ACTIVE CLASS WEEK 7

ACTIVITY 1:

Activity 1: Routing - Group Activity

\*\*1. Network Setup:\*\*

- \*\*Configuration:\*\*

- \*\*Router0\*\* is connected to \*\*Switch1\*\* and \*\*PC1\*\* on LAN \*\*10.1.1.0/24\*\*.

- \*\*Router1\*\* is connected to \*\*Switch2\*\* and \*\*PC3\*\* on LAN \*\*198.168.10.0/24\*\*.

- \*\*Router0\*\* and \*\*Router1\*\* are directly connected to each other.

- \*\*Roles and Responsibilities:\*\*

- \*\*Nadia:\*\* Manages LAN \*\*10.1.1.0/24\*\* (handles PC1).

- \*\*Archit:\*\* Manages LAN \*\*198.168.10.0/24\*\* (handles PC3).

- \*\*Jasveena:\*\* Operates as the data plane for Router0.

- \*\*Pranika:\*\* Operates as the data plane for Router1.

- \*\*Gitanshi:\*\* Manages the control plane for both routers.

\*\*2. Ping Test:\*\*

- \*\*Nadia\*\* (from PC1) will send two ping requests to \*\*Archit\*\* (PC3).

\*\*3. Step-by-Step Instructions:\*\*

- \*\*Gitanshi\*\* (control plane) will ensure that Router0 and Router1 are exchanging routing information properly.

- \*\*Jasveena\*\* (Router0’s data plane) will update the routing table to recognize LAN \*\*198.168.10.0/24\*\* from Router1.

- \*\*Pranika\*\* (Router1’s data plane) will update the routing table to recognize LAN \*\*10.1.1.0/24\*\* from Router0.

- \*\*Nadia\*\* (PC1) initiates a ping to \*\*Archit\*\* (PC3). The ping packet is forwarded to \*\*Jasveena\*\* (Router0).

- \*\*Jasveena\*\* (Router0) examines the routing table and forwards the packet to \*\*Pranika\*\* (Router1).

- \*\*Pranika\*\* (Router1) checks the routing table and forwards the packet to \*\*Archit\*\* (PC3).

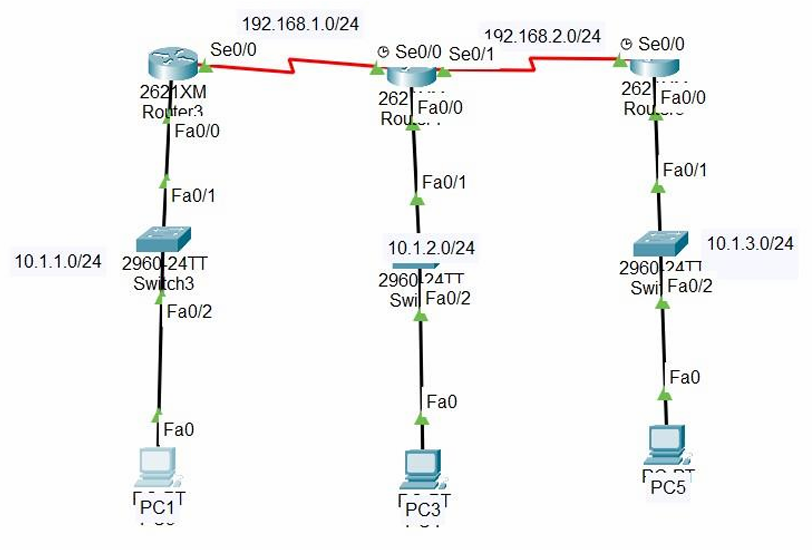
- \*\*Archit\*\* (PC3) receives the ping and sends a reply back to \*\*Nadia\*\* (PC1), following the same route in reverse.

\*\*4. Control Plane Responsibilities:\*\*

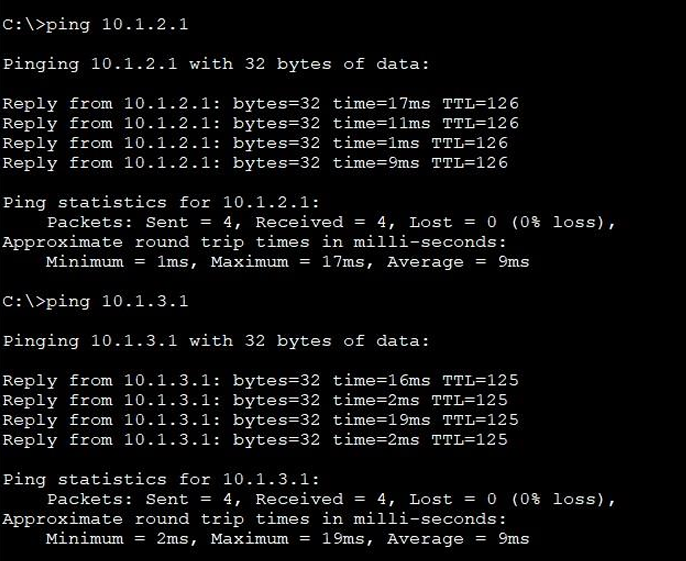
- \*\*Gitanshi\*\* (control plane) is responsible for maintaining up-to-date routing tables, exchanging routing information, and determining the optimal path for data packets. This includes ensuring that Router0 and Router1 are aware of each other’s network information.

