Lab 1

Computer Networks & Cyber Security

Name : Nada Mohamed Ahmed Hassan Eleshmawy.

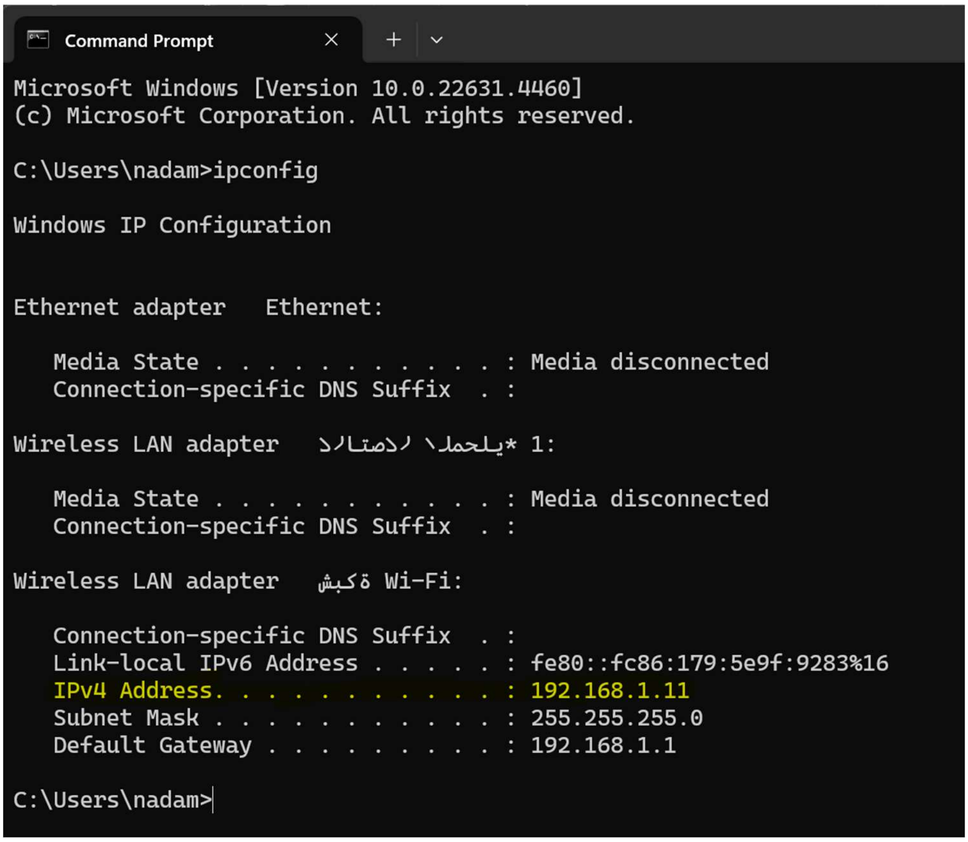
Track : Open Source Mansoura

Q1: explain how to get the private IP?

To know our private IP address :

Open CMD:

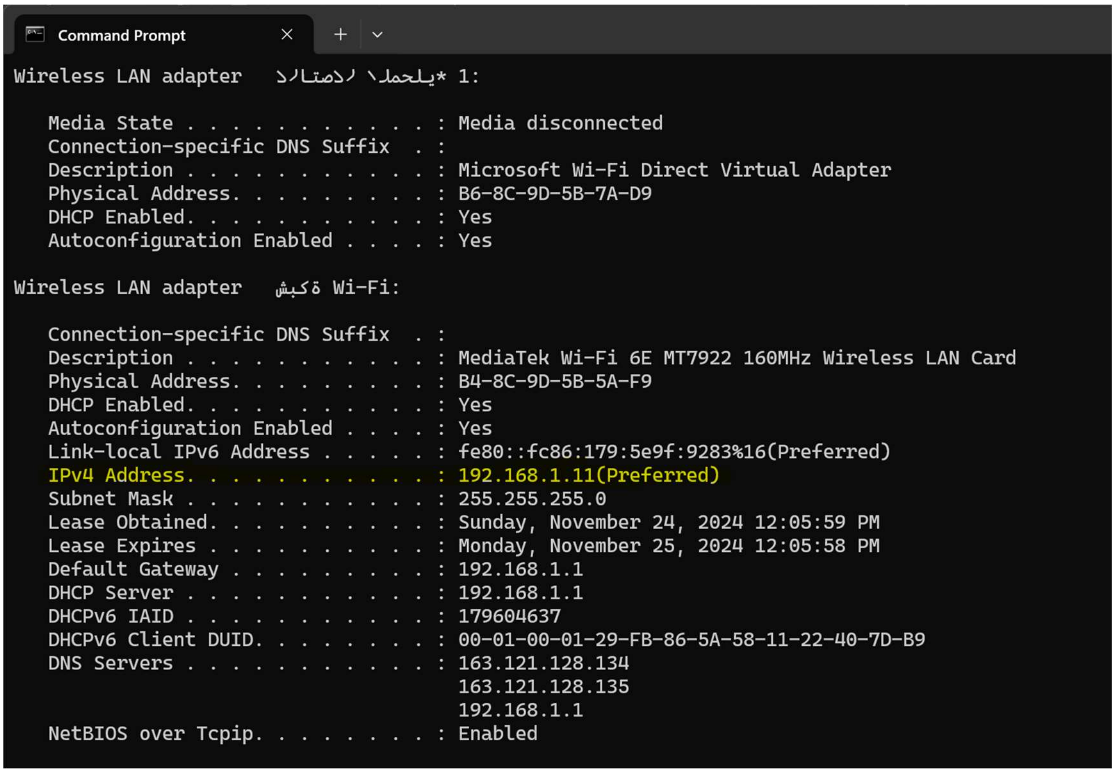
1-Using ipconfig



```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nadam>ipconfig

Windows IP Configuration


Ethernet adapter   Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter   د/اتصد/ \يلحمل* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter   ةكبش Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fc86:179:5e9f:9283%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Users\nadam>
```

