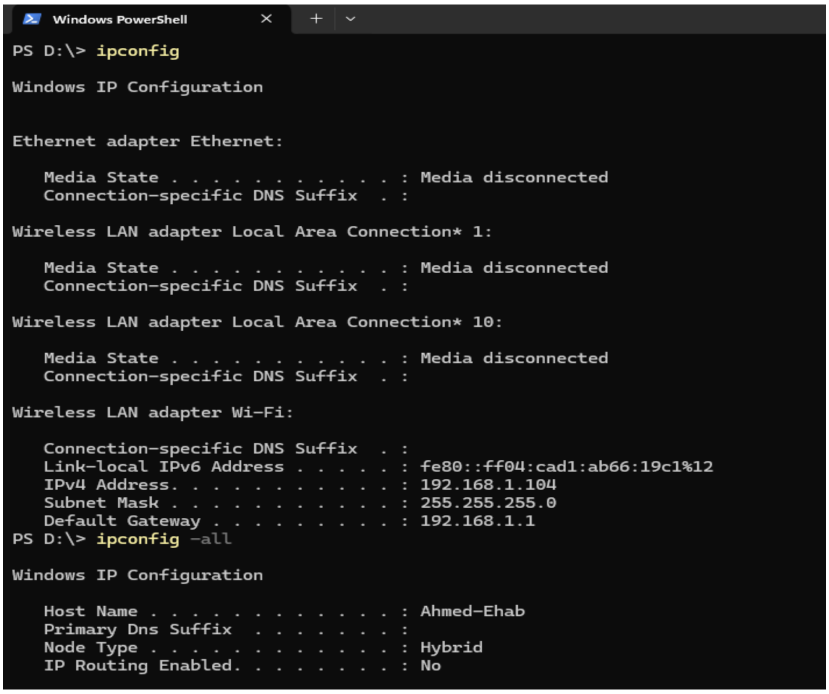
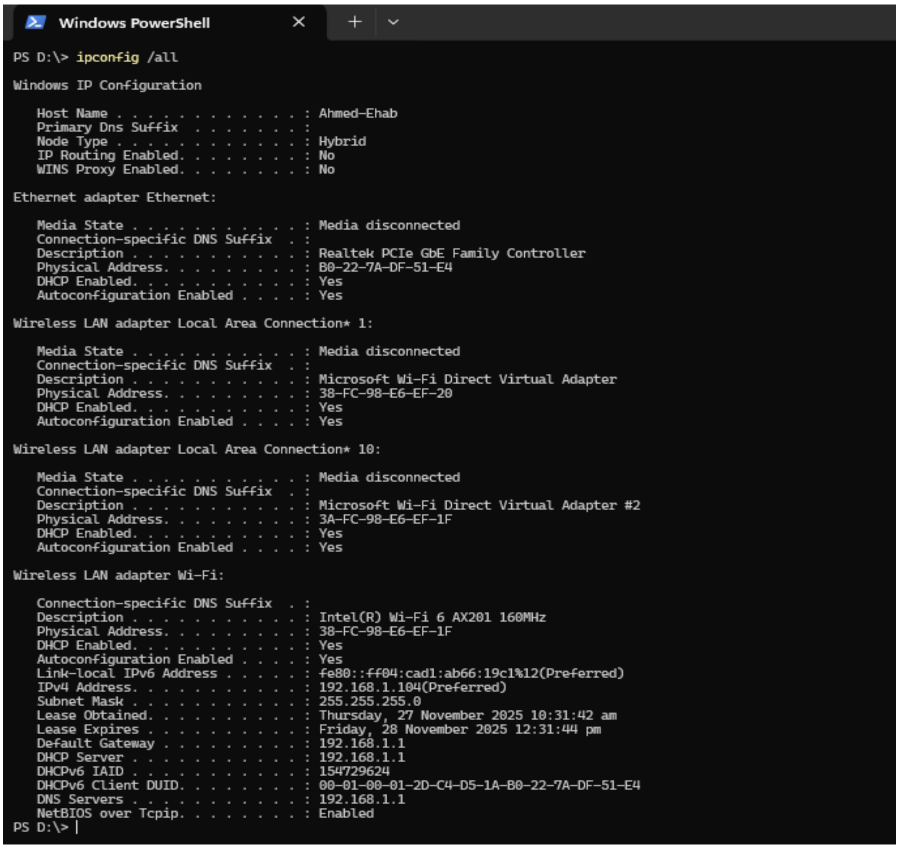
Network

