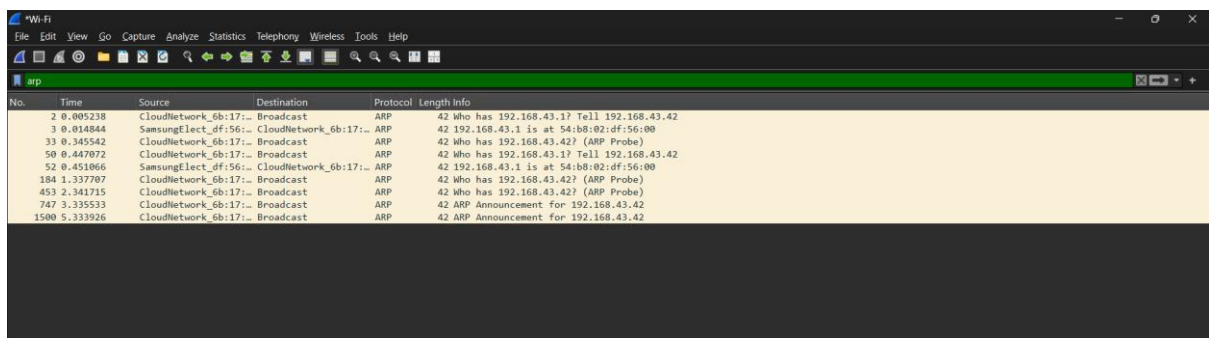


Networking Training Program Module 5

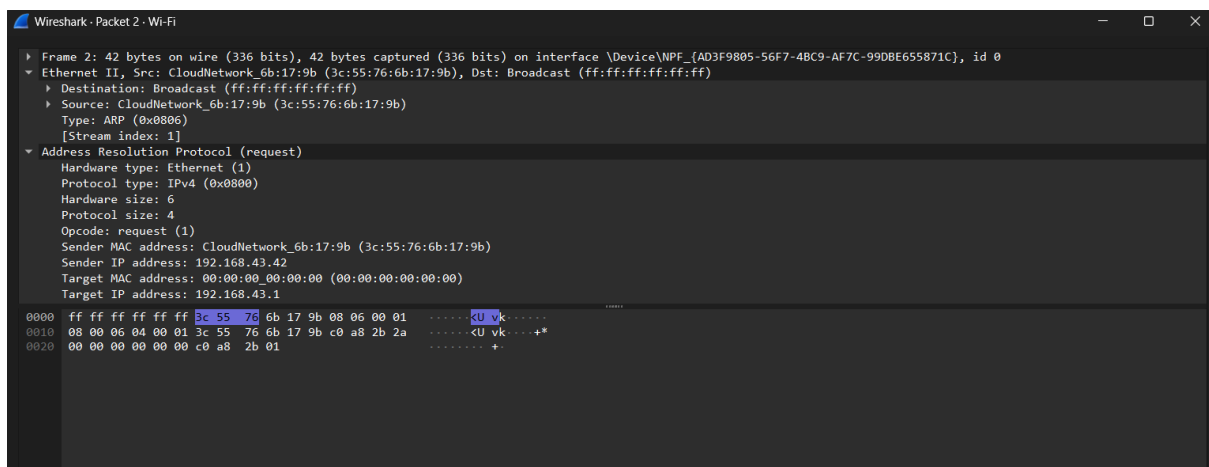
1.) Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.

