

Module 6 Assignment Solutions

Sri Gnana Saravan.N

VIT Chennai

1. Capture and Analyze Packets using Wireshark. Inspect the ARP Request and Reply frames when your device attempts to find the router MAC Address. Discuss the importance of ARP in packet forwarding?

Solution:

First of all clear the ARP cache for understanding the whole process of ARP because our device already stores the MAC Address of the router So it can directly unicast the message. In command prompt type `arp -d *` for clearing the ARP Cache and then ping to your router.

The image shows a Wireshark packet capture from a Wi-Fi interface. The packet list shows several ARP frames. The selected packet is frame 54, an ARP request from ChongqingFug_ab:de:25 to Broadcast (ff:ff:ff:ff:ff:ff). The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and the ARP request structure. The packet bytes pane shows the raw data of the frame.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-----------------------|-----------------------|----------|--------|---|
| 54 | 23.726546 | ChongqingFug_ab:de:25 | Broadcast | ARP | 42 | Who has 192.168.29.1? Tell 192.168.29.97 |
| 55 | 23.733708 | Arcadyan_b6:4c:01 | ChongqingFug_ab:de:25 | ARP | 42 | 192.168.29.1 is at c4:e5:32:b6:4c:01 |
| 56 | 23.924708 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 57 | 23.926422 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 262 | 32.153485 | Arcadyan_b6:4c:01 | ChongqingFug_ab:de:25 | ARP | 42 | Who has 192.168.29.97? Tell 192.168.29.1 |
| 263 | 32.153527 | ChongqingFug_ab:de:25 | Arcadyan_b6:4c:01 | ARP | 42 | 192.168.29.97 is at a4:97:b1:ab:de:25 |
| 271 | 35.020355 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.97? Tell 192.168.29.130 |
| 272 | 35.020407 | ChongqingFug_ab:de:25 | 5e:a6:e6:04:ab:42 | ARP | 42 | 192.168.29.97 is at a4:97:b1:ab:de:25 |
| 273 | 35.020705 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.1? Tell 192.168.29.130 |
| 276 | 36.044104 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 277 | 36.044412 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 281 | 40.959516 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.125? Tell 192.168.29.1 |
| 282 | 40.959621 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.126? Tell 192.168.29.1 |
| 283 | 40.959837 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.186? Tell 192.168.29.1 |
| 284 | 40.960174 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.96? Tell 192.168.29.1 |
| 287 | 40.978095 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.104? Tell 192.168.29.1 |
| 288 | 40.989638 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.160? Tell 192.168.29.1 |
| 290 | 41.983525 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.125? Tell 192.168.29.1 |

Frame 54: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{21D9BF2C-} 0000 ff ff ff ff ff ff a4 97 b1 ab de 25 08 06 00 01 %---
Ethernet II, Src: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 0010 08 00 06 04 00 01 a4 97 b1 ab de 25 c0 a8 1d 61 %---a
0020 00 00 00 00 00 00 c0 a8 1d 01
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25)
Type: ARP (0x0806)
[Stream index: 2]
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25)
Sender IP address: 192.168.29.97
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.29.1

Here in **Step 1** ----> Chongqing is our device, Firstly it sends the broadcast message to everyone with Destination IP Address that it gets from Upper layer. It asks Who has the IP Address of 192.168.29.1. Here you can see that Target MAC Address: 00:00:00_00:00:00 (Don't know the Target MAC) but knows the Target IP got it from the Transport layer.

