PRESTON UNIVERSITY

Serving the Nation Since 1984

NAME: QAZI SUBHAN

REG NO: 2121-

BSCS 3RD

PRESTON UNIVERSITY KOHAT
DEPARTMENT OF BSCS

Q1: Unicast Protocols

- Define **unicast communication** and explain how it works in networking.
- List and describe at least **three unicast protocols**.
- Explain the **advantages and disadvantages** of unicast communication.
- Provide real-world examples of unicast protocol usage.

Unicast Communication:

Unicast communication is a type of communication in which a single device (source) sends data to a single device (destination) on a network. In other words, a unicast transmission is a one-to-one communication between two devices. The source device sends a packet of data to the destination device, and the packet is addressed to a specific IP address, which is unique to the destination device.

How Unicast Works:

Here's a step-by-step explanation of how unicast communication works in networking:

1. Source Device: The source device, which is typically a computer or a server, wants to send data to a destination device.

2. IP Addressing: The source device uses the IP address of the destination device to address the packet of data. The IP address is a unique identifier that is assigned to each device on a network.

3. Packet Creation: The source device creates a packet of data, which includes the IP address of the destination device, the source device's IP address, and the data to be transmitted.

4. Routing: The packet is sent to a router, which examines the destination IP address and determines the best path to the destination device.

5. Forwarding: The router forwards the packet to the next hop on the path to the destination device.

6. Delivery: The packet is delivered to the destination device, which receives the data and sends an acknowledgement (ACK) packet back to the source device.

7. ACK Packet: The ACK packet is sent back to the source device, which confirms that the data was received successfully.

Unicast Communication Protocols:

Some common protocols that use unicast communication include:

1. TCP (Transmission Control Protocol): A connection-oriented protocol that ensures reliable data transfer between devices.

2. UDP (User Datagram Protocol): A connectionless protocol that provides best-effort delivery of data between devices.

3. HTTP (Hypertext Transfer Protocol): A protocol used for transferring data over the web, which uses unicast communication to send data between a client and a server.

Advantages of Unicast Communication:

1. Reliability: Unicast communication provides reliable data transfer, as the source device can ensure that the data is delivered to the destination device.

2. Security: Unicast communication provides a secure way to transfer data, as the data is addressed to a specific device and can be encrypted.

3. Efficient Use of Resources: Unicast communication makes efficient use of network resources, as only the destination device receives the data.

Disadvantages of Unicast Communication:

1. Scalability: Unicast communication can be less scalable than other types of communication, such as multicast or broadcast, as each device must send a separate packet to each destination device.

2. Network Congestion: Unicast communication can contribute to network congestion, as each packet must be routed through the network, which can lead to increased latency and packet loss.

REAL WORLD EXAMPLES:

1. Web Browsing: When you enter a URL in your web browser, your computer sends a unicast request to the web server hosting the website. The web server then sends the requested webpage back to your computer using unicast communication.

2. Email: When you send an email to someone, your email client uses unicast communication to send the email to the recipient's email server. The email server then forwards the email to the recipient's email client using unicast communication.

3. File Transfer: When you upload or download a file from a server, your computer uses unicast communication to send or receive the file. For example, when you upload a file to Google Drive, your computer sends the file to Google's servers using unicast communication.

Q2: Multicast Protocols

- Define **multicast communication** and how it differs from unicast.
- List and describe at least **three multicast protocols** (e.g., **IGMP, PIM, RTP**).
- Explain how **multicast routing** works and its benefits.

Provide real-world examples where multicast protocols are used (e.g., **video streaming, IPTV**).

Multicast Communication:

Multicast communication is a type of communication in which a single device (source) sends data to multiple devices (destinations) on a network. In other words, a multicast transmission is a one-to-many communication between a single source device and multiple destination devices. The source device sends a packet of data to a multicast address, which is a special address that is shared by multiple devices on the network.

How Multicast Differs from Unicast:

Multicast communication differs from unicast communication in the following ways:

1. Number of Destinations: Unicast communication is one-to-one, while multicast communication is one-to-many.

2. Addressing: Unicast communication uses a unique IP address for each destination device, while multicast communication uses a shared multicast address.

3. Packet Duplication: Unicast communication requires the source device to send a separate packet to each destination device, while multicast communication sends a single packet to multiple devices.

4. Network Efficiency: Multicast communication is more network-efficient than unicast communication, as it reduces the amount of traffic on the network.

5. Scalability: Multicast communication is more scalable than unicast communication, as it can support a large number of devices on the network.

Multicast Protocols:

Here are three multicast protocols:

1. IGMP (Internet Group Management Protocol): IGMP is a protocol used by devices to join or leave a multicast group. It allows devices to register their interest in receiving multicast traffic for a specific group.

2. PIM (Protocol Independent Multicast): PIM is a protocol used for multicast routing. It allows routers to forward multicast traffic to devices that have registered their interest in receiving it.