Or

2- using ipconfig /all



```
Wireless LAN adapter  لاصتا يلحم* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : B6-8C-9D-5B-7A-D9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter  ةكبش Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6E MT7922 160MHz Wireless LAN Card
   Physical Address. . . . . . . . . : B4-8C-9D-5B-5A-F9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fc86:179:5e9f:9283%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, November 24, 2024 12:05:59 PM
   Lease Expires . . . . . . . . . . : Monday, November 25, 2024 12:05:58 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 179604637
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-FB-86-5A-58-11-22-40-7D-B9
   DNS Servers . . . . . . . . . . . : 163.121.128.134
                                       163.121.128.135
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Note : our private address can be in these ranges only :

10.0.0.0 → 10.255.255.255

172.16.0.0 → 172.31.255.255

192.168.0.0 → 192.168.255 255

Q2: What is the difference between ipconfig & ipconfig/all?

As shown in the previous images :

Ipconfig : show the basic IP configuration like :

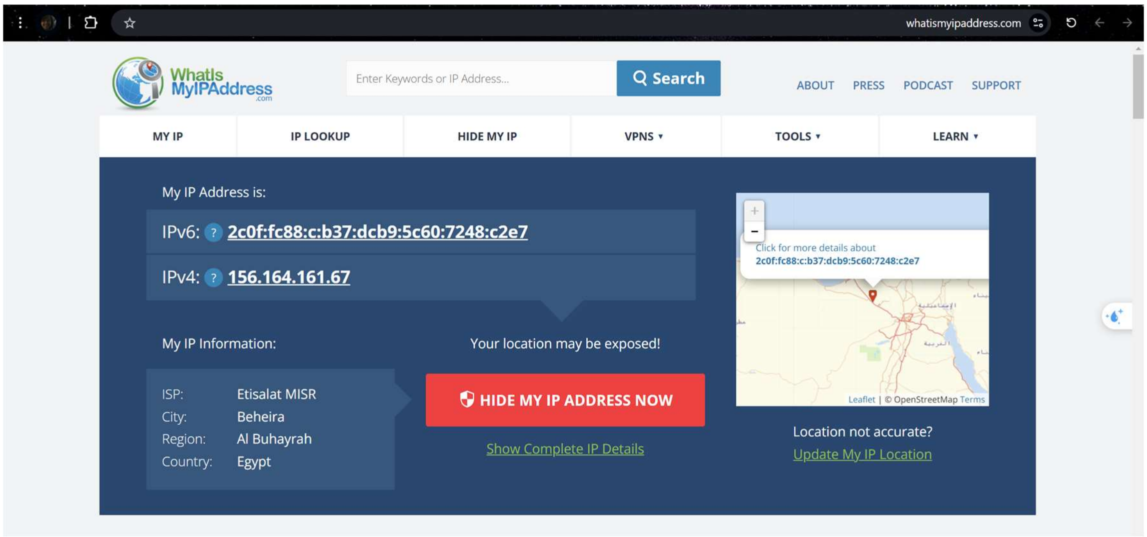
- IPv4 address.
- Subnet mask.
- Default gateway.

But **Ipconfig/all :** show details about all the network like :

- All information appear in **Ipconfig**
- DNS servers.
- DHCP Server.
- MAC address (Physical Address).
- DHCP status (Enabled/Disabled).
- DHCP lease information (Lease Obtained and Lease Expires).
- And More information

Q3: explain how to get the public IP?

To know our public IP address we can go to this website : https://whatismyipaddress.com/



My IP Address is:

IPv6: 2c0f:fc88:c:b37:dcb9:5c60:7248:c2e7

IPv4: 156.164.161.67

My IP Information:

ISP: Etisalat MISR
City: Beheira
Region: Al Buhayrah
Country: Egypt

Your location may be exposed!

Click for more details about 2c0f:fc88:c:b37:dcb9:5c60:7248:c2e7

Location not accurate?

Public IP addresses are assigned by **Internet Service Providers (ISPs).**

We use NAT to allows multiple devices on a local network to share a single public IP address.

It translates private IP addresses to a public one, making it possible for devices to communicate with external networks.

Q4: What is the difference between public IP & private IP?

What is the difference between public IP & private IP?