ARP Packets were captured in the WIFI interface using wireshark



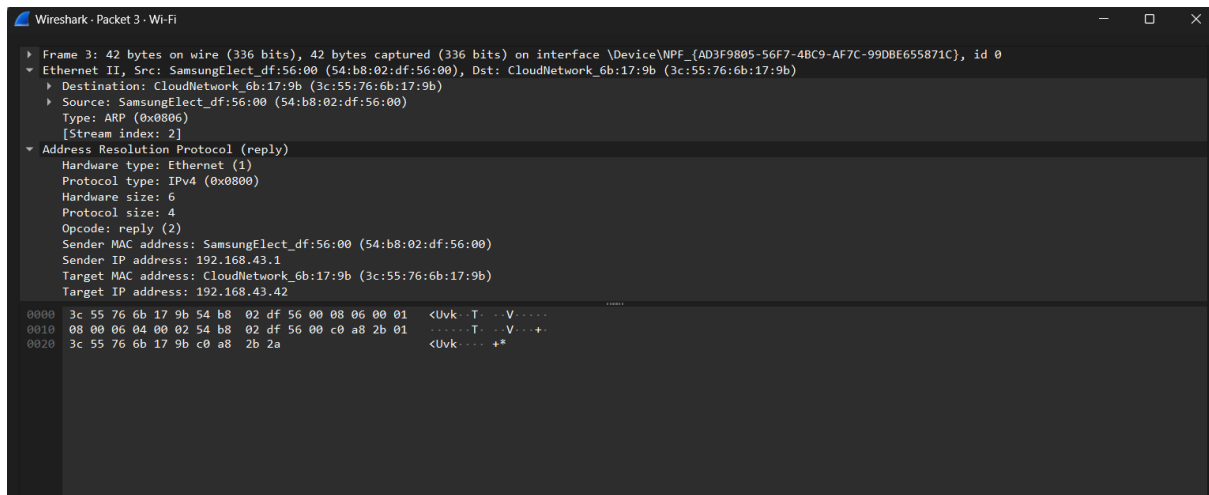
No.	Time	Source	Destination	Protocol	Length	Info
2	0.005238	CloudNetwork_6b:17:...	Broadcast	ARP	42	Who has 192.168.43.1? Tell 192.168.43.42
3	0.014844	SamsungElect_df:56:...	CloudNetwork_6b:17:...	ARP	42	192.168.43.1 is at 54:b8:02:df:56:00
33	0.345542	CloudNetwork_6b:17:...	Broadcast	ARP	42	Who has 192.168.43.42? (ARP Probe)
50	0.447072	CloudNetwork_6b:17:...	Broadcast	ARP	42	Who has 192.168.43.1? Tell 192.168.43.42
52	0.451066	SamsungElect_df:56:...	CloudNetwork_6b:17:...	ARP	42	192.168.43.1 is at 54:b8:02:df:56:00
184	1.337707	CloudNetwork_6b:17:...	Broadcast	ARP	42	Who has 192.168.43.42? (ARP Probe)
453	2.341715	CloudNetwork_6b:17:...	Broadcast	ARP	42	Who has 192.168.43.42? (ARP Probe)
747	3.335533	CloudNetwork_6b:17:...	Broadcast	ARP	42	ARP Announcement for 192.168.43.42
1500	5.333926	CloudNetwork_6b:17:...	Broadcast	ARP	42	ARP Announcement for 192.168.43.42

- Now, let us analyse the frames, the first frame is the broadcast frame



Wireshark - Packet 2 - Wi-Fi	
Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{AD3F9805-56F7-48C9-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)	
Target IP address: 192.168.43.1	
0000	ff ff ff ff ff ff 3c 55 76 6b 17 9b 08 06 00 01<U vk.....
0010	08 00 06 04 00 01 3c 55 76 6b 17 9b c0 a8 2b 2a<U vk....+*
0020	00 00 00 00 00 00 c0 a8 2b 01+.....

- Since it is an ARP request the packet is broadcasted notice that there is an Target ip addr but not any target MAC address it is all 00s indicating that this is an broadcasted ARP request packet.

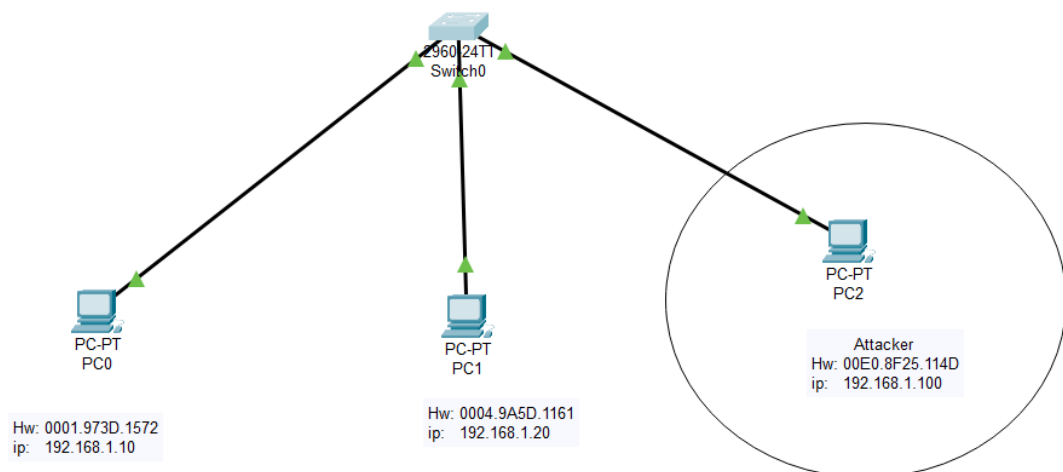


This is the ARP response packet and it can be noticed that here the packet is unicast to the ARP requested host by the device which had the target ip in the previous ARP request packet.

