup it.

**Step 7:** Choose the installation location and start menu folder and click the Next button.

**Step 8:** Now packet tracer is ready to install so click on the **Install** button and Installation will start.

**Step 9:** Click on the **Finish** button to complete the installation.

**Step 10:** Interface is initialized, and the software is ready to use.

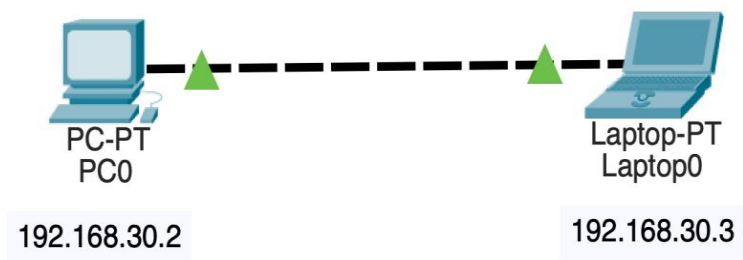
## ASSIGNMENT-4

Establish a peer-to-peer connection and show that delivery of packets is successful also check for MAC and physical address of systems being communicating.

### Step 1: Set up the devices in the Network

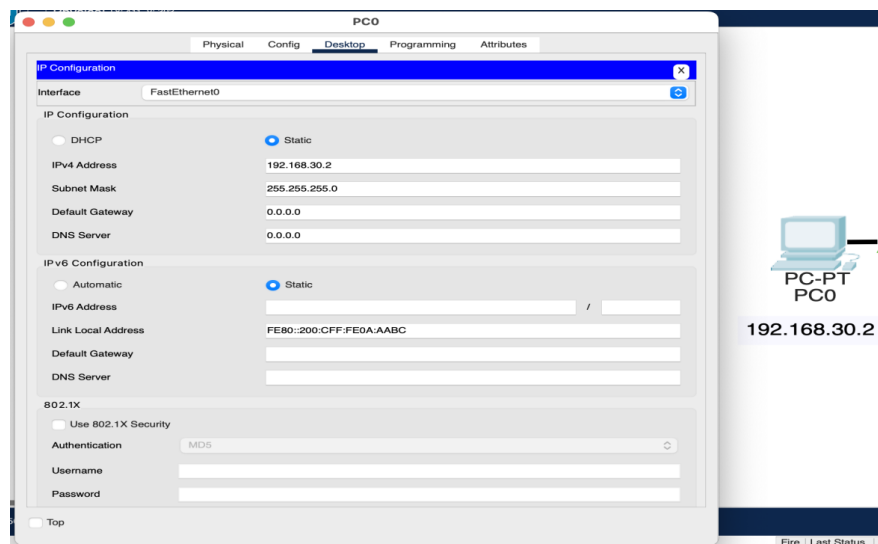
- Select two devices and place them in your workspace.
- Connect them with the appropriate cable.

#### PEER TO PEER CONNECTION



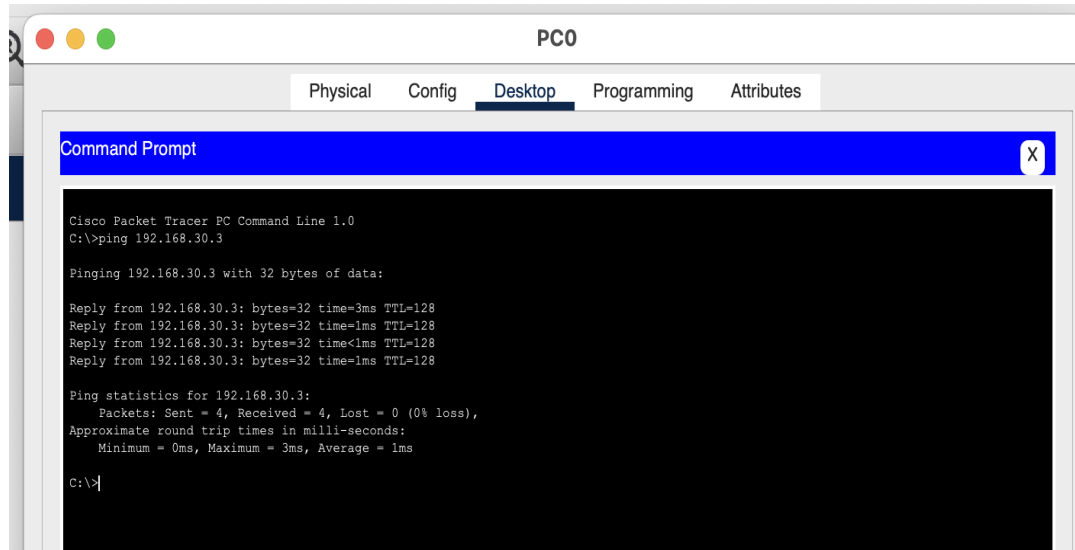
### Step 2: Configure the IP Addresses for the devices

- Click on each device to open the configuration window and configure IP addresses for both devices.



### Step 3: Verifying Packet delivery as well as connections

- Open the command prompt on each device by clicking on the desktop icon and use the ping command to test the connection as well as packet delivery. For device 1 type: **ping(IP address of device 2)**. Repeat for another device.



