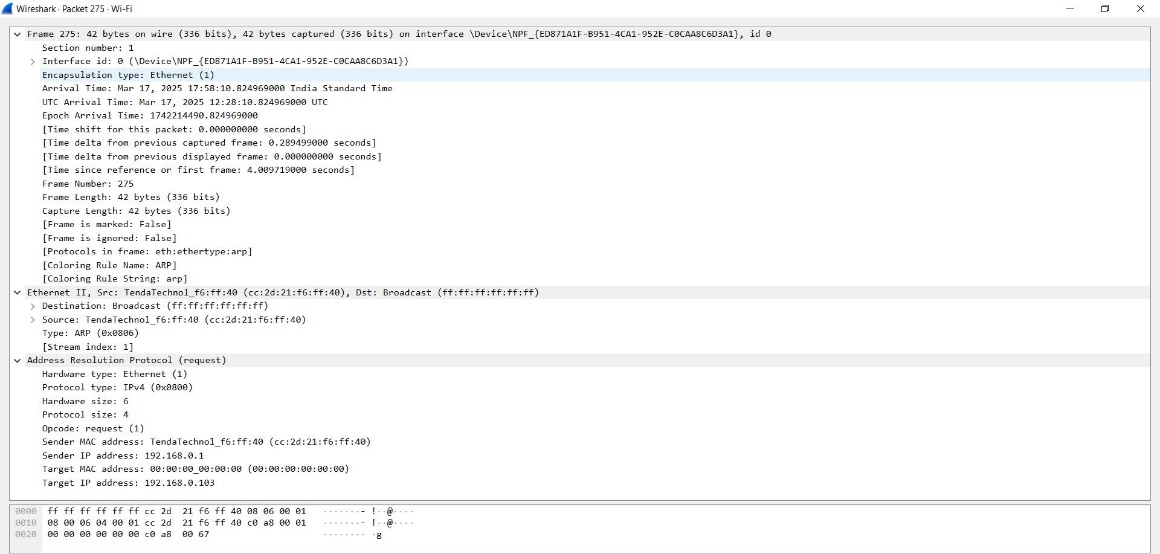
Assignment Questions for Layer-03 (Module 6)

Name: Gowtham S

College: Kumaraguru College of Technology

1. Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames when your device attempts to find the router's MAC address.

Discuss the importance of ARP in packet forwarding.



Frame structure of an ARP packet captured in wireshark

**Importance of ARP in Packet Forwarding:**

MAC Address Resolution:

* Since IP addresses are used for routing, devices need MAC addresses for local network delivery.
* ARP helps obtain these MAC addresses dynamically.

Facilitates Communication:

* Without ARP, devices wouldn’t know where to send Ethernet frames.

Role in Router Communication:

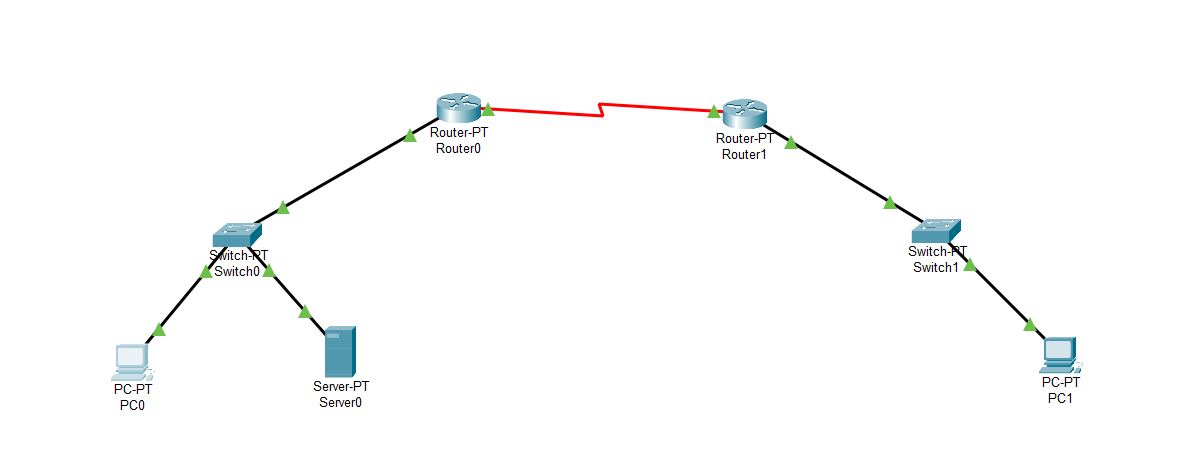
* When a device sends a packet outside its subnet, it first finds the default gateway’s MAC address using ARP.
* The packet is then sent to the router for further forwarding.