ACTIVITY2:

1. The cisco network setup

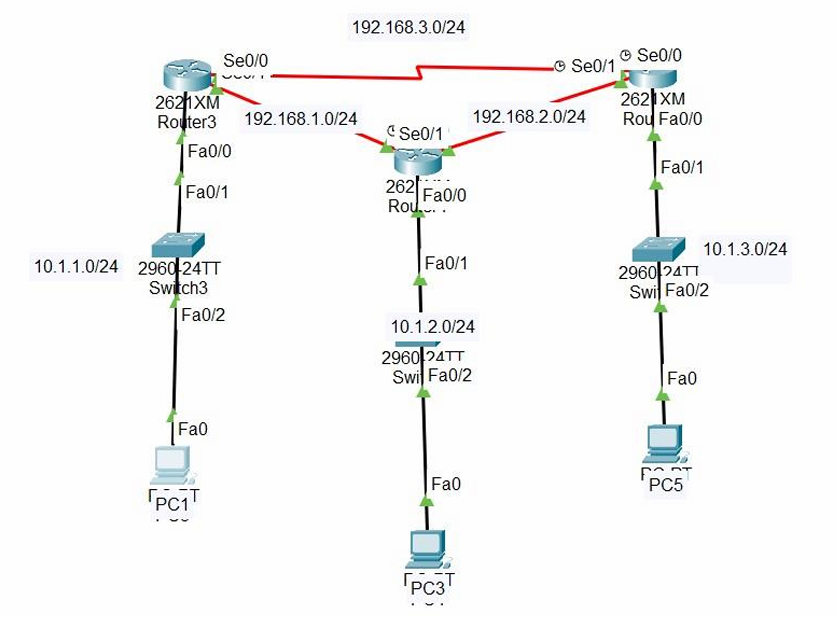


Now we need to verify that PC1 can communicate with both PC3 and PC5 using PING command and simulations.

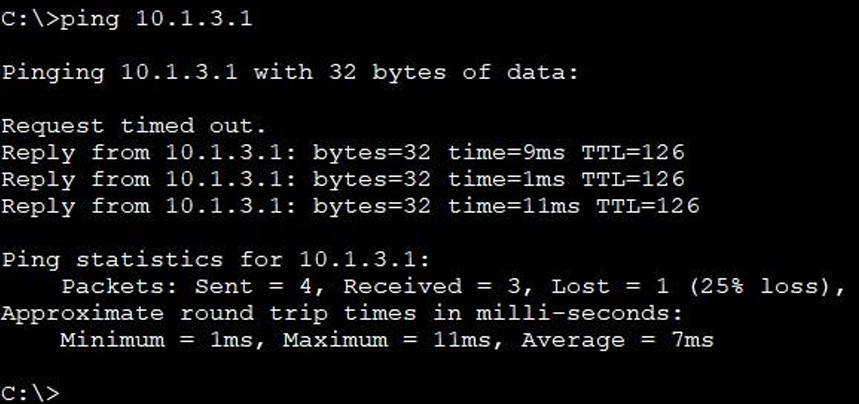


1. Discuss what changes now you need to make to enable the communication between PC1 and PC5 (Tip: what static routes you need to add).

* The modifications included adding extra WIC-1T cards to both Router 1 and Router 3 to create a direct serial connection between them. In terms of static routing, previously, the next hop for Router 1 and Router 3 pointed to the port numbers of Router 2, which connected to both routers. However, with the new setup, the port numbers for Router 1 and Router 3 are now directly linked to each other, eliminating the need for Router 2 in their communication.



Implement the changes and verify that PC1 and communicate with PC5 using PING command and simulations.



\*\*Activity 3: Alternatives to Static Routing\*\*

\*\*Question:\*\* Is there an alternative to manually configuring the routing table each time connectivity changes?

\*\*Answer:\*\* To avoid the need for manual updates to the routing table whenever there are changes in network connectivity, dynamic routing protocols can be utilized. Protocols such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and EIGRP (Enhanced Interior Gateway Routing Protocol) automatically adjust routing tables in response to network changes, streamlining network management and improving efficiency.

\*\*Question:\*\* What are the latest routing algorithms available?

\*\*Answer:\*\* Among the latest routing algorithms are:

- \*\*OSPFv3:\*\* This is an updated iteration of the OSPF protocol, designed specifically for IPv6 networks.

- \*\*BGP-4 (Border Gateway Protocol):\*\* This protocol is utilized for routing in large-scale Internet backbone networks, offering robust path selection and scalability.

- \*\*EIGRP:\*\* An enhanced version of IGRP, EIGRP provides improved convergence times and scalability, making it suitable for modern network environments.

\*\*Question:\*\* Are there routing algorithms available in Cisco Packet Tracer?

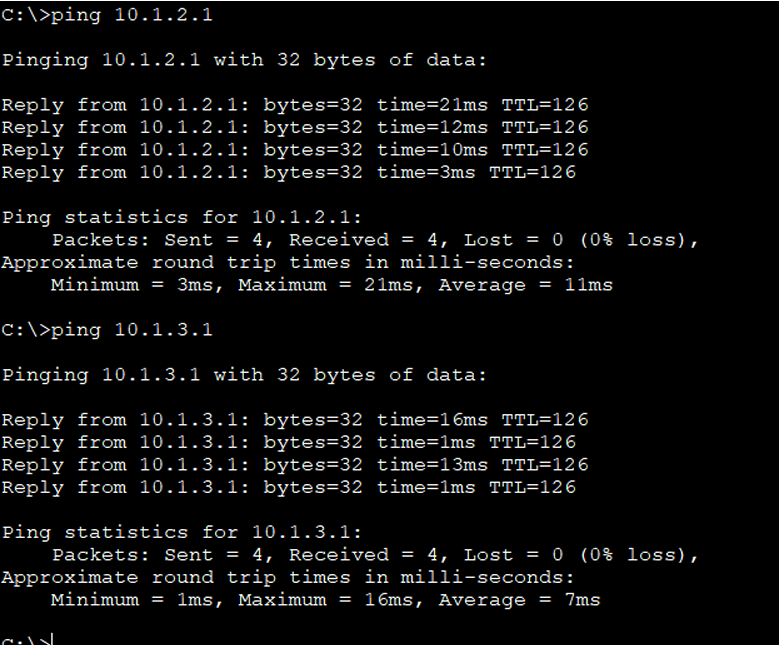
\*\*Answer:\*\* Cisco Packet Tracer supports several routing algorithms, including RIP v1/v2, OSPFv2, and EIGRP. These protocols can be configured through the graphical interface of the software by accessing the settings for each router.

Question: Use the simulation tool to send a packet from PC1 to PC5. Have you seen any differences compared to the route you have seen in Activity 2? Explain what happened.