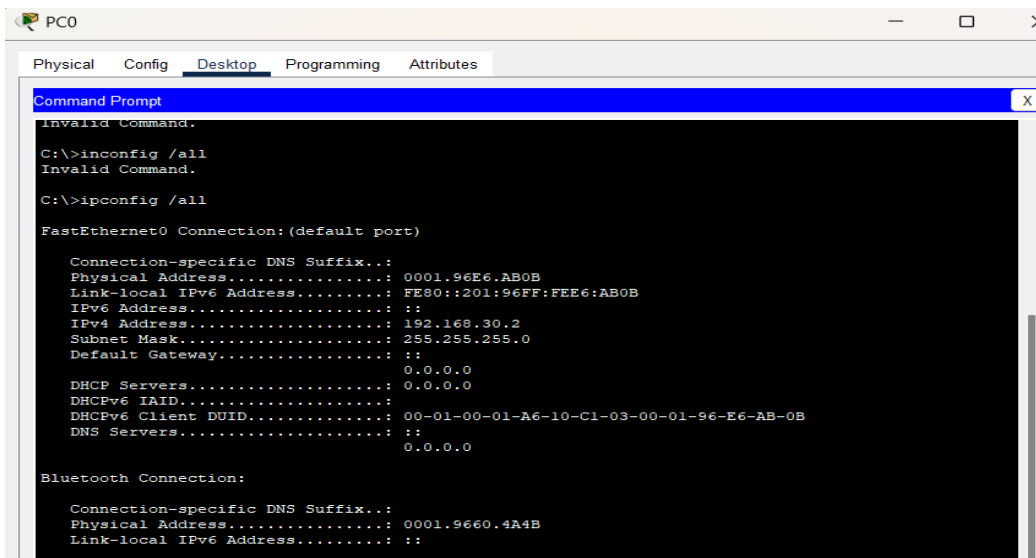
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=3ms TTL=128
Reply from 192.168.30.3: bytes=32 time=1ms TTL=128
Reply from 192.168.30.3: bytes=32 time<1ms TTL=128
Reply from 192.168.30.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```



```
Invalid Command.

C:\>inconfig /all
Invalid Command.

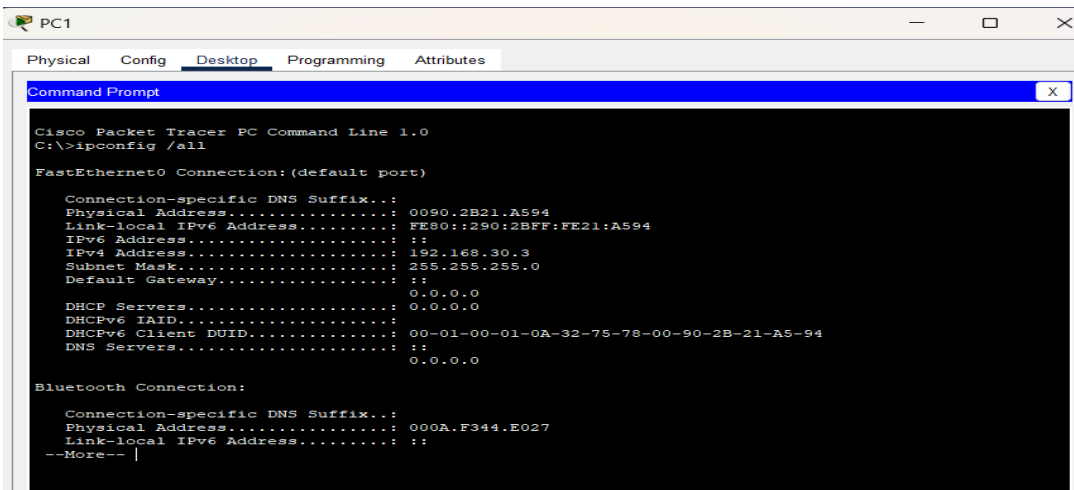
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...: 0001.96E6.AB0B
    Physical Address...: FE80::201:96FF:FEE6:AB0B
    IPv6 Address...: ::
    IPv4 Address...: 192.168.30.2
    Subnet Mask...: 255.255.255.0
    Default Gateway...: ::
    DHCP Servers...: 0.0.0.0
    DHCPv6 IAID...: 0.0.0.0
    DHCPv6 Client DUID...: 00-01-00-01-A6-10-C1-03-00-01-96-E6-AB-0B
    DNS Servers...: ::
    0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address...: 0001.9660.4A4B
    Link-local IPv6 Address...: ::
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...: 0090.2B21.A594
    Physical Address...: FE80::290:2BFF:FE21:A594
    IPv6 Address...: ::
    IPv4 Address...: 192.168.30.3
    Subnet Mask...: 255.255.255.0
    Default Gateway...: ::
    DHCP Servers...: 0.0.0.0
    DHCPv6 IAID...: 0.0.0.0
    DHCPv6 Client DUID...: 00-01-00-01-0A-32-75-00-90-2B-21-A5-94
    DNS Servers...: ::
    0.0.0.0

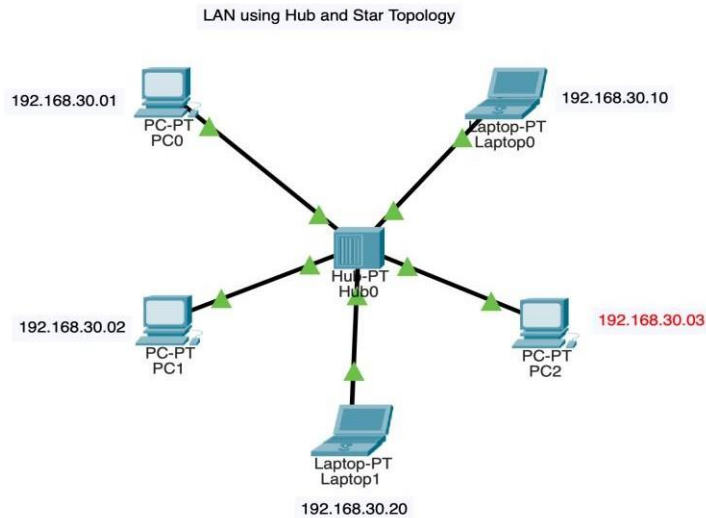
Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address...: 000A.F344.E027
    Link-local IPv6 Address...: ::
--More-- |
```

## **Simulate LAN using Hub and use Star Topology (Connect at least 5 machines).**

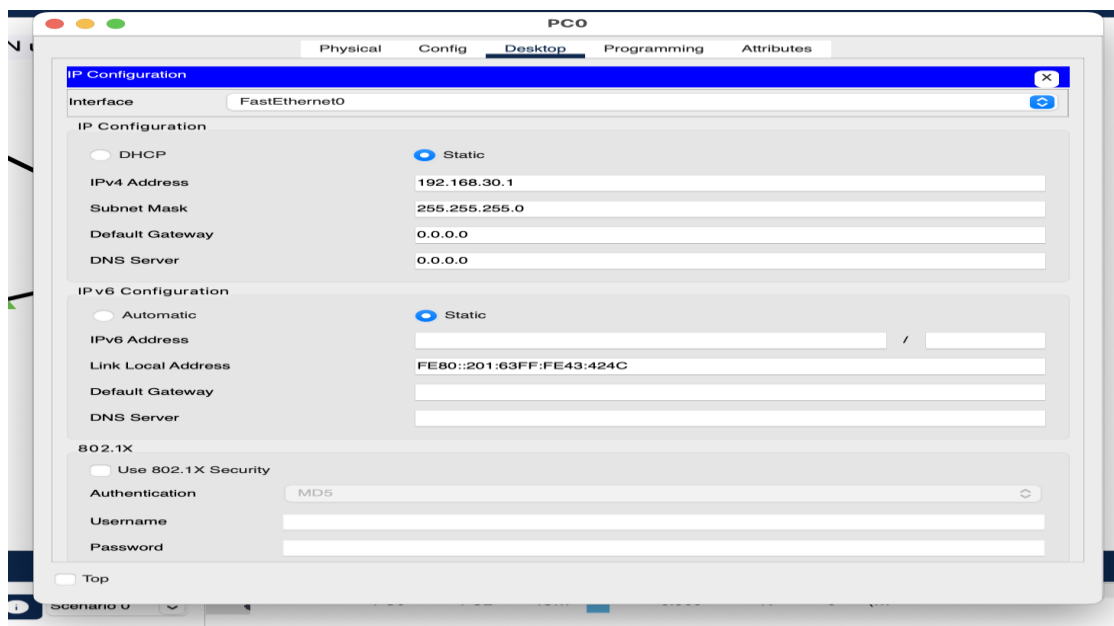
### **Step 1: Set up the devices in the Network**

- ? Place 5 devices in a star topology with a HUB in the middle.
- ? Connect all devices to the HUB using LAN.



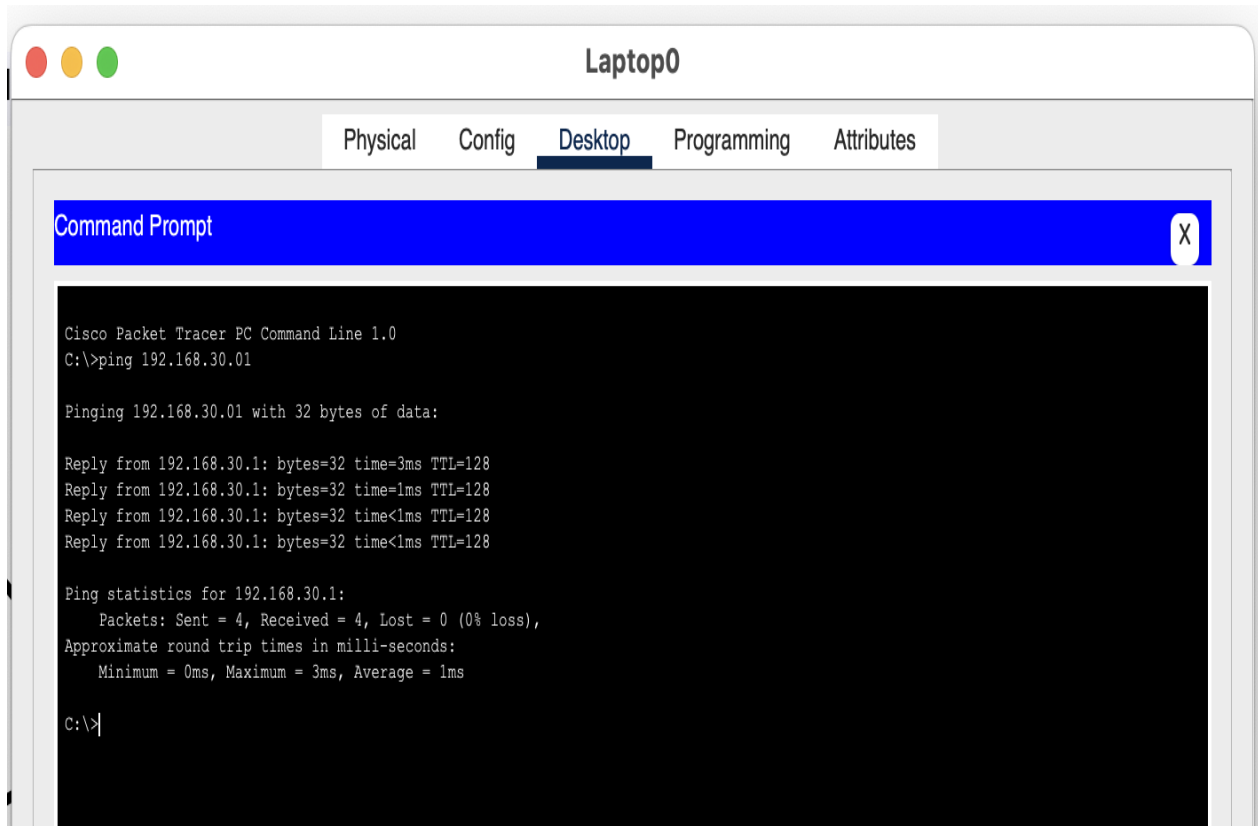
### **Step 2: Configure the IP Addresses for the devices.**