Public IP Address

- Public IP addresses are **visible** to anyone on the **internet** , used for communication over the internet.
- They are assigned by my **Internet Service Provider (ISP).**
- Each public IP address is unique across **the internet.**

Private IP Address

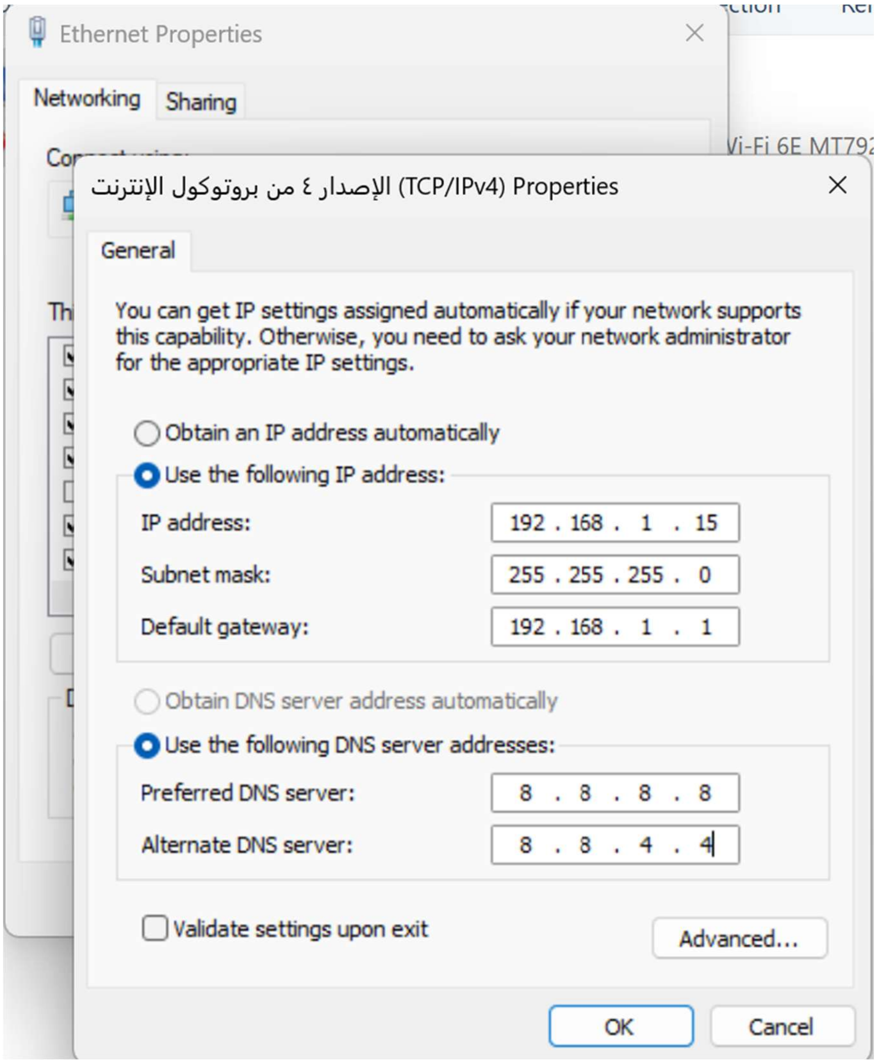
- Private IP addresses are **only visible** in the **local network ,** used for communication within a local network.
- They are assigned by our **router**.
- Each private IP address is unique within **its local network** (but can be reused in different local networks).

Q5: How does the device get its IP?

To assign IP address to device we have 3 ways :

1- Manually (static IP) .
Write IP address, subnet mask, gateway, and DNS server information.

- Open network setting .
- Select internet protocol version 4 (TCP/IPV4).
- Choose manual configuration as following:



الإصدار ٤ من بروتوكول الإنترنت (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 1 . 15
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

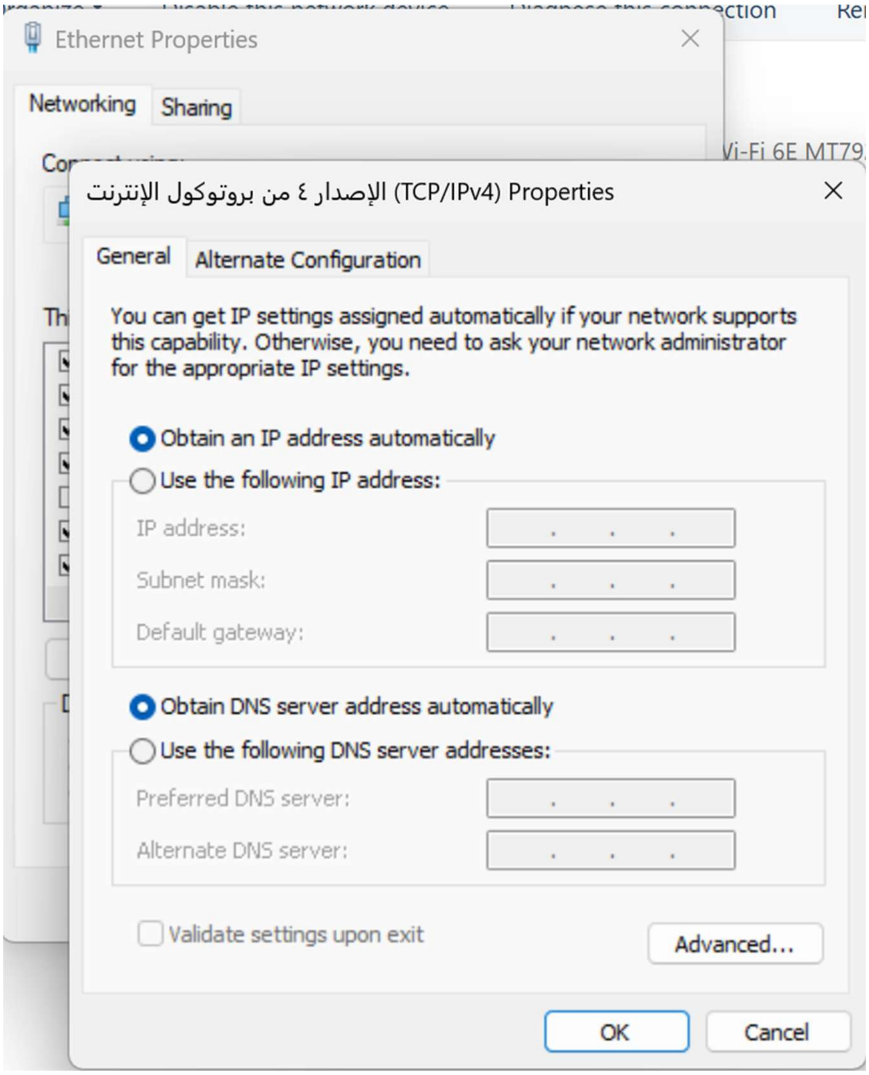
Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	8 . 8 . 4 . 4

□ Validate settings upon exit

2- **Automatic** (Dynamic IP)
Using a DHCP server (our router has this serves)

- When a device connects to a network.
- It sends a request to the DHCP server.
- The DHCP server assigns an available IP address to the device.
- This process is automatic and ensures that each device on the network has a unique IP address.

To apply chose the first option in the above image.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

3- APIPA (Automatic Private IP Addressing)

- If a device cannot obtain an IP address from a DHCP server (no DHCP server) and does not have a static IP configured → it may use APIPA.
- This allows the device to assign itself an IP address in the range of 169.254.0.1 → 169.254.255.254, enabling limited network communication within the local network.

Q6: Make your device get its private IP statically

- Open network setting.
- Select internet protocol version 4 (TCP/IPV4).
- Choose manual configuration and write
  - IP address
  - subnet mask
  - gateway
  - DNS server information.

Q7: Reset your device to get its private IP automatically

- Open network setting.
- Select internet protocol version 4 (TCP/IPV4).
- Choose **obtain IP address automatically**