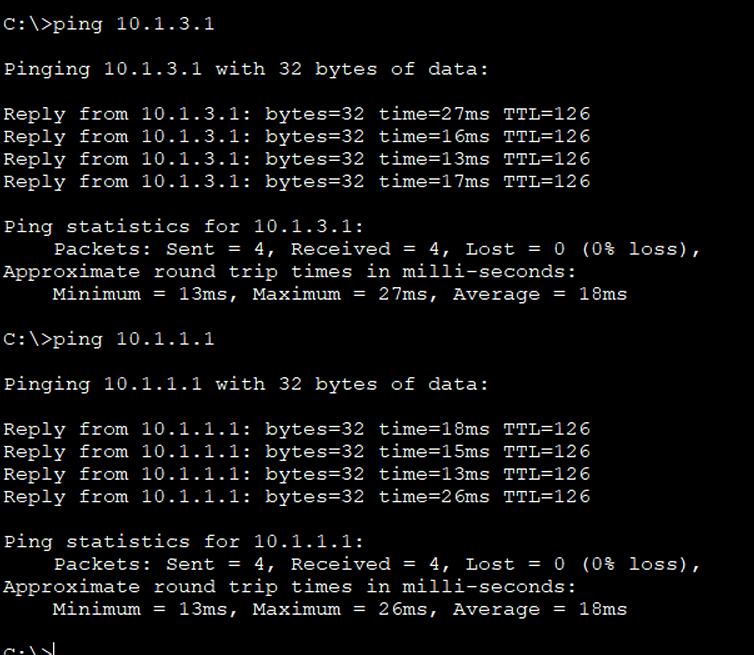
To send a packet form PC1 to PC5 the packet was sent to all the router and then from router 5 to PC5

Question: Verify the network connections using PING (in each PC).

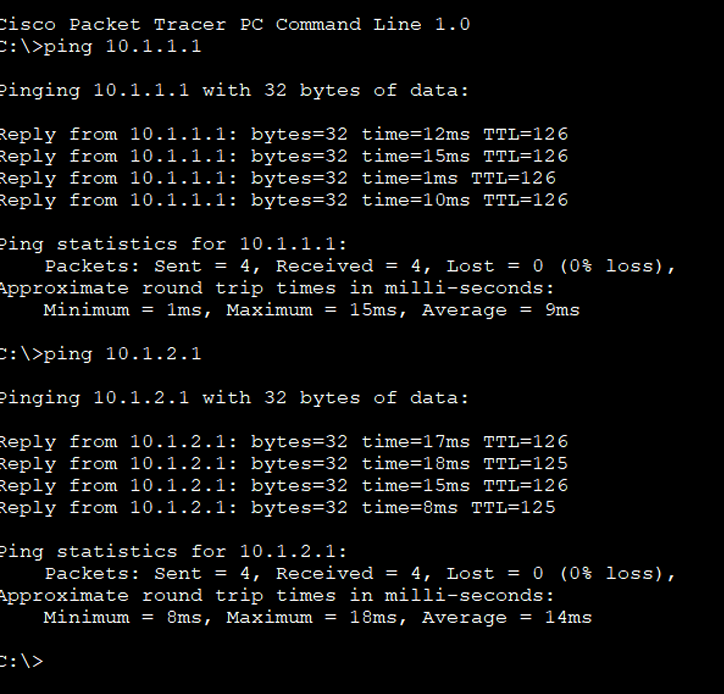
Pinging from PC1



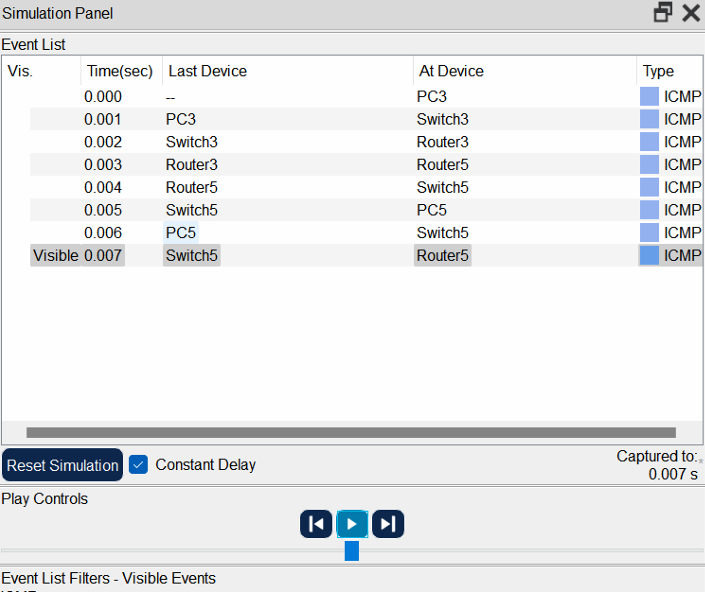
Pinging from PC3



Pinging from PC5

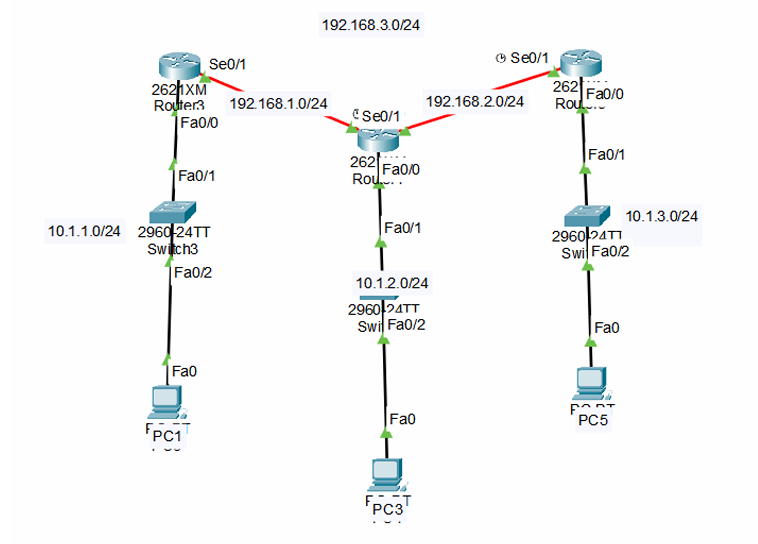


Question : Use the simulation tool to send a packet from PC1 to PC5. Have you seen any differences compared to the route you have seen in Activity 2? Explain what happened.