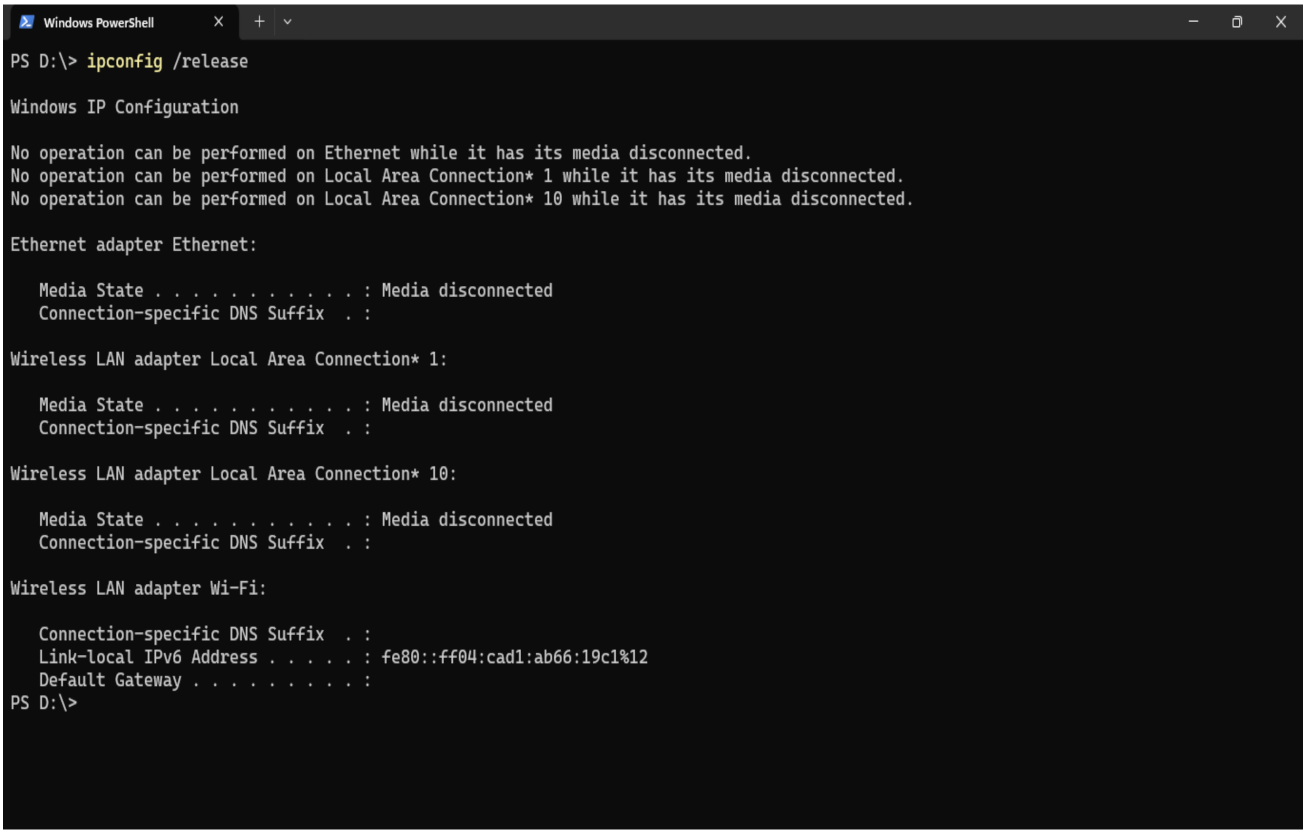
Ahmed Ehab Ahmed **Lab1**



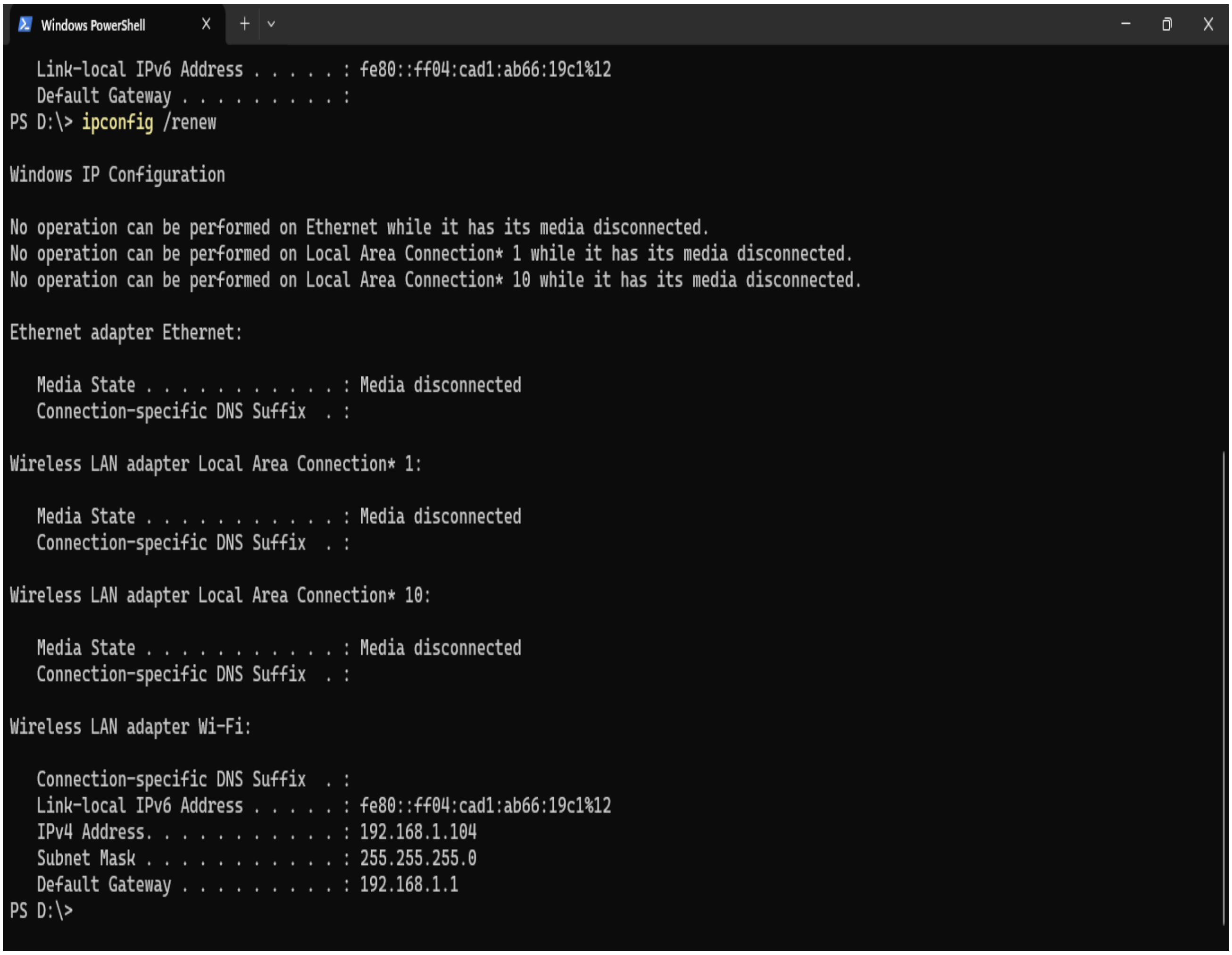
```
PS D:\> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ff04:cad1:ab66:19c1%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
PS D:\> ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Ahmed-Ehab
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
```



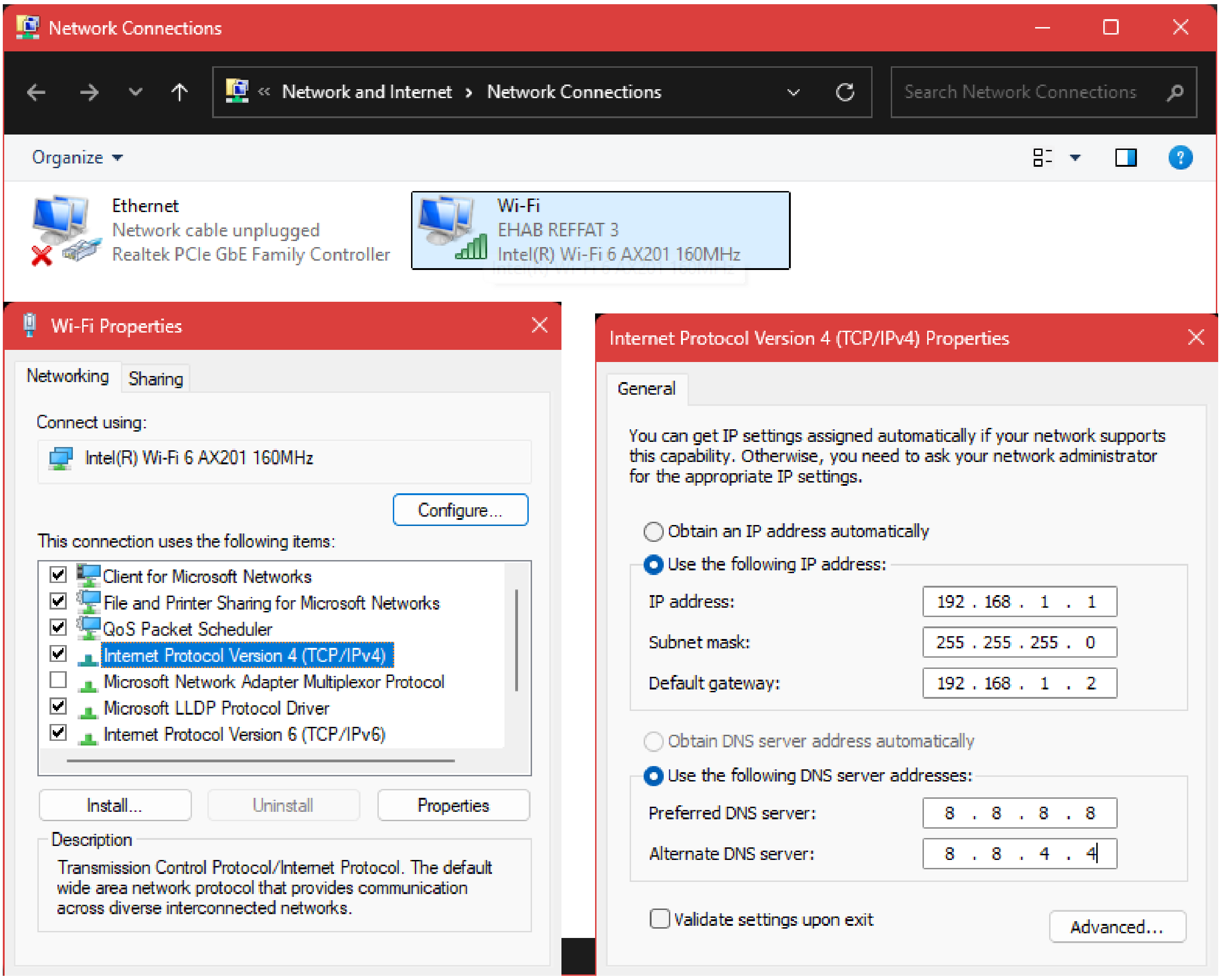
```
PS D:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Ahmed-Ehab
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : B0-22-7A-DF-51-E4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 38-FC-98-E6-EF-20
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 3A-FC-98-E6-EF-1F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 38-FC-98-E6-EF-1F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ff04:cad1:ab66:19c1%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, 27 November 2025 10:31:42 am
   Lease Expires . . . . . . . . . . : Friday, 28 November 2025 12:31:44 pm
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 154729624
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-C4-D5-1A-B0-22-7A-DF-51-E4
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS D:\> |
```



```
PS D:\> ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ff04:cad1:ab66:19c1%12
   Default Gateway . . . . . . . . . :
PS D:\>
```



```
   Link-local IPv6 Address . . . . . : fe80::ff04:cad1:ab66:19c1%12
   Default Gateway . . . . . . . . . :
PS D:\> ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ff04:cad1:ab66:19c1%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
PS D:\>
```



