

Basic IP Commands

Aim: To study basic IP commands.

Theory:

- PING
- IPCONFIG
- GETMAC
- HOSTNAME
- NSLOOKUP
- TRACERT
- NETSTAT
- ARP
- PATHPING

PING

The ping command is one of the most often used networking utilities for detecting devices on a network and for troubleshooting network problems.

When you ping a device you send that device a short message, which it then sends back (**the echo**).

The general format is **ping hostname** or **ping IPaddress**.

Example

ping www.google.com or **ping 216.58.208.68**

The Ping command allows you to test the reachability of a device on a network. Pinging a host should return four data packets, if the data packets are not returned you know there is a problem with your network connection.

A failed ping results in a **request timed out** response, and a success results in the **reply from** message with the **round-trip delay** in milliseconds.

```
C:\Users\91976>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=5ms TTL=64
Reply from 192.168.1.10: bytes=32 time=1ms TTL=64
Reply from 192.168.1.10: bytes=32 time<1ms TTL=64
Reply from 192.168.1.10: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms
```

```
C:\Users\91976>ping aيتدgoa.edu.in

Pinging aيتدgoa.edu.in [104.21.38.118] with 32 bytes of data:
Reply from 104.21.38.118: bytes=32 time=143ms TTL=54
Reply from 104.21.38.118: bytes=32 time=143ms TTL=54
Reply from 104.21.38.118: bytes=32 time=143ms TTL=54
Reply from 104.21.38.118: bytes=32 time=144ms TTL=54

Ping statistics for 104.21.38.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 143ms, Maximum = 144ms, Average = 143ms
```

ping /?

This command shows detailed help for all of ping options.

IPCONFIG

The ipconfig command is one of the more useful basic Windows network commands everyone should know and use to troubleshoot problems. The ipconfig command displays basic IP address configuration information for the Windows device you are working on. In fact, the command will display information for every network adapter that has ever been installed on your Windows 10 computer.

To run the basic command, at the prompt type:

ipconfig

The general information includes IP Addresses for both IPv4 and IPv6, the Default Gateway, and the Subnet Mask. Adding the parameter /all to the command will display DNS Server information and details concerning IP Address leases.

```
C:\Users\91976>ipconfig

Windows IP Configuration

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  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::70ad:e793:94c9:884f%4
    IPv4 Address. . . . . : 192.168.7.48
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 192.168.1.1

Wireless LAN adapter Wi-Fi:

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

Ethernet adapter Bluetooth Network Connection:

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

GETMAC

Every network capable device on the internet has a unique identifying number called its MAC address. The number is assigned during manufacture and is established in the hardware of the device. Using the Getmac command, a user can determine the MAC address of their various network devices. Some administrators will use the unique MAC addresses of devices to limit what can and cannot connect to a network.

To run the basic command, at the prompt type:

getmac

```
C:\Users\91976>getmac

Physical Address      Transport Name
=====
00-E0-4C-31-54-AE    \Device\Tcpip_{1610D77E-0933-4F79-B6B1-8525DE13D577}
AC-67-5D-56-34-BF    Media disconnected
AC-67-5D-56-34-BB    Media disconnected
```

HOSTNAME

The Windows 10 HostName network command will simply display the current name of your Windows 10 computer (**Figure B**). This is the name your computer uses to identify itself to the other devices and servers on your local network. You can find this name in the System information screen in the GUI, but this command is quicker.

To run the basic command, at the prompt type:

hostname

```
C:\Users\91976>hostname
LAPTOP-3GEQN09N
```

NSLOOKUP

The NSLookUp Windows 10 network command displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Using NSLookUp without a parameter will show the DNS server your PC is currently using to resolve domain names into IP addresses.

To run the basic command, at the prompt type:

nslookup

```
C:\Users\91976>nslookup
Default Server:  dns.google
Address:  8.8.8.8
```

Type **nslookup** and **domain name** and the command will return the A record for the domain you run a query for.

```
C:\Users\91976>nslookup aitdgoa.edu.in
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    aitdgoa.edu.in
Addresses:  2606:4700:3033::6815:2676
           2606:4700:3037::ac43:de95
           104.21.38.118
           172.67.222.149
```

TRACERT

Another handy tool for troubleshooting network connections in Windows 10 is the tracert command. This command will trace the route a data packet takes before reaching its destination, displaying information on each hop along the route. Each hop of the route will display the latency between your device and that particular hop and the IP address of the hop

To run the basic command, at the prompt type:

tracert [host]

Where [host] is the name or IP address of a common host server

```
C:\Users\91976>tracert aitdgoa.edu.in

Tracing route to aitdgoa.edu.in [104.21.38.118]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  10.0.0.1
  1  1 ms  2 ms  1 ms  103.29.249.213
  2  2 ms  3 ms  2 ms  192.168.100.1
  3  3 ms  2 ms  1 ms  gw.gwave.in [103.29.249.1]
  4  15 ms  15 ms  15 ms  aes-static-025.51.246.61.airtel.in [61.246.51.25]
  5  148 ms  142 ms  140 ms  182.79.206.46
  6  206 ms  135 ms  161 ms  linx-lon1.as13335.net [195.66.225.179]
  7  143 ms  142 ms  138 ms  172.70.94.2
  8  134 ms  138 ms  134 ms  104.21.38.118