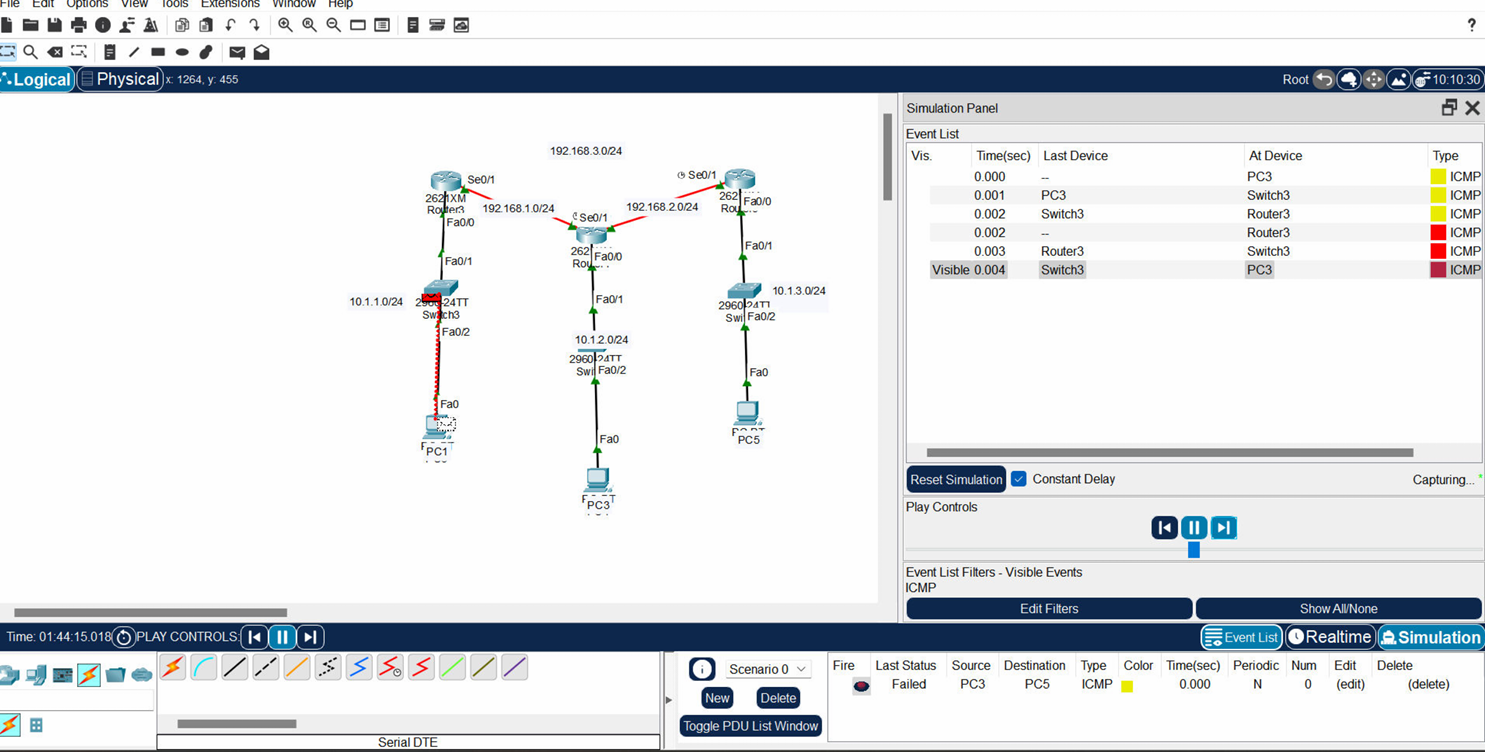


This packet chose the shortest and the easiest route which was going to router 3 and then to router 5, rather than going from router 4 to router 4.

Question : Now remove the connection between router 1 and 3 and use the simulation tool to send a packet from PC1 to PC5 without changing any configuration.



Screenshot of sending the packet :



Here , the packet transfer failed as we can see , this happened when the connection between the relevant server

Observation : we need to manually re-configure if we are using static routing in case when we physically remove a connection. If not re-configured manually, the packet transfer will fail.

ACTIVE CLASS WEEK 8

ACTIVITY 1

1.Role play:

Jasveena: Welcome everyone! Today, we need to discuss how we can manage the increasing number of IoT devices in our network. Let’s start with the first question. Do we have enough IP addresses to assign for each device that connects to the network?

Nadia: With the traditional IPv4 addressing scheme, we have approximately 4.3 billion unique IP addresses. However, with the rapid growth of IoT devices, this number is insufficient to provide a unique IP address for every device.

Pranika: That’s correct. We need to find a solution to address the shortage of IPv4 addresses.

Archit: One solution is to transition to IPv6, which provides a vastly larger address space. However, this transition is still in progress and not all devices support IPv6 yet.

Gitanshi: Another solution is to use Network Address Translation (NAT). NAT allows multiple devices on a local network to share a single public IP address, conserving the number of public IP addresses needed.

Jasveena: That’s a great point. We can also use the Dynamic Host Configuration Protocol (DHCP) to dynamically assign IP addresses to devices on the network. This helps manage IP address allocation efficiently. Archit: And don’t forget about the Internet Control Message Protocol (ICMP). ICMP is used for diagnostic and error-reporting purposes in network communication. It helps us troubleshoot and diagnose network problems.

Gitanshi: Exactly. By using these protocols together, we can effectively manage the IP address space and ensure smooth network operations.

• Discussion:

Do we have enough IP addresses to assign for each device that connect to the network?

Answer: With the traditional IPv4 addressing scheme, we have approximately 4.3 billion unique IP addresses. However, with the rapid growth of IoT devices, this number is insufficient to provide a unique IP address for every device.

Do we have any solution?

