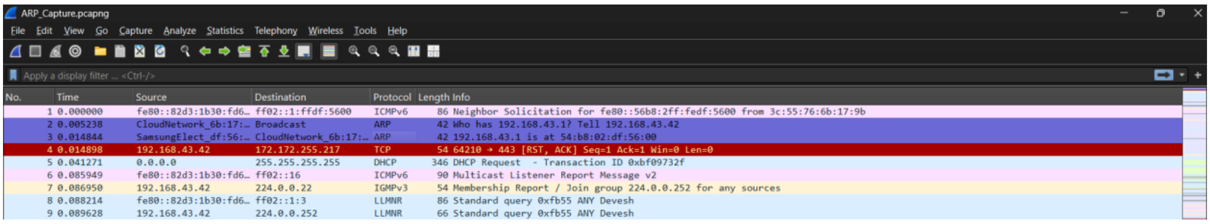
Networking Training Program Module 6

1.) Capture and analyze ARP packets using Wireshark. Inspect the ARP request

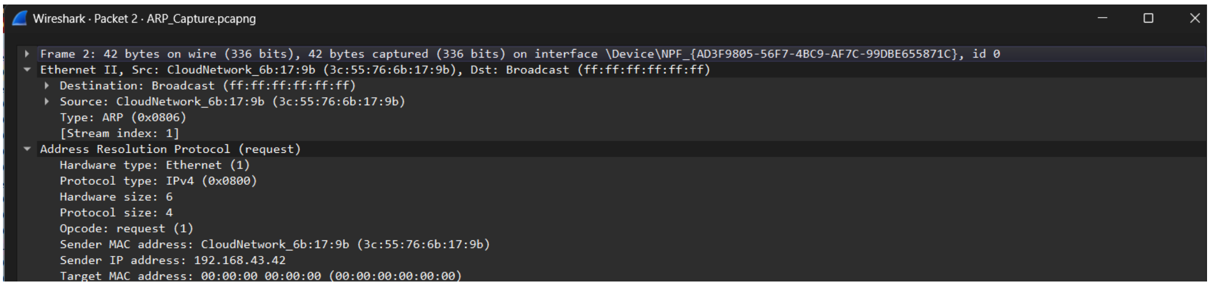
and reply frames when your device attempts to find the router's MAC address.

- Below is the captured ARP packets using wireshark


ARP_Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

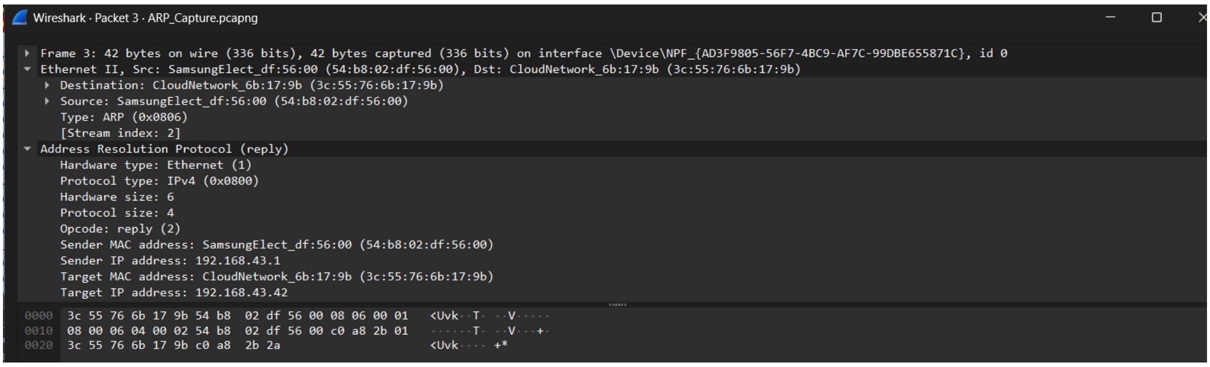
```
No.  Time      Source               Destination          Protocol Length Info
  1 0.000000  fe80::82d3:1b30:fd6… ff02::1:ffdf:5600    ICMPv6    86 Neighbor Solicitation for fe80::56b8:2ff:fedf:5600 from 3c:55:76:6b:17:9b
  2 0.005238  CloudNetwork_6b:17:… Broadcast            ARP       42 Who has 192.168.43.1? Tell 192.168.43.42
  3 0.014844  SamsungElect_df:56:… CloudNetwork_6b:17:… ARP       42 192.168.43.1 is at 54:b8:02:df:56:00
  4 0.014898  192.168.43.42        172.172.255.217      TCP       54 64210 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  5 0.041271  0.0.0.0              255.255.255.255      DHCP     346 DHCP Request  - Transaction ID 0xbf09732f
  6 0.085949  fe80::82d3:1b30:fd6… ff02::16             ICMPv6    90 Multicast Listener Report Message v2
  7 0.086950  192.168.43.42        224.0.0.22           IGMPv3    54 Membership Report / Join group 224.0.0.252 for any sources
  8 0.088214  fe80::82d3:1b30:fd6… ff02::1:3            LLMNR     86 Standard query 0xfb55 ANY Devesh
  9 0.089628  192.168.43.42        224.0.0.252          LLMNR     66 Standard query 0xfb55 ANY Devesh
```