| Capturing from Wi-Fi | | | | | | |
|--|-----------|------------------------|------------------------|----------|--------|---|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | | |
| arp | | | | | | |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 54 | 23.726546 | ChongqingFug_ab:de:... | Broadcast | ARP | 42 | Who has 192.168.29.1? Tell 192.168.29.97 |
| 55 | 23.733788 | Arcadyan_b6:4c:01 | ChongqingFug_ab:de:... | ARP | 42 | 192.168.29.1 is at c4:e5:32:b6:4c:01 |
| 56 | 23.924788 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 57 | 23.926422 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 262 | 32.153485 | Arcadyan_b6:4c:01 | ChongqingFug_ab:de:... | ARP | 42 | Who has 192.168.29.97? Tell 192.168.29.1 |
| 263 | 32.153527 | ChongqingFug_ab:de:... | Arcadyan_b6:4c:01 | ARP | 42 | 192.168.29.97 is at a4:97:b1:ab:de:25 |
| 271 | 35.020355 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.97? Tell 192.168.29.130 |
| 272 | 35.020407 | ChongqingFug_ab:de:... | 5e:a6:e6:04:ab:42 | ARP | 42 | 192.168.29.97 is at a4:97:b1:ab:de:25 |
| 273 | 35.020705 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.1? Tell 192.168.29.130 |
| 276 | 36.044184 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 277 | 36.044412 | 5e:a6:e6:04:ab:42 | Broadcast | ARP | 60 | Who has 192.168.29.174? Tell 192.168.29.130 |
| 281 | 40.959516 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.125? Tell 192.168.29.1 |
| 282 | 40.959621 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.126? Tell 192.168.29.1 |
| 283 | 40.959837 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.186? Tell 192.168.29.1 |
| 284 | 40.960174 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.96? Tell 192.168.29.1 |
| 287 | 40.978095 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.104? Tell 192.168.29.1 |
| 288 | 40.989638 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.160? Tell 192.168.29.1 |
| 290 | 41.983525 | Arcadyan_b6:4c:01 | Broadcast | ARP | 42 | Who has 192.168.29.125? Tell 192.168.29.1 |

| | | | |
|---|------|---|----------------|
| > Frame 55: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{21D9BF2C-...} | 0000 | a4 97 b1 ab de 25 c4 e5 32 b6 4c 01 08 06 00 01 | 2:L..... |
| > Ethernet II, Src: Arcadyan_b6:4c:01 (c4:e5:32:b6:4c:01), Dst: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25) | 0010 | 08 00 06 04 00 02 c4 e5 32 b6 4c 01 c0 a8 1d 01 | 2:L..... |
| > Destination: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25) | 0020 | a4 97 b1 ab de 25 c0 a8 1d 61 | a |
| > Source: Arcadyan_b6:4c:01 (c4:e5:32:b6:4c:01) | | | |
| Type: ARP (0x0806) | | | |
| [Stream index: 4] | | | |
| > Address Resolution Protocol (reply) | | | |
| Hardware type: Ethernet (1) | | | |
| Protocol type: IPv4 (0x0800) | | | |
| Hardware size: 6 | | | |
| Protocol size: 4 | | | |
| Opcode: reply (2) | | | |
| Sender MAC address: Arcadyan_b6:4c:01 (c4:e5:32:b6:4c:01) | | | |
| Sender IP address: 192.168.29.1 | | | |
| Target MAC address: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25) | | | |
| Target IP address: 192.168.29.97 | | | |

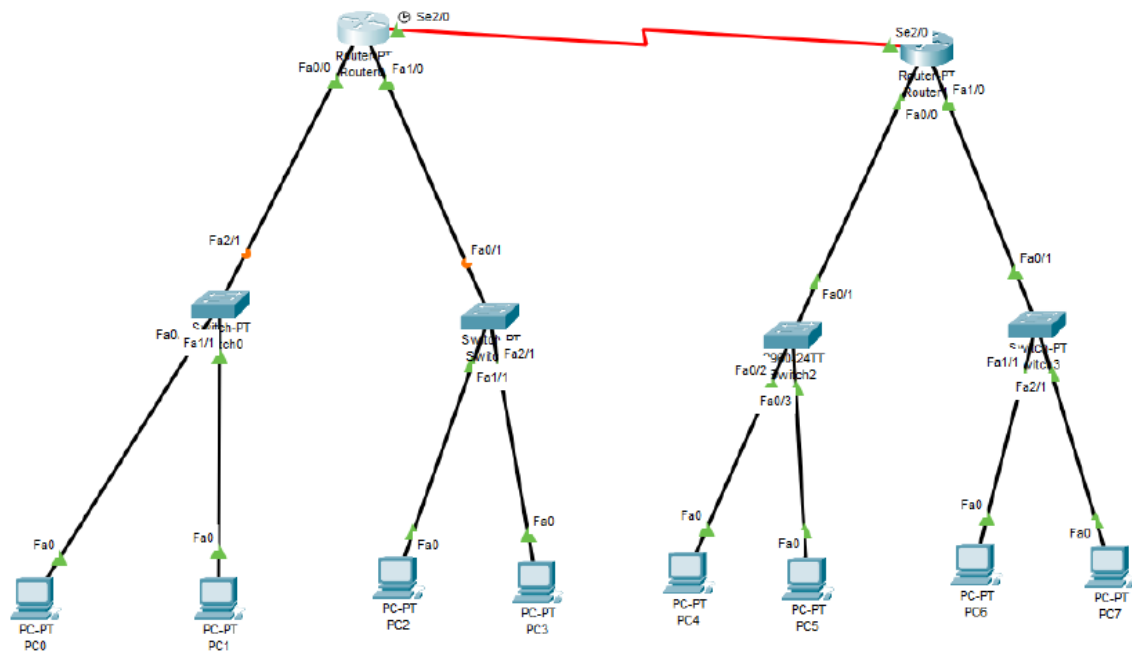
Step 2-----> The Router here is Arcadyan,It replies back for the ARP Request by sending its MAC Address to the source ip.But here the message is unicast because in ARP Request itself it knows the MAC Address of the Source IP,So it sends the reply directly to the source ip.