Network Connections
Network and Internet › Network Connections
Search Network Connections
Organize

Ethernet
Network cable unplugged
Realtek PCIe GbE Family Controller

Wi-Fi
EHAB REFFAT 3
Intel(R) Wi-Fi 6 AX201 160MHz

Connect using:

Intel(R) Wi-Fi 6 AX201 160MHz

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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:

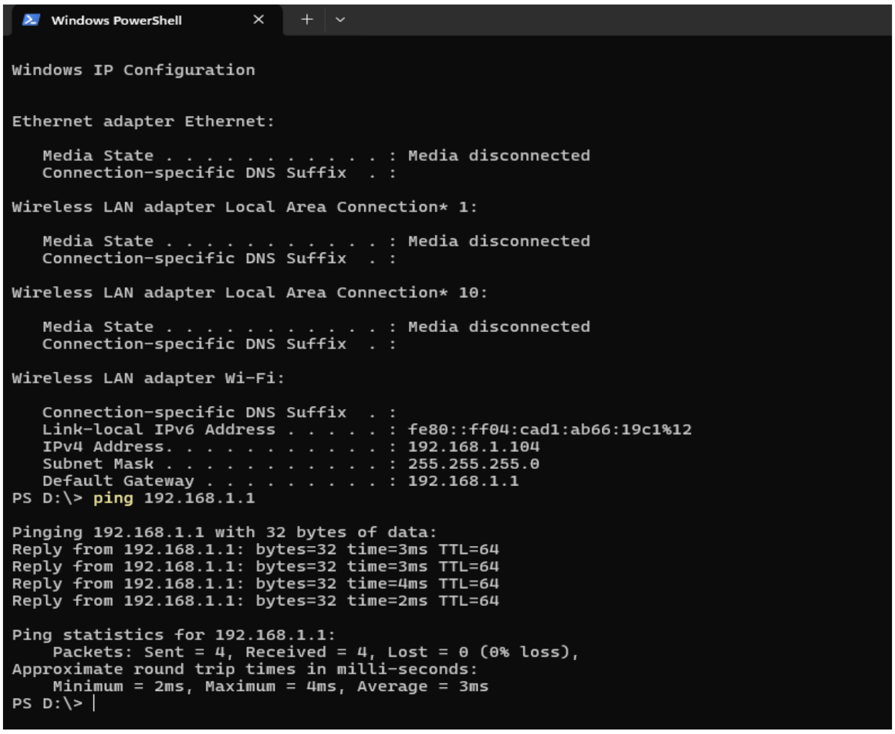
IP address:	192 . 168 . 1 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 2

○ Obtain DNS server address automatically

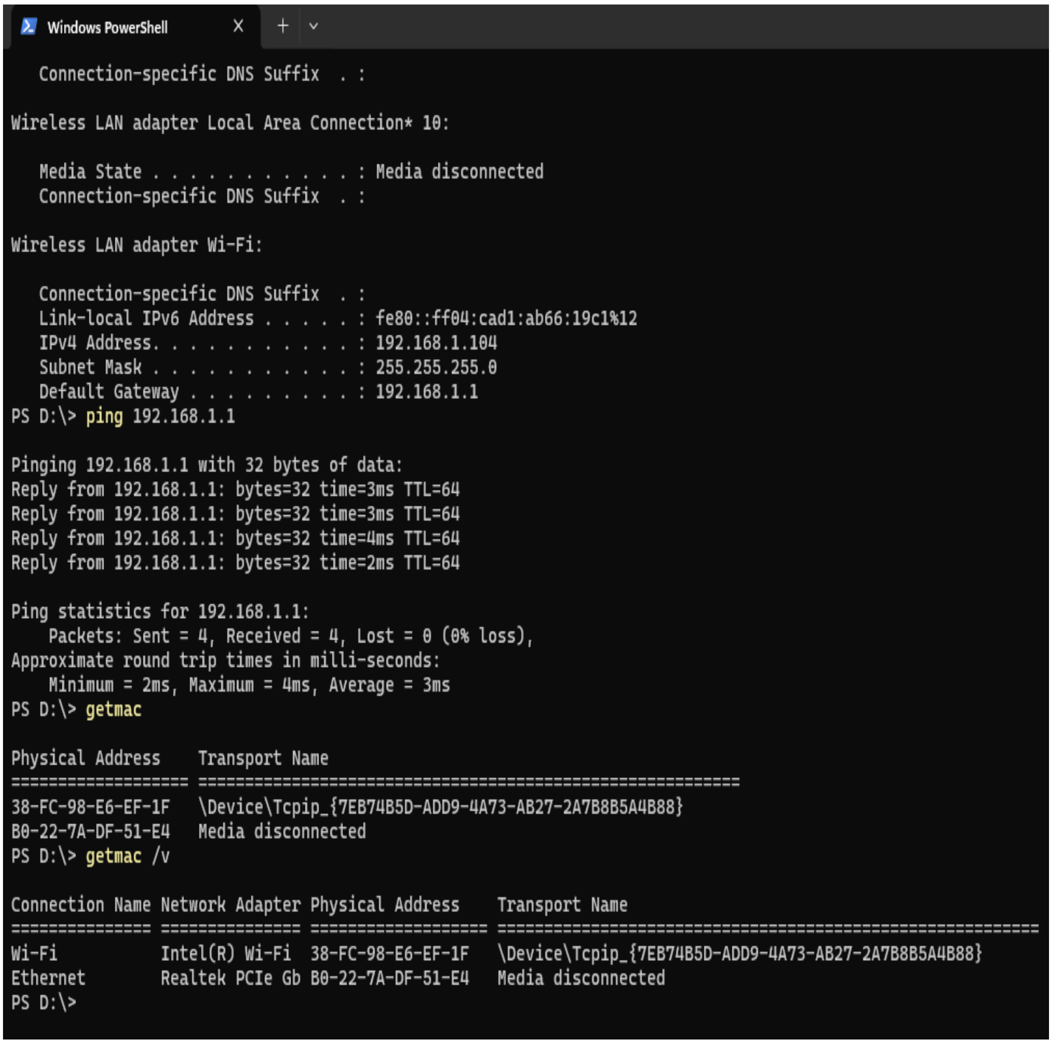
● Use the following DNS server addresses:

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

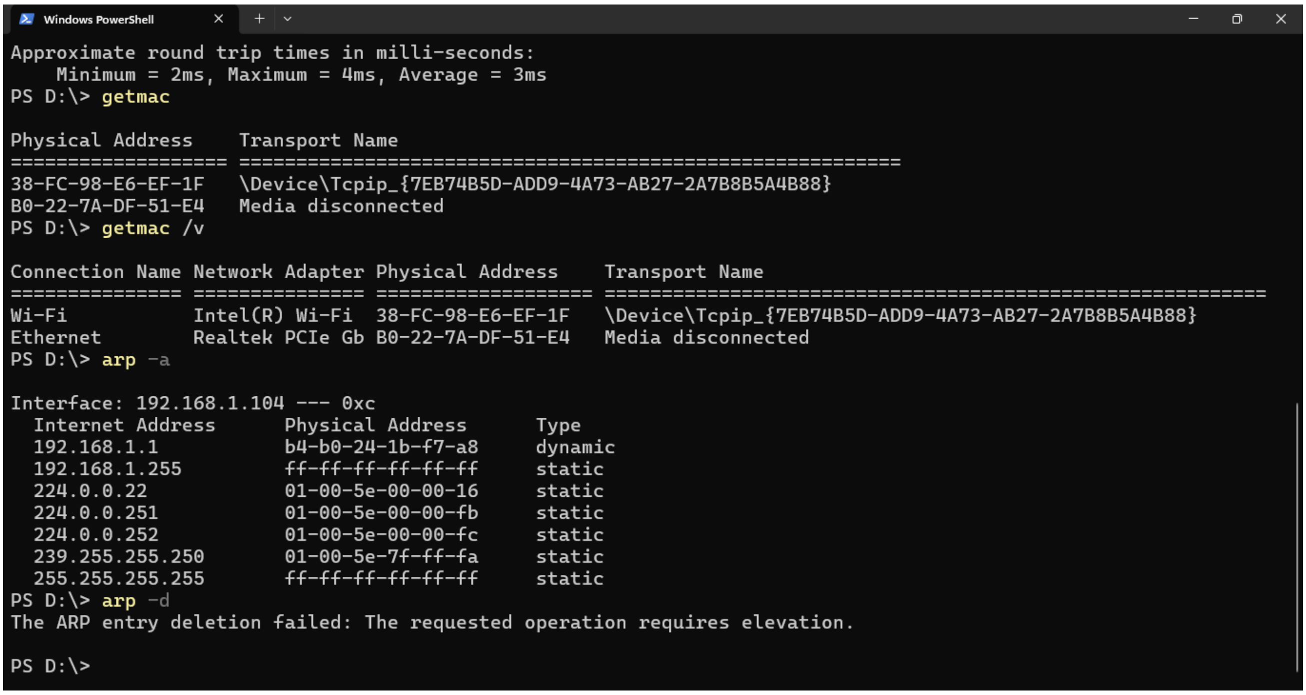
□ Validate settings upon exit



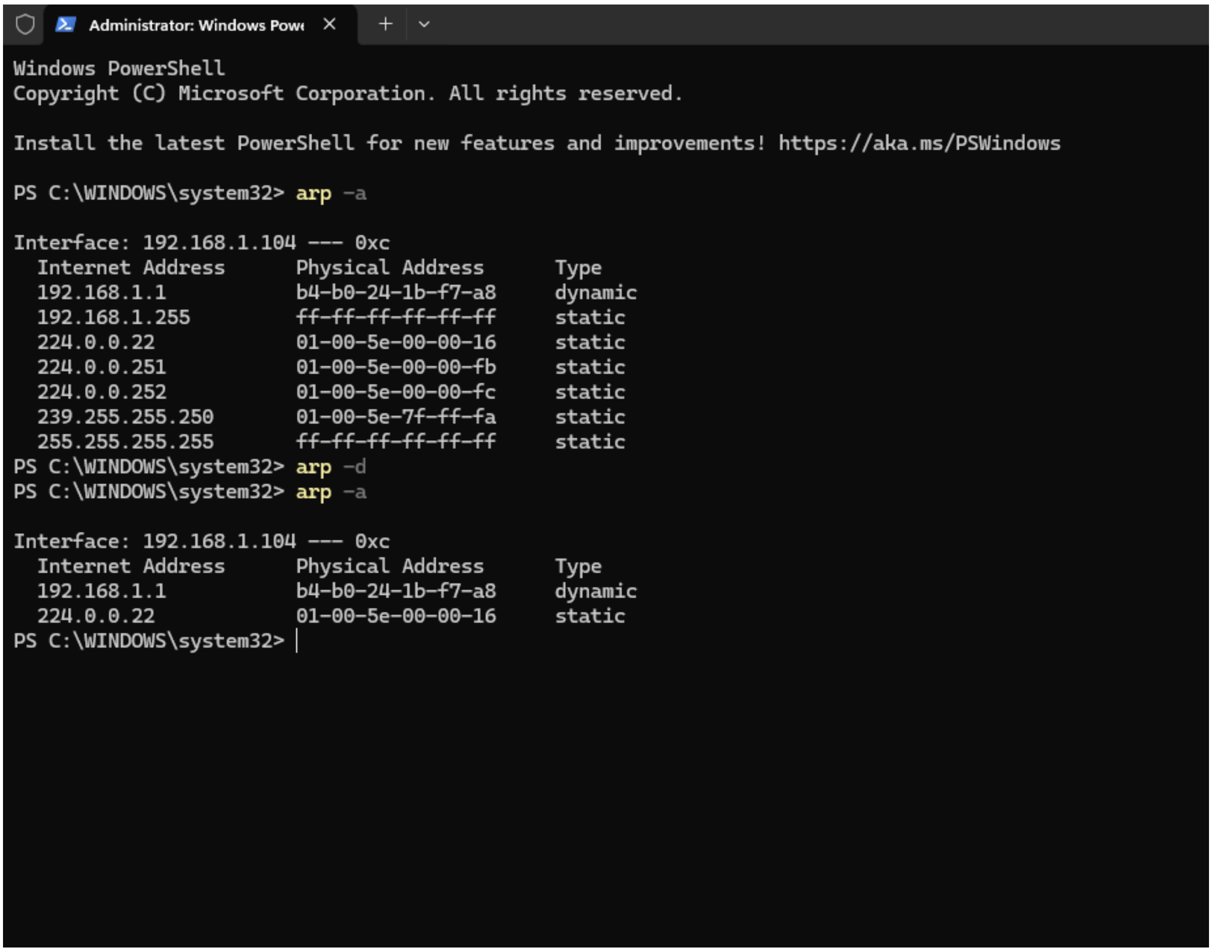
```
Windows IP Configuration


Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ff04:cad1:ab66:19c1%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
PS D:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms
PS D:\> |
```