Yes, there are several solutions to address the shortage of IPv4 addresses:

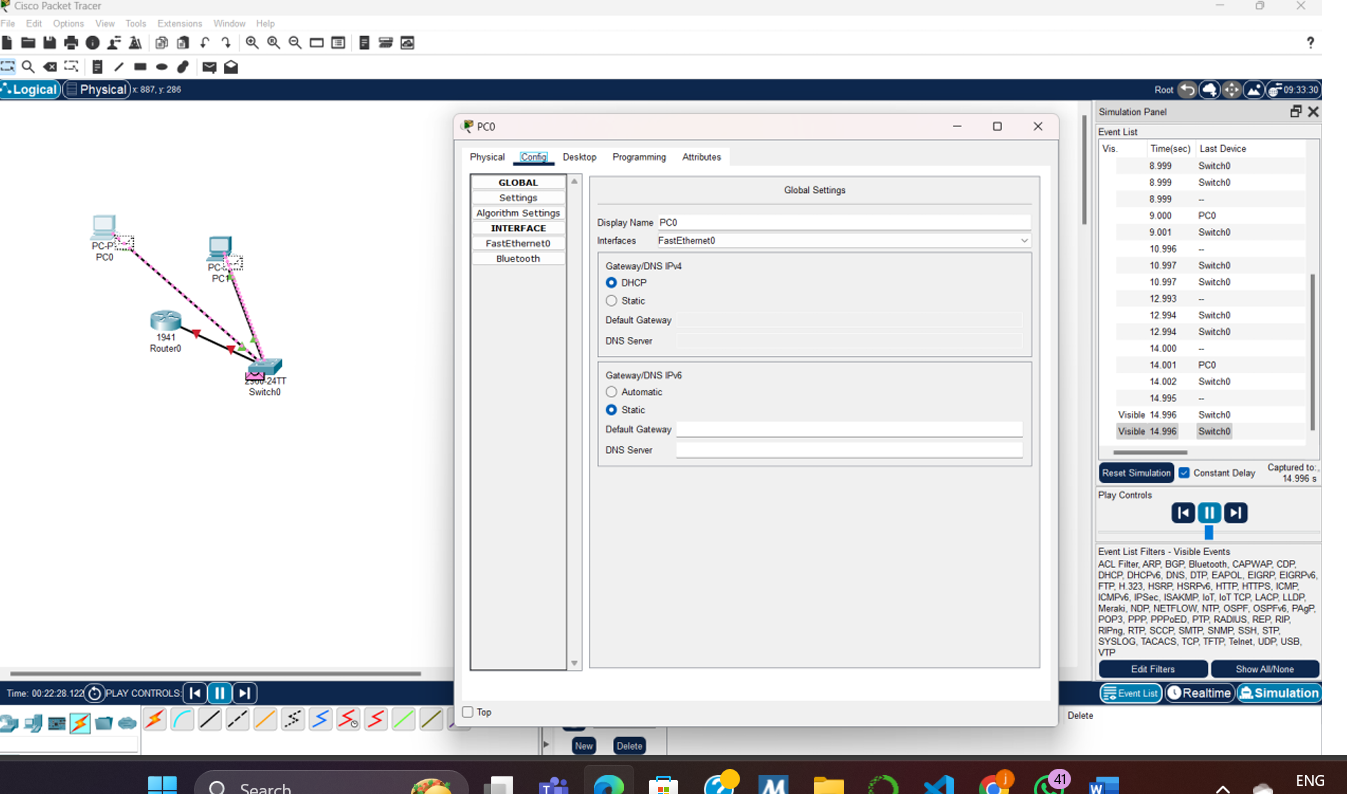
• IPv6: The most comprehensive solution is transitioning to IPv6, which provides a vastly larger address space (approximately 340 undecillion addresses).

• Network Address Translation (NAT): NAT allows multiple devices on a local network to share a single public IP address, conserving the number of public IP addresses needed.

• Dynamic Host Configuration Protocol (DHCP): DHCP dynamically assigns IP addresses to devices on a network, reusing addresses when devices are not actively connected

Explain a protocol that we can use along with IPv4 to conserve the global IP address space.

Answer: Network Address Translation (NAT): NAT is a protocol used to map multiple private IP addresses to a single public IP address (or a few public IP addresses). This allows multiple devices on a local network to access the internet using a single public IP address, effectively conserving the global IP address space. NAT is commonly used in home and office networks.

