Module 5 Assignment Solutions

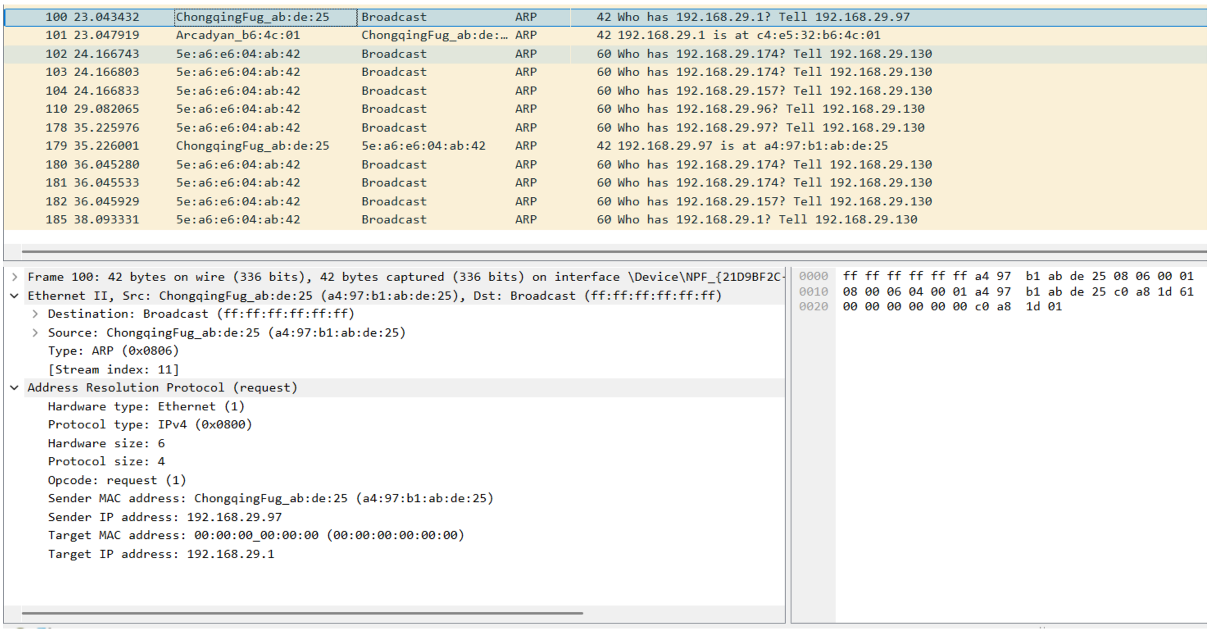
Sri Gnana Saravan.N

VIT Chennai

1. Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.

Solution:

Capture the ARP Packets in Wireshark using arp display filter.



Here Chongqing is the laptop device and Arcadyan is the router.First of all ARP (Address Resolution protocol) is used in network layer,basically it is used to resolve the MAC Address of the device given its IP address.The device which has the destination ip address wants to resolve the MAC address will broadcast its message to the network.In this request it will have sender ip and mac address and the destination ip address but it will not have the target MAC Address.So it will have 00:00:00_00:00:00 as the target MAC Address.The device which matches its IP Address replies back to this ARP Request by its MAC Address.So this message is unicast because it has the sender mac address in the arp request itself.So the ARP Table of the Source device will be updated so that next time it can directly sends the message to the respective mac address

```
101 23.047919   Arcadyan_b6:4c:01      ChongqingFug_ab:de:…  ARP   42 192.168.29.1 is at c4:e5:32:b6:4c:01
102 24.166743   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.174? Tell 192.168.29.130
103 24.166803   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.174? Tell 192.168.29.130
104 24.166833   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.157? Tell 192.168.29.130
110 29.082065   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.96? Tell 192.168.29.130
178 35.225976   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.97? Tell 192.168.29.130
179 35.226001   ChongqingFug_ab:de:25  5e:a6:e6:04:ab:42     ARP   42 192.168.29.97 is at a4:97:b1:ab:de:25
180 36.045280   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.174? Tell 192.168.29.130
181 36.045533   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.174? Tell 192.168.29.130
182 36.045929   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.157? Tell 192.168.29.130
185 38.093331   5e:a6:e6:04:ab:42      Broadcast             ARP   60 Who has 192.168.29.1? Tell 192.168.29.130
```

```
> Frame 101: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{21D9BF2C-
v Ethernet II, Src: Arcadyan_b6:4c:01 (c4:e5:32:b6:4c:01), Dst: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25)
  > Destination: ChongqingFug_ab:de:25 (a4:97:b1:ab:de:25)
  > Source: Arcadyan_b6:4c:01 (c4:e5:32:b6:4c:01)
    Type: ARP (0x0806)
    [Stream index: 3]
v 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
```

```
0000  a4 97 b1 ab de 25 c4 e5  32 b6 4c 01 08 06 00 01
0010  08 00 06 04 00 02 c4 e5  32 b6 4c 01 c0 a8 1d 01
0020  a4 97 b1 ab de 25 c0 a8  1d 61
```