- ? Configure IP addresses for all the devices.



### Step 3: Verifying Packet delivery as well as connections

- Open the command prompt on each device by clicking on the desktop icon and use the ping command to test the connection as well as packet delivery. For device 1 type: **ping(IP address of device 2)**. Repeat for another devices.

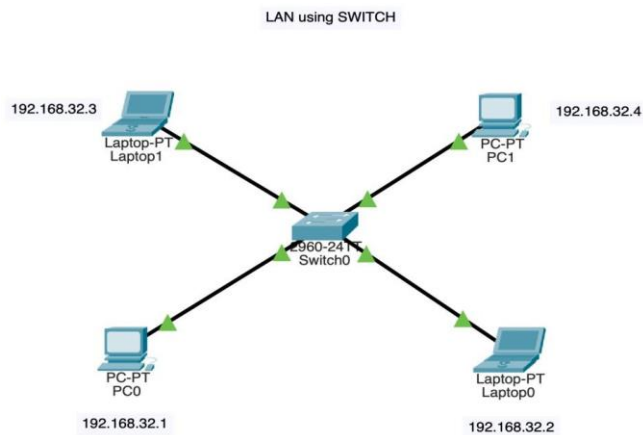


## ASSIGNMENT-5

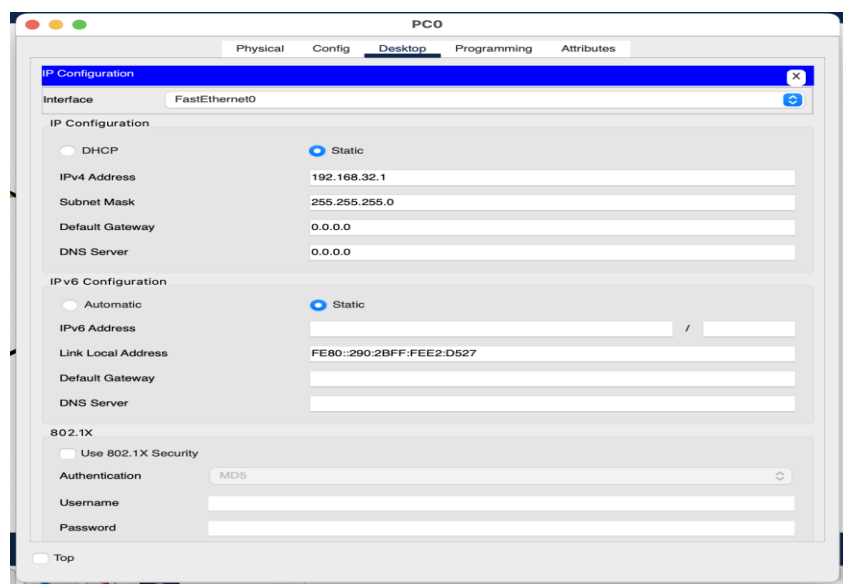
Demonstrate use of switch and show through simulation that switch is able to communicate often in LAN only.

### Set up the devices in the Network

- Place devices with a Switch in the middle.
- Connect all devices to the Switch using LAN.



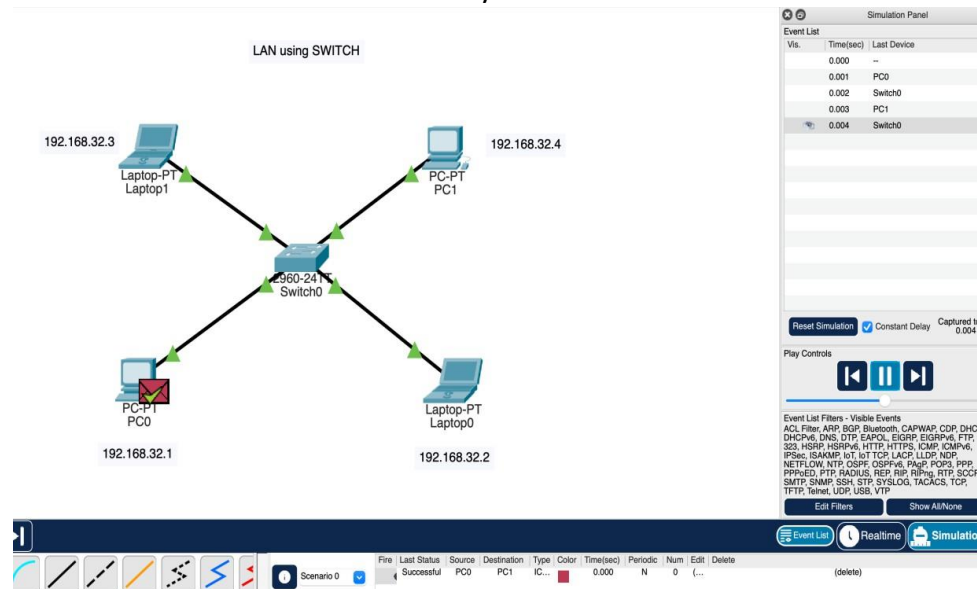
Click on each device to open the configuration window and configure IP addresses for both devices.





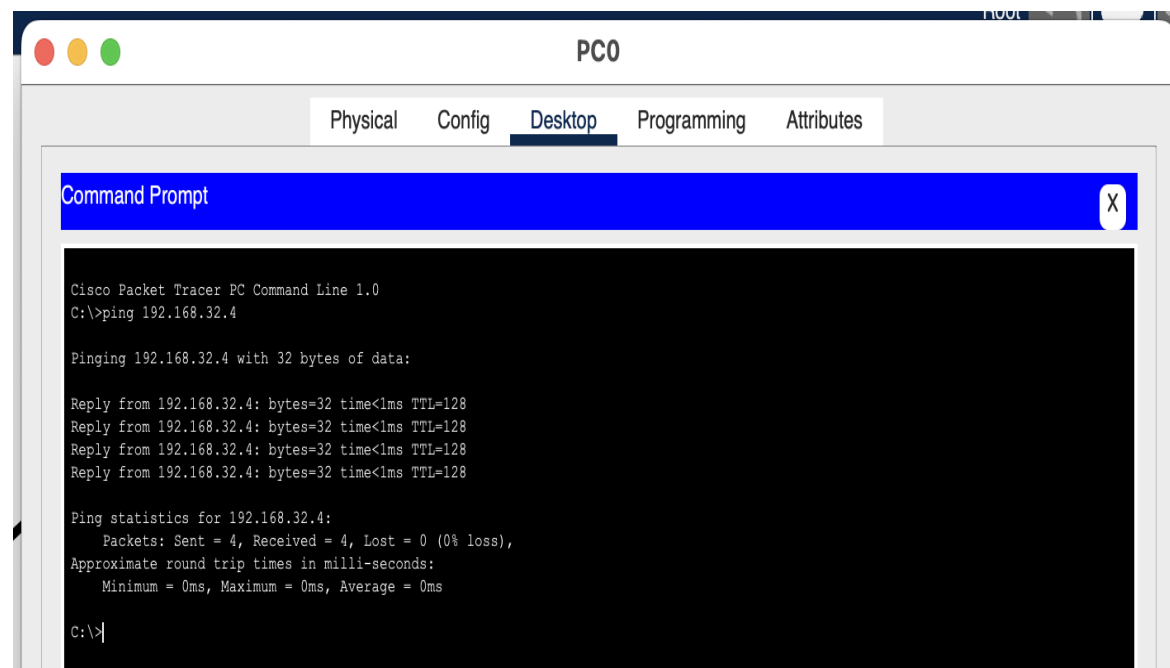
Click on the message symbol and select the devices for sending and receiving message respectively.