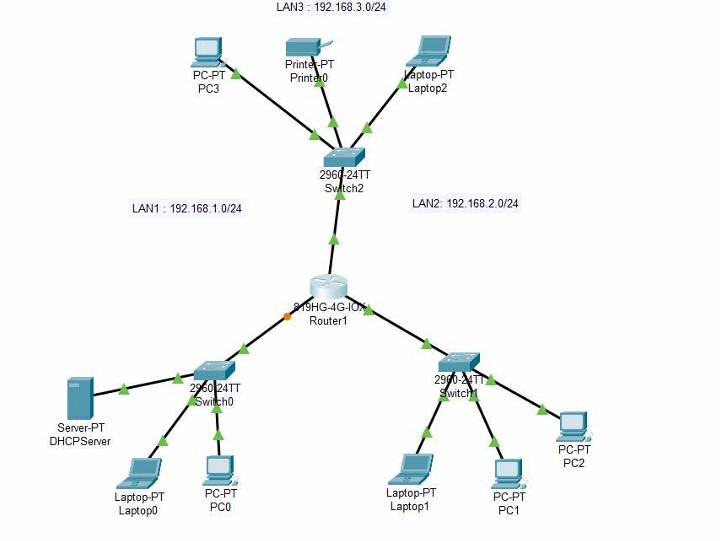


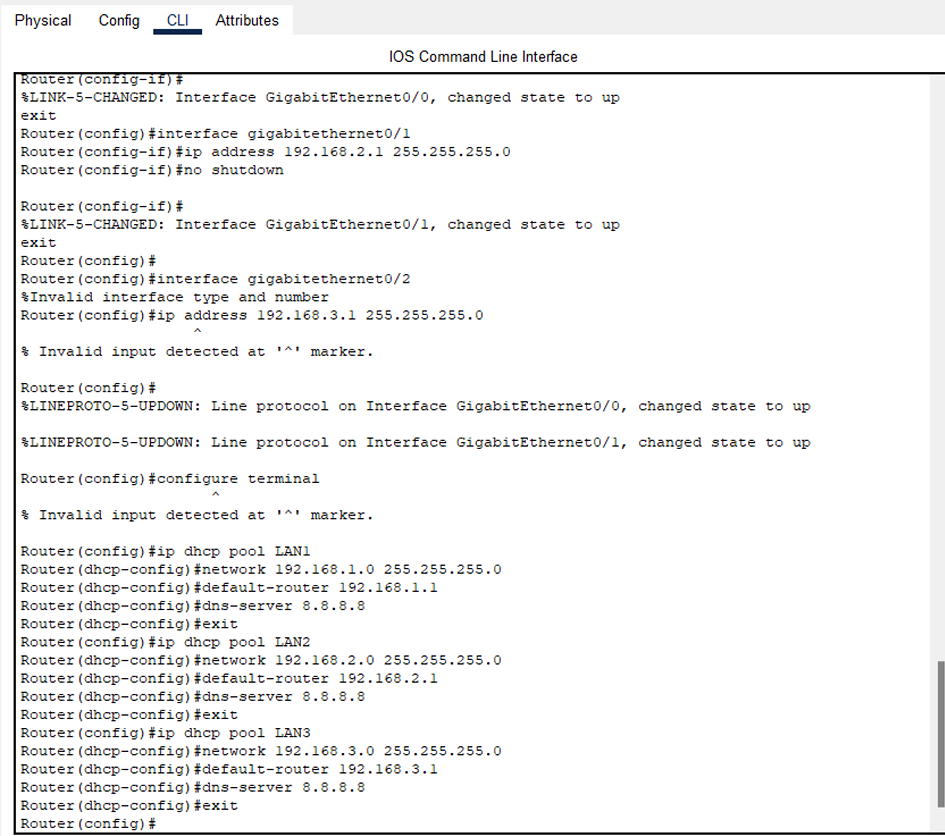
ACTIVITY 2

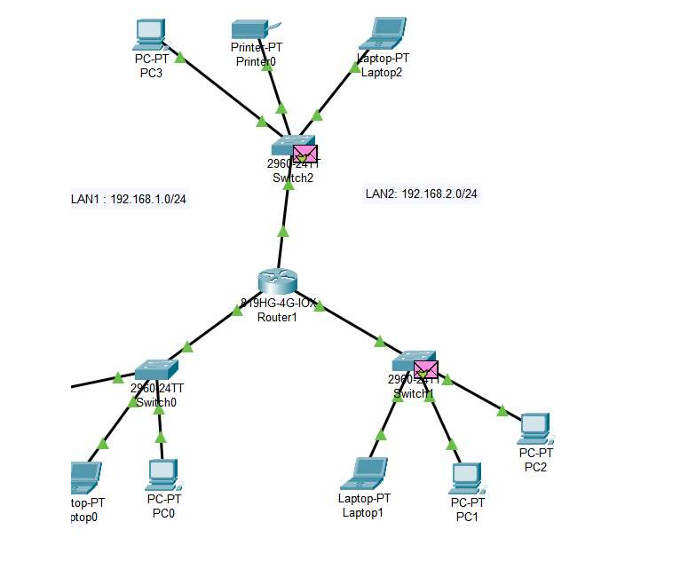
**Role Play Scenario**

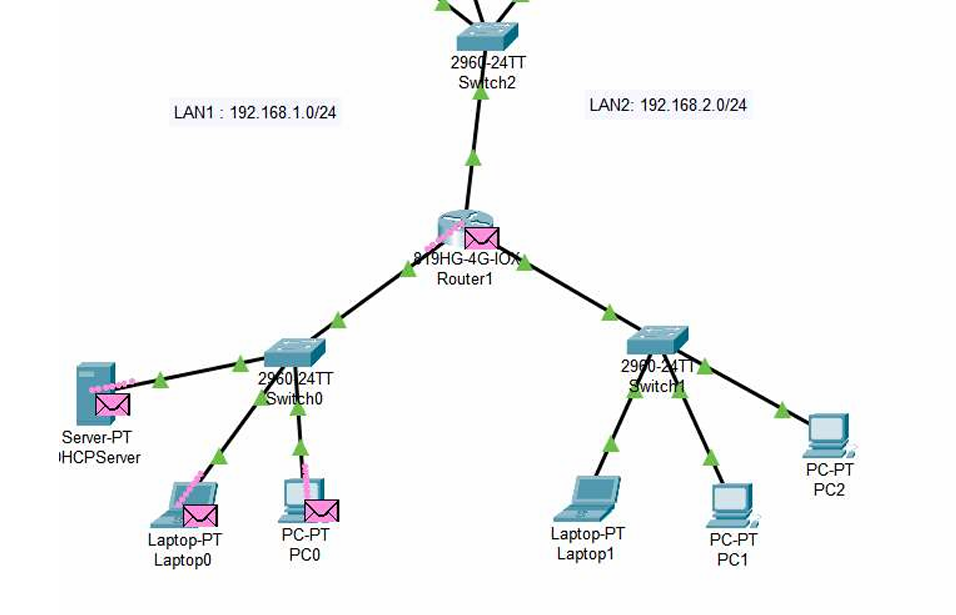
1. **Gitanshi (Router):** “Broadcasting DHCPDISCOVER to find DHCP clients.”
2. **Nadia (Switch):** “Receiving and forwarding DHCPDISCOVER to all devices on the network.”
3. **Pranika (PC):** “Receiving DHCPDISCOVER and responding with a DHCPOFFER message.”
4. **Nadia (Switch):** “Forwarding DHCPOFFER from Pranika to the DHCP server (Gitanshi).”
5. **Gitanshi (Router):** “Receiving DHCPOFFER and sending a DHCPREQUEST message.”
6. **Jasveena (Printer):** “Receiving DHCPREQUEST and responding with a DHCPACK message.”
7. **Archit (Network Storage Device):** “Receiving IP address from DHCPACK, connectivity established.”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | TIME | GITANSHI  (ROUTER) | Nadia (Switch) | Pranika (PC) | Jasveena (Printer) | Archit (Network Storage Device) |  | | T1 | Broadcasting DHCPDISCOVER | Receiving and forwarding DHCPDISCOVER |  |  |  |  | | T2 |  | Forwarding DHCPDISCOVER | Receiving and responding with DHCPOFFER |  |  |  | | T3 |  | Forwarding DHCPOFFER |  |  |  |  | | T4 | Receiving DHCPOFFER |  |  |  |  |  | | T5 | Sending DHCPREQUEST |  |  | Receiving DHCPREQUEST |  |  | | T6 |  |  |  | Responding with DHCPACK |  |  | | T7 |  |  |  |  |  | Receiving IP address, connectivity established | |