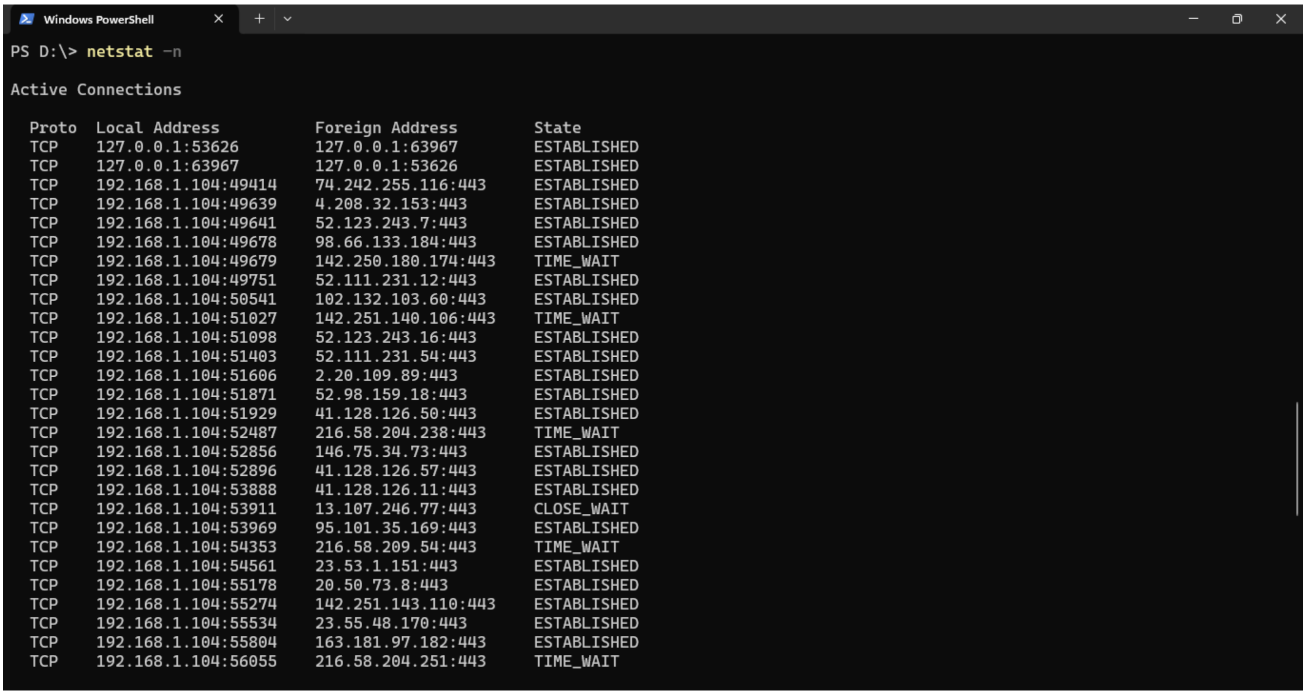
```
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ff04:cad1:ab66:19c1%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
PS D:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms
PS D:\> getmac

Physical Address    Transport Name
=================== ==========================================================
38-FC-98-E6-EF-1F   \Device\Tcpip_{7EB74B5D-ADD9-4A73-AB27-2A7B8B5A4B88}
B0-22-7A-DF-51-E4   Media disconnected
PS D:\> getmac /v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== =================== ==========================================================
Wi-Fi           Intel(R) Wi-Fi  38-FC-98-E6-EF-1F   \Device\Tcpip_{7EB74B5D-ADD9-4A73-AB27-2A7B8B5A4B88}
Ethernet        Realtek PCIe Gb B0-22-7A-DF-51-E4   Media disconnected
PS D:\>
```



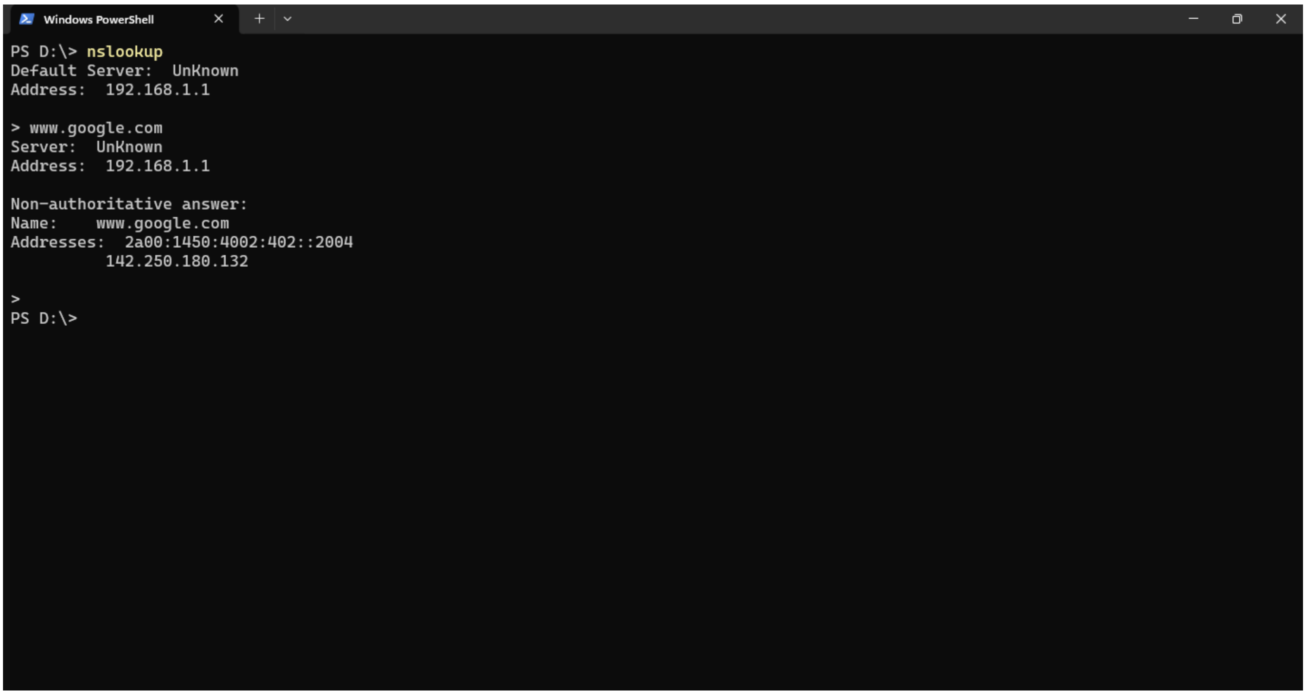
```
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms
PS D:\> getmac

Physical Address    Transport Name
=================== ==========================================================
38-FC-98-E6-EF-1F   \Device\Tcpip_{7EB74B5D-ADD9-4A73-AB27-2A7B8B5A4B88}
B0-22-7A-DF-51-E4   Media disconnected
PS D:\> getmac /v

Connection Name Network Adapter Physical Address    Transport Name
=============== =============== =================== ==========================================================
Wi-Fi           Intel(R) Wi-Fi  38-FC-98-E6-EF-1F   \Device\Tcpip_{7EB74B5D-ADD9-4A73-AB27-2A7B8B5A4B88}
Ethernet        Realtek PCIe Gb B0-22-7A-DF-51-E4   Media disconnected
PS D:\> arp -a

Interface: 192.168.1.104 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           b4-b0-24-1b-f7-a8     dynamic
  192.168.1.255         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
PS D:\> arp -d
The ARP entry deletion failed: The requested operation requires elevation.

PS D:\>
```