Importance in Packet forwarding:

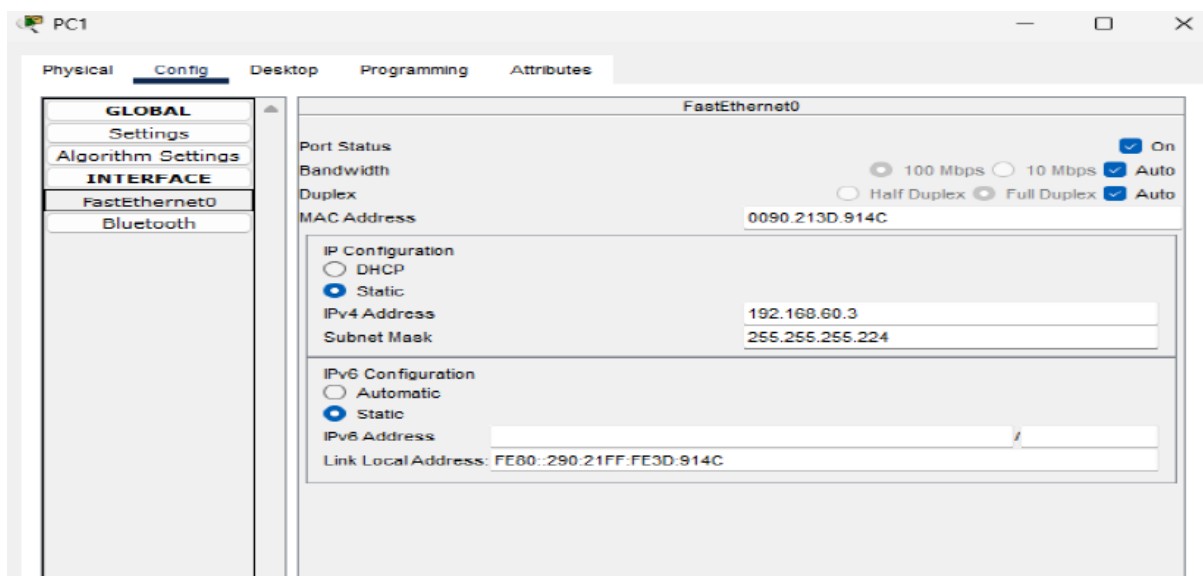
ARP Plays the huge role in Packet forwarding because its main job is to translate the destination ip address to its destination mac address(hardware address).Then only we can connect to the computer or pc to the network.Without ARP,we cannot talk to the hardware straightly.Also it stores the respective MAC address for the specific IP Address.So if next time when the device tries to send the message it can unicast its message to the ip.

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.