- Sender's ip and Sender's MAC address is given in the ARP request packet because then the host machine could just reply as an unicast frame to the device which send the ARP request.

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

- Below is a network with 3 PCs all connected with a switch



- Now after ping between the legitimate PCs the ARP table in PC0 is displayed below

```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.20          0004.9a5d.1161        dynamic
C:\>|
```

Let us now try to perform ARP spoofing using the attackers pc

- ARP spoofing was unable to be performed in the Cisco packet tracer.

It only has two possible options

arp -a -> it displays the arp table

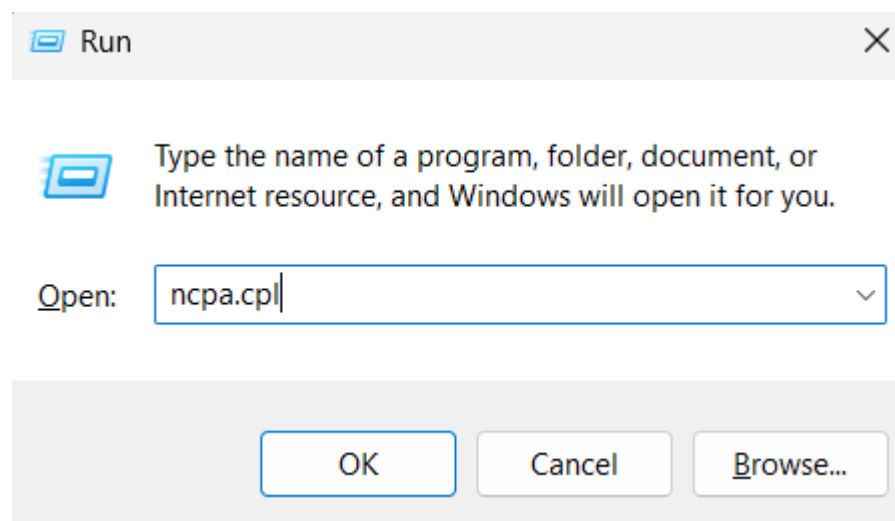
arp -d ->it clears arp table

This was the command that was tried to be executed to perform ARP spoofing.

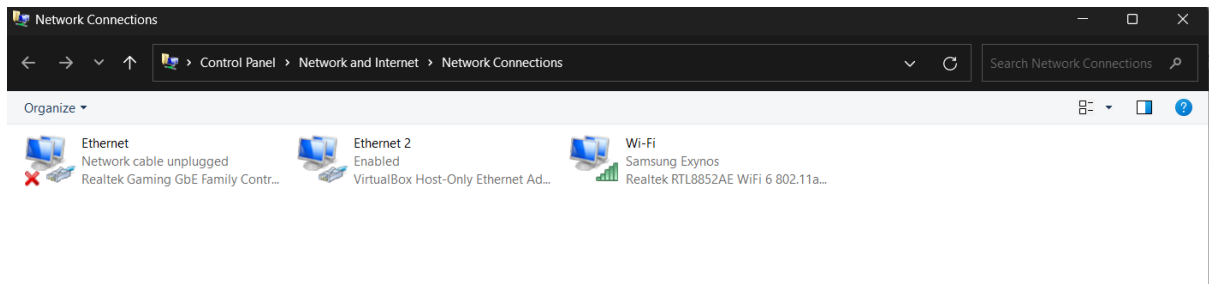
```
C:\>arp -s 192.168.1.20 00E0.8F25.114D
Invalid Command.
```