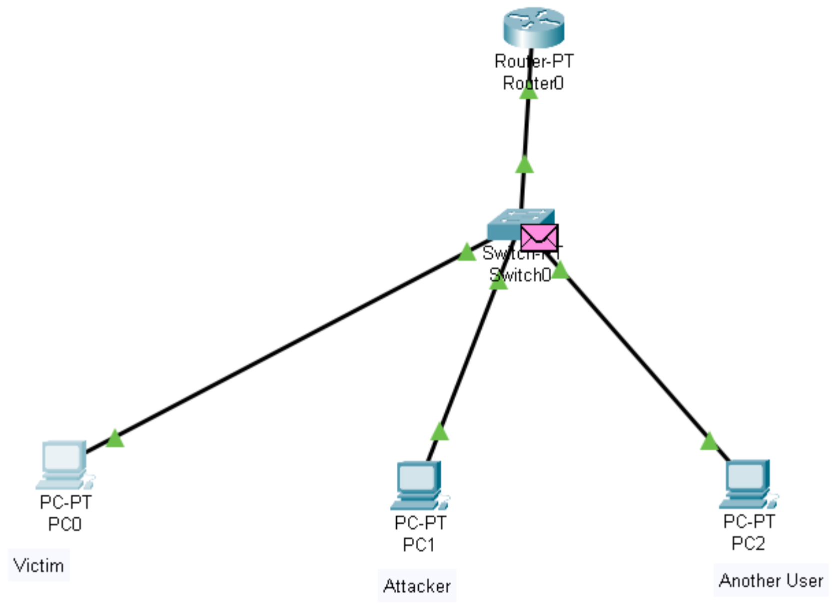
Updated ARP Table:

```
PS C:\WINDOWS\system32> arp -a

Interface: 192.168.29.97 --- 0x8
  Internet Address      Physical Address      Type
  192.168.29.1          c4-e5-32-b6-4c-01     dynamic
  192.168.29.130        5e-a6-e6-04-ab-42     dynamic
  192.168.29.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Note that clear the ARP Cache before capturing the ARP Packets because the device will directly unicast its message.

2. Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.

Solution:

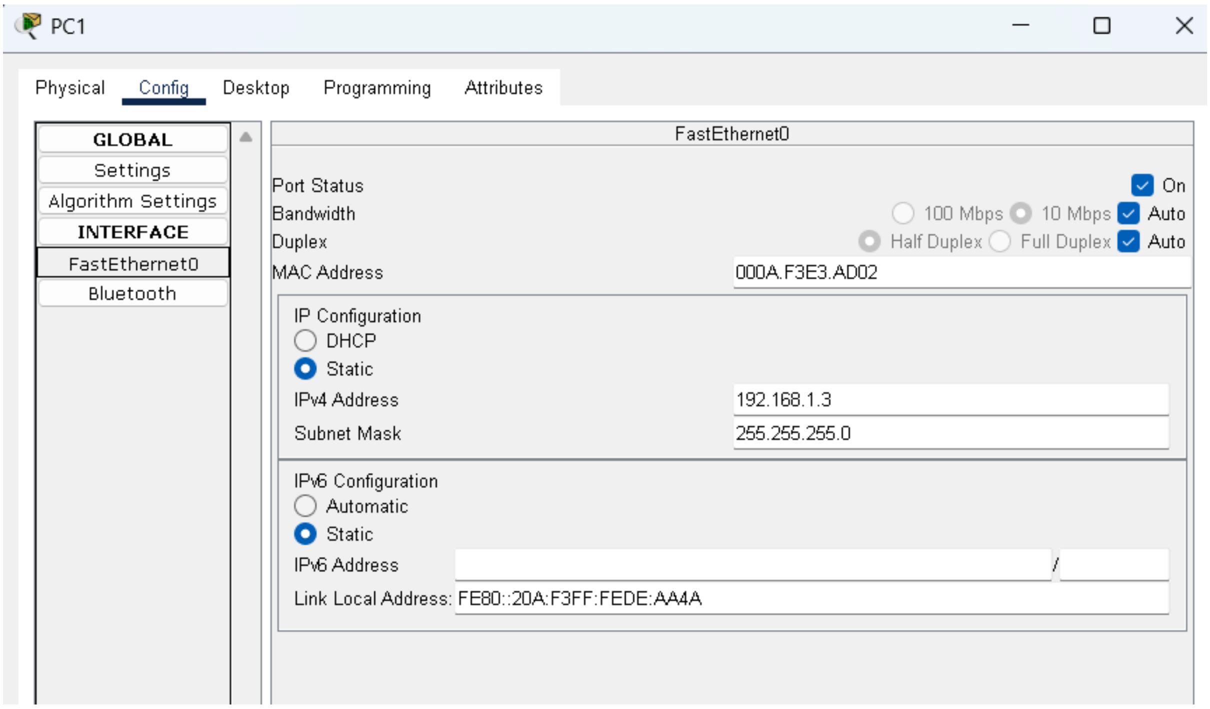


Pinging from Victim to Another User,So it resolves the 192.168.1.4 with its MAC Address and updates the ARP Table.

Before Spoofing Attack:

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.4           0030.a392.b51d        dynamic
```

Spoofing the MAC Address of the Router as MAC Address of Attacker:



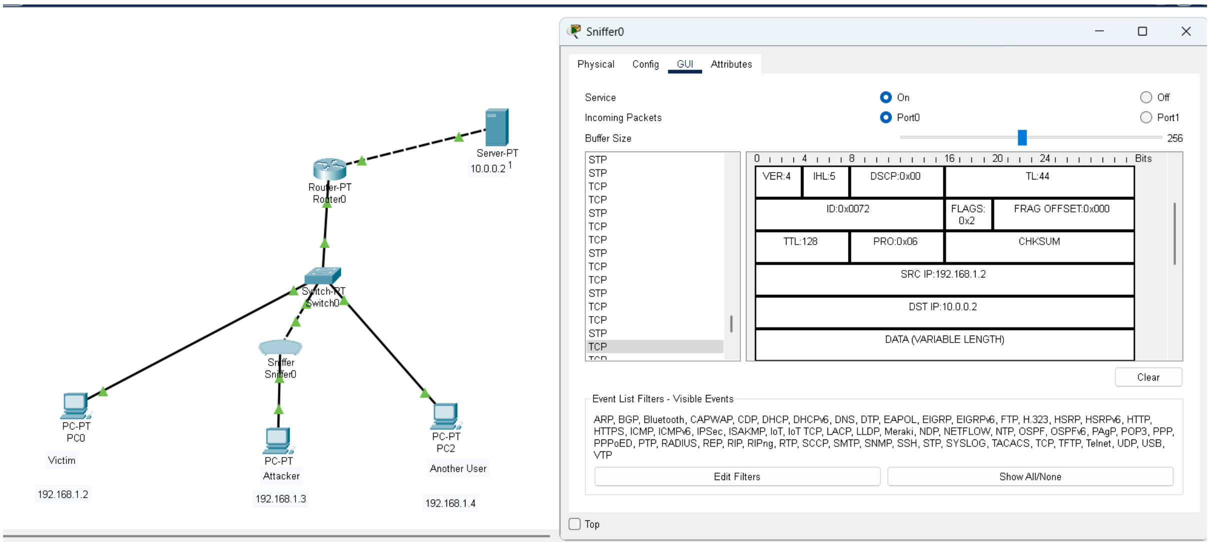
Attacker sents a ping request to victim:

```
C:\>ping -t 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 15, Received = 15, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 0ms
```

```
Switch#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000a.f3e3.ad02    DYNAMIC      Fa3/1
   1    000c.cf86.c217    DYNAMIC      Fa0/1
```