Click simulation to check the delivery.



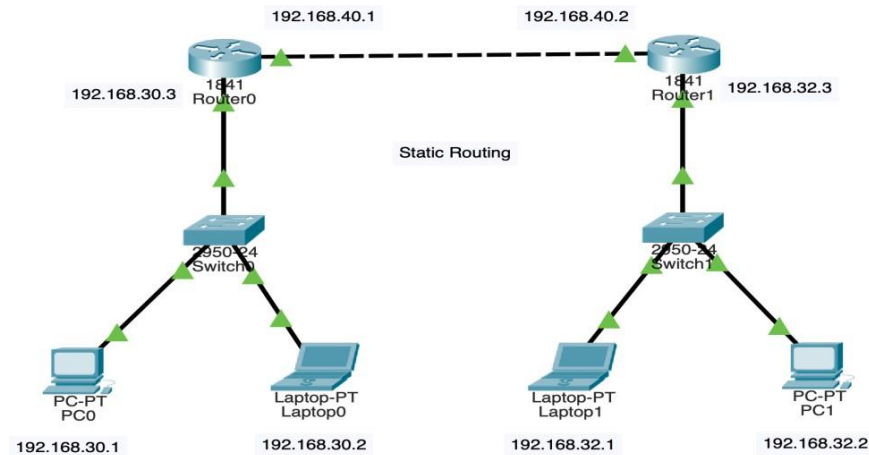
#### Step 4: Verifying Packet delivery as well as connections.

- ❓ Open the command prompt on each device by clicking on the desktop icon and use the ping command to test the connection as well as packet delivery. For device 1 type: **ping(IP address of device 2)**. Repeat for another devices.

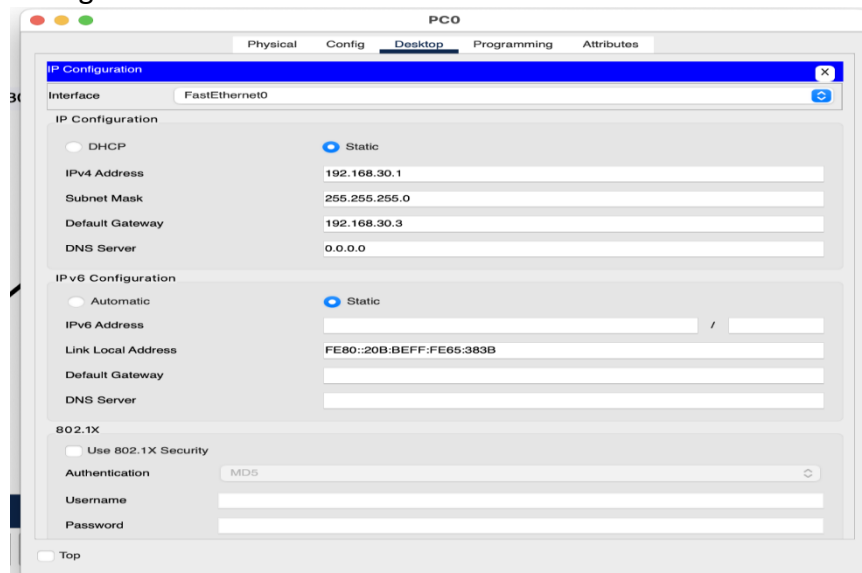


**Demonstrate use of static routing with use of router and switch simultaneously to establish communication in different LANs.**

Make the logical structure as shown in fig below.

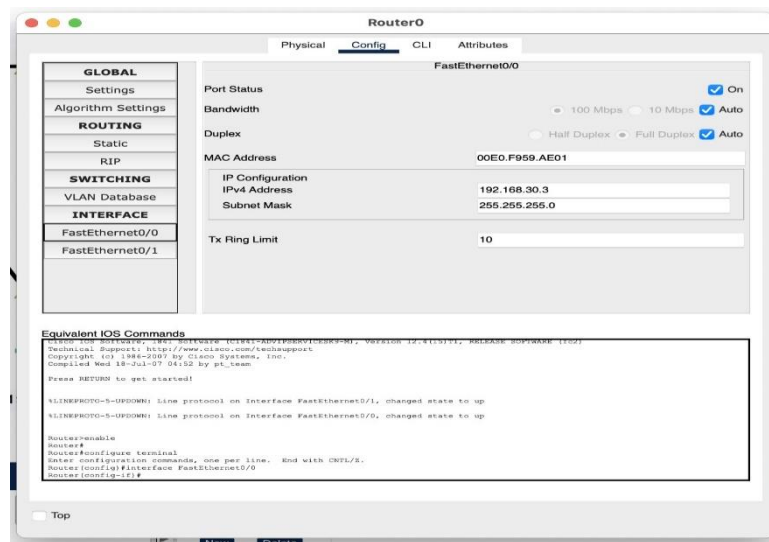


Configure IP addresses for all the devices.



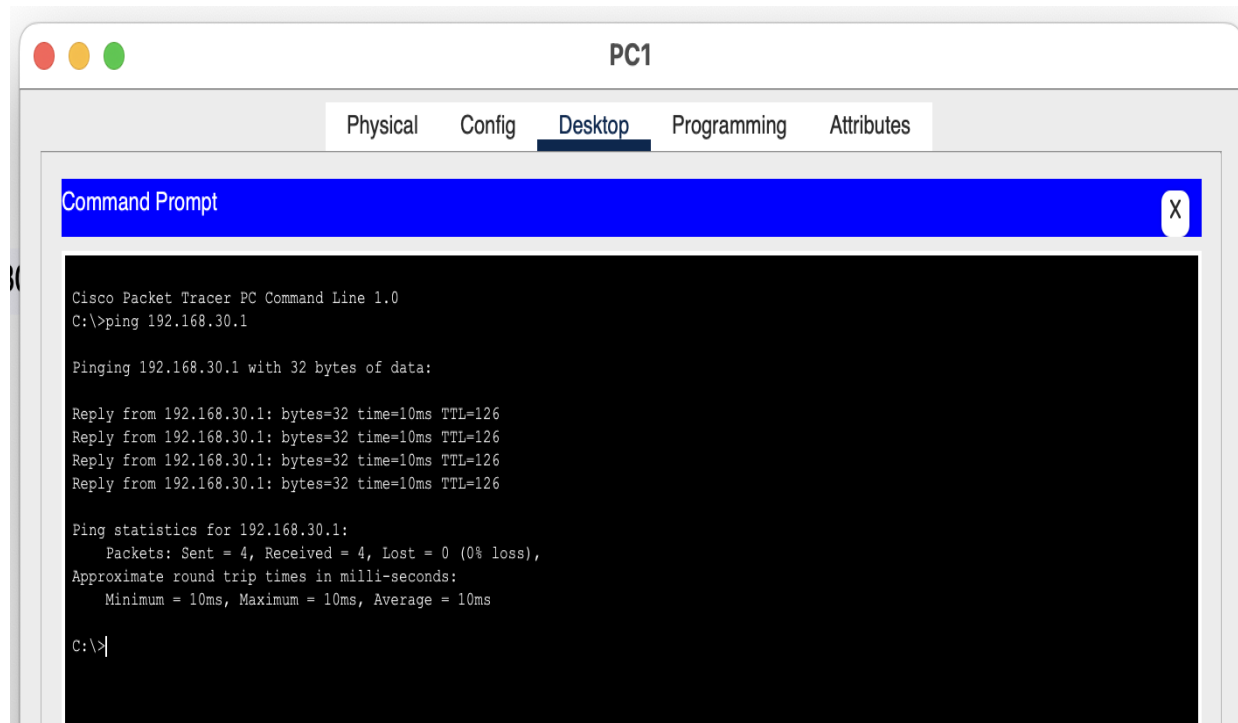
### Step 3: Configure the IP Addresses to the Routers for different Networks