- As you can see it consists of ARP request and response packets.



```
▸ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{AD3F9805-56F7-4BC9-AF7C-99DBE655871C}, id 0
▾ Ethernet II, Src: CloudNetwork_6b:17:9b (3c:55:76:6b:17:9b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: CloudNetwork_6b:17:9b (3c:55:76:6b:17:9b)
    Type: ARP (0x0806)
    [Stream index: 1]
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: CloudNetwork_6b:17:9b (3c:55:76:6b:17:9b)
    Sender IP address: 192.168.43.42
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
```

- This is the broadcasted ARP request packet and note that the target address is all 0s



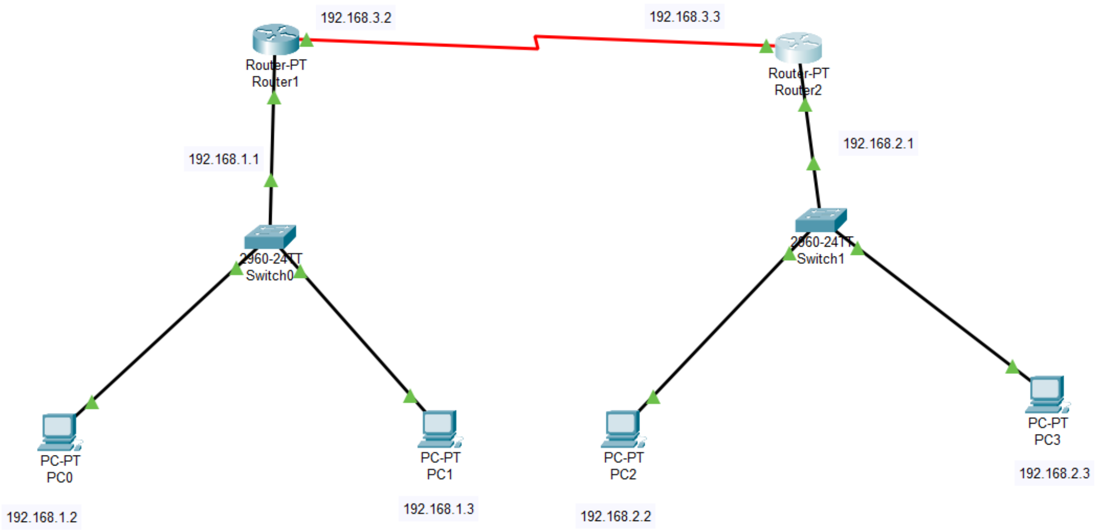
```
▸ Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{AD3F9805-56F7-4BC9-AF7C-99DBE655871C}, id 0
▾ Ethernet II, Src: SamsungElect_df:56:00 (54:b8:02:df:56:00), Dst: CloudNetwork_6b:17:9b (3c:55:76:6b:17:9b)
  ▸ Destination: CloudNetwork_6b:17:9b (3c:55:76:6b:17:9b)
  ▸ Source: SamsungElect_df:56:00 (54:b8:02:df:56:00)
    Type: ARP (0x0806)
    [Stream index: 2]
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: SamsungElect_df:56:00 (54:b8:02:df:56:00)
    Sender IP address: 192.168.43.1
    Target MAC address: CloudNetwork_6b:17:9b (3c:55:76:6b:17:9b)
    Target IP address: 192.168.43.42

0000  3c 55 76 6b 17 9b 54 b8  02 df 56 00 08 06 00 01   <Uvk··T· ··V·····
0010  08 00 06 04 00 02 54 b8  02 df 56 00 c0 a8 2b 01   ······T· ··V···+·
0020  3c 55 76 6b 17 9b c0 a8  2b 2a                     <Uvk···· +*
```

- Note that ARP reply comes from the server and it contains all four address fields.
- Importance of ARP in packet forwarding is that, inside a network, MAC address is used to transfer packets locally, so in this case the device must have the receiver's MAC in it's ARP table.