- This include
  Host IP– Subnet mask– Default Gateway– DNS server IP– Lease Time

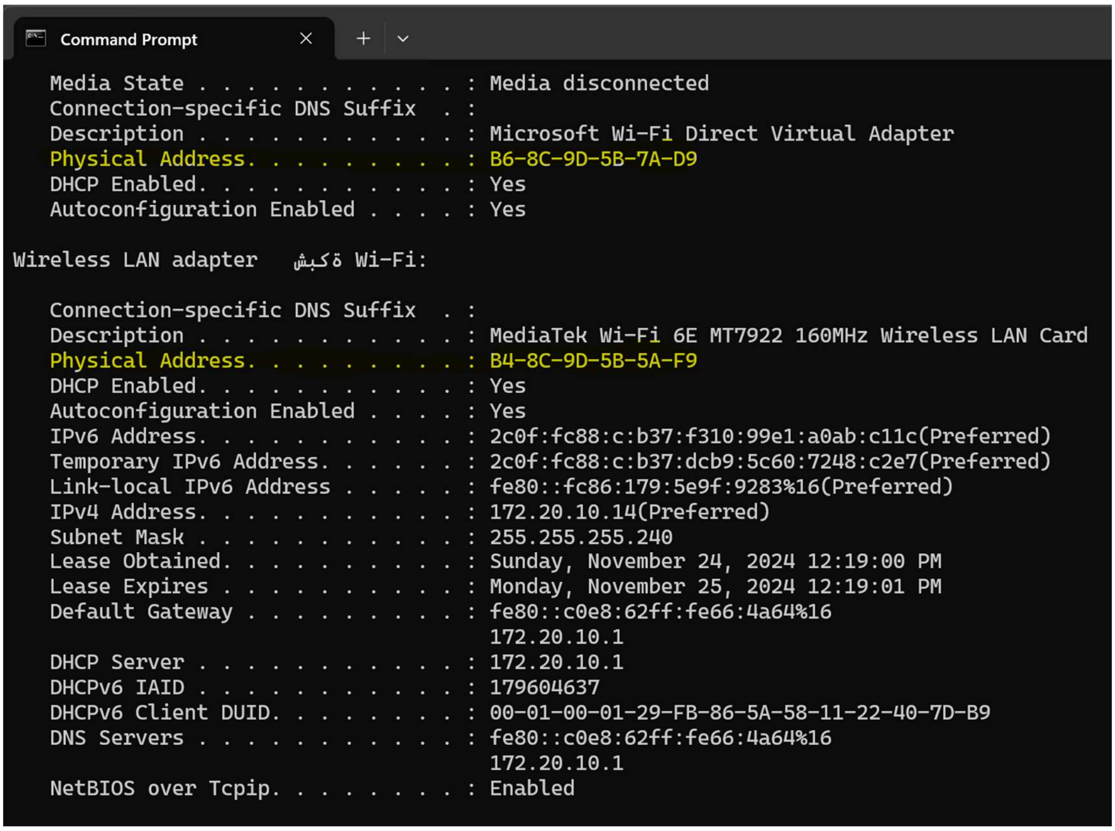
Q8: What do you know about APIPA Address ?

APIPA (Automatic Private IP Addressing) is a feature used by devices to assign themselves an IP address when they cannot obtain one from a DHCP server (no DHCP server available).

- APIPA assigns IP addresses in the range of 169.254.0.1 → 169.254.255.254.
- It allows devices to communicate within a local network even if the DHCP server is unavailable.
- APIPA addresses are not routable on the internet, so they can only be used for **local network communication**.

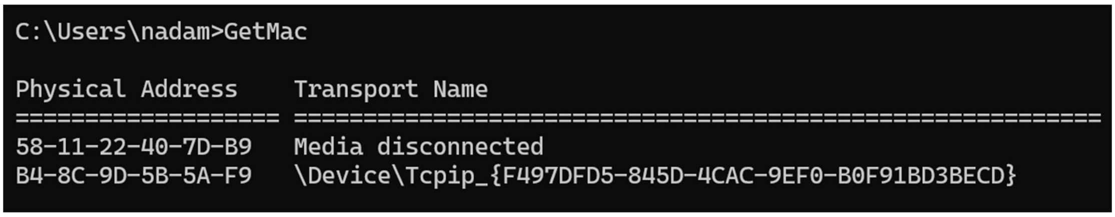
Q9: Give me 2 ways to find out your device's MAC address.

First we can use **ipconfig /all** as shown above



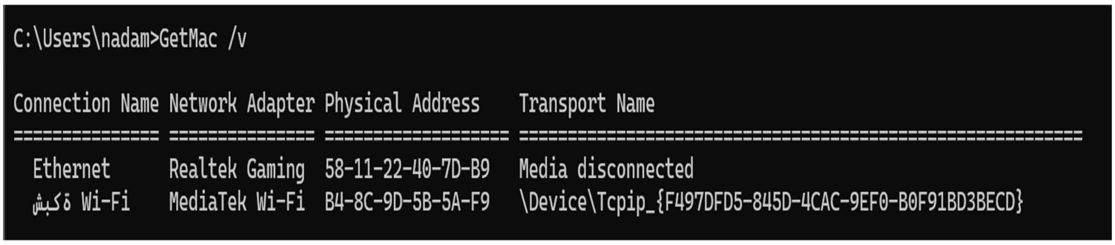
```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : B6-8C-9D-5B-7A-D9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter  ةكبش Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6E MT7922 160MHz Wireless LAN Card
   Physical Address. . . . . . . . . : B4-8C-9D-5B-5A-F9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2c0f:fc88:c:b37:f310:99e1:a0ab:c11c(Preferred)
   Temporary IPv6 Address. . . . . . : 2c0f:fc88:c:b37:dcb9:5c60:7248:c2e7(Preferred)
   Link-local IPv6 Address . . . . . : fe80::fc86:179:5e9f:9283%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.20.10.14(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Lease Obtained. . . . . . . . . . : Sunday, November 24, 2024 12:19:00 PM
   Lease Expires . . . . . . . . . . : Monday, November 25, 2024 12:19:01 PM
   Default Gateway . . . . . . . . . : fe80::c0e8:62ff:fe66:4a64%16
                                       172.20.10.1
   DHCP Server . . . . . . . . . . . : 172.20.10.1
   DHCPv6 IAID . . . . . . . . . . . : 179604637
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-FB-86-5A-58-11-22-40-7D-B9
   DNS Servers . . . . . . . . . . . : fe80::c0e8:62ff:fe66:4a64%16
                                       172.20.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Or using **GetMac**



```
C:\Users\nadam>GetMac

Physical Address    Transport Name
=================== ==========================================================
58-11-22-40-7D-B9   Media disconnected
B4-8C-9D-5B-5A-F9   \Device\Tcpip_{F497DFD5-845D-4CAC-9EF0-B0F91BD3BECD}
```