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

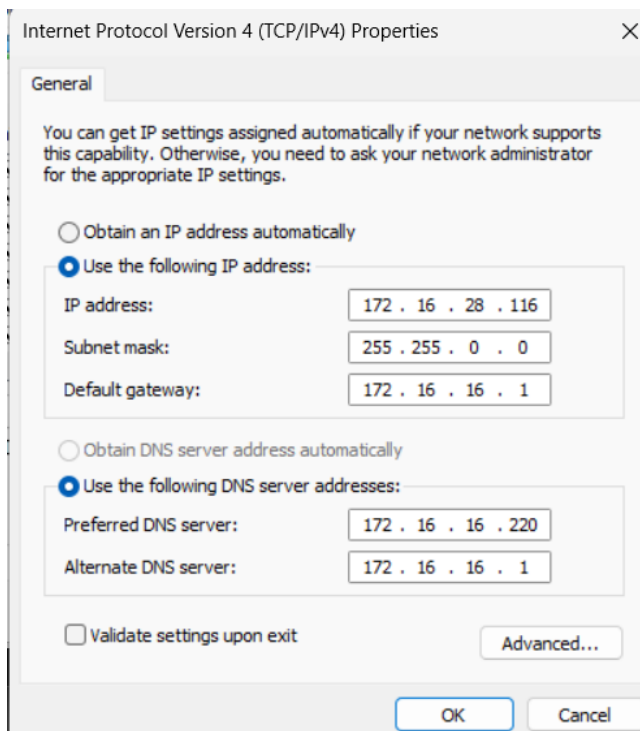
- Manually ip address can be configured in laptops
- Click win +r and then type in ncpa.cpl



- Inside that select the interface in which you would like to configure a static ip



- After then you can click properties and Ipv4 inside it, then a similar box like the one displayed below will be shown



In here we can try pinging the default gateway or other websites to check connectivity.

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

- Using wireshark the DHCP DORA process was captured and the snapshot is attached below.

No.	Time	Source	Destination	Protocol	Length	Info
90	8.222165	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x2ba10393
93	8.228957	10.10.0.1	10.10.5.78	DHCP	342	DHCP ACK - Transaction ID 0x2ba10393
109	8.311849	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1b64fea2
249	9.637208	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xae51dbf8
327	11.241615	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1afa4
367	11.958850	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xdda3da60
380	11.969221	10.10.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xdda3da60
400	12.267411	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xcc547cfb
476	12.781283	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0x8ff36a85
546	12.982695	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1b64fea2
767	13.751243	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0x8ff36a85
980	15.218391	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb2b13388
1031	15.599084	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0x8ff36a85
1065	15.752046	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0xbf64356d
1271	17.779775	0.0.0.0	255.255.255.255	DHCP	349	DHCP Request - Transaction ID 0x685971c6

DORA process:

Discover : The client broadcasts a DHCP discover message as it does not know the ip of DHCP server

Offer : The server offers an ip to the client in an unicast mode

Reply : The client asks for confirmation by broadcasting again to check if it can use the given ip .

Acknowledgement : The server unicasts the same ip again with details such as lease to fulfil the DHCP process.

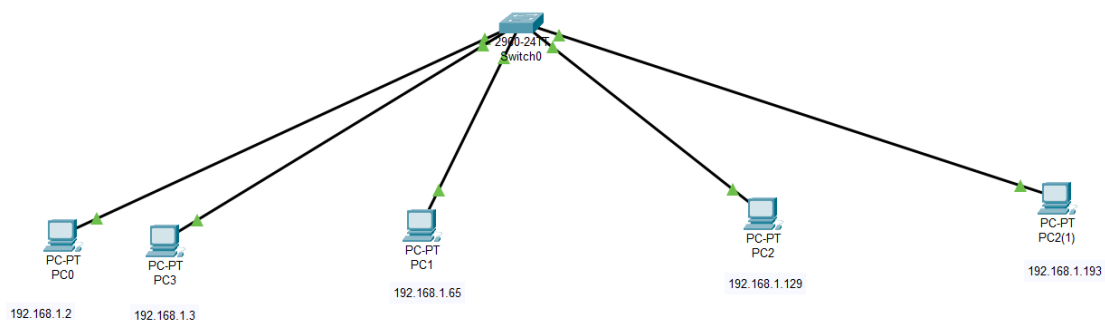
5.) Given an IP address range of 192.168.1.0/24, divide the network into 4 subnets.

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.