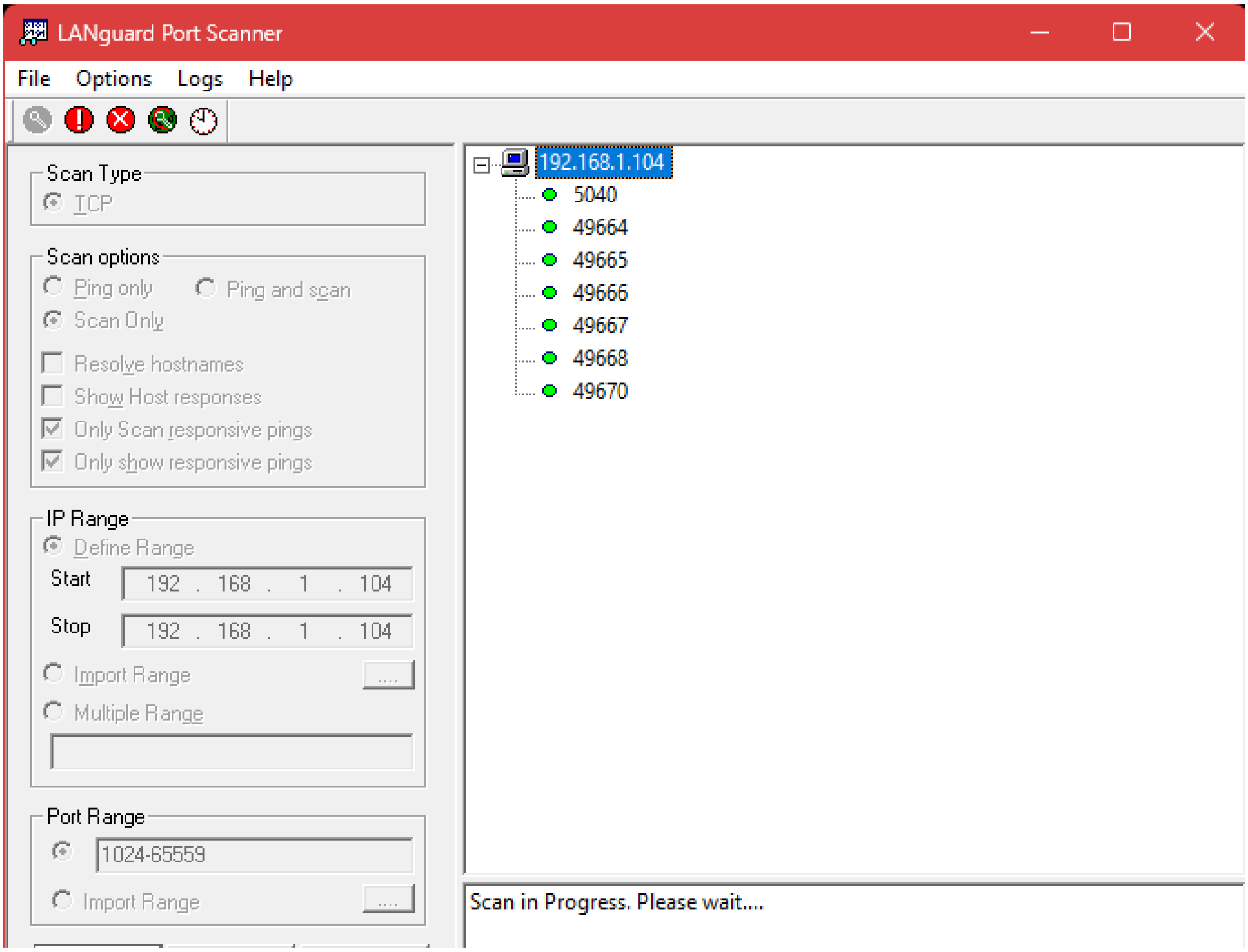
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> arp -a

Interface: 192.168.1.104 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           b4-b0-24-1b-f7-a8     dynamic
  192.168.1.255         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
PS C:\WINDOWS\system32> arp -d
PS C:\WINDOWS\system32> arp -a

Interface: 192.168.1.104 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           b4-b0-24-1b-f7-a8     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
PS C:\WINDOWS\system32>
```



```
PS D:\> netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:53626        127.0.0.1:63967        ESTABLISHED
  TCP    127.0.0.1:63967        127.0.0.1:53626        ESTABLISHED
  TCP    192.168.1.104:49414    74.242.255.116:443     ESTABLISHED
  TCP    192.168.1.104:49639    4.208.32.153:443       ESTABLISHED
  TCP    192.168.1.104:49641    52.123.243.7:443       ESTABLISHED
  TCP    192.168.1.104:49678    98.66.133.184:443      ESTABLISHED
  TCP    192.168.1.104:49679    142.250.180.174:443    TIME_WAIT
  TCP    192.168.1.104:49751    52.111.231.12:443      ESTABLISHED
  TCP    192.168.1.104:50541    102.132.103.60:443     ESTABLISHED
  TCP    192.168.1.104:51027    142.251.140.106:443    TIME_WAIT
  TCP    192.168.1.104:51098    52.123.243.16:443      ESTABLISHED
  TCP    192.168.1.104:51403    52.111.231.54:443      ESTABLISHED
  TCP    192.168.1.104:51606    2.20.109.89:443        ESTABLISHED
  TCP    192.168.1.104:51871    52.98.159.18:443       ESTABLISHED
  TCP    192.168.1.104:51929    41.128.126.50:443      ESTABLISHED
  TCP    192.168.1.104:52487    216.58.204.238:443     TIME_WAIT
  TCP    192.168.1.104:52856    146.75.34.73:443       ESTABLISHED
  TCP    192.168.1.104:52896    41.128.126.57:443      ESTABLISHED
  TCP    192.168.1.104:53888    41.128.126.11:443      ESTABLISHED
  TCP    192.168.1.104:53911    13.107.246.77:443      CLOSE_WAIT
  TCP    192.168.1.104:53969    95.101.35.169:443      ESTABLISHED
  TCP    192.168.1.104:54353    216.58.209.54:443      TIME_WAIT
  TCP    192.168.1.104:54561    23.53.1.151:443        ESTABLISHED
  TCP    192.168.1.104:55178    20.50.73.8:443         ESTABLISHED
  TCP    192.168.1.104:55274    142.251.143.110:443    ESTABLISHED
  TCP    192.168.1.104:55534    23.55.48.170:443       ESTABLISHED
  TCP    192.168.1.104:55804    163.181.97.182:443     ESTABLISHED
  TCP    192.168.1.104:56055    216.58.204.251:443     TIME_WAIT
```



```
PS D:\> nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> www.google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4002:402::2004
          142.250.180.132