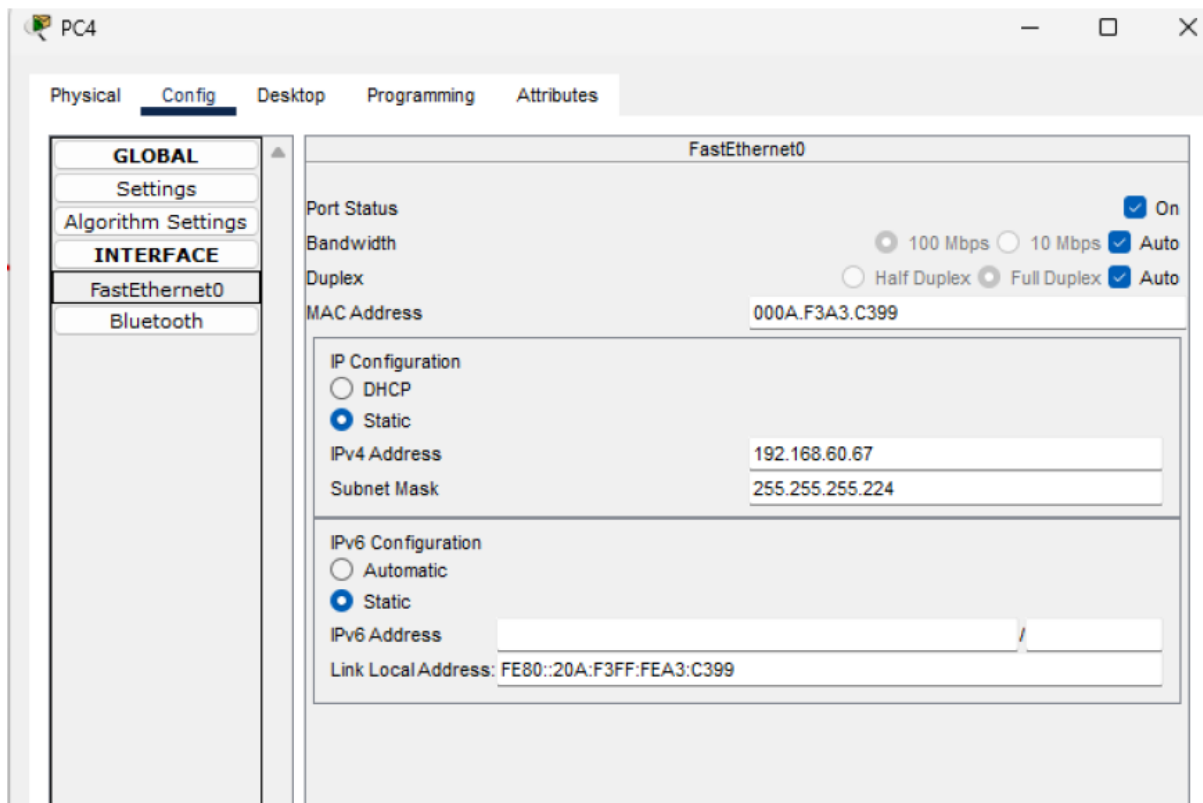
Solution:



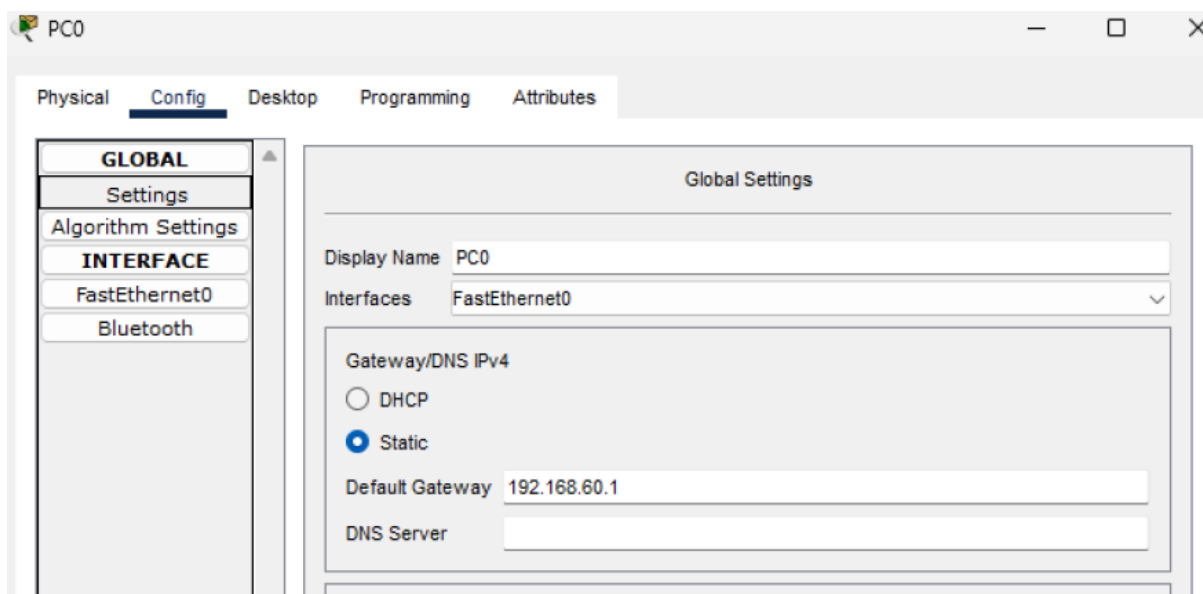
Creating the four subnets with the Class C Block