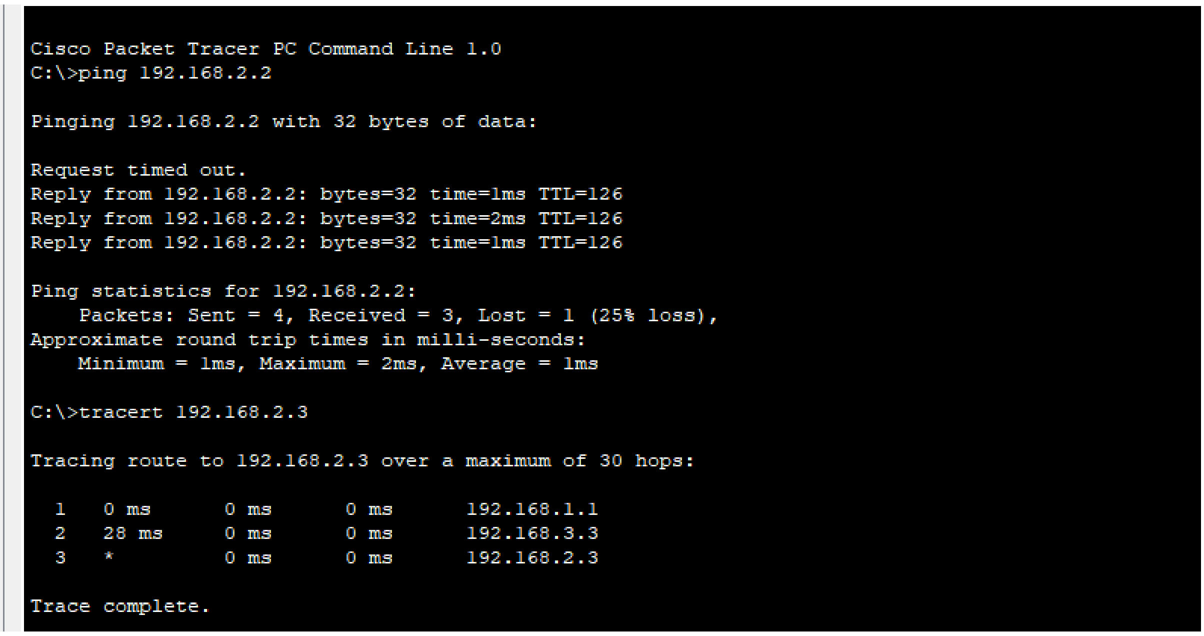
2.) Manually configure static routes on a router to direct packets to different subnets.

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

- Below is the network configured with static ip routes.



- The output of ping and traceroute are shown below.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>tracert 192.168.2.3

Tracing route to 192.168.2.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.1
  2   28 ms     0 ms      0 ms      192.168.3.3
  3   *         0 ms      0 ms      192.168.2.3