Trace complete.
```

NETSTAT

The Netstat command displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics, and IPv6 statistics. When used without parameters, this command displays active TCP connections. The information this command provides can be useful in pinpointing problems in your network connections.

To run the basic command, at the prompt type:

netstat

```
C:\Users\91976>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.7.48:61779	20.198.162.76:https	ESTABLISHED
TCP	192.168.7.48:61833	20.198.162.76:https	ESTABLISHED
TCP	192.168.7.48:61854	bom05s12-in-f10:https	ESTABLISHED
TCP	192.168.7.48:61857	bom07s26-in-f14:https	ESTABLISHED
TCP	192.168.7.48:61858	bom07s25-in-f14:https	ESTABLISHED
TCP	192.168.7.48:61861	bom07s28-in-f3:https	ESTABLISHED
TCP	192.168.7.48:61862	sa-in-f188:https	ESTABLISHED
TCP	192.168.7.48:61864	bom05s12-in-f10:https	ESTABLISHED
TCP	192.168.7.48:61944	dns:https	ESTABLISHED
TCP	192.168.7.48:61948	bom05s15-in-f3:https	ESTABLISHED
TCP	192.168.7.48:61994	bom07s27-in-f2:https	ESTABLISHED
TCP	192.168.7.48:62468	192.168.14.138:8009	ESTABLISHED

ARP

The Windows 10 network command Arp displays entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet physical addresses. To get useful information from the Arp command you must provide a parameter. The most general parameter is /a, which displays current Arp cache tables for all interfaces.

To run the basic command, at the prompt type:

```
arp /a
```

```
C:\Users\91976>arp /a
```

```
Interface: 192.168.7.48 --- 0x4
```

Internet Address	Physical Address	Type
192.168.0.22	68-f7-28-6e-b3-61	dynamic
192.168.0.40	a4-1f-72-58-27-55	dynamic
192.168.1.1	c0-ea-e4-f9-0b-d2	dynamic
192.168.1.10	44-a8-42-3a-0a-17	dynamic
192.168.1.121	d4-be-d9-bb-47-1c	dynamic
192.168.2.113	b0-83-fe-6f-ac-47	dynamic
192.168.3.5	f4-81-39-49-e4-67	dynamic
192.168.14.138	28-ad-18-65-17-a8	dynamic
192.168.15.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.250	01-00-5e-00-00-fa	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
224.0.0.253	01-00-5e-00-00-fd	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

PATHPING

Generally speaking, the Windows 10 network command PathPing combines the ping command with the tracert command, providing information about network latency and network loss at intermediate hops between a source and destination. As you can see in **output**, the PathPing command provides more detail than either ping or tracert can provide, such as latency reports and statistics on packet loss.

To run the basic command, at the prompt type:

```
pathping [host]
```


Where [host] is the name or IP address of a common host server (google.com, techrepublic.com, etc.).

Be patient when using the pathping command as it will take five minutes in order to gather all of the statistics for you.

```
C:\Users\91976>pathping aitdgoa.edu.in

Tracing route to aitdgoa.edu.in [104.21.38.118]
over a maximum of 30 hops:
 0  LAPTOP-3GEQN09N [192.168.7.48]
 1  103.29.249.213
 2  192.168.100.1
 3  gw.gwave.in [103.29.249.1]
 4  aes-static-025.51.246.61.airtel.in [61.246.51.25]
 5  182.79.206.46
 6  *      linx-lon1.as13335.net [195.66.225.179]
 7  172.70.94.2
 8  104.21.38.118

Computing statistics for 200 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
     Lost/Sent = Pct Lost/Sent = Pct  Lost/Sent = Pct  Address
 0      0/ 100 = 0%      0/ 100 = 0%      0/ 100 = 0%      LAPTOP-3GEQN09N [192.168.7.48]
 1    2ms      0/ 100 = 0%      0/ 100 = 0%      0/ 100 = 0%      103.29.249.213
 2    3ms      0/ 100 = 0%      0/ 100 = 0%      0/ 100 = 0%      192.168.100.1
 3    4ms      0/ 100 = 0%      0/ 100 = 0%      0/ 100 = 0%      gw.gwave.in [103.29.249.1]
 4   17ms      1/ 100 = 1%      0/ 100 = 0%      0/ 100 = 0%      aes-static-025.51.246.61.airtel.in [61.246.51.25]
 5  151ms      1/ 100 = 1%      0/ 100 = 0%      0/ 100 = 0%      182.79.206.46
 6  143ms      1/ 100 = 1%      0/ 100 = 0%      0/ 100 = 0%      linx-lon1.as13335.net [195.66.225.179]
 7  131ms      1/ 100 = 1%      0/ 100 = 0%      0/ 100 = 0%      172.70.94.2
 8  136ms      1/ 100 = 1%      0/ 100 = 0%      0/ 100 = 0%      104.21.38.118

Trace complete.
```

Conclusion: Basic IP commands were studied successfully.