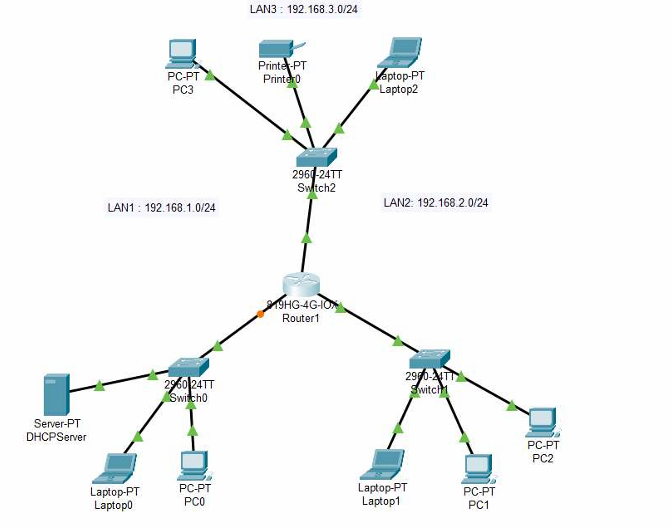


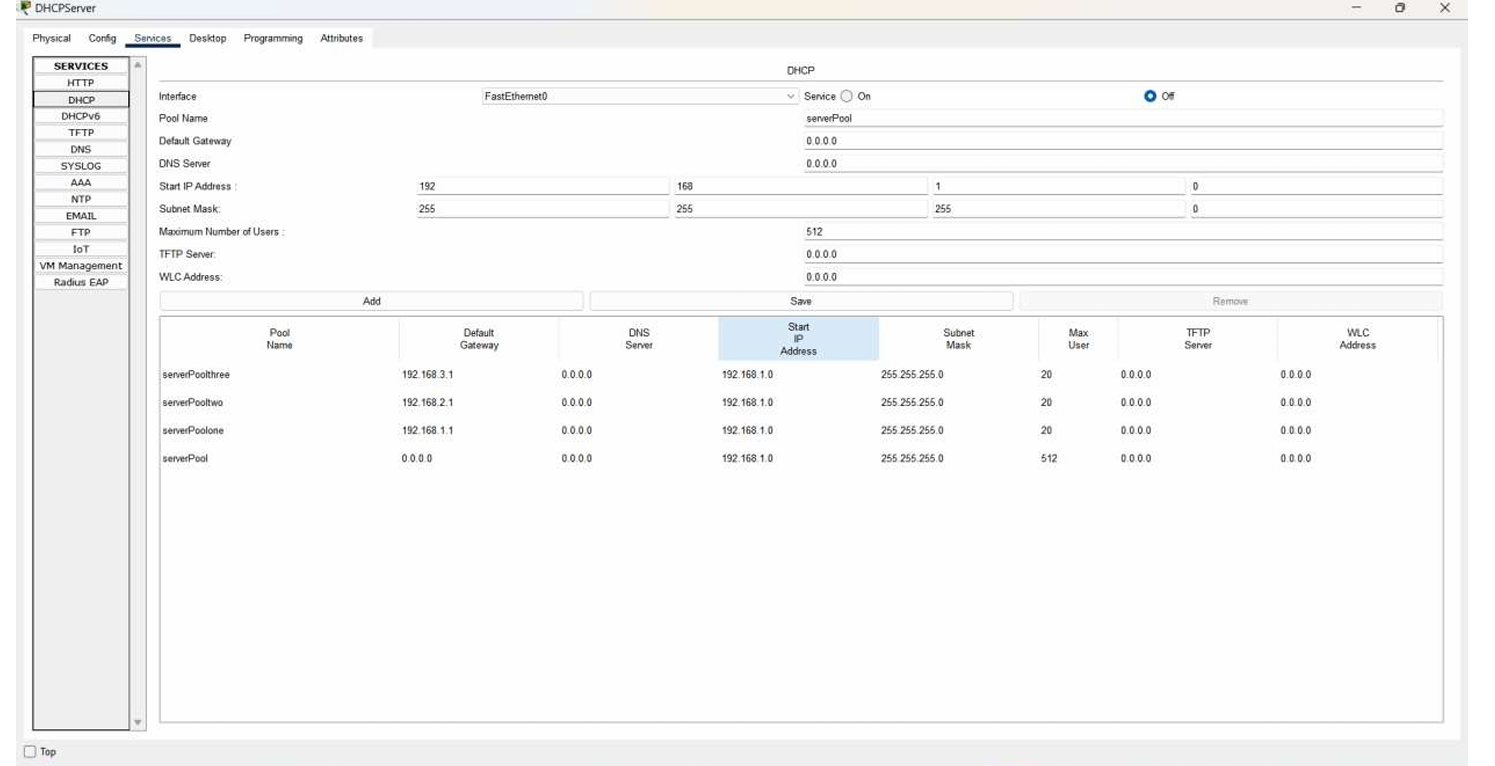


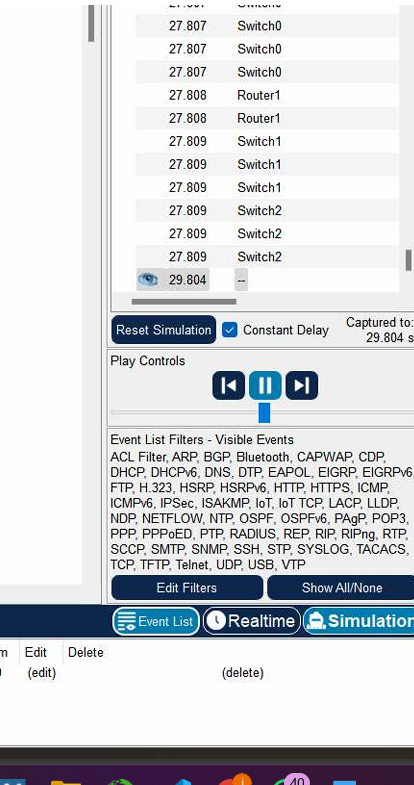


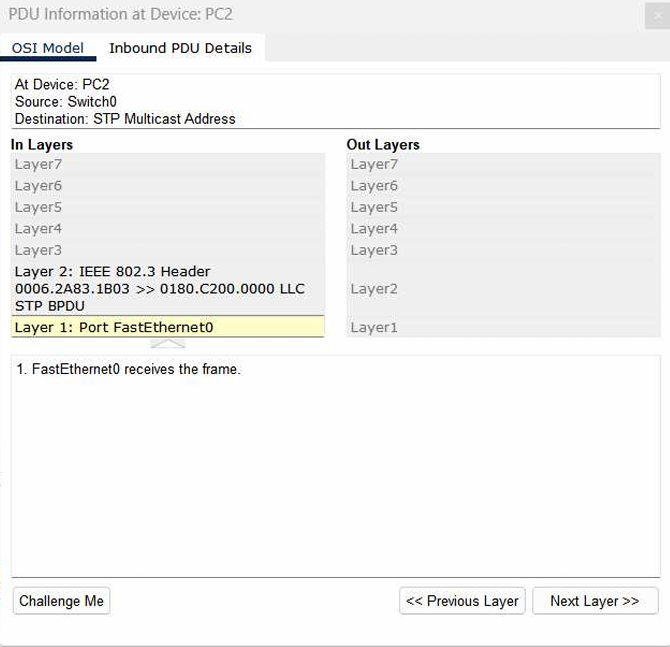
ACTIVITY 3

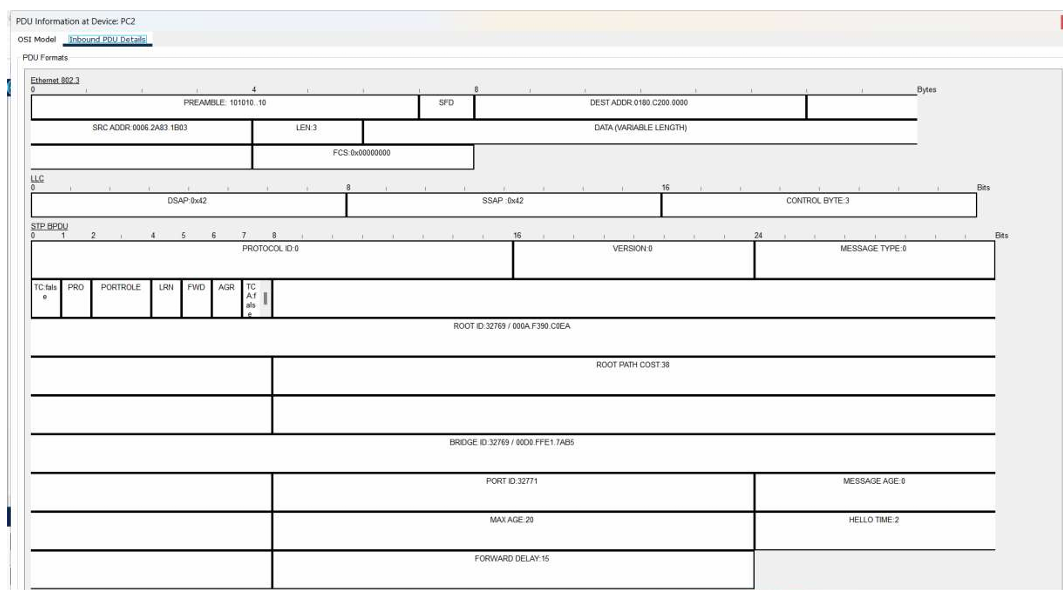
1.











QUES 5 AND 6

\*\*ICMP Message Format and Details\*\*

\*\*ICMP Message Format:\*\*

The Internet Control Message Protocol (ICMP) message format consists of the following fields:

1. \*\*Type:\*\* Indicates the type of the ICMP message (e.g., Echo Request, Echo Reply).

2. \*\*Code:\*\* Provides further information about the type (e.g., for Type 3 (Destination Unreachable), Code 0 means "Network Unreachable").

3. \*\*Checksum:\*\* Error-checking data to ensure the message has not been corrupted.

4. \*\*Identifier:\*\* Used to match requests and replies (mainly for Echo Requests and Replies).

5. \*\*Sequence Number:\*\* Used to identify multiple messages or packets of the same type.

6. \*\*Data:\*\* Contains additional information relevant to the ICMP message type, such as the payload of an Echo Request or Reply.

\*\*ICMP Message Types:\*\*

- \*\*Type 0:\*\* Echo Reply

- \*\*Type 3:\*\* Destination Unreachable

- \*\*Type 8:\*\* Echo Request