- ? For routers add serial ports if required.
- ? Assign the IP's in serial ports and fast ethernet port for all the routers.



### Step 5: Verifying Packet delivery as well as connections.

- Open the command prompt on each device by clicking on the desktop icon and use the ping command to test the connection as well as packet delivery. For device 1 type: **ping(IP address of device 2)**. Repeat for another devices.



## ASSIGNMENT-6

### Interpreting Ping and Traceroute Output.

**Ping** and **Traceroute** outputs is essential for diagnosing network connectivity and latency issues. By using **Ping** to test reachability and **Traceroute** to map the route and identify delays, you can pinpoint where network issues may be occurring. These tools are valuable in troubleshooting and understanding network paths and performance.

**1.)Ping Command:** Ping tests connectivity between two devices by sending **ICMP (Internet Control Message Protocol) Echo Request** packets and waiting for **Echo Reply** packets. The command checks if a device is reachable and provides basic details on response time.

#### Example Ping Output:

```
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=5ms TTL=64
Reply from 192.168.1.10: bytes=32 time=5ms TTL=64
Reply from 192.168.1.10: bytes=32 time=4ms TTL=64
Reply from 192.168.1.10: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round-trip times in milliseconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

#### Key Elements in Ping Output:

- **Reply from [IP Address]: bytes=... time=... TTL=...**
  - **Reply from [IP Address]:** Confirms the destination device responded. If this is shown, it indicates that there is a network path to the destination and that the destination is reachable.
  - **bytes=...:** Packet size, often 32 bytes by default.
  - **time=...:** Round-trip time in milliseconds. Lower values indicate a faster response.
  - **TTL (Time to Live):** Shows the maximum number of hops the packet can take. Each router along the path reduces the TTL by 1; a smaller TTL value in the reply indicates the number of hops taken.

### Common Ping Results:

- **Request Timed Out:** No response from the target, which could mean the target is unreachable, blocked by a firewall, or experiencing network issues.
- **Destination Host Unreachable:** The ping packet couldn't reach the destination, usually due to incorrect routing or an unreachable intermediate device.
- **Unknown Host:** DNS cannot resolve the domain name, often caused by incorrect hostname spelling or DNS issues.

**2.)Traceroute Command:** Traceroute (or **tracert** on Windows) maps the route data packets take from the source to the destination. It identifies each router or hop along the way, giving insights into where delays or issues may occur.

```
Tracing route to 192.168.2.10 over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms  192.168.1.1
  2      5 ms      4 ms      5 ms  10.0.0.2
  3      7 ms      7 ms      8 ms  192.168.2.10

