Experiment No: 4	
Name	Vaibhav Sharma
PRN	22070126125
Date of Performance	28/08/2024
Title	3 router connection and wireless connection
Theory (short)	**1. Triangular Topology (Full Mesh Network)** • **Configuration**: Each of the three routers is connected directly to the other two routers. This forms a triangle, where each side of the triangle represents a direct connection between two routers. • **Data Transmission**: In a full mesh topology, data can be sent from one router to another through multiple paths. For example, data from Router A to Router B can be sent directly or via Router C. • **Fault Tolerance**: This topology is highly fault-tolerant. If one link fails, data can still be routed through the remaining connections. For instance, if the link between Router A and Router B fails, data can still reach Router B through Router C. • **Latency and Speed**: Because there are multiple paths for data, the network can choose the shortest or least congested path, potentially reducing latency and increasing speed. • **Complexity**: While this topology provides robust fault tolerance, it increases the complexity of routing, as each router must maintain a routing table that includes multiple paths to each destination. **2. Linear Topology (Chain)** • **Configuration**: Router A is connected to Router B, and Router B is connected to Router C, but there is no direct connection between Router A and Router C. This forms a linear chain of routers. • **Data Transmission**: In this topology, data transmission between non-adjacent routers must pass through the intermediate router. For example, data from Router A to Router C must pass through Router B. • **Fault Tolerance**: This topology is less fault-tolerant. If the central router (Router B) fails, communication between Router A and Router C is completely cut off. • **Latency and Speed**: Latency is higher when data has to pass through intermediate routers. Additionally, the central router

may become a bottleneck if it handles a large amount of traffic.

- **Complexity**: The routing complexity is lower compared to the triangular topology, as each router only needs to maintain knowledge of its immediate neighbors.

3. Star Topology

- **Configuration**: One router serves as a central hub (e.g., Router B), with the other two routers (Router A and Router C) connected only to this central hub. There is no direct connection between Router A and Router C.
- **Data Transmission**: All data between the outer routers (A and C) must pass through the central router (B). If Router A wants to communicate with Router C, the data is sent to Router B, which then forwards it to Router C.
- **Fault Tolerance**: The central router becomes a single point of failure. If Router B fails, Router A and Router C cannot communicate with each other, nor can they connect to any external network. However, if either Router A or Router C fails, the rest of the network remains operational.
- **Latency and Speed**: The central router can become a bottleneck, potentially increasing latency if it is overwhelmed with traffic. However, the straightforward nature of this topology often leads to simpler routing and faster decision-making.
- **Complexity**: The star topology is the simplest in terms of routing. Each router only needs to know how to reach the central hub.

Implications and Use Cases

1. **Triangular Topology (Full Mesh)**:
    - **Best Use Case**: Mission-critical networks where redundancy and fault tolerance are paramount.
    - **Drawback**: Higher cost and complexity due to the need for more connections and sophisticated routing protocols.
2. **Linear Topology (Chain)**:
    - **Best Use Case**: Simple, small-scale networks where routers are connected in a line, and cost or simplicity is more important than fault tolerance.
    - **Drawback**: Susceptible to single points of failure and may suffer from higher latency.
3. **Star Topology**: ○ **Best Use Case**: Networks where simplicity and central management are key, such as in small office or home networks.

	○ **Drawback**: Vulnerable to failure if the central router fails, and potential bottlenecks in the central router. The routers must support compatible wireless communication protocols to maintain stable connections: • **Wi-Fi Standards (e.g., 802.11ac, 802.11ax)**: The performance of the network depends on the Wi-Fi standards supported by the routers. Newer standards like 802.11ax (Wi-Fi 6) offer better efficiency, lower latency, and improved throughput in environments with multiple devices. • **Routing Protocols**: Dynamic routing protocols (e.g., OSPF, BGP) can be used to manage the routes between the routers. In a mesh network, these protocols can dynamically adjust the routing paths based on the network's current state, ensuring optimal data flow. Static routing is simpler but less flexible, making it less ideal for dynamic environments. • **Security Protocols**: Encryption (e.g., WPA3) is crucial to securing the wireless connections between the routers. Without proper security measures, the network is vulnerable to unauthorized access and potential attacks.