Or using **GetMac /v** (more information)



```
C:\Users\nadam>GetMac /v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== =================== ==========================================================
  Ethernet      Realtek Gaming  58-11-22-40-7D-B9   Media disconnected
  ةكبش Wi-Fi    MediaTek Wi-Fi  B4-8C-9D-5B-5A-F9   \Device\Tcpip_{F497DFD5-845D-4CAC-9EF0-B0F91BD3BECD}
```

Q10: What is the difference between getmac & getmac/v ?

getmac

- show the **basic** MAC address information like:
  - **Physical Address:** The MAC address .
  - **Transport Name:** The system-assigned name for the network interface.

getmac /v

- show **detailed** information about the MAC address like:
  - Everything shown by getmac.

  - **Connection Name:** The name of the network connection (e.g., "Wi-Fi," "Ethernet").
  - **Network Adapter Description:** A description of the network adapter hardware.

Q11: How can you request a new IP from a DHCP server?

- Release Current IP:
  ipconfig /release , This will release your current IP address.
- Request New IP:
  ipconfig /renew , This will request a new IP address from the DHCP server.

Q12: Explain what you understand about ARP protocol?

ARP (Address resolution) protocol used to **map** an **IP address** to **MAC address**, on a local network.

This mapping is essential for devices to communicate within the same network.

1-ARP Request:

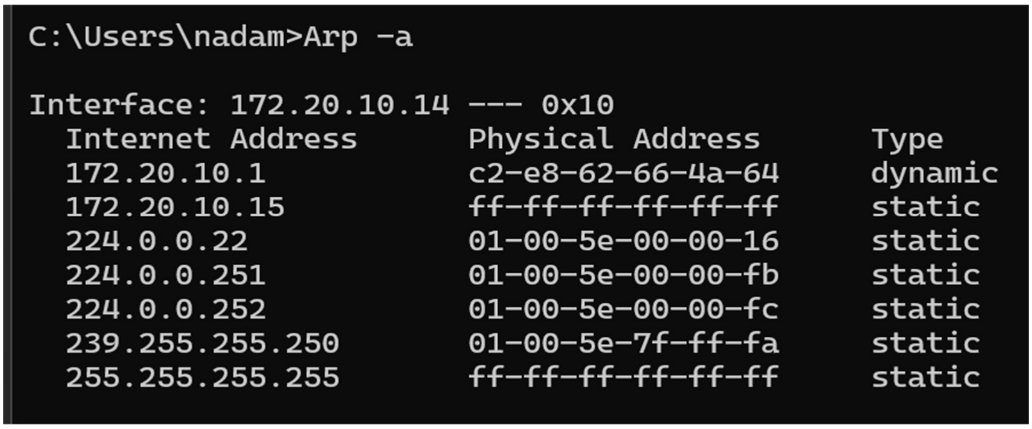
- a device wants to communicate with another device on the same local network
- it sends out an ARP request which is a broadcast message that asks, "**Who has this IP address? Please send me your MAC address.**"

2-**ARP Reply**:

- The device with the matching IP address responds with an ARP reply (which includes its MAC address)

3-**Caching**:

- The requesting device stores this IP-to-MAC address mapping in its ARP cache for future use (we don't need to send an ARP request every time wants to communicate with the same device)

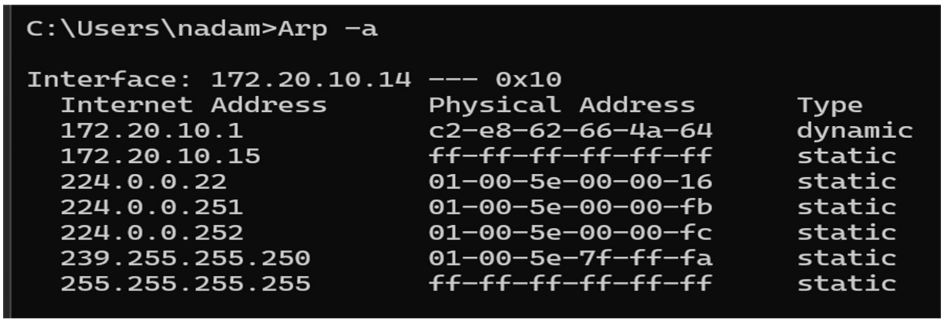


```
C:\Users\nadam>Arp -a

Interface: 172.20.10.14 --- 0x10
  Internet Address      Physical Address      Type
  172.20.10.1           c2-e8-62-66-4a-64     dynamic
  172.20.10.15          ff-ff-ff-ff-ff-ff     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
```