Trace complete.
```

### Key Elements in Traceroute Output:

- **Hop Number:** Indicates the sequence of routers from the source to the destination.
- **Router IP Address or Hostname:** Displays the IP or name of each router encountered.
- **Response Times:** Shows three response times for each hop in milliseconds. Consistently high values or timeouts at specific hops can signal a bottleneck or network problem.

For the above example:

- 🔍 **Hop 1 (192.168.1.1):** The first router (Router 1) has a very low response time, indicating it's directly reachable without delay.
- 🔍 **Hop 2 (10.0.0.2):** Router 2 shows slightly higher response times (4-5 ms), which is typical for a router connecting two subnets.
- 🔍 **Hop 3 (192.168.2.10):** This is the destination (Server 2), and the response times are slightly higher than the previous hop, indicating successful connectivity with minimal delay.

### Common Traceroute Results:

- **Request Timed Out:** This means no response was received from that hop within the timeout. It could be due to a firewall blocking the packets or a device that's set not to respond to ICMP requests.
- **Repeated High Latency:** High response times at a particular hop suggest a delay at that router. Multiple hops with high latency likely indicate congestion on the path.

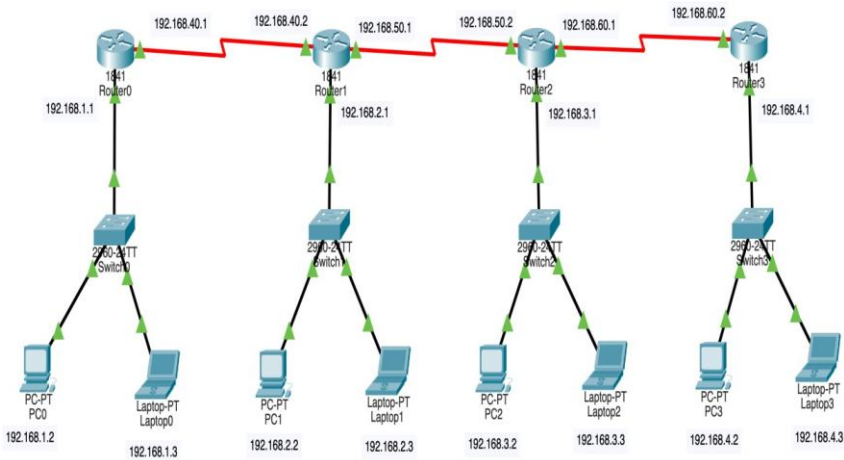
## ASSIGNMENT-7

**Configure Static routing using 4 switches, 4 routers and at least 8 machines.**

Make the logical structure as shown in fig below.

Place all the devices as shown and connect them with switches using suitable wires.

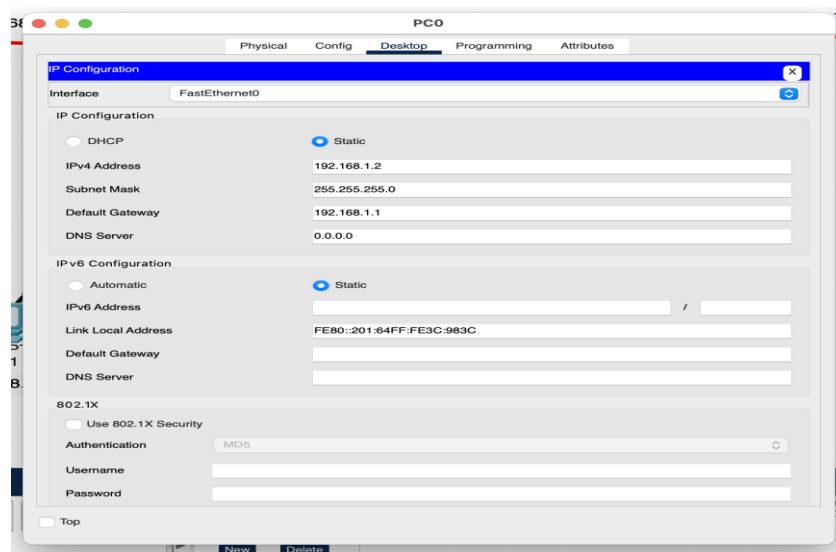
Now, connect switches to routers then connect routers with adjacent routers.



Static Routing using 4 Router and 4 Switches

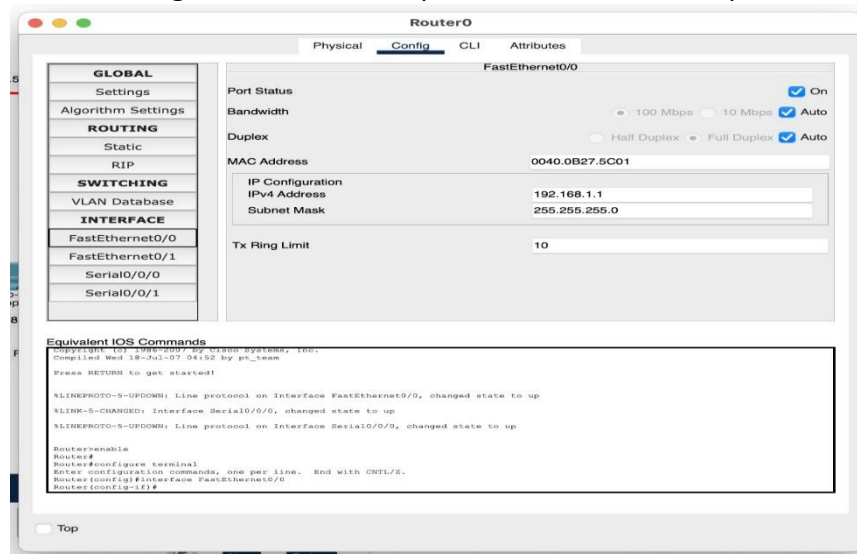
**Step 2: Configure the IP Addresses for the devices.**

Click on each device to open the configuration window and configure IP addresses for all devices.



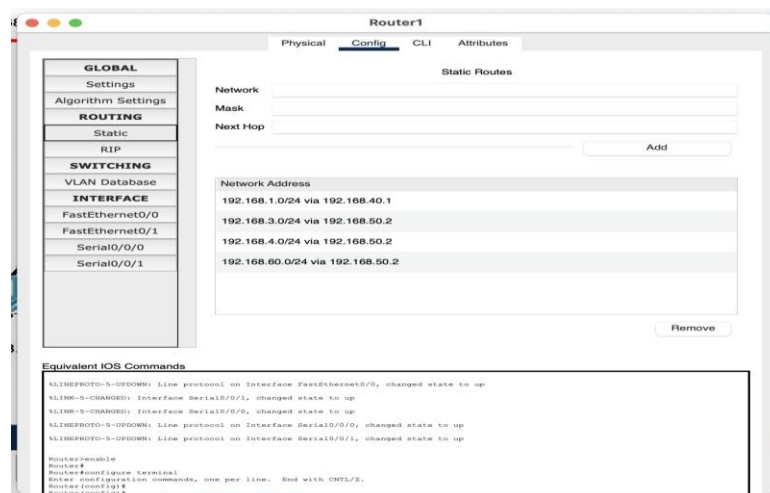
### Step 3: Configure the IP Addresses to the Routers for different Networks

- ? For routers add serial ports if required.
- ? Assign the IP's in serial ports and fast ethernet port for all the routers.



### Step 4: Configure the Network Addresses to Router for Static Routing.

Set up the static routes to each router to connect networks from where the message will be sent or received.



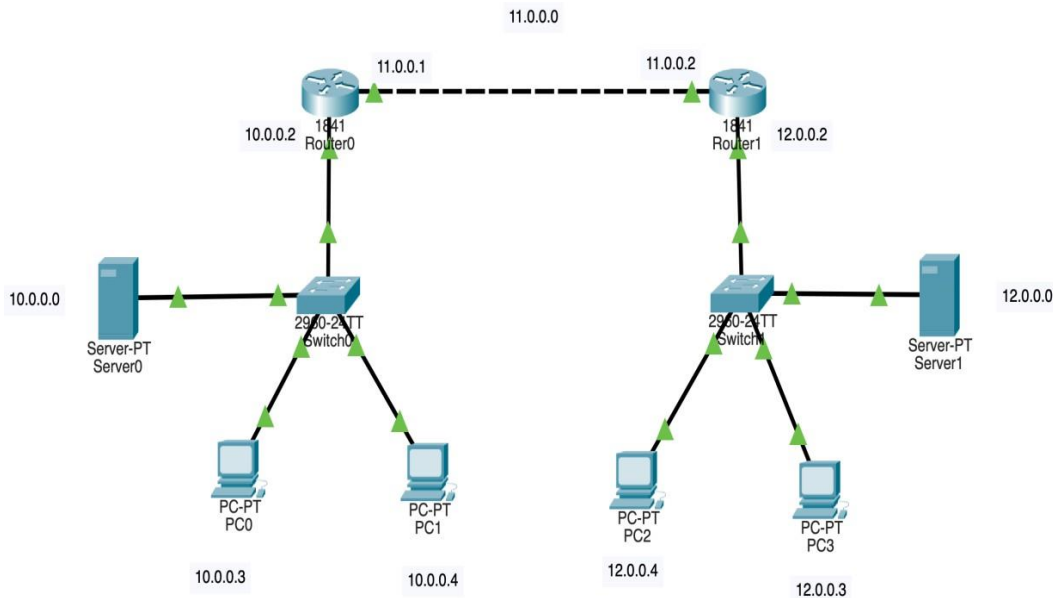