Security Concerns (ARP Spoofing):

* Attackers can manipulate ARP tables using spoofed ARP replies, leading to Man-in-the-Middle (MITM) attacks.

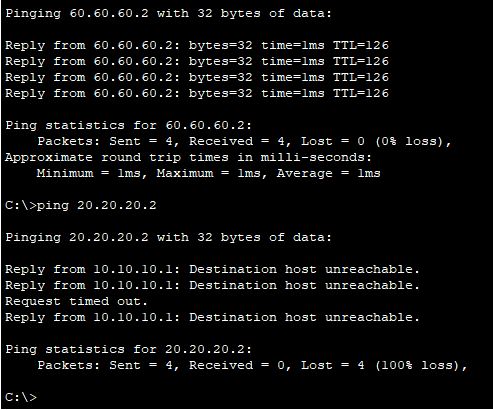
2. Manually configure static routes on a router to direct packets to different subnets.

Use the ip route command and verify connectivity using ping and traceroute.



Ip route <public ip to be reached> <subnet mask of public ip> <next hop>

Using this we can establish communication between systems and server connected with different routers.



Ping <public ip> successful ping

Whereas unsuccessful while pinging private IP

3. Given a network address of 10.0.0.0/24, divide it into 4 equal subnets.

Calculate the new subnet mask: 255.255.255.192 (borrowed 2 bits so now its /26 [CIDR])

Determine the valid host range for each subnet:

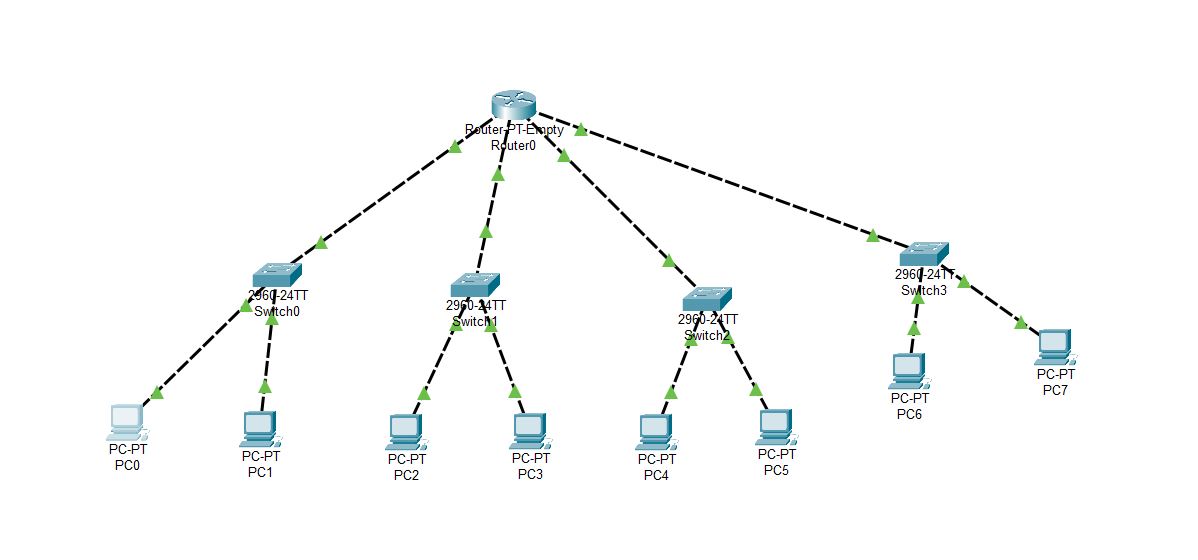
Subnet1- 10.0.0.2 – 10.0.0.62

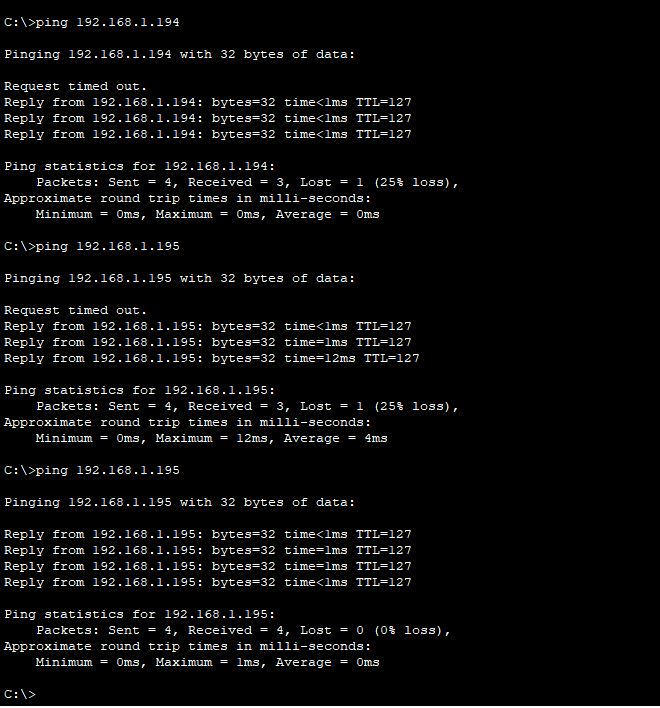
Subnet2- 10.0.0.65 – 10.0.0.126

Subnet3- 10.0.0.129 – 10.0.0.190

Subnet4- 10.0.0.193 – 10.0.0.252

Assign IP addresses to devices in Packet Tracer and verify connectivity.





4. You are given three IP addresses: 192.168.10.5, 172.20.15.1, and 8.8.8.8.

Identify the class of each IP address:

192.168.10.5 – Class C (Private IP)

172.20.15.1 – Class B (Public IP)

8.8.8.8 – Class A (Public IP)

Explain how NAT would handle a private IP when accessing the internet.

Since private IPs (192.168.x.x, 172.16.x.x - 172.31.x.x, 10.x.x.x) are not routable on the internet, they need Network Address Translation (NAT) to access the internet.

Steps of NAT Process:

* A device with a private IP (e.g., 192.168.10.5) requests access to the internet.
* The router, acting as a NAT device, replaces the private IP with its public IP.
* Example: Source IP 192.168.10.5 → Translated to → 203.0.113.1 (router's public IP)
* The request is sent to the internet using the router's public IP.
* The response from the internet is sent back to the router’s public IP.
* The router translates the public IP back to the private IP and delivers the response to the original device.

Types of NAT:

* Static NAT: One-to-one mapping between a private and a public IP.
* Dynamic NAT: Assigns a public IP from a pool of available addresses.
* PAT (Port Address Translation): Many private IPs share one public IP by using different port numbers.

Example Scenario:

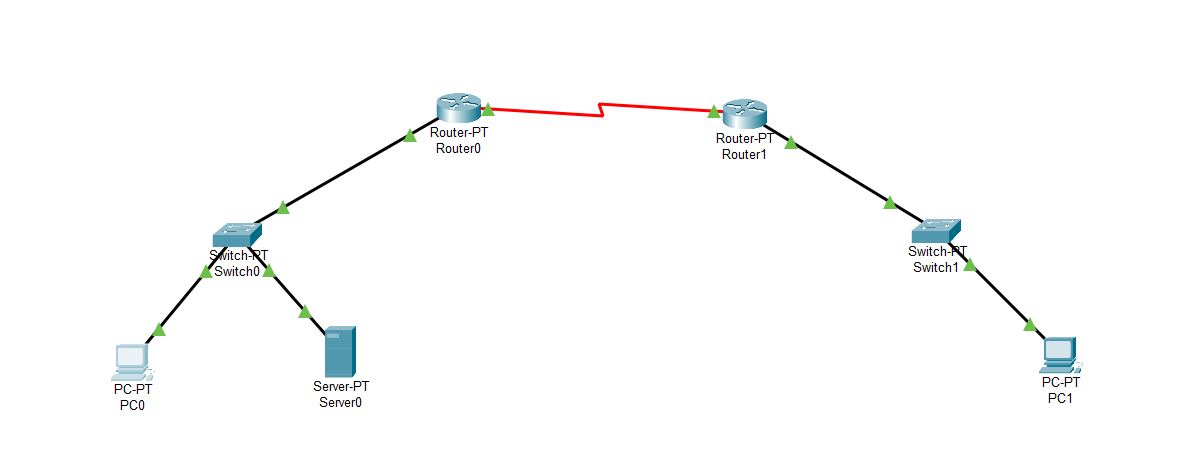
1. A computer 192.168.10.5 accesses www.google.com.
2. NAT translates it to 203.0.113.1 (router’s public IP).
3. Google’s server replies to 203.0.113.1.
4. The router translates it back to 192.168.10.5 and forwards it.

This ensures security, conserves public IPs, and allows multiple devices to share a single internet connection.

5. In Cisco Packet Tracer, configure NAT on a router to allow internal devices (192.168.1.x) to access the internet.

Test connectivity by pinging an external public IP.

Capture the traffic in Wireshark and analyze the source IP before and after NAT translation.



NAT network configuration in CISCO