Q13. How do we view the contents of the ARP cache?

using **arp -a**

This will display the current ARP cache, showing the IP addresses and MAC addresses.



```
C:\Users\nadam>Arp -a

Interface: 172.20.10.14 --- 0x10
  Internet Address      Physical Address      Type
  172.20.10.1           c2-e8-62-66-4a-64     dynamic
  172.20.10.15          ff-ff-ff-ff-ff-ff     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
```

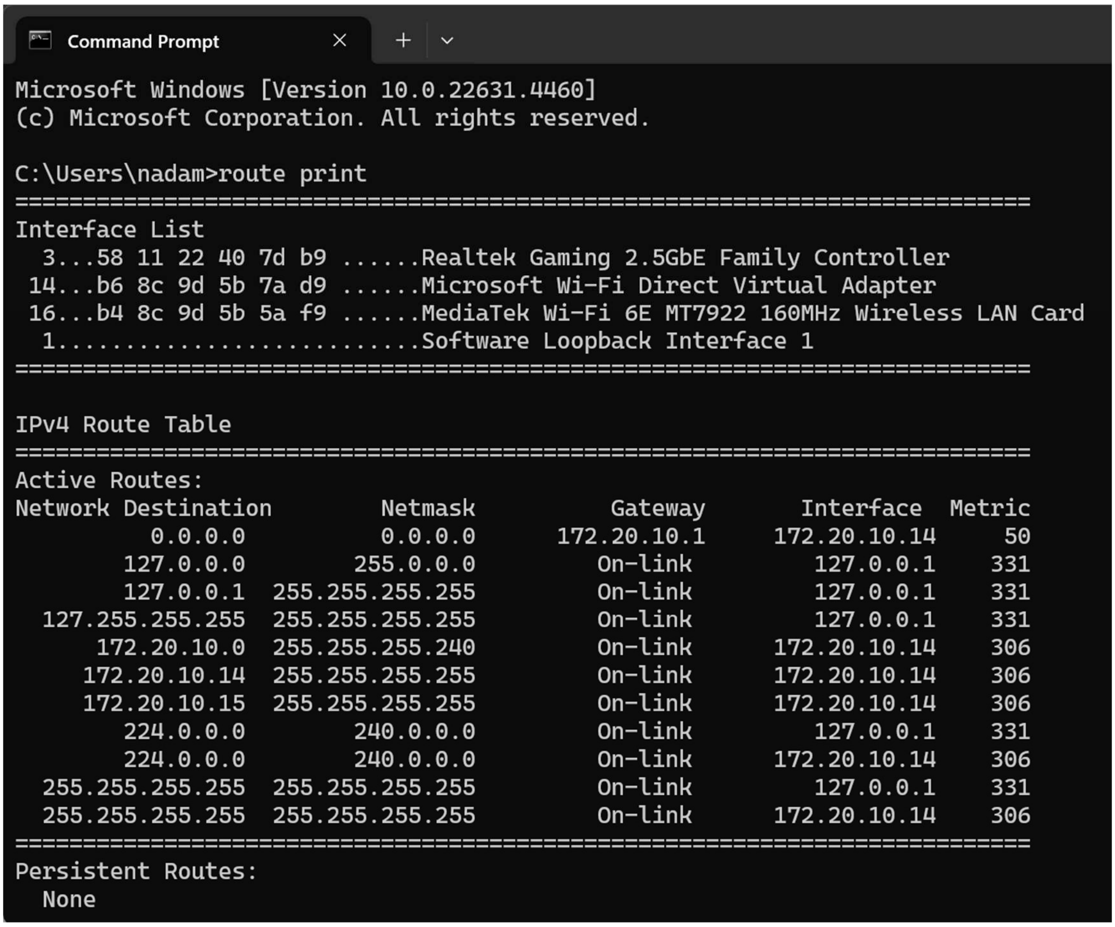
Q14. How do we delete the ARP cache?

Using **arp -d ***

This will delete all entries in the ARP cache.

Q15. How do we view the local routing table?

using **route print**.



```
Microsoft Windows [Version 10.0.22631.4460]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nadam>route print
===========================================================================
Interface List
  3...58 11 22 40 7d b9 ......Realtek Gaming 2.5GbE Family Controller
 14...b6 8c 9d 5b 7a d9 ......Microsoft Wi-Fi Direct Virtual Adapter
 16...b4 8c 9d 5b 5a f9 ......MediaTek Wi-Fi 6E MT7922 160MHz Wireless LAN Card
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.20.10.1     172.20.10.14     50
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      172.20.10.0  255.255.255.240         On-link      172.20.10.14    306
     172.20.10.14  255.255.255.255         On-link      172.20.10.14    306
     172.20.10.15  255.255.255.255         On-link      172.20.10.14    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      172.20.10.14    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      172.20.10.14    306
===========================================================================
Persistent Routes:
  None
```