Trace complete.
```

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

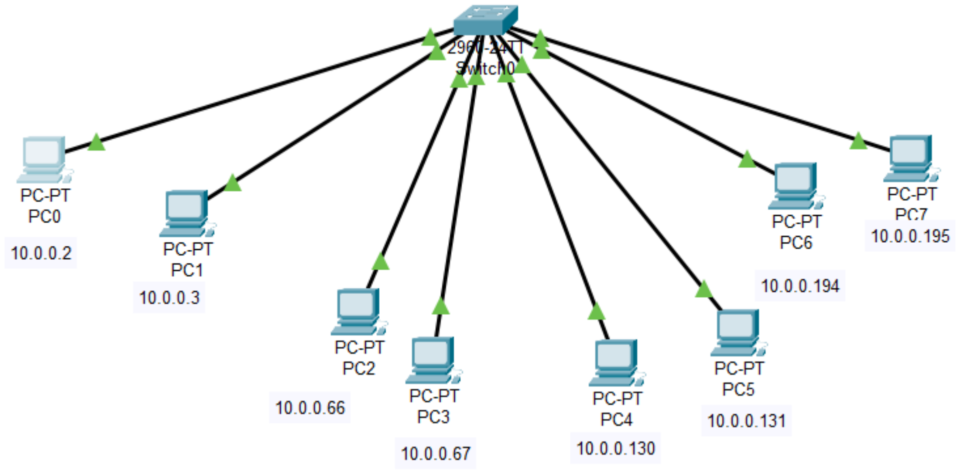
Calculate the new subnet mask.

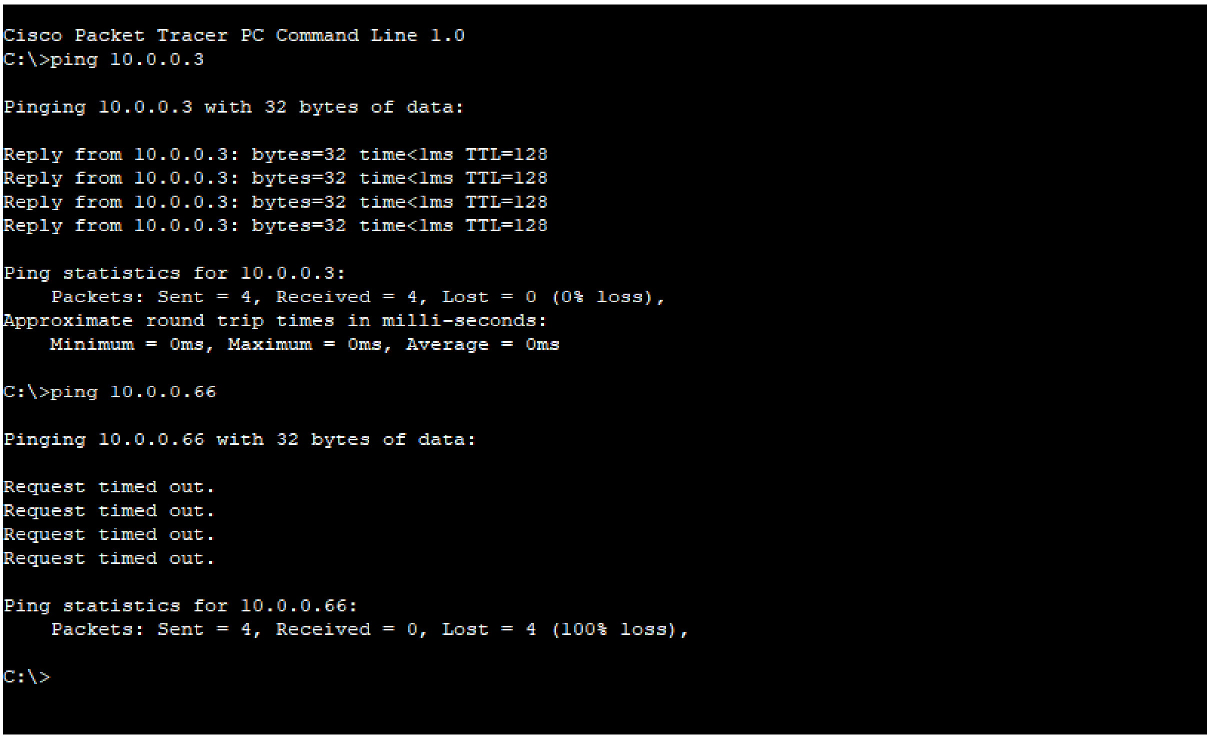
Determine the valid host range for each subnet.

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

S.no	Network address	Subnet Mask	Valid Host range
1	10.0.0.0	255.255.255.192	10.0.0.1 – 10.0.0.62
2	10.0.0.64	255.255.255.192	10.0.0.65 – 10.0.0.126
3	10.0.0.128	255.255.255.192	10.0.0.129 – 10.0.0.190
4	10.0.0.192	255.255.255.192	10.0.0.193 – 10.0.0.254

- In the snapshot attached below, it is verified that the connectivity is available for hosts that are in the same subnet but not with other subnets even though they are all connected under a same switch.





```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128
Reply from 10.0.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.0.0.66

Pinging 10.0.0.66 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

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.

Determine if it is private or public.