### Step 5: Verifying Packet delivery as well as connections.

- ? Open the command prompt on each device by clicking on the desktop icon and use the ping command to test the connection as well as packet delivery. For device 1 type: ping(IP address of device 2). Repeat for another devices.

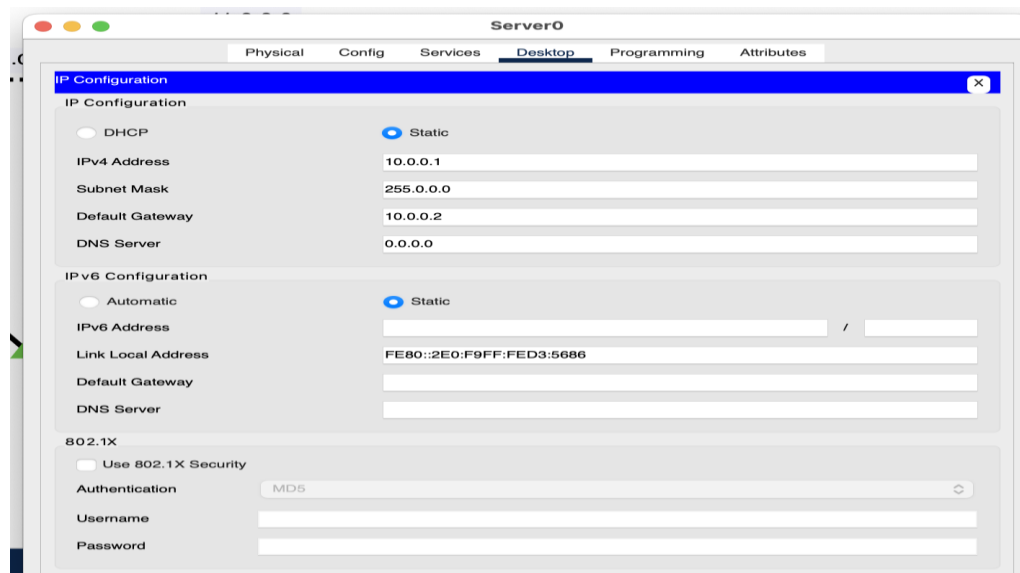


Build a basic network using static routing, use server in each network and connect each router to one another (at least 2 routers).

### Step 1: Set up the devices in the Network



### Step 2: Configure the IP Addresses for the server and default gateways.

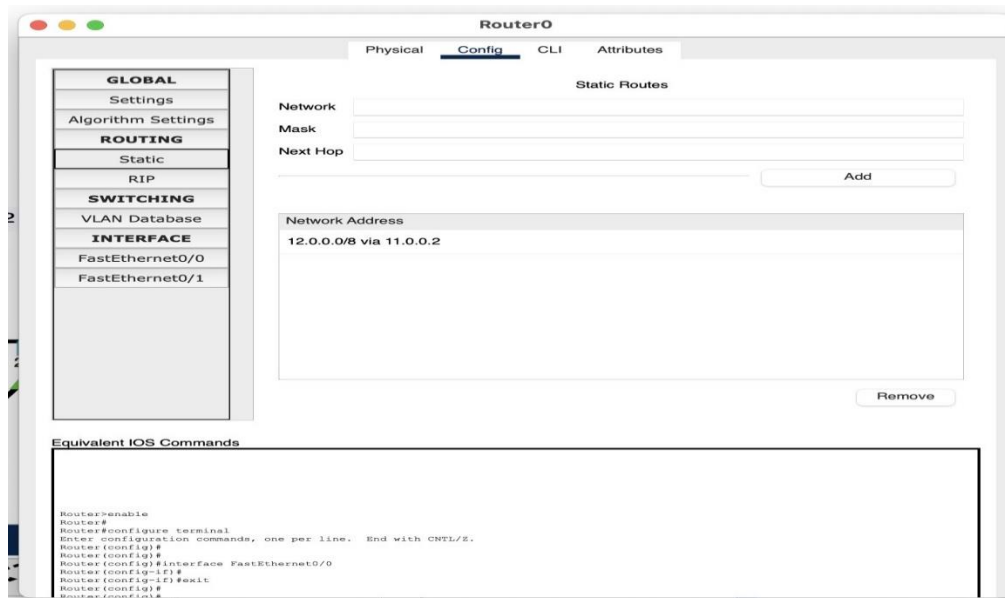


### Step 3: Set the server configuration via DHCP

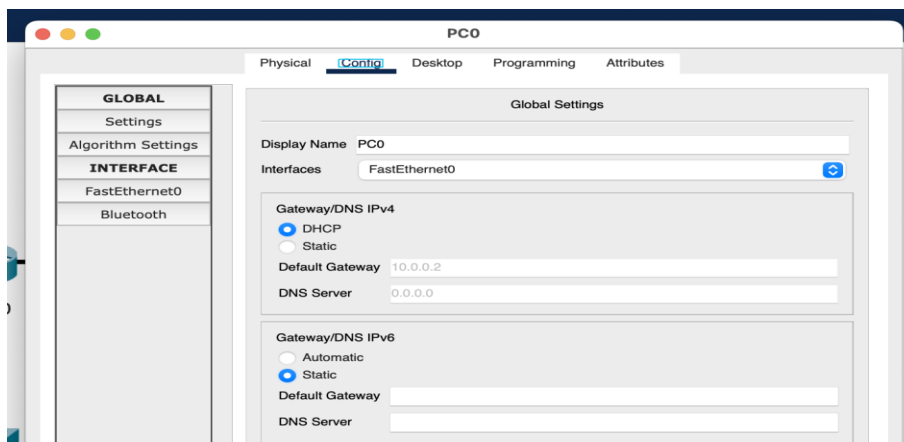
### Step 4: Configure the IP Addresses to the Routers for different Networks



## Step 5: Configure the Network Addresses to Router for Static Routing



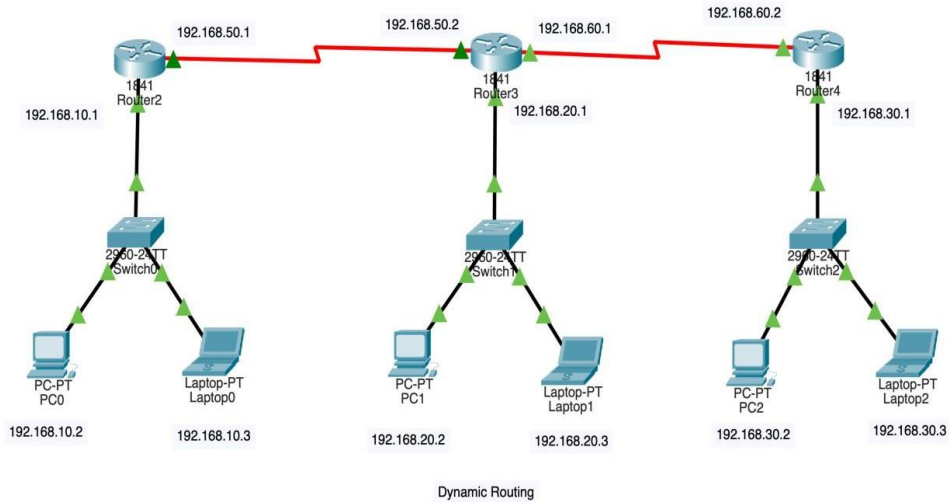
## Step 6: Configure the IP address of devices via DHCP



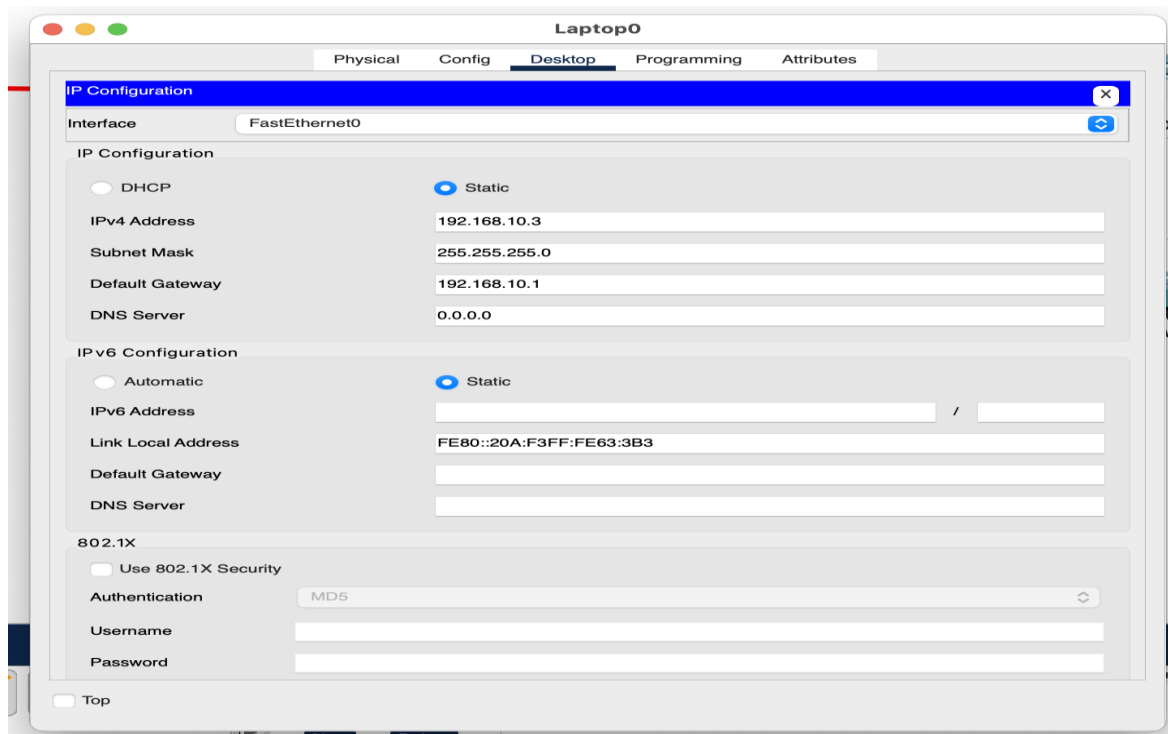
## ASSIGNMENT-8

Demonstrate use of Dynamic routing with use of router and switch simultaneously to establish communication in different LANs.

### Step 1: Set up the devices in the Network



### Step 2: Configure the IP Addresses for the devices and default gateways.



### Step 3: Configure the IP Addresses to the Routers for different Networks

The screenshot shows the configuration window for Router3, specifically the 'Config' tab for the 'FastEthernet0/0' interface. The left sidebar contains a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING (with sub-items Static and RIP), SWITCHING, VLAN Database, and INTERFACE (with sub-items FastEthernet0/0, FastEthernet0/1, Serial0/0/0, and Serial0/0/1). The main area displays the configuration for FastEthernet0/0, including Port Status (On), Bandwidth (100 Mbps), Duplex (Full Duplex), MAC Address (0001.C9D5.E101), IP Configuration (IPv4 Address: 192.168.20.1, Subnet Mask: 255.255.255.0), and Tx Ring Limit (10). Below the configuration fields is a section titled 'Equivalent IOS Commands' containing a list of commands to replicate the configuration in a CLI environment.

**Router3**

Physical **Config** CLI Attributes

**FastEthernet0/0**

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.C9D5.E101

IP Configuration

IPv4 Address 192.168.20.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

**Equivalent IOS Commands**