S. No.	Subnet Mask	Ip start range	Ip range end
1	255.255.255.192	192.168.1.0	192.168.1.63
2	255.255.255.192	192.168.1.64	192.168.1.127
3	255.255.255.192	192.168.1.128	192.168.1.191
4	255.255.255.192	192.168.1.192	192.168.1.255

- Below is the simulated network



- In this PC0 and PC3 are under a same network the other 3 PCs are under different network each.
- When we ping the PC inside the same network i.e) PC0 to PC3 connectivity is there but for no other PC pair ping works
- The snapshot is attached below

```

PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:

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

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
  
```

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.

- The below table contains all the required details.

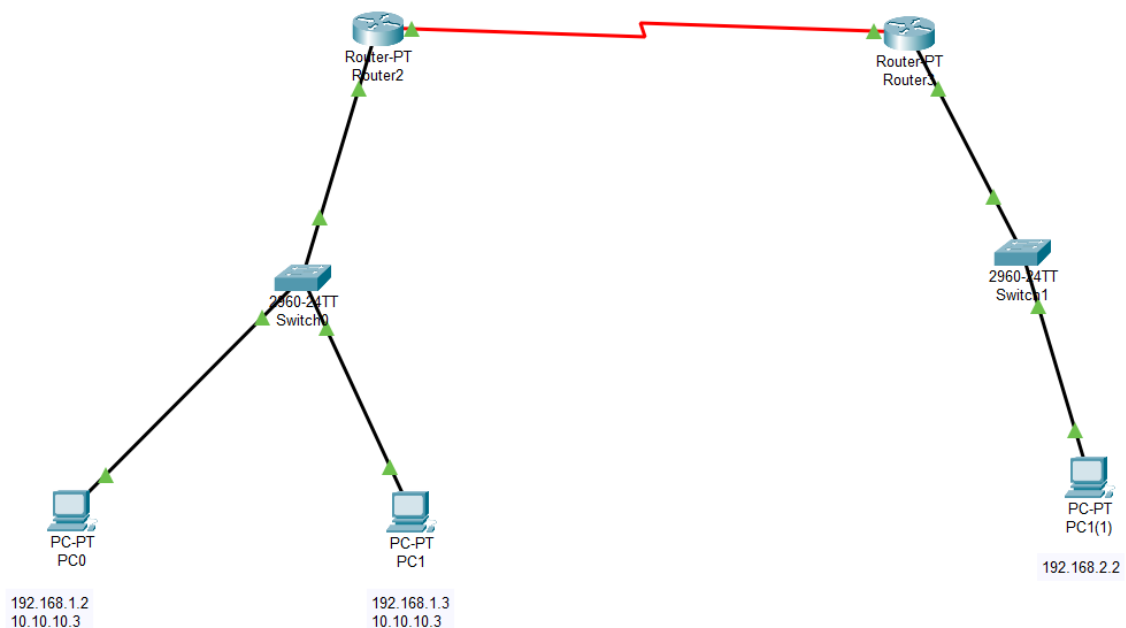
Ip Address	Class	Default Subnet	Range of ip in the class
10.1.1.1	A	255.0.0.0	1.0.0.0 – 127.255.255.255
172.16.5.10	B	255.255.0.0	128.0.0.0 – 191.255.255.255
192.168.1.5	C	255.255.255.0	192.0.0.0 – 223.255.255.255
-	D	-	224.0.0.0 – 239.255.255.255
-	E	-	240.0.0.0 – 255.255.255.255

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 traffic using Wireshark.

What is the source IP address before and after NAT?

- Below is the topology constructed in Cisco Packet Tracer



- From the diagram the first network is configured with NAT inside the router.
- Ping was attempted from the pc with 192.168.2.2 to the PC inside NAT, the following results were observed

```
Cisco Packet Tracer PC Command Line 1.0
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=20ms TTL=126
Reply from 10.10.10.2: bytes=32 time=1ms TTL=126
Reply from 10.10.10.2: bytes=32 time=9ms TTL=126
Reply from 10.10.10.2: bytes=32 time=9ms 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 = 20ms, Average = 9ms

C:\>
```

It can be seen that the reply comes from the public ip address of the device and without the private ip

- This is the NAT table inside the First Router.

```
Router#show ip nat t
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  10.10.10.2          192.168.1.2       ---                ---
---  10.10.10.3          192.168.1.3       ---                ---
Router#
```

Copy Paste

- Before NAT the ip was 192.168.1.2
- After NAT the ip was 10.10.10.2