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           000a.f3e3.ad02        dynamic
  192.168.1.3           000a.f3e3.ad02        dynamic
  192.168.1.4           0030.a392.b51d        dynamic
```

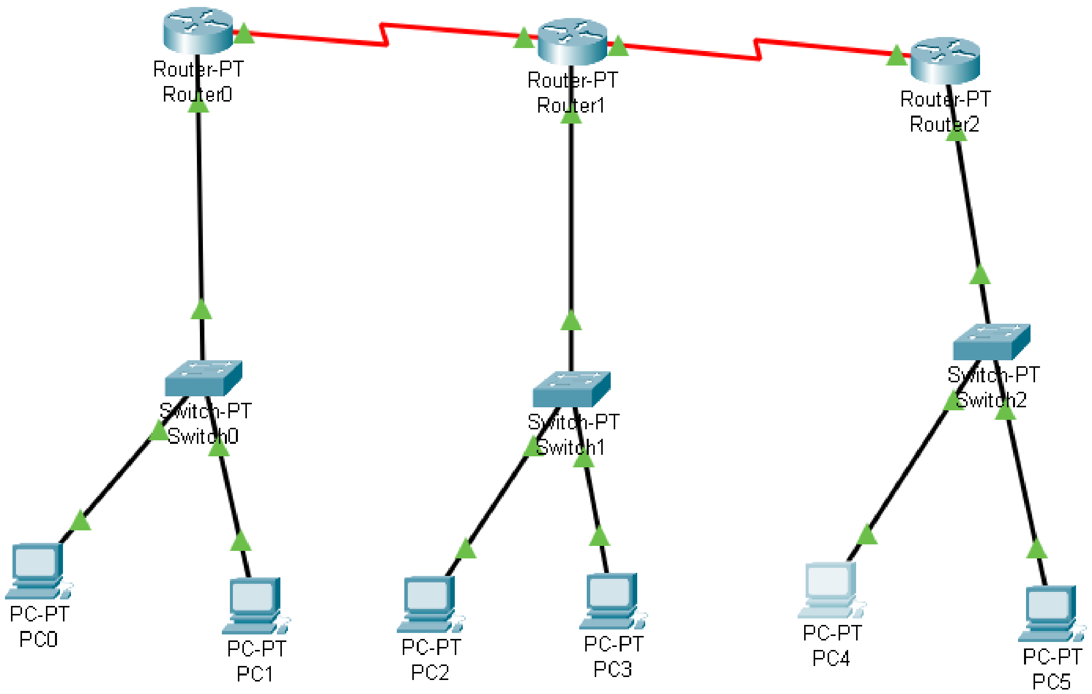
Now you can see that Attacker spoofed the ARP request and spoofed the mac address of the router as its address.So all the requests sent by the Victim to the server also been sent to the attacker id's.



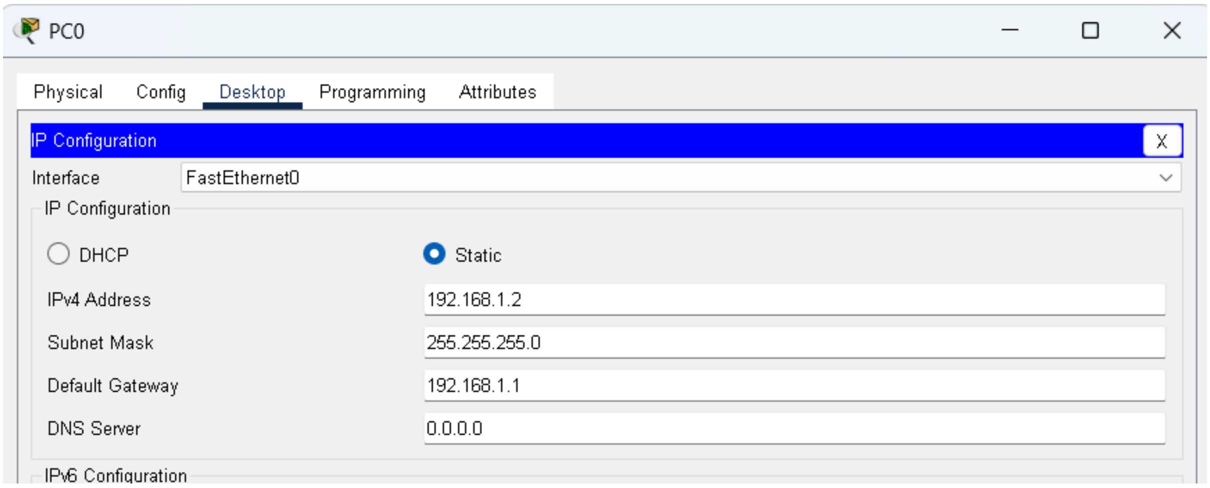
Now if you see if the Victim(192.168.1.2) tries to access the server via router get rerouted to the Attacker's id,So the Attacker can read the data from tha PC0(like if its any important details like banking etc..),it can be hacked by the attacker.So there will be not reliable network connectivity between devices.There will be unstable network connectivity.So the Victim device updates its ARP table with wrong information which can lead to the re-routing to the attacker's id.

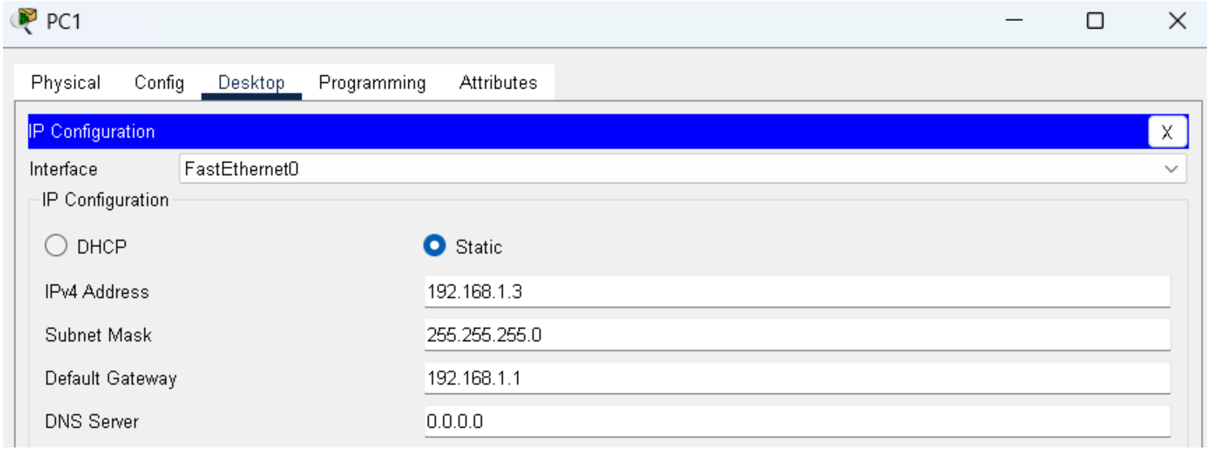
3. Manually configure static IPs on the client devices(like Pc or your mobile phone) and verify connectivity using Ping.

Solution:

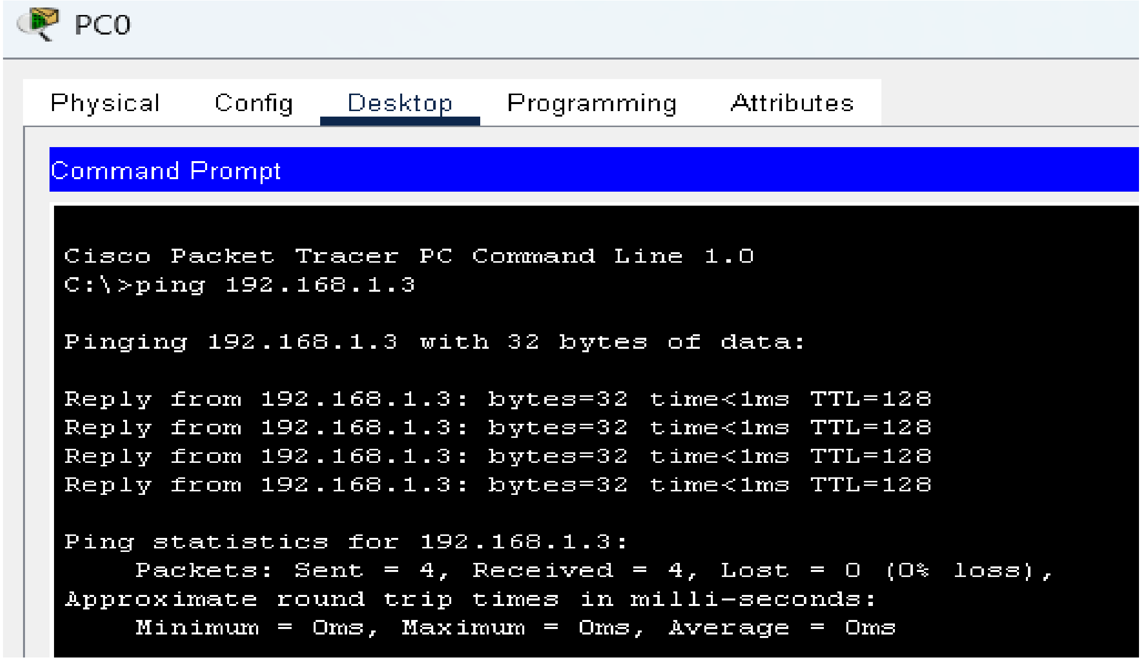


Statically configuring the IP's of all the PC Devices





Pinging to internal subnet:



Pinging to external subnet:

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=32ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 32ms, Average = 12ms
```