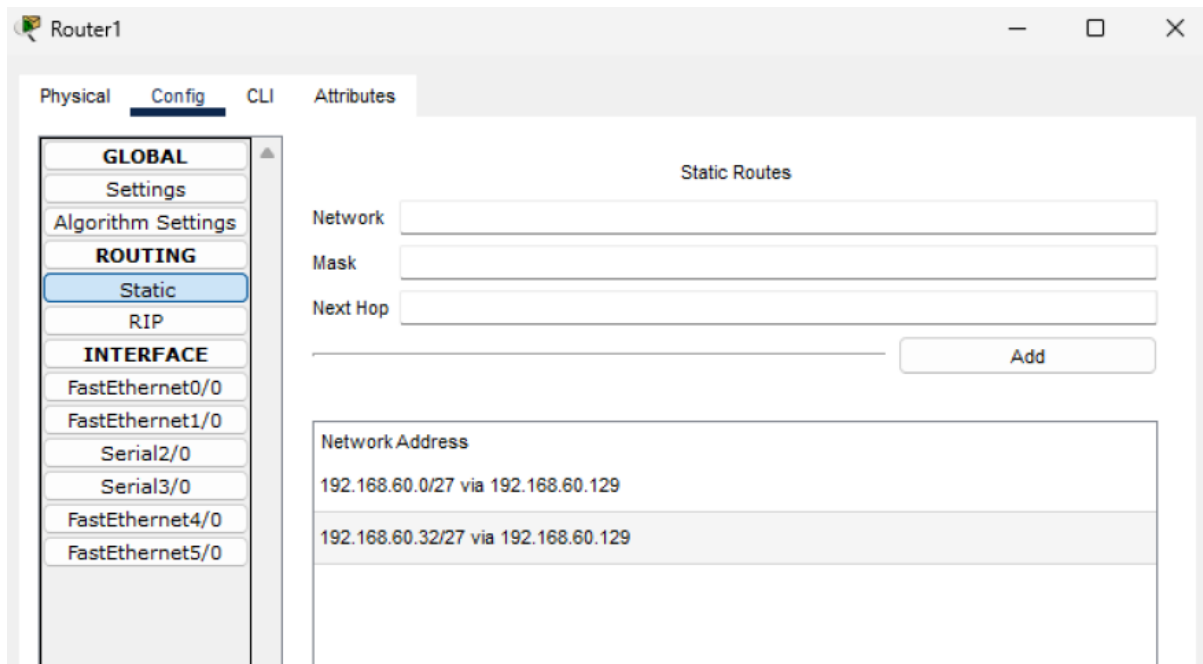
Statically configuring the IP Address instead of DHCP Server.



Default Gateway configurations:



Static entries about other subnets:



Ip route command to statically add the IP addresses

```
Router(config)#ip route 192.168.60.0 255.255.255.224 192.168.60.129
Router(config)#ip route 192.168.60.32 255.255.255.224 192.168.60.129
Router(config)#
Router(config)#
Router(config)#
```

After giving static entries:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.60.0/27 is subnetted, 5 subnets
C       192.168.60.0 is directly connected, FastEthernet0/0
C       192.168.60.32 is directly connected, FastEthernet1/0
S       192.168.60.64 [1/0] via 192.168.60.130
S       192.168.60.96 [1/0] via 192.168.60.130
C       192.168.60.128 is directly connected, Serial2/0
```

Pinging from one subnet to the other:

```

C:\>ping 192.168.60.35

Pinging 192.168.60.35 with 32 bytes of data:

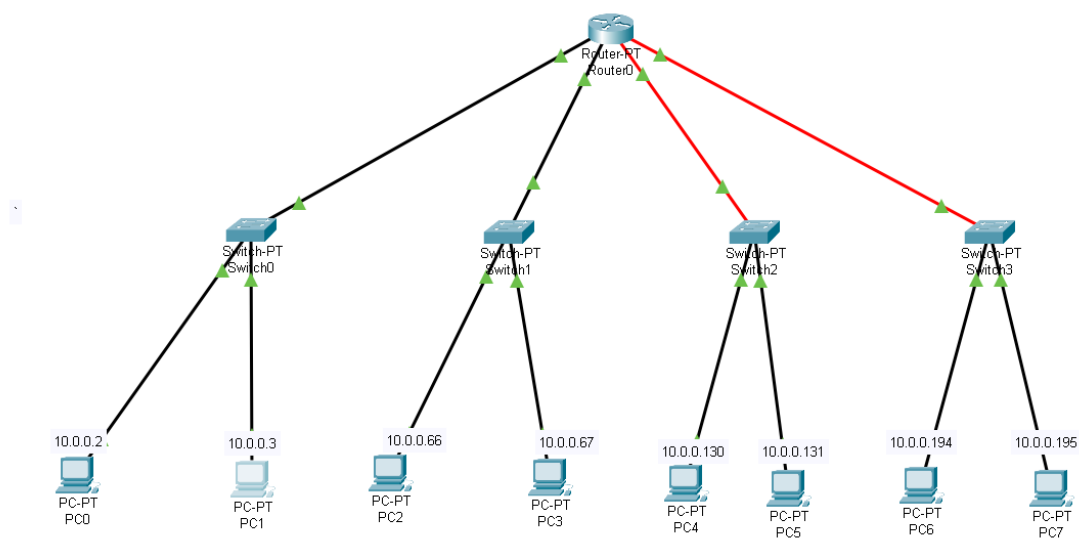
Request timed out.
Reply from 192.168.60.35: bytes=32 time<1ms TTL=127
Reply from 192.168.60.35: bytes=32 time<1ms TTL=127
Reply from 192.168.60.35: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.60.35:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

- 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.

Solution:



Pinging to different subnets from subnet 1:

```
C:\>ping 10.0.0.131
```

```
Pinging 10.0.0.131 with 32 bytes of data:
```

```
Request timed out.
```

```
Reply from 10.0.0.131: bytes=32 time=1ms TTL=127
```

```
Reply from 10.0.0.131: bytes=32 time<1ms TTL=127
```

```
Reply from 10.0.0.131: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.0.0.131:
```

```
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 10.0.0.194
```

```
Pinging 10.0.0.194 with 32 bytes of data:
```

```
Request timed out.
```

```
Reply from 10.0.0.194: bytes=32 time<1ms TTL=127
```

```
Reply from 10.0.0.194: bytes=32 time<1ms TTL=127
```

```
Reply from 10.0.0.194: bytes=32 time=8ms TTL=127
```

```
Ping statistics for 10.0.0.194:
```

```
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

```
C:\>ping 10.0.0.2
```

```
Pinging 10.0.0.2 with 32 bytes of data:
```

```
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
```

```
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
```

```
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
```

```
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.0.0.2:
```

```
    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.
```

```
Reply from 10.0.0.66: bytes=32 time<1ms TTL=127
```

```
Reply from 10.0.0.66: bytes=32 time<1ms TTL=127
```

```
Reply from 10.0.0.66: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.0.0.66:
```

```
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Subnet Assignments:

Since we need to split into 4 different subnets for 10.0.0.0/24

We need 2 extra bits to achieve this so the new subnet mask is 255.255.255.11000000-
->255.255.255.192

Valid host ranges :

Subnet 1 ----> 10.0.0.0 is given for identifying network ,10.0.0.1 for the default gateway and 10.0.0.63 for broadcasting . So the valid range is 10.0.0.2 – 10.0.0.62.

Subnet 2 ----> 10.0.0.64 is given for identifying network ,10.0.0.65 for the default gateway and 10.0.0.127 for broadcasting . So the valid range is 10.0.0.66 – 10.0.0.126.

Subnet 3 ----> 10.0.0.128 is given for identifying network ,10.0.0.129 for the default gateway and 10.0.0.191 for broadcasting . So the valid range is 10.0.0.130 – 10.0.0.190.

Subnet 4----> 10.0.0.192 is given for identifying network ,10.0.0.193 for the default gateway and 10.0.0.255 for broadcasting . So the valid range is 10.0.0.194 – 10.0.0.254.

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.

Solution:

192.168.10.5 -----> It comes under the Class C range .

172.20.15.1 -----> It comes under Class B Range.