>
PS D:\>
```



Scan Type

● TCP

Scan options

○ Ping only ○ Ping and scan

● Scan Only

☐ Resolve hostnames

☐ Show Host responses

☑ Only Scan responsive pings

☑ Only show responsive pings

IP Range

● Define Range

Start 192 . 168 . 1 . 104

Stop 192 . 168 . 1 . 104

○ Import Range ....

○ Multiple Range

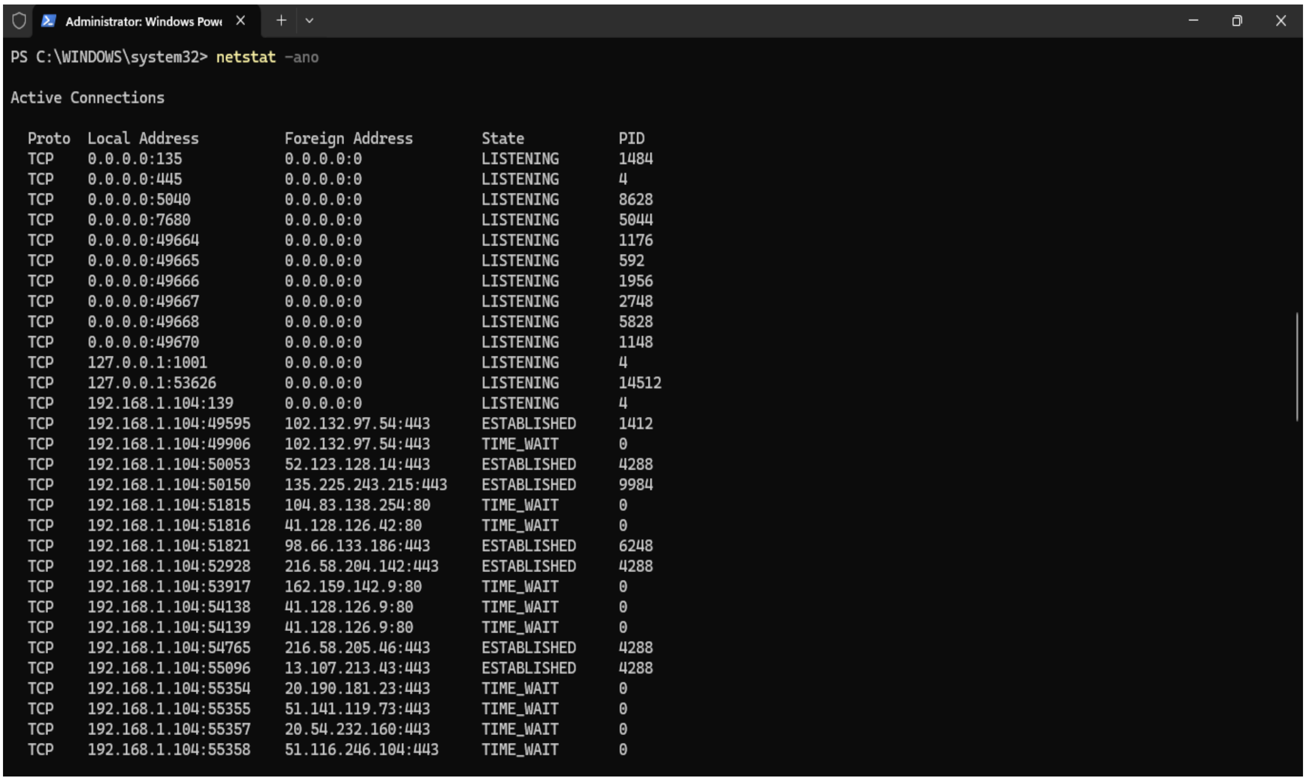
Port Range

● 1024-65559

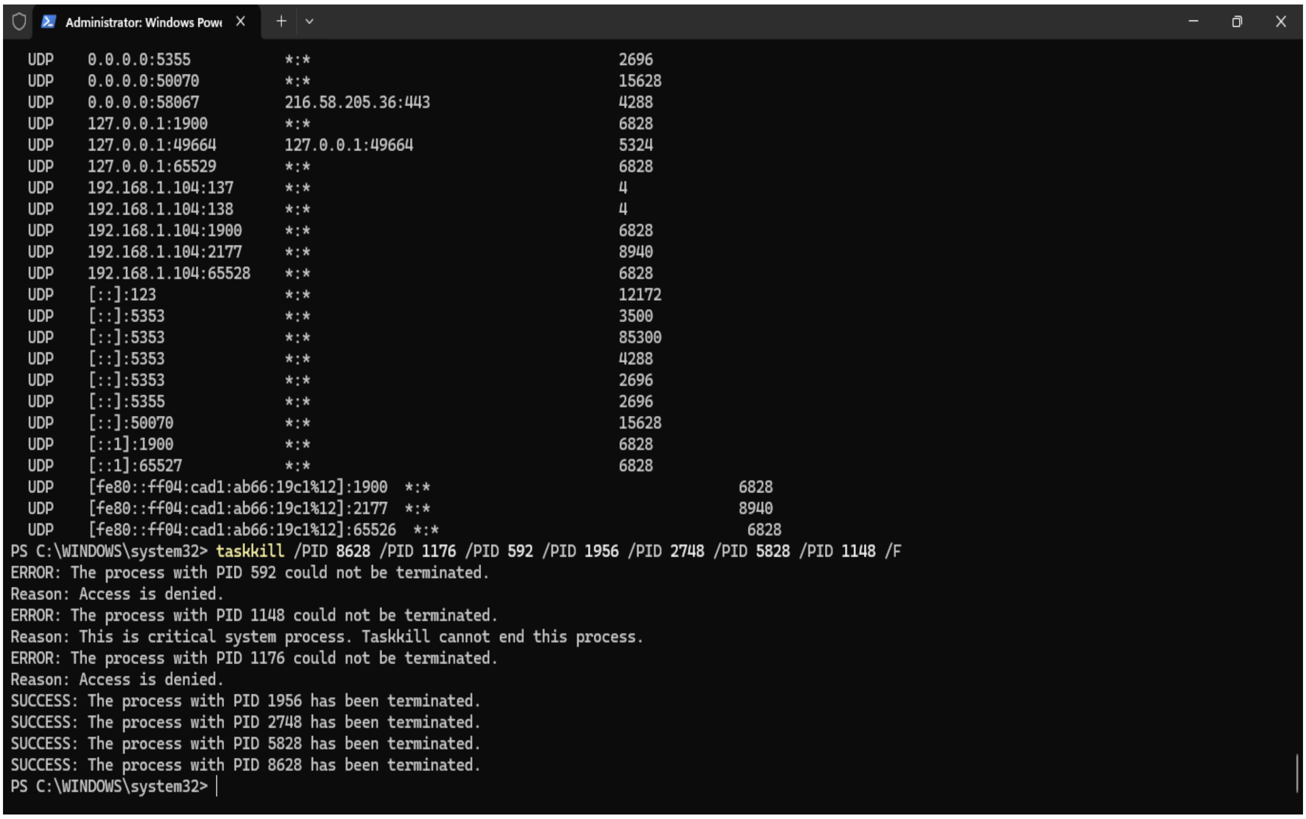
○ Import Range ....

```
⊟ 192.168.1.104
   ● 5040
   ● 49664
   ● 49665
   ● 49666
   ● 49667
   ● 49668
   ● 49670
```

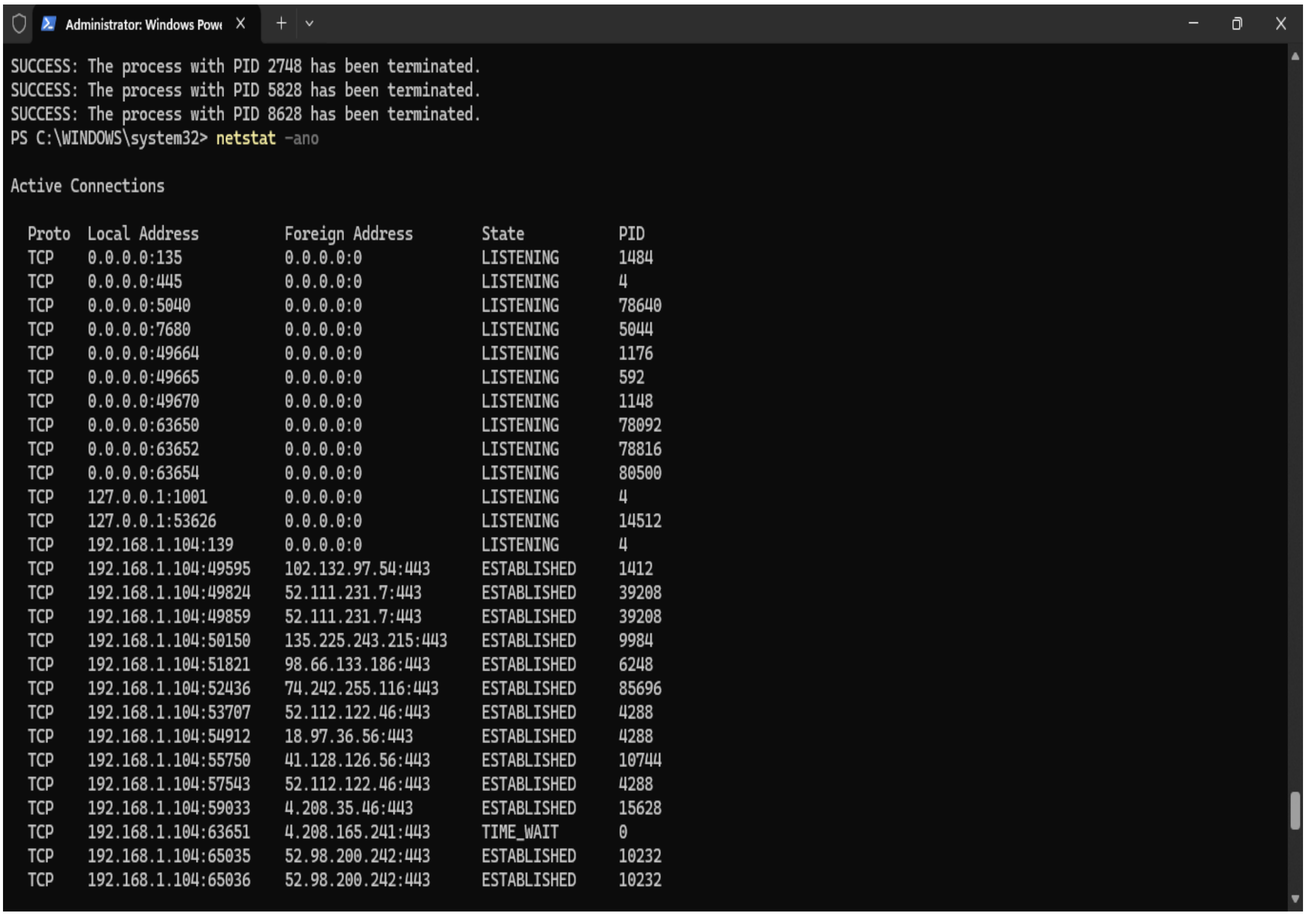
Scan in Progress. Please wait....