Hence we manually configured the static IP's and statically add the entries in router using ip route command.

4. Use Wireshark to capture DHCP Discover, Offer, Request, and Acknowledge messages and explain the process.

Solution:

Basically DHCP Server Assigns IP Addresses dynamically rather than static.It consists of four step process.

Step 1 ----> When a client connected to the network,It broadcasts the DHCP discover message to find the DHCP Server.This step is called **Discovery.**

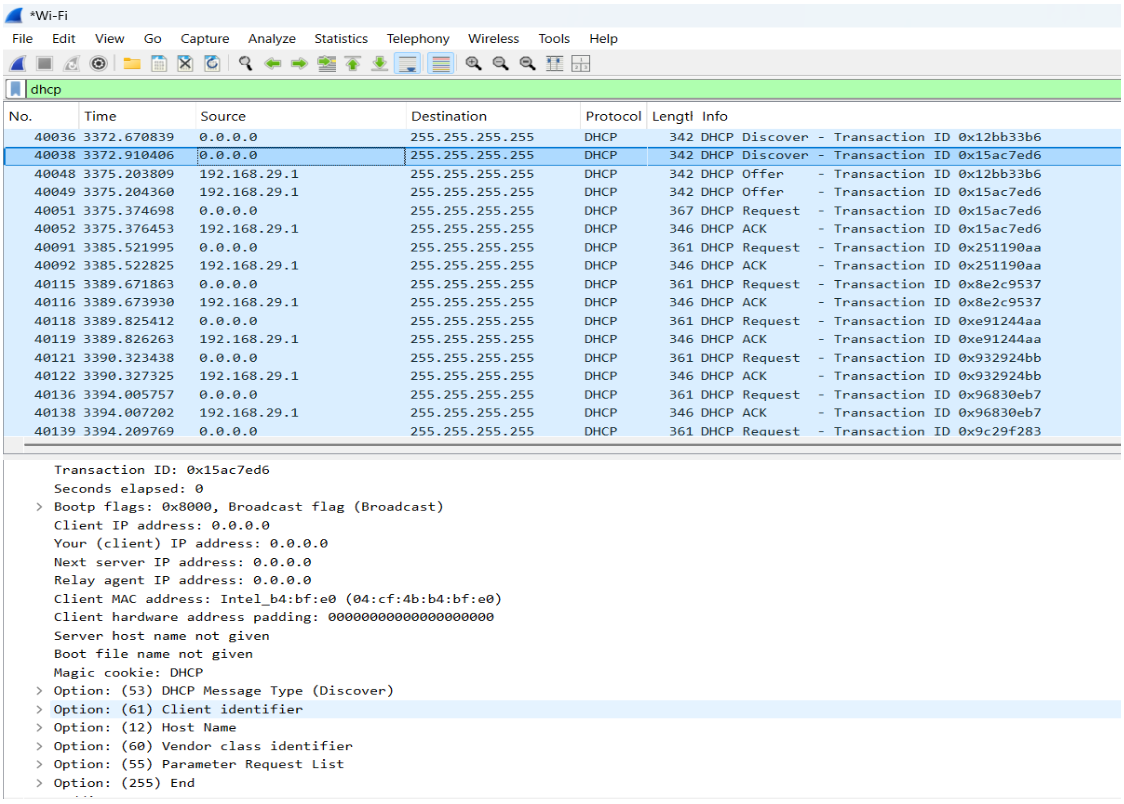
Step 2 ----> Then the DHCP Server replies with DHCPOFFER to assigning a available ip addresses.This step is called **Offer.**

Step 3 -----> Then the client replies back with DHCPREQUEST to accept the assigned IP Address and wants to use with the assigned settings. It is broadcast message.This step is called as **REQUEST**

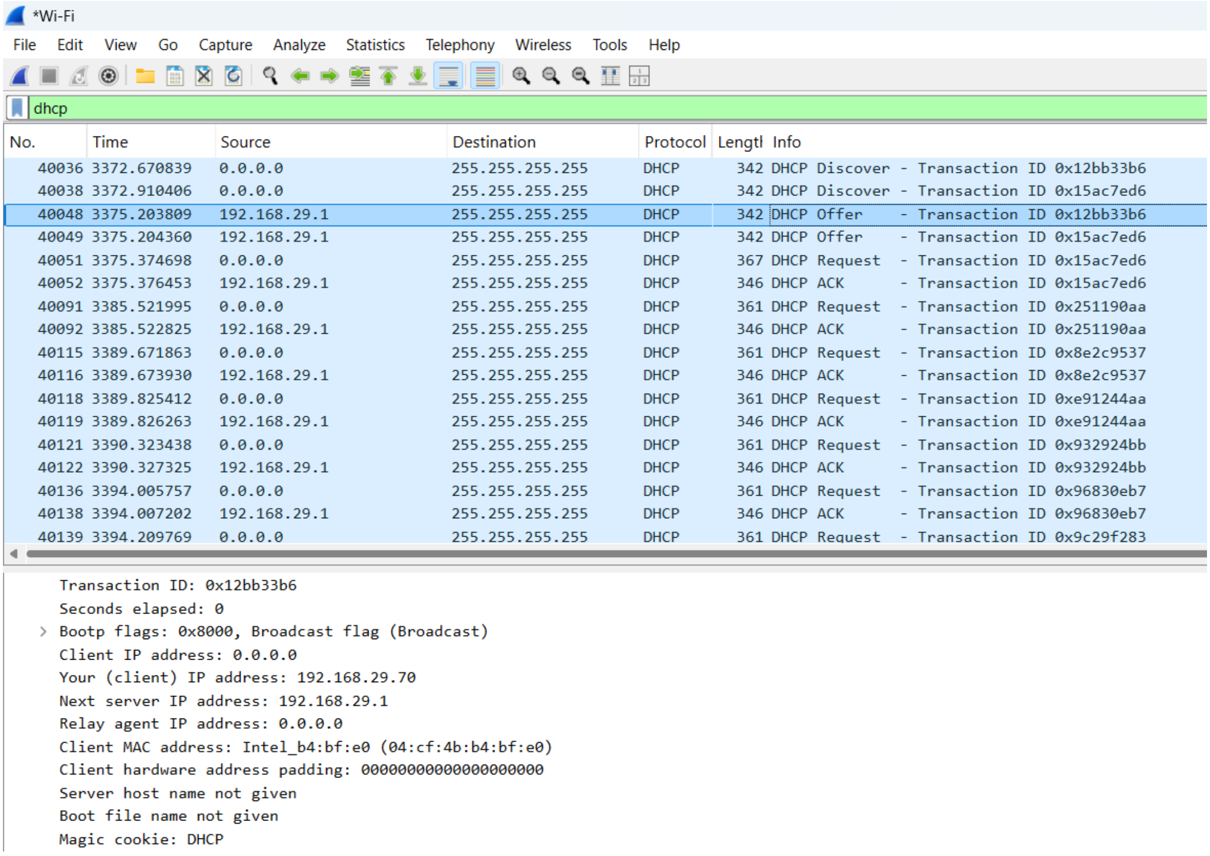
Step 4 -----> Then the DHCP Server acknowledges the message and sends the message to confirm the IP Address and the other configurable network settings.This step is called as **ACKNOWLEDGEMENT**.

