

Command Prompt in administrator mode →

ping google.com →

Pinging google.com [2404:6800:4009:82d::200e]
with 32 bytes of data:

Reply from 2404:6800:4009:82d::200e: time=49ms

ping statistics for 2404:6800:4009:82d::200e;
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip time in milli-seconds:
Minimum = 42ms, Maximum = 44ms, Average = 43ms

Explanation:- It tells the system to send "ping" requests to the domain google.com, which is used to check if the computer can reach Google's server over the network.

Pinging google.com [2404:6800:4009:82d::200e] with 32 bytes of data:

This line shows the domain google.com that is being pinged, along with its resolved IP address 2404:6800:4009:82d::200e. This is an IPv6 address, meaning it uses the newer

format for network addressing. The 32 bytes of data refers to the size of each ping request being sent.

Ping statistics for 2404:6800:4009:82d::200e:
This line begins the summary of the ping test.

packets : Sent = 4 , Received = 4 , Lost = 0 (0% loss),
It shows that 4 ping packets were sent, all
4 were successfully received, and there was no
packet loss (0%). This indicates a stable network
connection.

Minimum = 42 ms → minimum round-trip

Maximum = 44 ms → maximum round-trip

Average = 43 ms → average round-trip

b) ping -n 6 -l 50 google.com →

Pinging google.com [2404:6800:4009:82d::200e]
with 50 bytes of data:

Reply from 2404:6800:4009:82d::200e: time=94ms

ping statistics for 2404:6800:4009:82d::200e :

packets : sent = 6 , Received = 6 , Lost = 0 (0% Loss),

Approximate round trip times in milli-seconds:
Minimum = 42 ms, Maximum = 47 ms, Average = 44 ms

Explanation:-

The connection to google.com is stable, with no packet loss.

The round-trip time (RTT) is within a small range (42 - 47 ms), indicating a consistent network performance.

The use of -l 50 increased the packet size, but the network handled it well without issues.

The response times slightly varied, which is normal due to network fluctuations.

c) ping /?

usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v tos]

Explanation →

This help menu provides details on how to use ping with various options.

Key take aways:

-n → controls the number of packets sent

-l → changes packet size

-4 or -6 forces IPv4 or IPv6
-t enables continuous ping
-w sets timeout duration.
Advanced options like -r, -s, -j, and -k
help analyze network routing.

d) ipconfig →

windows IP configuration

Wireless LAN adapter Local Area Connection 3:

Wireless LAN adapter Local Area Connection 4:

Ethernet adapter ~~VMware~~ VMware Network Adapter
VHNet1:

Wireless LAN adapter Wi-Fi:

Ethernet adapter Bluetooth Network Connection:

Explanation:
The system has multiple network adapters (Wi-Fi,
VMware, Bluetooth, virtual adapters)

The Wi-Fi adapter (192.168.29.172) is the active internet connection.

The VMware adapters are used for virtual machine networking.

The Bluetooth and virtual LAN adapters are disconnected.

e) netstat →
active connections

Explanations:- netstat command displays active network connections, listening ports, and network statistics.

Proto (Protocol) → The type of protocol being used (TCP or UDP)

Local Address → The IP address and port number of your device.

Foreign Address → The IP address and port number of the remote device.

State → The status of the connection.

State	Meaning
Listen	The socket waiting for incoming request
Established	Connection established
syn_sent	Connection request has been sent
syn_received	Receive syn request waiting for acknowledgement
Fin_wait1	Connecting is closing ; waiting other side
Fin_wait2	acknowledge close request
Timewait	Connection is closed waiting to ensure
close_wait	system wait program to close
LastAck	waiting for final acknowledgement
closed	connection is fully closed.

b) netstat -b -f →

Active connections

Explanation:-

This command output lists active network connections, showing which executables

are responsible for each ~~current~~ connections, and resolving foreign addresses into Fully qualified Domain Names (FQDNs)

g) netstat -rn →

Interface List

:

IPv4 Route Table

:

Persistent Routes

IPv6 Route Table

:

Persistent Routes

None

Explanation → displays the routing table, which contains information about how network traffic is routed through your system.

h) netstat -rn →

Interface List

IPv4 Route Table

Persistent Routes

IPv6 Route Table

Persistent Routes

Explanation:- displays no routing table of the machine

i) ping amazon.in

Pinging amazon.in [52.95.120.67] with 32 bytes of data.