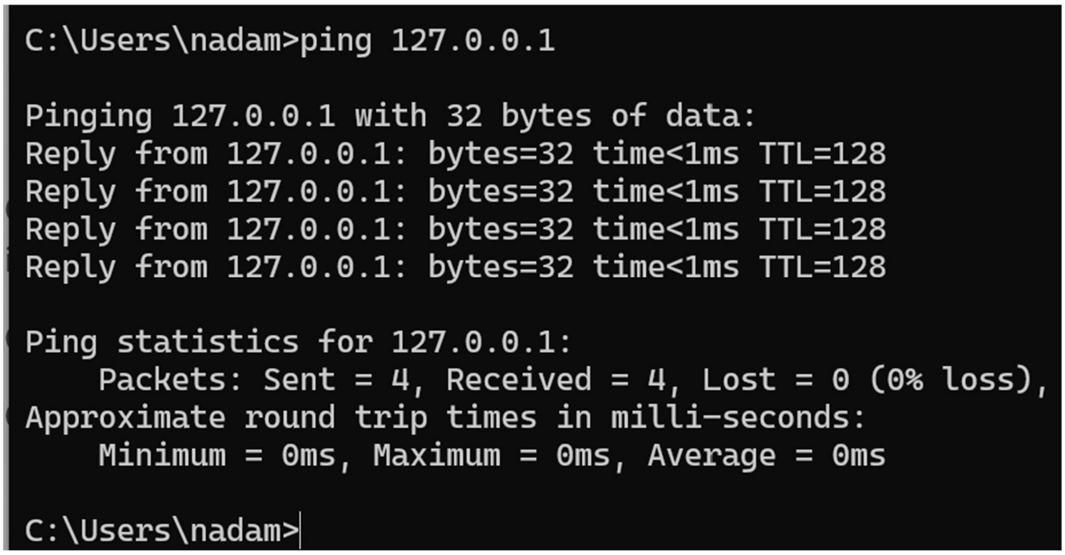
Q16. Can you tell me which command that could check connectivity between 2 devices?

Using **Ping IP**

And then:

a) check connectivity of your loopback IP address “127.0.0.1” .

using **ping 127.0.0.1**



```
C:\Users\nadam>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\nadam>
```

b) How many packets are sent to check availability?

By default ping sends 4 packets

c) How many packages did your device receive? What does this mean?

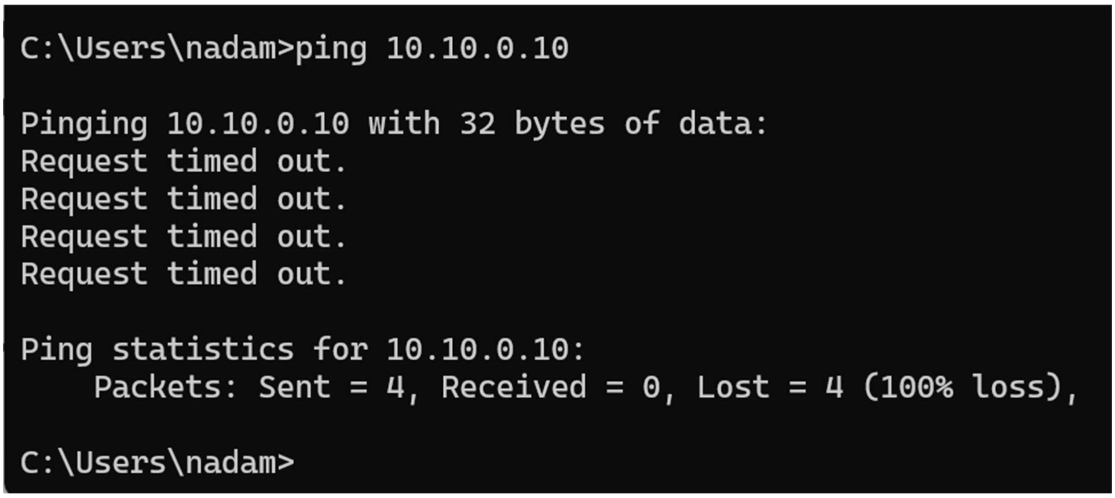
4 packets were sent

4 were received

This mean that there is **no packet loss**.

This mean also that the device is **reachable** and the network **connection is stable**.

d) Check connectivity between your device and this IP "10.10.0.10". then explain the result



```
C:\Users\nadam>ping 10.10.0.10

Pinging 10.10.0.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\nadam>
```

4 packets were sent

0 were received

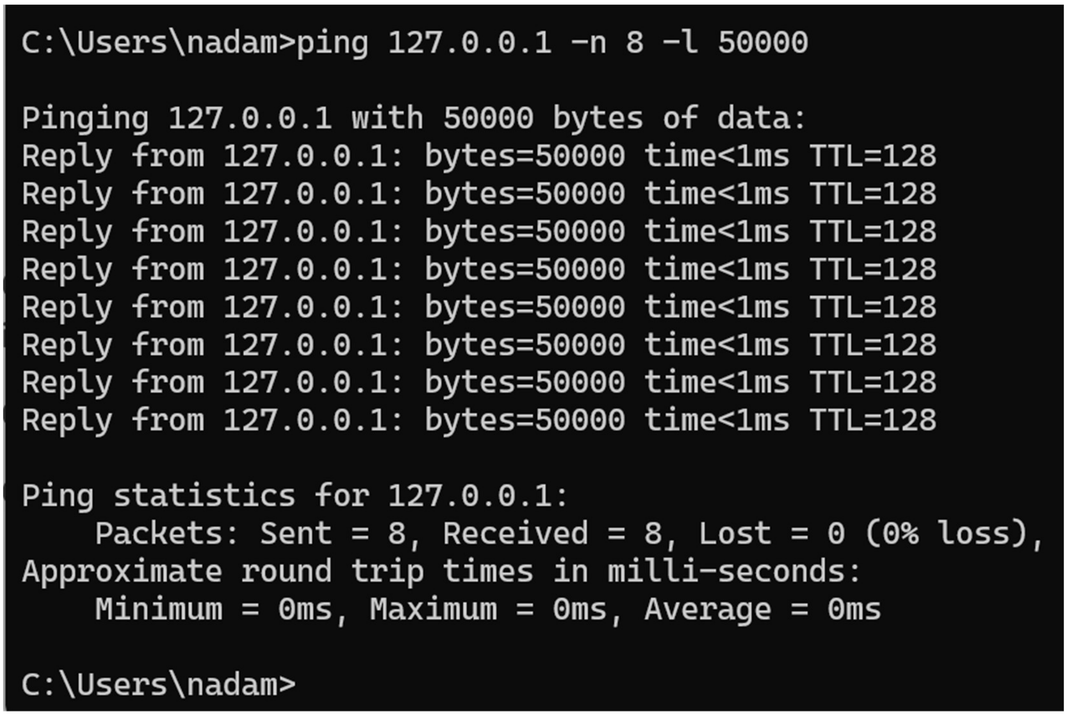
This mean that there is **packet loss** or no response.