It is the DORA Process.

Step 1:



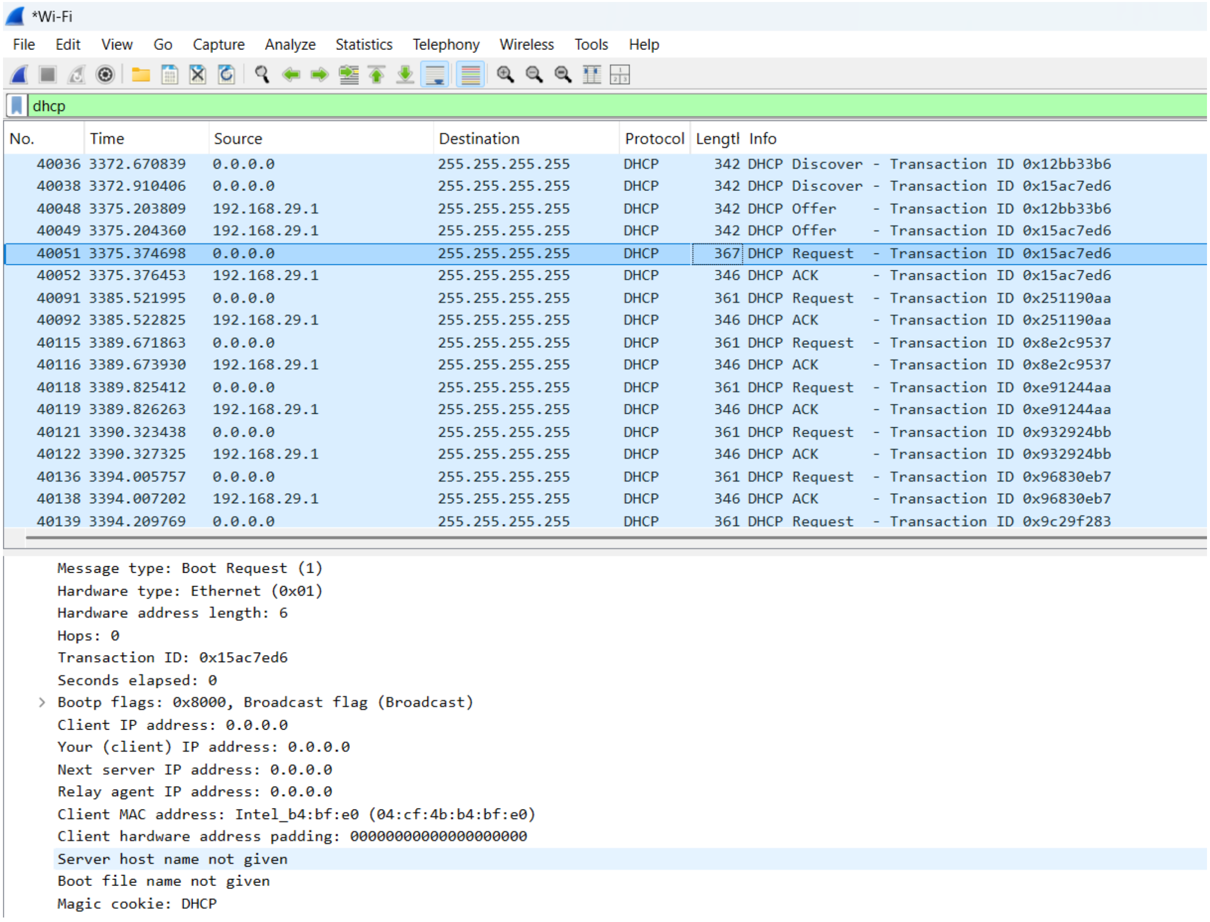
In step 1: The client who wants a IP Address broadcasts the DHCP DISCOVER message.In this packet,The client ip address:0.0.0.0(yet to assign).Next DHCP Server Address:0.0.0.0(client does'nt know about the address of the DHCP Server),Client MAC Address (it broadcasts its mac address to all the devices)



