

1) IPCONFIG: IPCONFIG stands for **Internet Protocol Configuration**. Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters. Default Gateway: ip address of nearest router or the router through which your pc is directly connected.

Subnet mask: It helps to identify either the node is at your local network or remote network.

```
Windows IP Configuration

Ethernet adapter Ethernet:

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

Ethernet adapter vEthernet (WSL):

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::3157:5b0d:884d:b4dc%40
    IPv4 Address. . . . . : 172.17.160.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::e17b:5cd8:db9d:e348%15
    IPv4 Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter Bluetooth Network Connection:

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

2) **Nslookup** (stands for "Name Server Lookup") is used to get information from DNS(Domain Name Service) about any domain name or ip address from DNS records.

```
Command Prompt - nslookup

C:\Users\paras>nslookup google.com
Server:  dsldevice.lan
Address:  192.168.1.254

Non-authoritative answer:
Name:     google.com
Addresses: 2404:6800:4009:812::200e
          142.250.67.174

C:\Users\paras>nslookup
Default Server:  dsldevice.lan
Address:  192.168.1.254

> google.com
Server:  dsldevice.lan
Address:  192.168.1.254

Non-authoritative answer:
Name:     google.com
Addresses: 2404:6800:4009:812::200e
          142.250.67.174

>
```

3) ping command is used to ensure that a computer can communicate to a specified device over the network. ping command sends Internet Control Message Protocol(ICMP) Echo Request messages in the form of packets to the destination computer and waits in order to get the response back. Once the packets are received by the destined computer, it starts sending the packets back. ping command provides details such as

- number of packets transmitted
- number of packets received
- time taken by the packet to return

```
Command Prompt
Microsoft Windows [Version 10.0.19041.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\paras>ping google.com

Pinging google.com [172.217.160.174] with 32 bytes of data:
Reply from 172.217.160.174: bytes=32 time=434ms TTL=119
Reply from 172.217.160.174: bytes=32 time=24ms TTL=119
Reply from 172.217.160.174: bytes=32 time=22ms TTL=119
Reply from 172.217.160.174: bytes=32 time=21ms TTL=119

Ping statistics for 172.217.160.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 434ms, Average = 125ms

C:\Users\paras>
```

4) Tracert / traceroute:

This command is used to get the route of a packet. In other words, traceroute command is used to determine the path along which a packet travels. It also returns the number of hops taken by the packet to reach the destination. This command prints to the console, a list of hosts through which the packet travels to the destination.

How to Use the TRACERT Utility

The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

TRACERT sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum TTL is reached. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. Note however that some routers silently drop packets that have expired TTLs, and these packets are invisible to TRACERT.

TRACERT prints out an ordered list of the intermediate routers that return ICMP "Time Exceeded" messages. Using the -d option with the tracert command instructs TRACERT not to perform a DNS lookup on each IP address, so that TRACERT reports the IP address of the near-side interface of the routers. 3 packets are sent.

```
Command Prompt

C:\Users\paras>tracert google.com

Tracing route to google.com [172.217.160.174]
over a maximum of 30 hops:

  1    1 ms    1 ms    1 ms    dslddevice.lan [192.168.1.254]
  2   23 ms   24 ms   22 ms   10.153.128.1
  3   24 ms   24 ms   23 ms   45.127.44.242
  4   73 ms   23 ms   23 ms   108.170.248.177
  5   23 ms   23 ms   21 ms   74.125.251.133
  6   21 ms   23 ms   23 ms   bom05s12-in-f14.1e100.net [172.217.160.174]

Trace complete.

C:\Users\paras>
```

5) ARP: Displays and modifies entries in the Address Resolution Protocol (ARP) cache. The ARP cache contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer. Used without parameters, **arp** displays help information.

ARP -a

Displays current arp cache tables for all interfaces.

```
C:\Users\paras>arp -a

Interface: 192.168.1.7 --- 0xf
Internet Address      Physical Address      Type
192.168.1.5           ce-56-8a-b0-cf-3e     dynamic
192.168.1.254         78-17-35-dd-b2-d0     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
239.192.152.143       01-00-5e-40-98-8f     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.17.160.1 --- 0x28
Internet Address      Physical Address      Type
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
239.192.152.143       01-00-5e-40-98-8f     static
239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\paras>
```

6) Rarp: Reverse Address Resolution Protocol. This is obsolete so it does not work on windows. Reverse mapping. Physical to ip address.

7) Hostname: Prints the name of current host. Basically your device name.

8) Whois: We needed to download whois.exe file to run this command. It is a query and response protocol that is used to find out details about any registered user or internet resource such as domain name, ip address and other info.

9) TCPdump/Windump: Windump is windows version of Tcpdump. We need to download winpcap and windump. Tcp dump is a packet analysing tool to troubleshoot connectivity issue in linux. It is used to capture, filter and analyse network traffic such as TCP/IP packets going through your system. It captures logs in the form of pcap file which can be opened through a tool called wireshark.