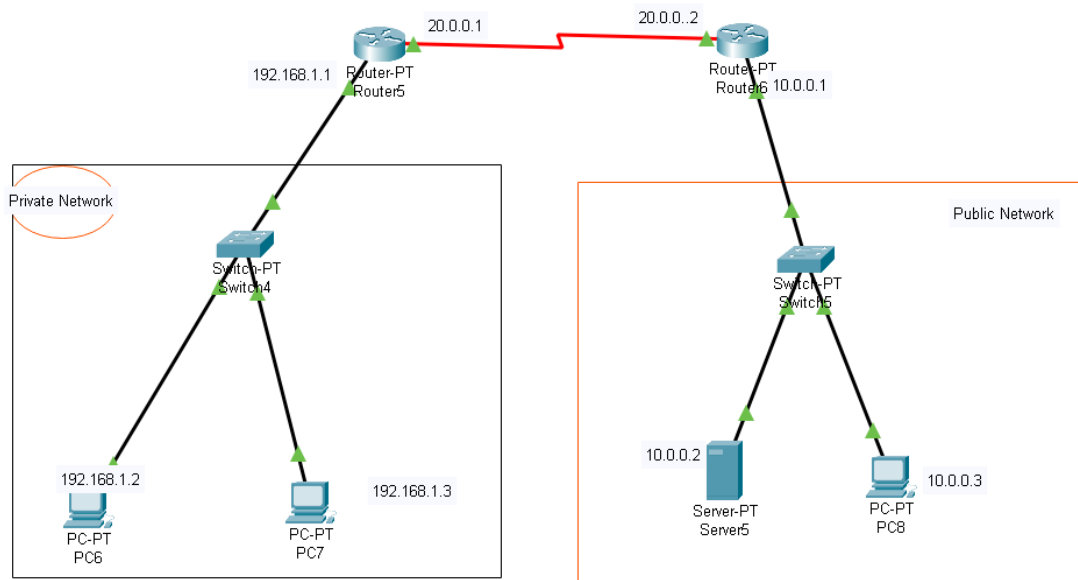
8.8.8.8 -----> It comes under Class A range.

192.168.10.5 and 172.20.15.1 are the private IP Addresses. 8.8.8.8 is the public IP Address and it's the Google DNS Server.

With the Private IP Addresses we can communicate within the Local LAN but when we try to connect to the network we need Public IP. So when a device with Private IP sends request to internet server, it first sends to the default gateway router. The Router is running NAT (Network Address Translation) Translates the Private IP Address to the Public IP Address. So the internet server responds to this Public IP and sends the reply back. Again Router Translates this Public IP to respective Private IP. In this method multiple devices with different IP's in the private network can share a single IP so they can keep their Private IP hidden.

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

Solution:



From Private Network to Public Network:

```
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=12ms TTL=126
Reply from 10.0.0.3: bytes=32 time=10ms TTL=126
Reply from 10.0.0.3: bytes=32 time=5ms TTL=126
Reply from 10.0.0.3: bytes=32 time=1ms TTL=126

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 7ms
```

As you can see that from Private Network PC (IP = 192.168.1.3) Tries to ping to the Public network it gets successful.