3. RTP (Real-time Transport Protocol): RTP is a protocol used for real-time data transmission, such as video and audio streaming. It provides timestamping and sequence numbering to ensure that data is delivered in the correct order.

Multicast Routing:

Multicast routing is the process of forwarding multicast traffic from a source device to multiple destination devices on a network. Here's how it works:

1. Source Device: The source device sends a multicast packet to a multicast address.

2. Router: The packet is received by a router, which examines the multicast address and determines which devices on the network are members of the multicast group.

3. Forwarding: The router forwards the packet to the devices that are members of the multicast group.

4. Delivery: The packet is delivered to each device that is a member of the multicast group.

Benefits of Multicast Routing:

Multicast routing has several benefits, including:

1. Network Efficiency: Multicast routing reduces the amount of traffic on the network, making it more efficient.

2. Scalability: Multicast routing can support a large number of devices on the network, making it more scalable.

3. Reduced Latency: Multicast routing can reduce latency, as packets are sent to multiple devices simultaneously.

Real-World Examples:

Multicast protocols are used in a variety of real-world applications, including:

1. Video Streaming: Multicast protocols are used in video streaming applications, such as online video conferencing and live video broadcasts.

2. IPTV (Internet Protocol Television): Multicast protocols are used in IPTV applications, such as live TV broadcasts and video-on-demand services.

3. Online Gaming: Multicast protocols are used in online gaming applications, such as multiplayer games and virtual reality experiences.

4. Distance Learning: Multicast protocols are used in distance learning applications, such as online lectures and virtual classrooms.

Question : 03

To complete the Packet Tracer task of configuring RIP or OSPF with loopback addresses, follow the detailed steps below:

Step 1: Network Setup:

1. Open Cisco Packet Tracer and create a network topology with:

   - Three routers (e.g., Router0, Router1, Router2).
   - Two PCs (e.g., PC0 and PC1) connected to different routers.
   - Use Serial connections (DCE/DTE) to link the routers.
   - Use Ethernet connections to connect the PCs to the routers.

Step 2: Assign IP Addresses:

1. Configure IP addresses for router interfaces:

- Use a **/30 subnet mask** for WAN links (serial connections).
  - Example:
    - Router0 Serial0/0/0: `192.168.1.1/30`
    - Router1 Serial0/0/0: `192.168.1.2/30`
    - Router1 Serial0/0/1: `192.168.2.1/30`
    - Router2 Serial0/0/1: `192.168.2.2/30`
- Use a **/24 subnet mask** for Ethernet connections.
  - Example:
    - Router0 GigabitEthernet0/0: `192.168.10.1/24` (connected to PC0)
    - Router2 GigabitEthernet0/0: `192.168.20.1/24` (connected to PC1)

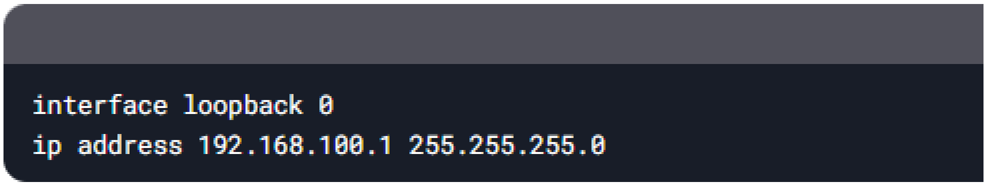
2. Assign IP addresses to PCs:

- PC0: `192.168.10.10/24` (Gateway: `192.168.10.1`)
- PC1: `192.168.20.10/24` (Gateway: `192.168.20.1`)

Step 3: Configure Loopback Addresses:

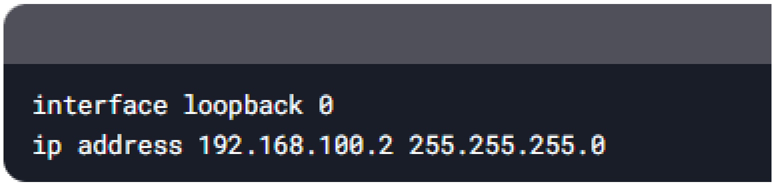
1. Assign a loopback address on each router:

Router0:



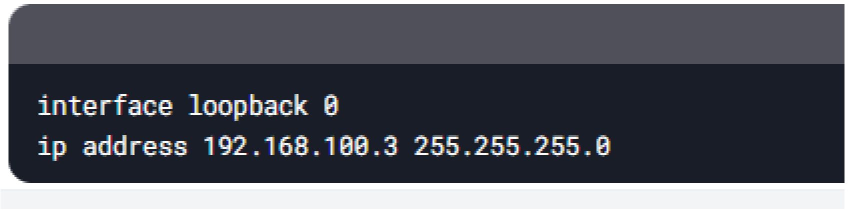
```
interface loopback 0
ip address 192.168.100.1 255.255.255.0
```