Explanation:-

Your system successfully communicated with amazon.in (IP: 52.95.120.67) with an average response time of 201 ms, indicating a stable but slightly high latency connection (possibly due to geographical distance or network congestion).

j) tracert amazon.in →

Tracing route to amazon.in [52.95.116.115]

over a maximum of 30 hops:

1	15ms	22ms	11ms	reliance.reliance[192.168.2.1]
26	*	*	*	Request timed out
27	228ms	242ms	245ms	52.95.116.115

Trace complete.

Explanation:- The tracert command is used to trace the route packets take to reach a

destination (amazon.in in this case) and identify the network hops along the way.

k) getmac →

Physical Address Transport Name

E4 - AA - EA - FF - BC - 05
Device \ Tcpip - [F61ACBED - BBAA-47EB - B0EA -
D362CB2B286F]

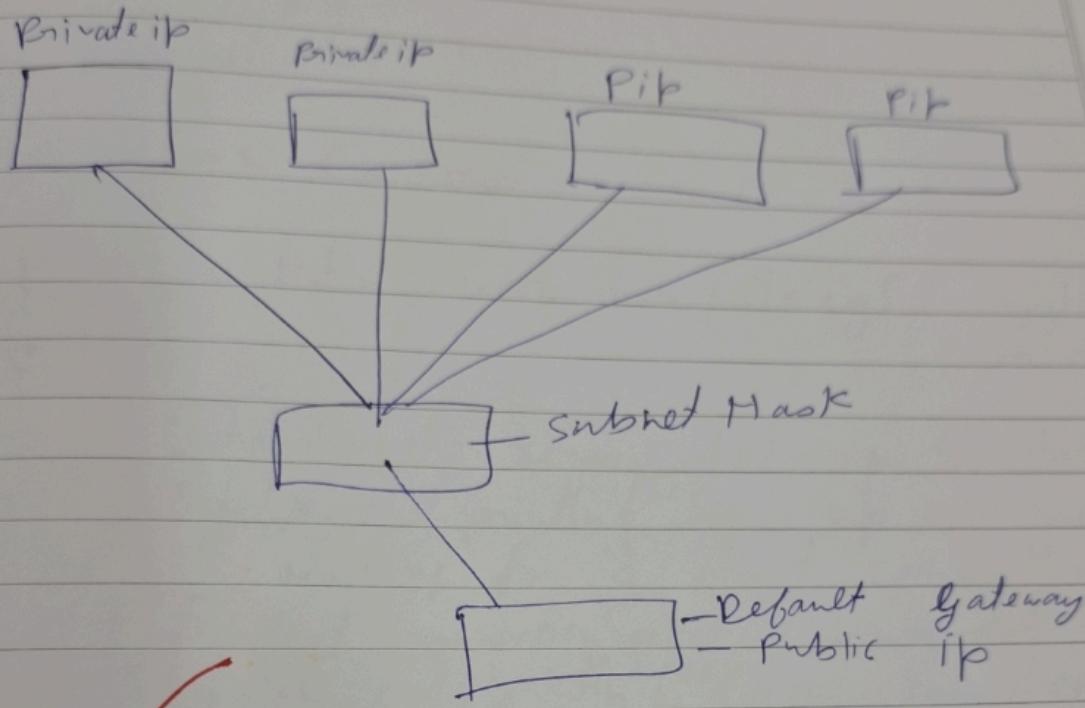
E4 - AA - EA - FF - BC - 06 Media disconnected

Explanation:- It retrieves the MAC access (Media Access control) of all network adapters in your system, which are unique identifiers for network interfaces.

l) hostName →

LAPTOP - EAFVU51T

Explanation:- It retrieves and displays the hostName of your computer, which is the name assigned to the system within the network.



✓
192.168.11.42
— Network — Host