From Public Network to Private Network:

```
C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time=11ms TTL=126
Reply from 20.0.0.1: bytes=32 time=1ms TTL=126
Reply from 20.0.0.1: bytes=32 time=1ms TTL=126
Reply from 20.0.0.1: bytes=32 time=1ms TTL=126

Ping statistics for 20.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>ping 192.168.1.3

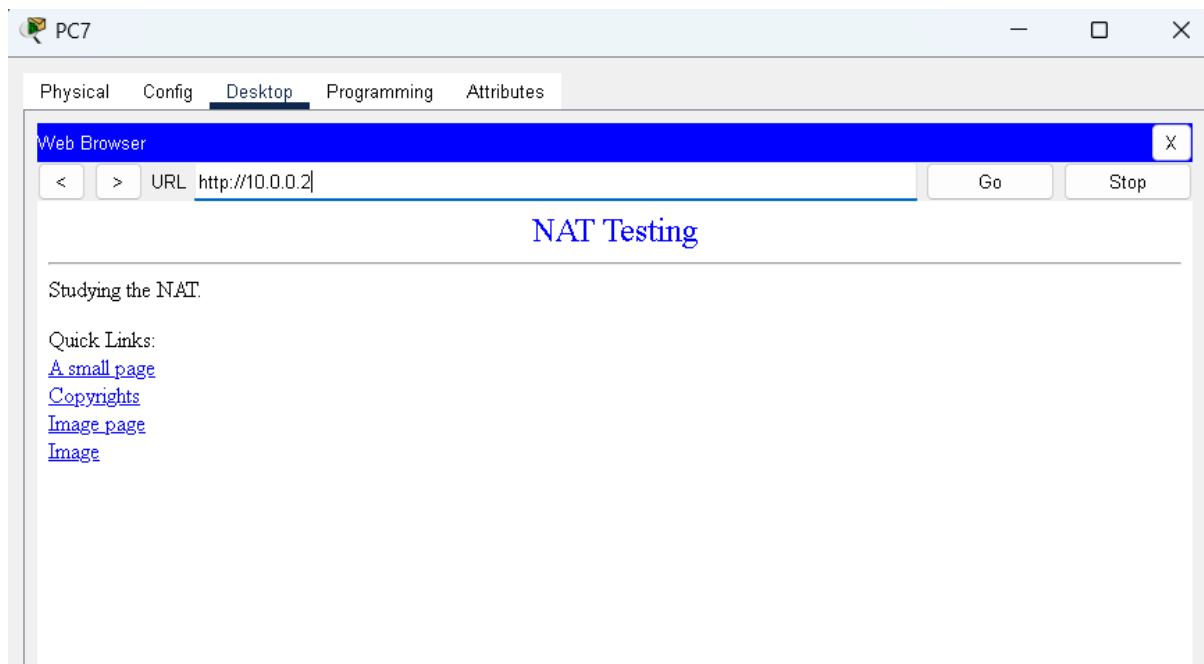
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Request timed out.
Reply from 10.0.0.1: Destination host unreachable.
|
```

But from Public Network to Private Network, if we try to ping to the Public IP 20.0.0.1 it gets successful. But if we try to ping the Private IP it shows Destination host unreachable. That's why router converts the Private IP to the Public IP Using NAT (Network Address Translation)

Configuring NAT in Private Network Router:

```
Router(config)#ip nat inside source static 192.168.1.2 20.0.0.1
Router(config)#ip nat inside source static 192.168.1.3 20.0.0.1
Router(config)#
Router(config)#int f0/0
Router(config-if)#int f0/0
Router(config-if)#ip nat inside
Router(config-if)#int s2/0
Router(config-if)#ip nat outside
..
```



IP Addresses Before and After NAT Translations:

```
Router (config)#exit
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 20.0.0.1:29        192.168.1.3:29   10.0.0.2:29       10.0.0.2:29
icmp 20.0.0.1:30        192.168.1.3:30   10.0.0.2:30       10.0.0.2:30
icmp 20.0.0.1:31        192.168.1.3:31   10.0.0.2:31       10.0.0.2:31
icmp 20.0.0.1:32        192.168.1.3:32   10.0.0.2:32       10.0.0.2:32
icmp 20.0.0.1:33        192.168.1.3:33   10.0.0.2:33       10.0.0.2:33
icmp 20.0.0.1:34        192.168.1.3:34   10.0.0.2:34       10.0.0.2:34
icmp 20.0.0.1:35        192.168.1.3:35   10.0.0.2:35       10.0.0.2:35
icmp 20.0.0.1:36        192.168.1.3:36   10.0.0.2:36       10.0.0.2:36
---  20.0.0.1           192.168.1.3      ---               ---
tcp  20.0.0.1:1025     192.168.1.3:1025 10.0.0.2:80       10.0.0.2:80
```

Before the Router performs NAT:

In Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 192.168.1.3,
Dest. IP: 10.0.0.2 ICMP Message Type: 8


Layer 2: Ethernet II Header
000A.F305.1714 >> 00E0.A39A.00E1

Layer 1: Port FastEthernet0/0

After the Router Performs NAT:

Out Layers

| |
|--|
| Layer7 |
| Layer6 |
| Layer5 |
| Layer4 |
| > Layer 3: IP Header Src. IP: 20.0.0.1, Dest. IP: 10.0.0.2 ICMP Message Type: 8 |
| Layer 2: Ethernet II Header 0000.0CAA.C8D1 >> 00D0.FF8E.785C |
| Layer 1: Port(s): FastEthernet0/0 |



So you can see that IP Src header changed to 20.0.0.1 which is the Public IP.