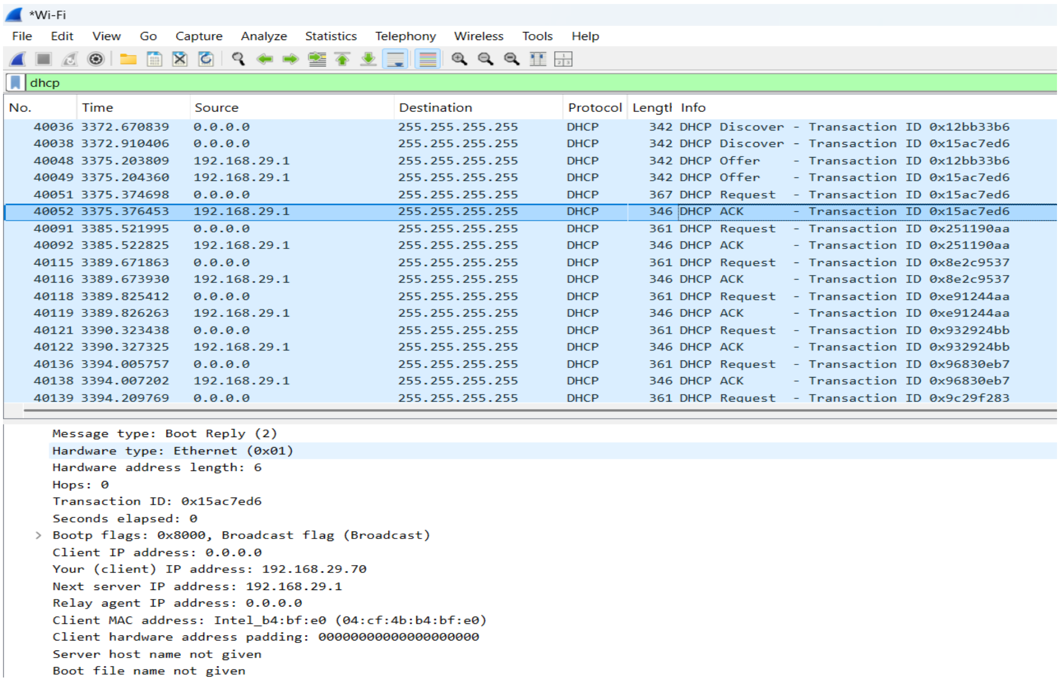
No.	Time	Source	Destination	Protocol	Lengtl	Info
40036	3372.670839	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x12bb33b6
40038	3372.910406	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x15ac7ed6
40048	3375.203809	192.168.29.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x12bb33b6
40049	3375.204360	192.168.29.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x15ac7ed6
40051	3375.374698	0.0.0.0	255.255.255.255	DHCP	367	DHCP Request - Transaction ID 0x15ac7ed6
40052	3375.376453	192.168.29.1	255.255.255.255	DHCP	346	DHCP ACK - Transaction ID 0x15ac7ed6
40091	3385.521995	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0x251190aa
40092	3385.522825	192.168.29.1	255.255.255.255	DHCP	346	DHCP ACK - Transaction ID 0x251190aa
40115	3389.671863	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0x8e2c9537
40116	3389.673930	192.168.29.1	255.255.255.255	DHCP	346	DHCP ACK - Transaction ID 0x8e2c9537
40118	3389.825412	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xe91244aa
40119	3389.826263	192.168.29.1	255.255.255.255	DHCP	346	DHCP ACK - Transaction ID 0xe91244aa
40121	3390.323438	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0x932924bb
40122	3390.327325	192.168.29.1	255.255.255.255	DHCP	346	DHCP ACK - Transaction ID 0x932924bb
40136	3394.005757	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0x96830eb7
40138	3394.007202	192.168.29.1	255.255.255.255	DHCP	346	DHCP ACK - Transaction ID 0x96830eb7
40139	3394.209769	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0x9c29f283

```
Transaction ID: 0x12bb33b6
Seconds elapsed: 0
> Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.29.70
Next server IP address: 192.168.29.1
Relay agent IP address: 0.0.0.0
Client MAC address: Intel_b4:bf:e0 (04:cf:4b:b4:bf:e0)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
```

In step 2: The DHCP Server sents a DHCP OFFER to the requested client which contains the IP Address of the client.This IP Address will be assigned from the pool of IP's which DHCP possess.It's a unicast message since the mac address of the client is available in the DHCP DISCOVER Packet.



In step 3: The client replies back with DHCP REQUEST packet to accept the assigned IP Address.



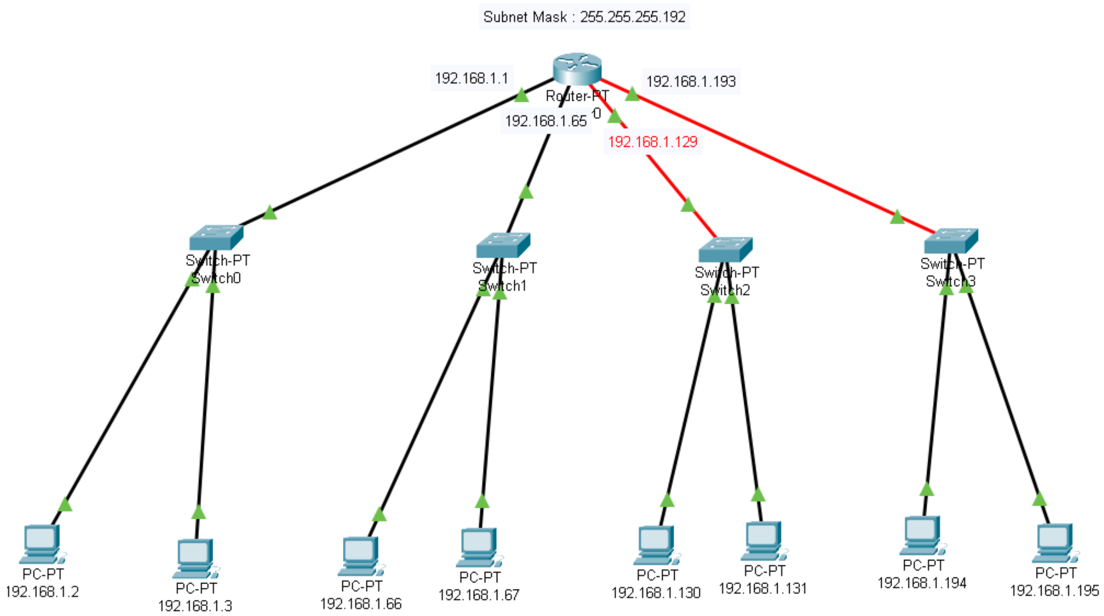
In step 4: The Server acknowledges the message and confirms the IP Address.

6. Given an IP address range of 192.168.1.0/24, divide the network into 4 subnets.

Task: Manually calculate the new subnet mask and the range of valid IP addresses for

each subnet.Assign IP addresses from these subnets to devices in Cisco Packet Tracer and verify connectivity using ping between them.

Solution:



Subnet Assignements:

Since we need to split into 4 different subets for 192.168.1.0/24

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 :

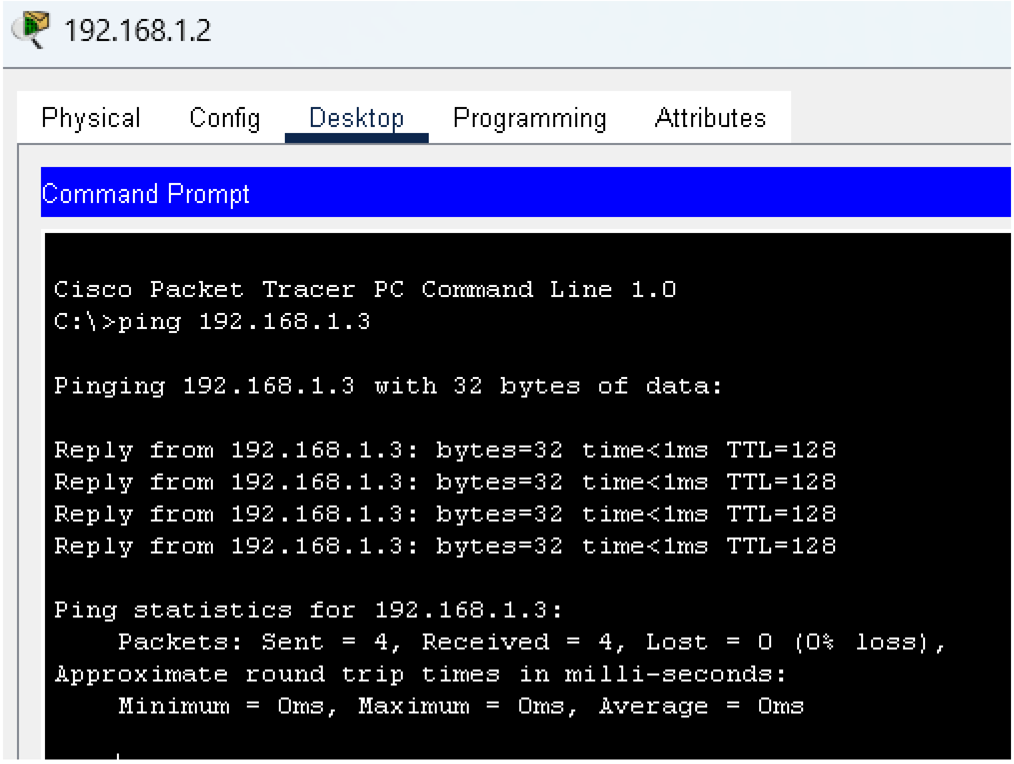
Subnet 1 ----> 192.168.1.0 is given for identifying network ,192.168.1.1for the default gateway and 192.168.1.63 for broadcasting.So the valid range is 192.168.1.2 – 192.168.1.62.