```
%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 FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#
```

☐ Top

The screenshot shows the configuration window for Router2, specifically the 'Config' tab for the 'RIP Routing' section. The left sidebar is identical to the one in the Router3 window. The main area displays the 'RIP Routing' configuration, including a 'Network' section with a list of network addresses: 192.168.10.0, 192.168.20.0, 192.168.30.0, 192.168.50.0, and 192.168.60.0. There is an 'Add' button to the right of the list and a 'Remove' button at the bottom right. Below the configuration fields is a section titled 'Equivalent IOS Commands' containing a list of commands to replicate the configuration in a CLI environment.

**Router2**

Physical **Config** CLI Attributes

**RIP Routing**

Network

Network Address

192.168.10.0

192.168.20.0

192.168.30.0

192.168.50.0

192.168.60.0

Add

Remove

**Equivalent IOS Commands**

```
Press RETURN to get started!

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

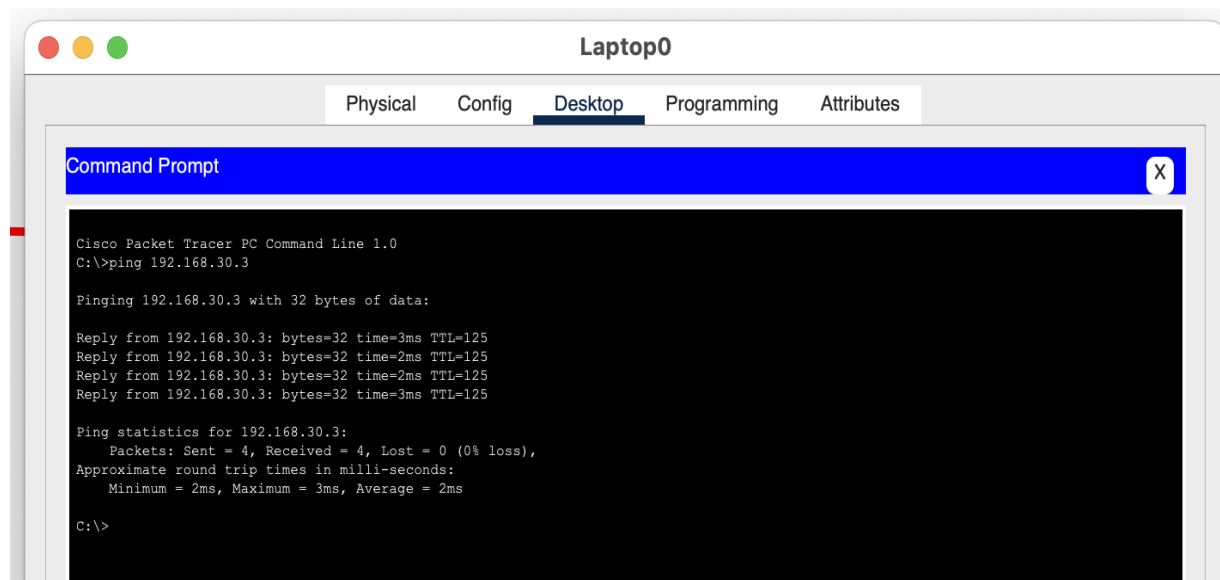
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#
```

☐ Top

### Step 4: Configure the Network Addresses to Router for Dynamic Routing

### Step 5: Verifying Packet delivery as well as connections

- Open the command prompt on each device by clicking on the device icon and use the ping command to test the connection as well as packet delivery. For device 1 type: ping(IP address of device 2). Repeat for another device.



**Build a basic network using dynamic routing, use a server in each network and connect each router to one another.**

### Step 1: Set up the devices in the Network



### Step 2: Configure the IP Addresses for the devices and default gateways.

- Click on each device to open the configuration window and configure IP addresses for both devices.

Server0

Physical Config Services Desktop Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80:209:7CFF:FEBA:7336

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Server2

Physical Config Services Desktop Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80:290:21FF:FEE1:3B60

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

### Step 3: Configure the IP Addresses to the Routers for different Networks

- ? For routers add serial ports if required.
- ? Assign the IP's in serial ports and fast ethernet port for all the routers.

Router0

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

INTERFACE

FastEthernet0/0

FastEthernet1/0

Serial2/0

Serial3/0

FastEthernet4/0

FastEthernet5/0

FastEthernet0/0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0006.2A58.89CC

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

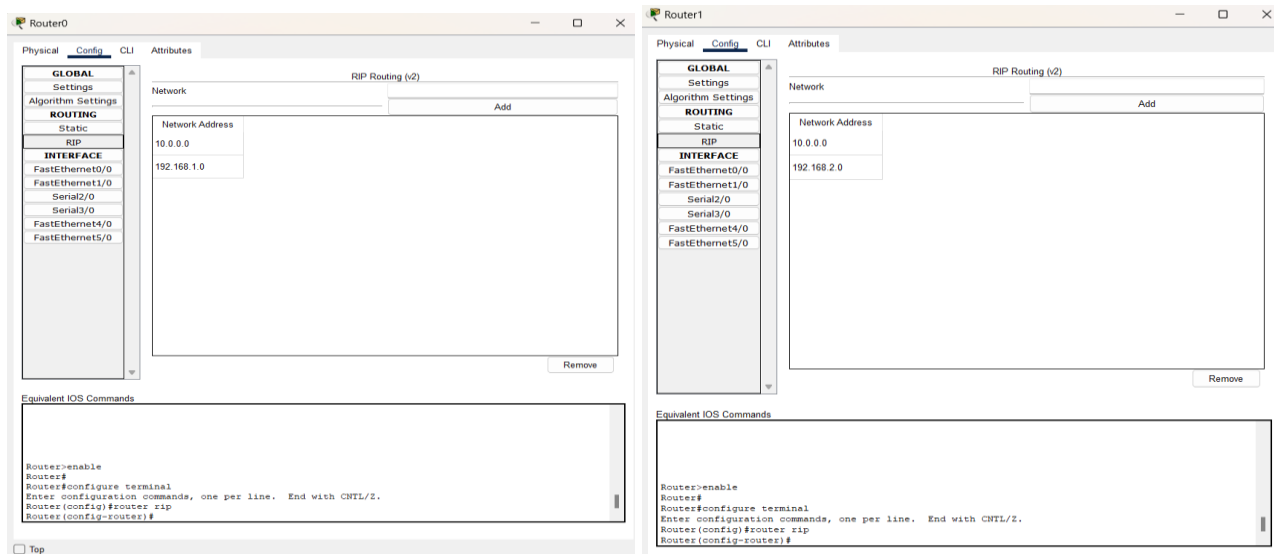
```
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

☐ Top

#### Step 4: Configure the Network Addresses to Router for Dynamic Routing

- Set the RIP routes to each router to connect networks from where the message will be sent or received.



#### Step 5: Verifying Packet delivery as well as connections

- ❓ Open the command prompt on each device by clicking on the device icon and use the ping command to test the connection as well as packet delivery. For device 1 type: ping(IP address of device 2). Repeat for another device.