Procedure	**1. Setup the Routers** 1. **Open Cisco Packet Tracer**: Launch the Cisco Packet Tracer application. 2. **Add Routers**: o From the bottom left-hand panel, select **Network Devices** > **Routers**. o Drag three routers onto the workspace (e.g., Router0, Router1, and Router2). 3. **Connect the Routers**: o Select the **Connections** option (represented by a lightning bolt). o Choose the **copper straight-through cable** if connecting routers via FastEthernet or GigabitEthernet ports, or **serial DCE** cable for serial connections. o Click on Router0, select an appropriate port (e.g., GigabitEthernet0/0 or Serial0/0/0), then click on Router1 to connect it to an equivalent port. o Repeat the process to connect Router1 to Router2 and Router2 back to Router0 (for a triangular connection). 4. **Assign IP Addresses**: o Click on each router, and navigate to the **CLI (Command Line Interface)** tab. o Assign IP addresses to the interfaces: ▯ For instance you can take 192.168.1.1 for gateway and for the end devices you proceed with the gateway ipv4 address i.e. 192.168.1.2 and so on **2. Setup Wireless Network** 1. **Add Wireless Devices**: o Go to the **End Devices** tab and drag a **Wireless Router** (e.g., HomeRouter0) onto the workspace. o Drag a **Laptop** or **PC** with a wireless capability onto the workspace.

2. **Configure the Wireless Router**: ○ Click on the wireless router, go to the **GUI** tab, and configure the following:
    - **SSID**: Set the SSID to something like MyNetwork.
    - **Security**: Set the security to WPA2-PSK and configure a password.
    - **IP Configuration**: Configure the IP address, subnet mask, and DHCP settings.
3. **Connect the Laptop to the Wireless Network**: ○ Click on the Laptop, go to the **Desktop** tab, and select the **PC Wireless** option.
    - ○ Scan for available networks, select MyNetwork, and enter the password to connect.
4. **Test Connectivity**:
    - ○ From the command prompt of any connected device (e.g., the laptop), ping other devices on the network to ensure connectivity.

3. Final Testing 1. **Ping Test**: ○ From one router, try pinging the IP addresses of interfaces on other routers to ensure the connections are properly set up.

- ○ From the laptop, try pinging the IP addresses of the routers or other devices to test connectivity over the wireless network.

2. **Verify Routing**: ○ On each router, use the command show ip route to verify that the correct routes have been installed.