Subnet 2 ---->192.168.1.64 is given for identifying network ,192.168.1.65 for the default gateway and 192.168.1.127 broadcasting.So the valid range is 192.168.1.66-192.168.1.126.

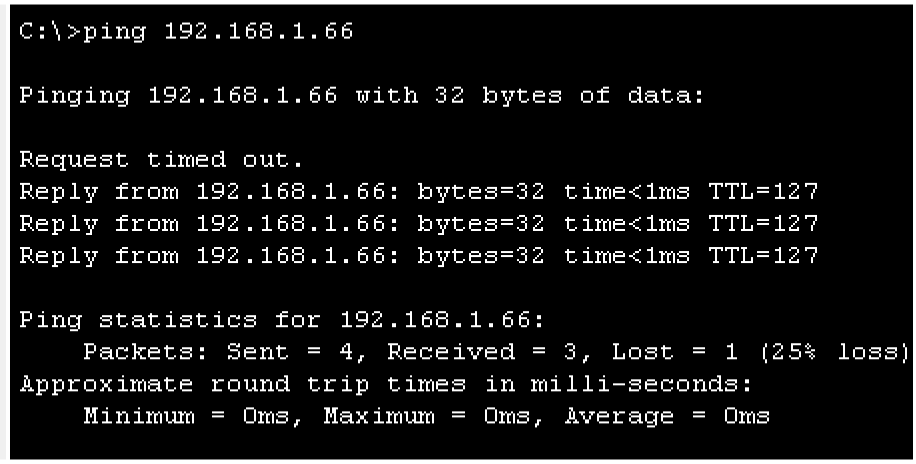
Subnet 3 ----> 192.168.1.128 is given for identifying network , 192.168.1.129 for the default gateway and 192.168.1.191 for broadcasting . So the valid range is 192.168.1.130-192.168.1.190.

Subnet 4----> 192.168.1.192 is given for identifying network , 192.168.1.193 for the default gateway and 192.168.1.255 for broadcasting . So the valid range is 192.168.1.193-192.168.1.254.

Pinging to Internal Subnet:



Pinging to 2nd Subnet:



Pinging to 3rd Subnet:

```
C:\>ping 192.168.1.131

Pinging 192.168.1.131 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.131: bytes=32 time<1ms TTL=127
Reply from 192.168.1.131: bytes=32 time<1ms TTL=127
Reply from 192.168.1.131: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.131:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pinging to 4th Subnet:

```
C:\>ping 192.168.1.194

Pinging 192.168.1.194 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.194: bytes=32 time<1ms TTL=127
Reply from 192.168.1.194: bytes=32 time<1ms TTL=127
Reply from 192.168.1.194: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.194:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Hence the ping is successful to all other subnets ensuring the network connectivity between them.

6. You are given three IP addresses: 10.1.1.1, 172.16.5.10, and 192.168.1.5.

Task: Identify the class of each IP address (Class A, B. or C). What is the default subnet mask for each class?Provide the range of IP addresses for each class.

Solution:

IP Address --------> 10.0.0.1

- 10.0.0.1 falls under Class A range.
- Default Subnet Mask – 255.0.0.0
- Range – 1.0.0.0 to 126.255.255.255

IP Address---------> 172.16.5.10

- 172.16.5.10 falls under Class B Range
- Default Subnet mask – 255.255.0.0

- Range – 128.0.0.0 to 191.255.255.255

IP Address -----------> 192.168.1.5

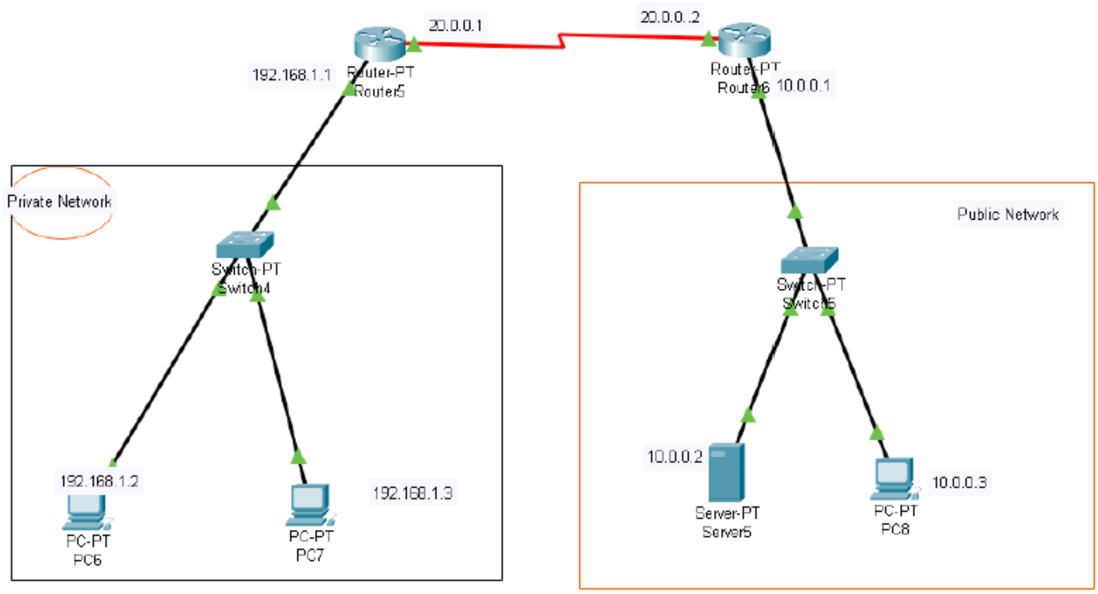
- 192.168.1.5 falls under Class C category
- Default Subnet mask – 255.255.255.0
- Range – 192.0.0.0 to 223.255.255.255

7. In Cisco Packet Tracer, create a small network with multiple devices (e.g., 2 PCs and a router). Use private IP addresses (e.g., 192.168.1 .x) on the PCs and configure the router to perform NAT to allow the PCs to access the internet.