- \*\*Type 11:\*\* Time Exceeded (used by traceroute)

### \*\*Changes in ICMP Messages between Ping and Traceroute\*\*

\*\*Ping:\*\*

- \*\*Type:\*\* 8 (Echo Request) for sending, 0 (Echo Reply) for responses.

- \*\*Code:\*\* Generally 0 for both Echo Requests and Replies.

- \*\*Purpose:\*\* Used to check if a host is reachable and to measure round-trip time.

\*\*Traceroute:\*\*

- \*\*Type:\*\* 11 (Time Exceeded) for reporting hops along the path to the destination.

- \*\*Code:\*\* Typically 0 for TTL Expired in Transit.

- \*\*Purpose:\*\* Determines the path packets take to reach the destination by sending packets with incrementally increasing TTL (Time-to-Live) values and recording the ICMP Time Exceeded messages returned by intermediate routers.

\*\*Behavior in Traceroute vs. Ping\*\*

- \*\*Ping:\*\* Sends Echo Request packets to the destination and waits for Echo Reply packets. It measures the round-trip time and checks reachability.

- \*\*Traceroute:\*\* Sends packets with increasing TTL values. Each router along the path decrements the TTL and, when it reaches zero, sends back an ICMP Time Exceeded message. This process helps in mapping out the route by identifying each hop between the source and destination.