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

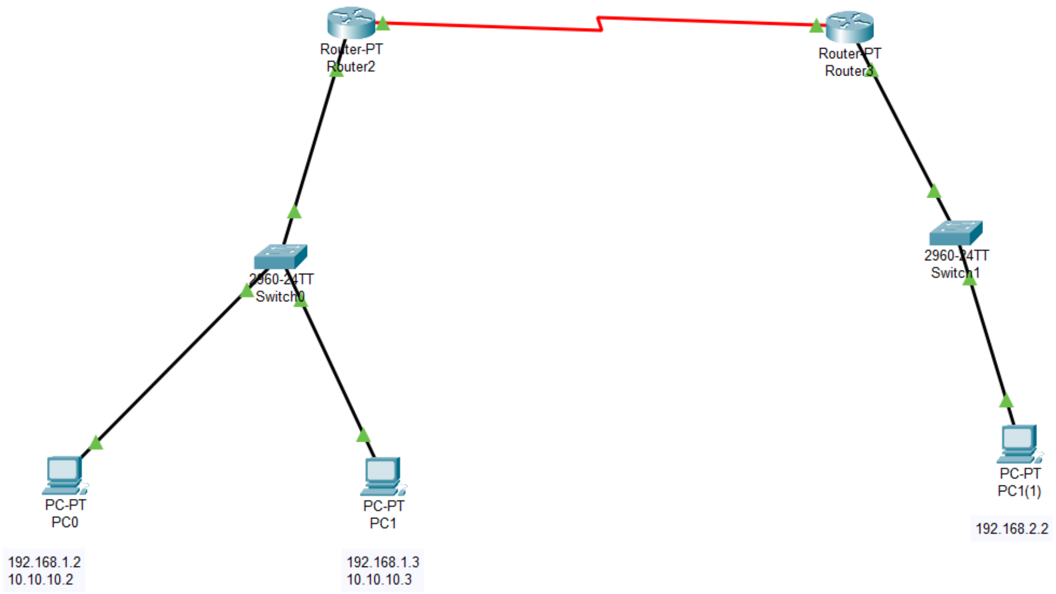
S No.	Ip address	Class	Private or Public
1	192.168.10.5	C	Private
2	172.20.25.1	B	Private
3	8.8.8.8	A	Public

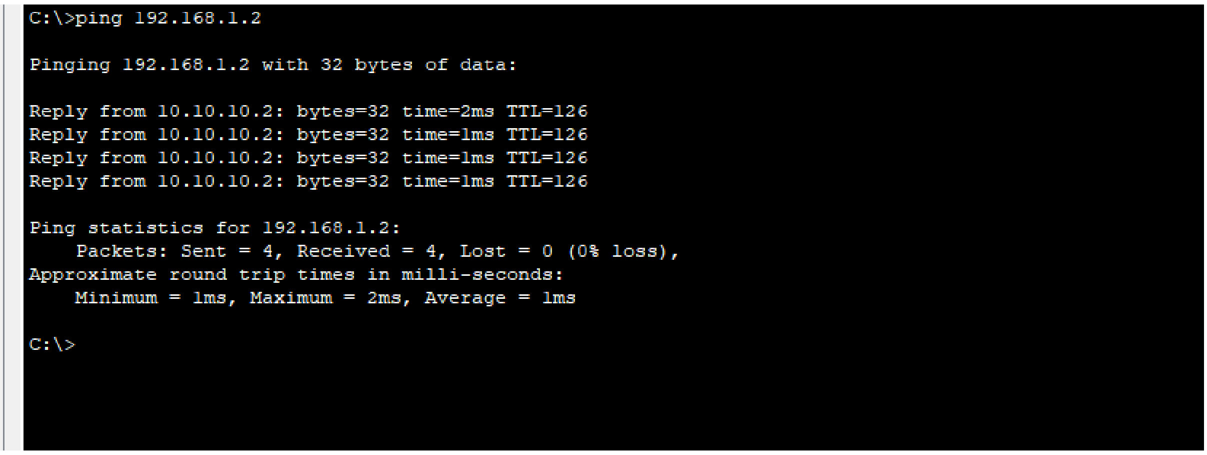
- Private IPs cannot be used to access the internet therefore the NAT changes those private ip's into public Ip of the NAT enabled router, to access the internet.

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.





```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=2ms TTL=126
Reply from 10.10.10.2: bytes=32 time=1ms TTL=126
Reply from 10.10.10.2: bytes=32 time=1ms TTL=126
Reply from 10.10.10.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```