```
C:\Users\paras\Downloads\WinDump.exe
C:\Users\paras\Downloads\WinDump.exe: listening on \Device\NPF_{9D587809-62E1-4F57-B2C9-192A3F8ED65F}
10:29:46.600224 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 PTR? _sleep-proxy._udp.local. (41)
10:34:50.917315 IP Paras-PC.mshome.net.56425 > 239.255.255.250.1900: UDP, length 137
10:34:53.920333 IP Paras-PC.mshome.net.56425 > 239.255.255.250.1900: UDP, length 137
10:34:56.925235 IP Paras-PC.mshome.net.56425 > 239.255.255.250.1900: UDP, length 137
10:38:50.556608 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? wpad.local. (28)
10:38:50.558476 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? wpad.local. (28)
10:38:50.780576 IP Paras-PC.mshome.net.63843 > 239.255.255.250.1900: UDP, length 174
10:38:51.561503 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? wpad.local. (28)
10:38:51.562101 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? wpad.local. (28)
10:38:51.785193 IP Paras-PC.mshome.net.63843 > 239.255.255.250.1900: UDP, length 174
10:38:52.377296 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? wpad.local. (28)
10:38:52.377829 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? wpad.local. (28)
10:38:52.785670 IP Paras-PC.mshome.net.63843 > 239.255.255.250.1900: UDP, length 174
10:38:53.386056 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? wpad.local. (28)
10:38:53.386912 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? wpad.local. (28)
10:38:53.785394 IP Paras-PC.mshome.net.63843 > 239.255.255.250.1900: UDP, length 174
10:38:57.343538 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? xezkmiqgjwr.local. (35)
10:38:57.344440 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? xunhqjvk.local. (32)
10:38:57.345300 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? xunhqjvk.local. (32)
10:38:57.345896 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? xunhqjvk.local. (32)
10:38:57.346547 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? ecyxoxu.local. (31)
10:38:57.347125 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? ecyxoxu.local. (31)
10:38:57.695010 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 PTR? _googlecast._tcp.local. (40)
10:38:57.696122 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? xezkmiqgjwr.local. (35)
10:38:58.343442 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? xunhqjvk.local. (32)
10:38:58.344262 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? xunhqjvk.local. (32)
10:38:58.359121 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? ecyxoxu.local. (31)
10:38:58.360148 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? ecyxoxu.local. (31)
10:38:58.361302 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 PTR? _googlecast._tcp.local. (40)
10:38:58.711859 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? wpad.local. (28)
10:38:58.712163 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? wpad.local. (28)
10:38:59.566732 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? wpad.local. (28)
10:38:59.567477 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 A? wpad.local. (28)
10:39:00.575774 IP6 Paras-PC.5353 > ff02::fb.5353: 0 A? wpad.local. (28)
10:39:00.576597 IP Paras-PC.mshome.net.5353 > 224.0.0.251.5353: 0 PTR? _googlecast._tcp.local. (40)
```


Netstat: Current listed connections. Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

```
Command Prompt
Microsoft Windows [Version 10.0.19041.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\paras>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:62963          Paras-PC:65001         ESTABLISHED
TCP    127.0.0.1:63364          Paras-PC:63395         ESTABLISHED
TCP    127.0.0.1:63395          Paras-PC:63364         ESTABLISHED
TCP    127.0.0.1:65001          Paras-PC:62963         ESTABLISHED
TCP    192.168.1.7:5040        192.168.1.5:44966      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45116      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45458      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45532      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45610      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45644      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45712      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45788      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45808      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45946      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:45988      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:46024      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:46164      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:46232      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:46242      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:46282      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:46350      CLOSE_WAIT
TCP    192.168.1.7:5040        192.168.1.5:46370      ESTABLISHED
TCP    192.168.1.7:63414      40.90.189.152:https    ESTABLISHED
TCP    192.168.1.7:63542      bom05s09-in-f10:https  CLOSE_WAIT
TCP    192.168.1.7:63543      bom12s01-in-f10:https  ESTABLISHED
TCP    192.168.1.7:63545      bom05s09-in-f10:https  CLOSE_WAIT
TCP    192.168.1.7:63793      a104-89-113-52:https   CLOSE_WAIT
TCP    192.168.1.7:63794      a104-89-113-52:https   CLOSE_WAIT
TCP    192.168.1.7:63796      a104-89-113-52:https   CLOSE_WAIT
TCP    192.168.1.7:63799      a23-212-241-219:http   CLOSE_WAIT
TCP    192.168.1.7:63800      a23-212-241-219:http   CLOSE_WAIT
TCP    192.168.1.7:63801      a23-212-241-219:http   CLOSE_WAIT
TCP    192.168.1.7:63802      a23-212-241-219:http   CLOSE_WAIT
TCP    192.168.1.7:63803      a23-212-241-219:http   CLOSE_WAIT
TCP    192.168.1.7:63804      a23-212-241-219:http   CLOSE_WAIT
TCP    192.168.1.7:65017      52.139.250.253:https   ESTABLISHED
TCP    192.168.1.7:65125      52.111.240.8:https     ESTABLISHED
TCP    192.168.1.7:65137      52.109.124.33:https    ESTABLISHED
TCP    192.168.1.7:65186      bom07s18-in-f10:https  CLOSE_WAIT
TCP    192.168.1.7:65250      whatsapp-cdn-shv-02-bom1:https ESTABLISHED
TCP    192.168.1.7:65284      ec2-52-42-154-79:https ESTABLISHED
TCP    192.168.1.7:65293      13.89.202.241:https    ESTABLISHED
TCP    192.168.1.7:65295      161.69.38.37:http      TIME_WAIT
TCP    192.168.1.7:65299      1drv:https              ESTABLISHED
TCP    192.168.1.7:65300      52.109.120.3:https     TIME_WAIT
TCP    192.168.1.7:65301      a-0001:https            ESTABLISHED
TCP    192.168.1.7:65302      52.109.120.3:https     TIME_WAIT
```