This mean also that there is network issues, such as the device being offline, network congestion, or configuration problems..

Q17. Verify the connectivity of the loopback IP address "127.0.0.1" by sending “8” packets which the size of each packet is "50000".

Using **ping 127.0.0.1 -n 8 -l 50000**

There is no problem or lose

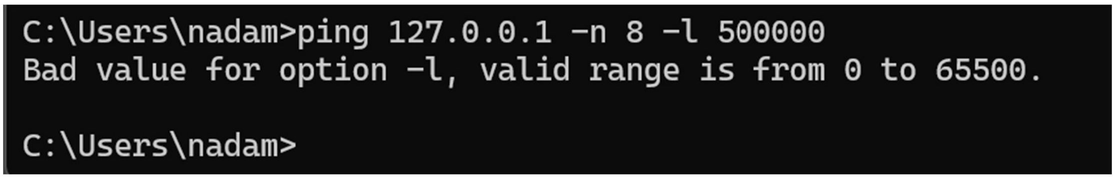


```
C:\Users\nadam>ping 127.0.0.1 -n 8 -l 50000

Pinging 127.0.0.1 with 50000 bytes of data:
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128
Reply from 127.0.0.1: bytes=50000 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 8, Received = 8, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\nadam>
```

But if we increase the size to 500000

Using **ping 127.0.0.1 -n 8 -l 50000**

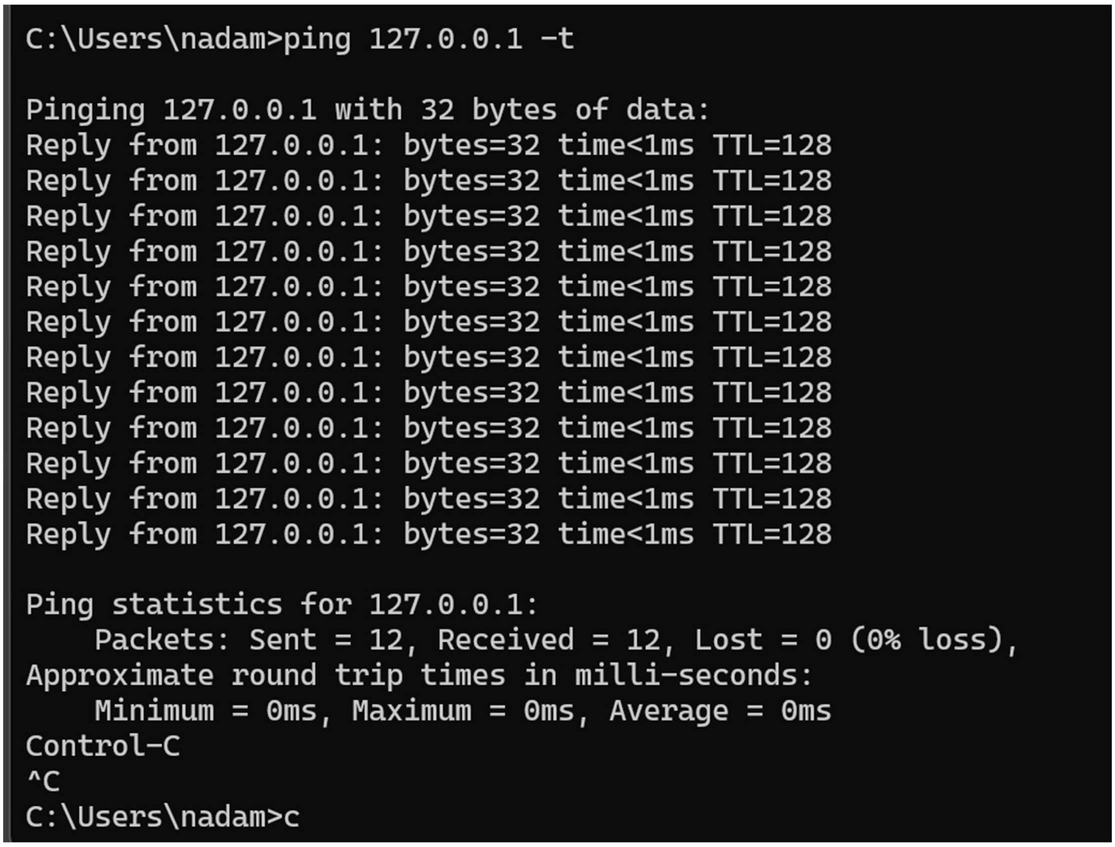
There is problem because of the size



```
C:\Users\nadam>ping 127.0.0.1 -n 8 -l 500000
Bad value for option -l, valid range is from 0 to 65500.

C:\Users\nadam>
```

Q18. Explain what is the meaning of this command: “ping 127.0.0.1 -t “

ping 127.0.0.1 -t is used to continuously ping the loopback IP address (127.0.0.1) until you manually stop it using control + c



```
C:\Users\nadam>ping 127.0.0.1 -t

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\nadam>c
```

Q19. What is the meaning of “ DOS Attack” ?

is a type of cyber attack where the attacker aims to make a machine or network resource unavailable .

Ping is a tool of DOS attack causing Buffer Overflow Attacks (if you continuously ping) Overloading a system's memory, causing it to crash.