Task: Test the NAT configuration by pinging an external IP address from the PCs and capture the traffc using Wireshark.

What is the source IP address before and after NAT?

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.

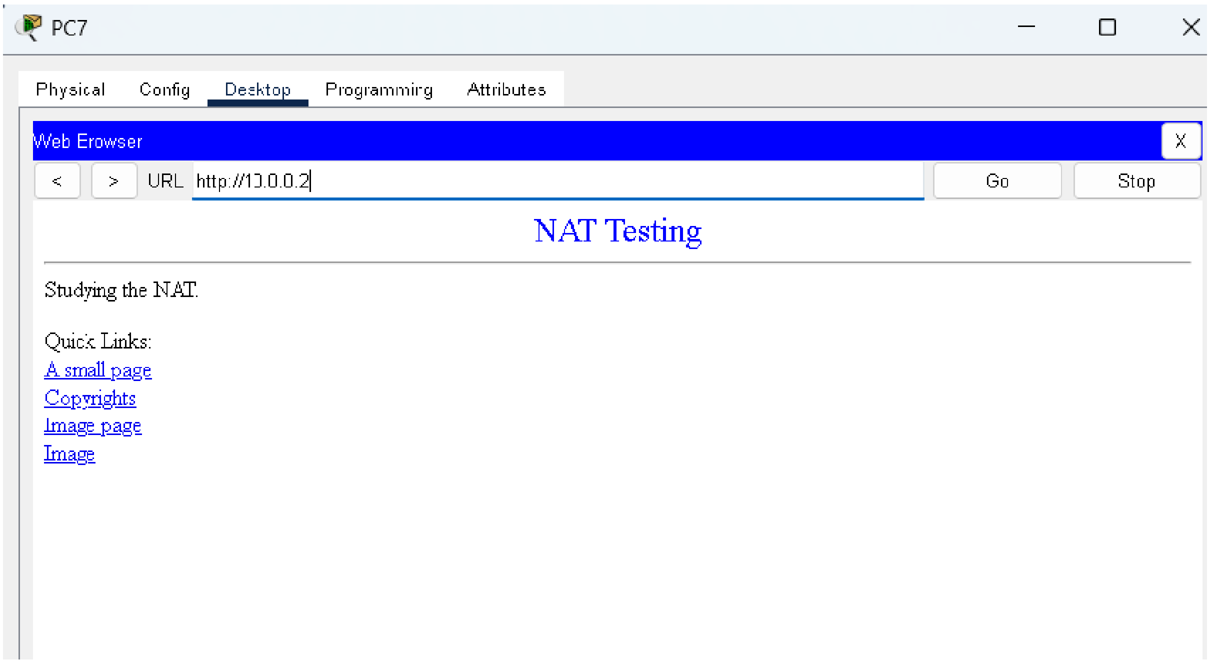
From Public Network to Private Network:

```
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.
```

From Public Network to Private Network,if we tries to ping to the Public IP 20.0.0.1 it gets successful.But if we tries 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)#ipiip 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:

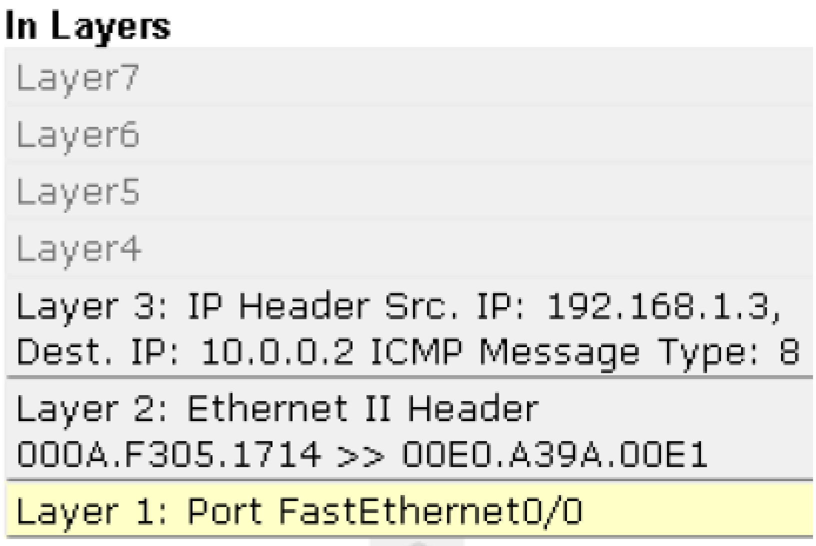
```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 20.0.0.1:29       192.168.1.3:29     10.0.0.2:29        10.0.0.2:29
icmp 20.0.0.1:30       192.168.1.3:30     10.0.0.2:30        10.0.0.2:30
icmp 20.0.0.1:31       192.168.1.3:31     10.0.0.2:31        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
```

Inside local – Private LAN Network,**Inside Global –** After converting to Public IP

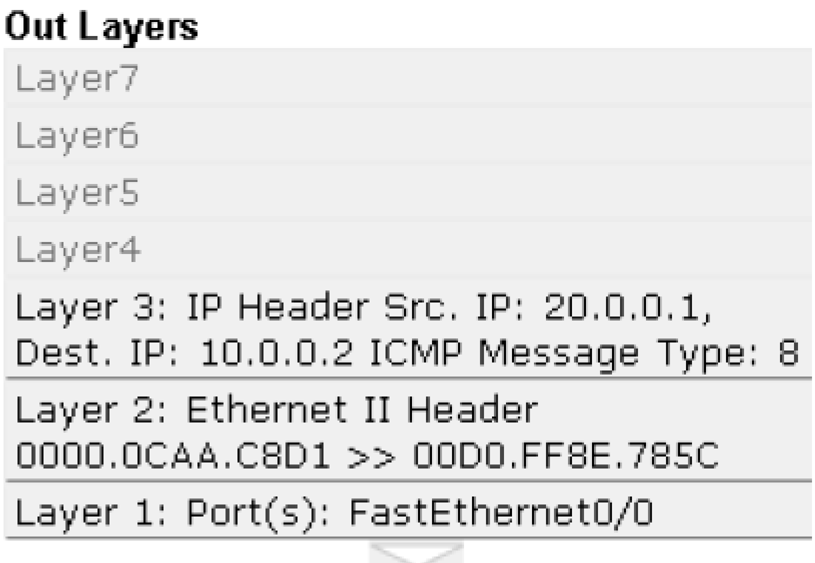
Outside local – External IP address as seen from the local Network

Outside Global – Public IP of the Server which we tries to access.

Before the Router performs NAT:



After the Router Performs NAT:



Before NAT Source IP : 192.168.1.3

After NAT Source IP : 20.0.0.1

Translation of Private IP to the Public IP.

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