```
PS C:\WINDOWS\system32> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1484
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       8628
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       5044
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1176
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       592
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1956
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2748
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       5828
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       1148
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:53626        0.0.0.0:0              LISTENING       14512
  TCP    192.168.1.104:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.1.104:49595    102.132.97.54:443      ESTABLISHED     1412
  TCP    192.168.1.104:49906    102.132.97.54:443      TIME_WAIT       0
  TCP    192.168.1.104:50053    52.123.128.14:443      ESTABLISHED     4288
  TCP    192.168.1.104:50150    135.225.243.215:443    ESTABLISHED     9984
  TCP    192.168.1.104:51815    104.83.138.254:80      TIME_WAIT       0
  TCP    192.168.1.104:51816    41.128.126.42:80       TIME_WAIT       0
  TCP    192.168.1.104:51821    98.66.133.186:443      ESTABLISHED     6248
  TCP    192.168.1.104:52928    216.58.204.142:443     ESTABLISHED     4288
  TCP    192.168.1.104:53917    162.159.142.9:80       TIME_WAIT       0
  TCP    192.168.1.104:54138    41.128.126.9:80        TIME_WAIT       0
  TCP    192.168.1.104:54139    41.128.126.9:80        TIME_WAIT       0
  TCP    192.168.1.104:54765    216.58.205.46:443      ESTABLISHED     4288
  TCP    192.168.1.104:55096    13.107.213.43:443      ESTABLISHED     4288
  TCP    192.168.1.104:55354    20.190.181.23:443      TIME_WAIT       0
  TCP    192.168.1.104:55355    51.141.119.73:443      TIME_WAIT       0
  TCP    192.168.1.104:55357    20.54.232.160:443      TIME_WAIT       0
  TCP    192.168.1.104:55358    51.116.246.104:443     TIME_WAIT       0
```



```
  UDP    0.0.0.0:5355           *:*                                    2696
  UDP    0.0.0.0:50070          *:*                                    15628
  UDP    0.0.0.0:58067          216.58.205.36:443                      4288
  UDP    127.0.0.1:1900         *:*                                    6828
  UDP    127.0.0.1:49664        127.0.0.1:49664                        5324
  UDP    127.0.0.1:65529        *:*                                    6828
  UDP    192.168.1.104:137      *:*                                    4
  UDP    192.168.1.104:138      *:*                                    4
  UDP    192.168.1.104:1900     *:*                                    6828
  UDP    192.168.1.104:2177     *:*                                    8940
  UDP    192.168.1.104:65528    *:*                                    6828
  UDP    [::]:123               *:*                                    12172
  UDP    [::]:5353              *:*                                    3500
  UDP    [::]:5353              *:*                                    85300
  UDP    [::]:5353              *:*                                    4288
  UDP    [::]:5353              *:*                                    2696
  UDP    [::]:5355              *:*                                    2696
  UDP    [::]:50070             *:*                                    15628
  UDP    [::1]:1900             *:*                                    6828
  UDP    [::1]:65527            *:*                                    6828
  UDP    [fe80::ff04:cad1:ab66:19c1%12]:1900  *:*                                    6828
  UDP    [fe80::ff04:cad1:ab66:19c1%12]:2177  *:*                                    8940
  UDP    [fe80::ff04:cad1:ab66:19c1%12]:65526  *:*                                    6828
PS C:\WINDOWS\system32> taskkill /PID 8628 /PID 1176 /PID 592 /PID 1956 /PID 2748 /PID 5828 /PID 1148 /F
ERROR: The process with PID 592 could not be terminated.
Reason: Access is denied.
ERROR: The process with PID 1148 could not be terminated.
Reason: This is critical system process. Taskkill cannot end this process.
ERROR: The process with PID 1176 could not be terminated.
Reason: Access is denied.
SUCCESS: The process with PID 1956 has been terminated.
SUCCESS: The process with PID 2748 has been terminated.
SUCCESS: The process with PID 5828 has been terminated.
SUCCESS: The process with PID 8628 has been terminated.
PS C:\WINDOWS\system32>
```



```
SUCCESS: The process with PID 2748 has been terminated.
SUCCESS: The process with PID 5828 has been terminated.
SUCCESS: The process with PID 8628 has been terminated.
PS C:\WINDOWS\system32> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1484
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       78640
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       5044
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1176
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       592
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       1148
  TCP    0.0.0.0:63650          0.0.0.0:0              LISTENING       78092
  TCP    0.0.0.0:63652          0.0.0.0:0              LISTENING       78816
  TCP    0.0.0.0:63654          0.0.0.0:0              LISTENING       80500
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:53626        0.0.0.0:0              LISTENING       14512
  TCP    192.168.1.104:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.1.104:49595    102.132.97.54:443      ESTABLISHED     1412
  TCP    192.168.1.104:49824    52.111.231.7:443       ESTABLISHED     39208
  TCP    192.168.1.104:49859    52.111.231.7:443       ESTABLISHED     39208
  TCP    192.168.1.104:50150    135.225.243.215:443    ESTABLISHED     9984
  TCP    192.168.1.104:51821    98.66.133.186:443      ESTABLISHED     6248
  TCP    192.168.1.104:52436    74.242.255.116:443     ESTABLISHED     85696
  TCP    192.168.1.104:53707    52.112.122.46:443      ESTABLISHED     4288
  TCP    192.168.1.104:54912    18.97.36.56:443        ESTABLISHED     4288
  TCP    192.168.1.104:55750    41.128.126.56:443      ESTABLISHED     10744
  TCP    192.168.1.104:57543    52.112.122.46:443      ESTABLISHED     4288
  TCP    192.168.1.104:59033    4.208.35.46:443        ESTABLISHED     15628
  TCP    192.168.1.104:63651    4.208.165.241:443      TIME_WAIT       0
  TCP    192.168.1.104:65035    52.98.200.242:443      ESTABLISHED     10232
  TCP    192.168.1.104:65036    52.98.200.242:443      ESTABLISHED     10232
```

Port 5040:

Why It's Open
Part of the Windows Diagnostics Hub, used by developers and system administrators to collect logs and diagnostic info remotely.

Common Risks

- Information Leakage: Can expose detailed system logs and telemetry.
- Privilege Escalation: Debug services can sometimes be misused for local privilege escalation.
- Poor Access Controls: Not always well protected in default setups.

Port 49666:

Why It's Open
Port 49666 is in the dynamic/ephemeral port range and is commonly used by Windows RPC services, malware command and control, backdoor applications, and dynamic service bindings. The "666" suffix makes it particularly suspicious as it's often chosen by malicious software for psychological impact or to evade basic filtering rules.

Common Risks

- Malware command and control
  Port commonly used by trojans and backdoors for remote access
- Windows RPC exploitation
  Remote Procedure Call vulnerabilities may allow system compromise
- Data exfiltration
  Malicious software may use this port to steal sensitive information
- Unauthorized remote access
  Attackers may establish persistent backdoor connections
- Dynamic service binding abuse
  Legitimate services may be hijacked or impersonated
- Network reconnaissance
  Port scanning may reveal active Windows services
- Covert communication channels
  Attackers may use high ports to avoid detection