Output Screenshots

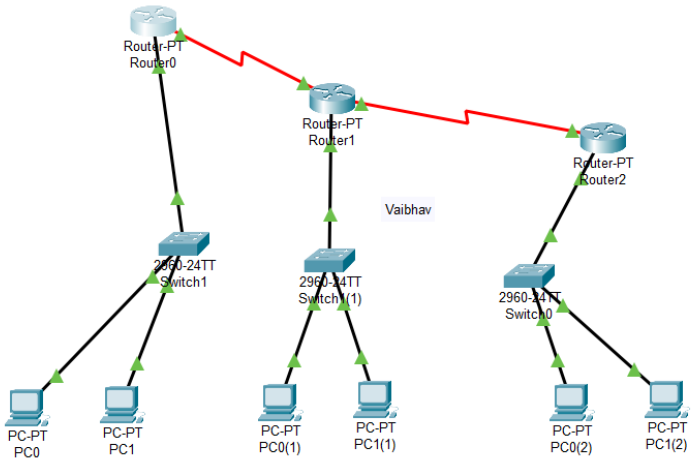

Figure 1: 3 router connection

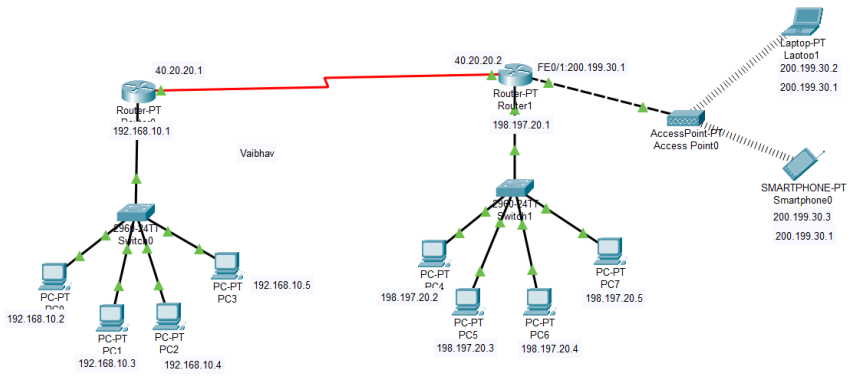

Figure 2- Wireless connection

Observation	**1. Connectivity Status** • **Link Lights**: Each connection between devices will show link lights (green, amber, or red) indicating the status of the physical connection. • **Interface Status**: You can check whether interfaces are up or down by hovering over the connection or viewing interface details in the router's configuration. • **Connectivity Test**: By using tools like ping or traceroute, you can observe if devices are reachable and if the network paths are correctly established. **2. Routing Information** • **Routing Tables**: Each router maintains a routing table that can be viewed using the show ip route command. This table shows the known routes, their next hops, and the interfaces through which the data should be sent. • **Routing Protocol Behavior**: If dynamic routing protocols (e.g., OSPF, EIGRP, RIP) are configured, you can observe how routes are learned and advertised between routers. • **Route Propagation**: By simulating link failures or adding new routes, you can observe how quickly routing updates propagate and how the network converges. **3. Traffic Flow and Latency** • **Packet Tracer Simulation**: You can simulate data traffic between devices and observe how packets move through the network. This includes seeing the path taken by the packet, the protocols involved, and how each router processes the packet. • **Latency and Delay**: Although Packet Tracer doesn't simulate real-world latency perfectly, you can observe the logical delay and processing time within the network, especially in larger topologies. **4. Network Layer Operations** • **ARP Table**: You can observe how Address Resolution Protocol (ARP) tables are populated as devices

communicate. ARP tables map IP addresses to MAC addresses, which is crucial for network communication.

- **DNS Resolution**: If you have a DNS server in your network, you can observe how domain names are resolved into IP addresses and how devices interact with the DNS server.

5. Security Mechanisms

- **Access Control Lists (ACLs)**: You can implement ACLs on routers to filter traffic and observe how they affect network traffic flow, blocking or allowing specific types of traffic based on rules.
- **Wireless Security**: On wireless connections, you can observe the effects of different security protocols (WEP, WPA2) on device connectivity and access to the network.

6. Network Address Translation (NAT)

- **NAT Operations**: If NAT is configured, you can observe how private IP addresses are translated to public IP addresses when data is sent to external networks, and vice versa.

7. DHCP Operations

- **IP Assignment**: If a DHCP server is configured, you can observe how devices obtain IP addresses automatically, and view the DHCP leases and settings.
- **Scope and Pool**: You can monitor the DHCP scope (range of IPs) and the allocation of these IPs to different devices in the network.

8. Device Configuration and Management

- **Device Configuration**: By observing how routers, switches, and other devices are configured, you can see the impact of different configurations (e.g., static vs. dynamic routing, security settings) on network behavior.
- **CLI Commands**: Using the CLI on routers and switches, you can run various commands to monitor and troubleshoot the network, such as show ip interface brief, show running-config, etc.

	9. Wireless Network Behaviour • **Signal Coverage**: You can observe the range and signal strength of wireless connections, helping to understand the placement of wireless routers and access points. • **Client Connectivity**: The behaviour of wireless clients (e.g., laptops) connecting and disconnecting from the network, including how they roam between access points if multiple is present. **10. Troubleshooting and Debugging** • **Error Messages**: You can observe error messages during the simulation, such as incorrect configurations, IP conflicts, or downed interfaces, which helps in diagnosing and fixing network issues. • **Protocol Debugging**: Using debugging commands (e.g., debug ip rip, debug ip ospf), you can observe detailed protocol operations and troubleshoot issues with routing, traffic flow, or network performance.
Self-assessment Q&A	NA
Conclusion	This setup should give us a basic network with three interconnected routers and a wireless connection for end devices. We can further customize the setup by adding more devices, implementing security measures, or configuring advanced routing protocols based on your needs. Observing these aspects in Cisco Packet Tracer helps in understanding the logical operation of networks, practicing configuration and troubleshooting, and learning how different network protocols and devices interact.