Router1:



```
interface loopback 0
ip address 192.168.100.2 255.255.255.0
```

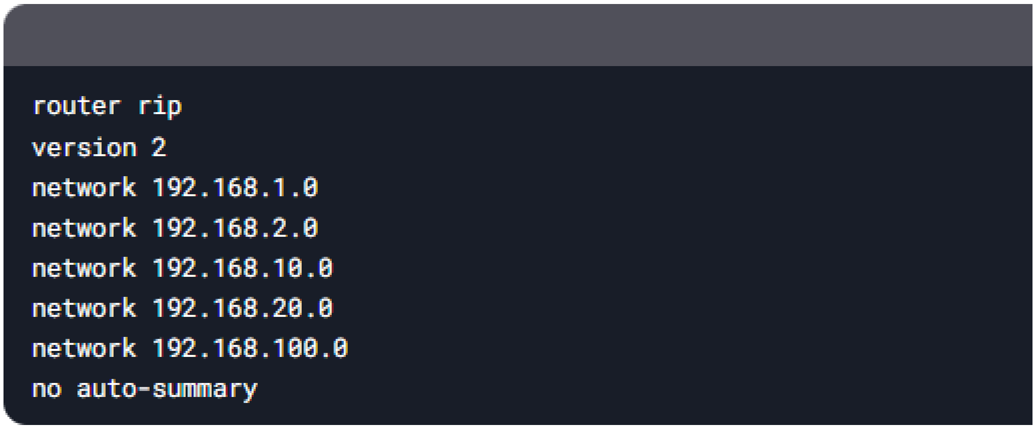
Router2:



```
interface loopback 0
ip address 192.168.100.3 255.255.255.0
```

Step 4: Enable Routing Protocol (RIP or OSPF):

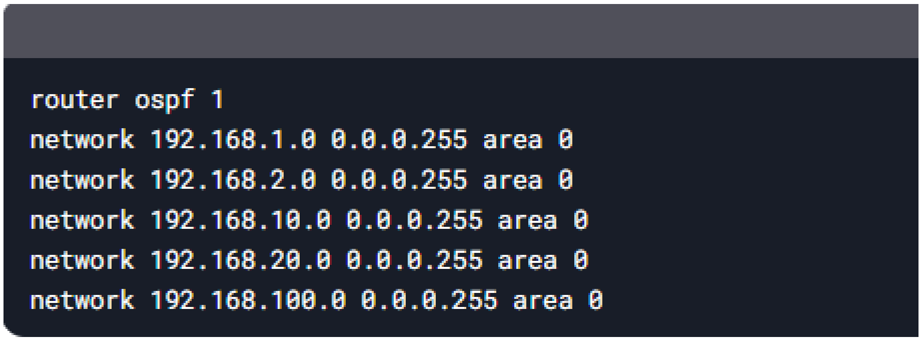
Option 1: Configure RIP v2



```
router rip
version 2
network 192.168.1.0
network 192.168.2.0
network 192.168.10.0
network 192.168.20.0
network 192.168.100.0
no auto-summary
```

Option 2: Configure OSPF:

1. On each router, enable OSPF:



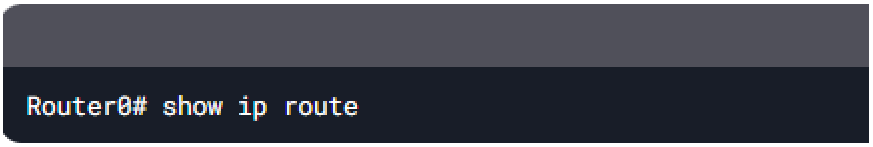
```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
```

Step 5: Verify Connectivity:

1. Check the routing table:

- Use the `show ip route` command on each router to verify that the routes are learned via RIP or OSPF.

  - Example:



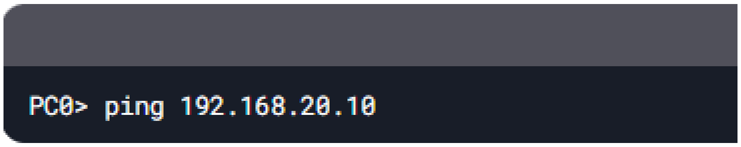
```
Router0# show ip route
```

Look for routes marked with `R` (RIP) or `O` (OSPF).

2. Test connectivity:

- Use the `ping` command from PC0 to PC1 to ensure end-to-end connectivity.

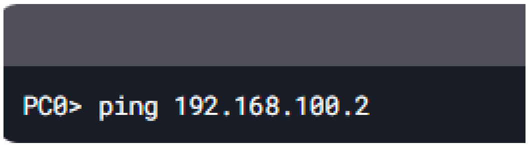
  - Example:



```
PC0> ping 192.168.20.10
```

- Ping the loopback addresses from the PCs or routers to verify connectivity.

  - Example:



```
PC0> ping 192.168.100.2
```

Expected Output:

- The routing tables on all routers should show routes to all connected networks and loopback addresses.

- PCs should be able to ping each other and the loopback addresses.

By following these steps, you will successfully configure RIP or OSPF with loopback addresses in Packet Tracer and understand how routers manage multiple networks.