**Computer Network**

**(Day -3)**

1) **What is Ping** command?

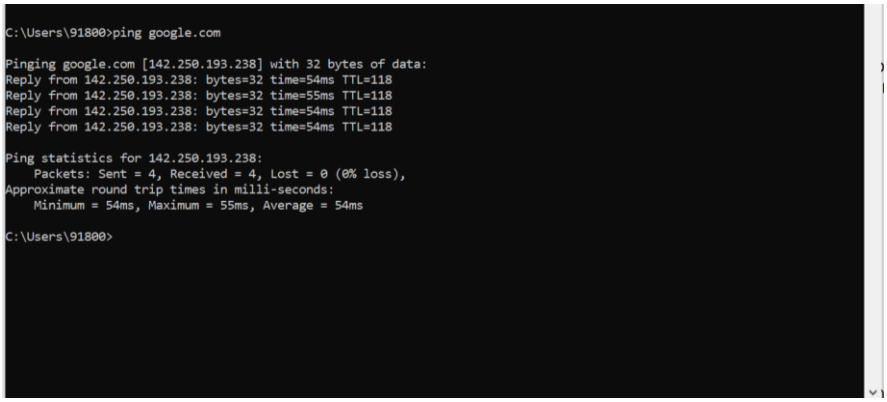
The Ping command allows you to test the reachability of a device on a network. Pinging a host should return four data packets, if the data packets are not returned you know there is a problem with your network connection.

To run the basic command, at the prompt type:

ping [host]

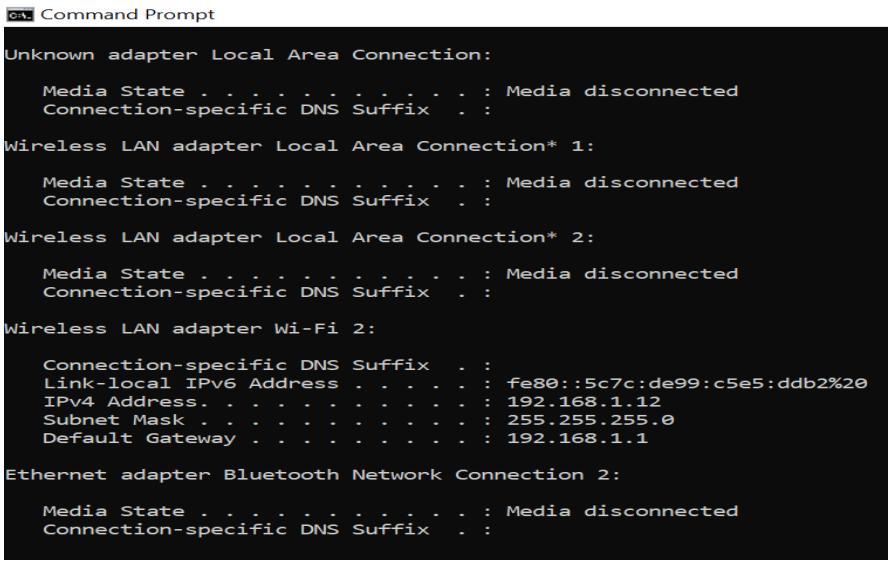
Where [host] is the name or IP address of a common host server (google.com, techrepublic.com, etc.). **Figure A** shows you what happens when we ping the google.com.

**Figure A**




2) **what is IPConfig**

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.




ipconfig

To display the full TCP/IP configuration for all adapters, type:
ipconfig /all
To renew a DHCP-assigned IP address configuration for only the Local Area Connection adapter, type:

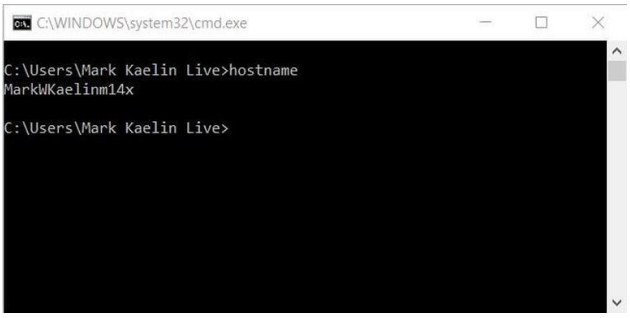
ipconfig /renew Local Area Connection
To flush the DNS resolver cache when troubleshooting DNS name resolution problems, type:
ipconfig /flushdns
To display the DHCP class ID for all adapters with names that start with Local, type:

ipconfig /showclassid Local*
To set the DHCP class ID for the Local Area Connection adapter to TEST, type:

ipconfig /setclassid Local Area Connection TEST

### 3) what is 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.



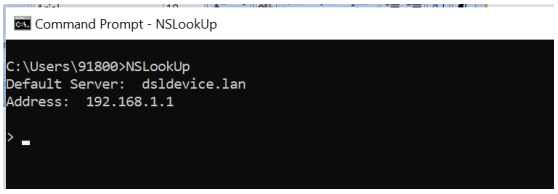

To run the basic command, at the prompt type:

hostname

Check out Microsoft Docs for a more advanced look at the HostName command and its variables and switches.

### 4) what is 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.

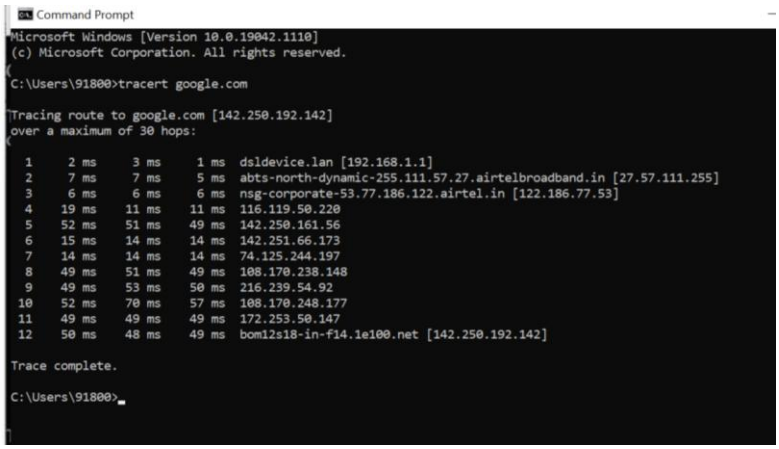



To run the basic command, at the prompt type:

nslookup

### 5) what is Tracert command

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, as shown in **Figure D**.



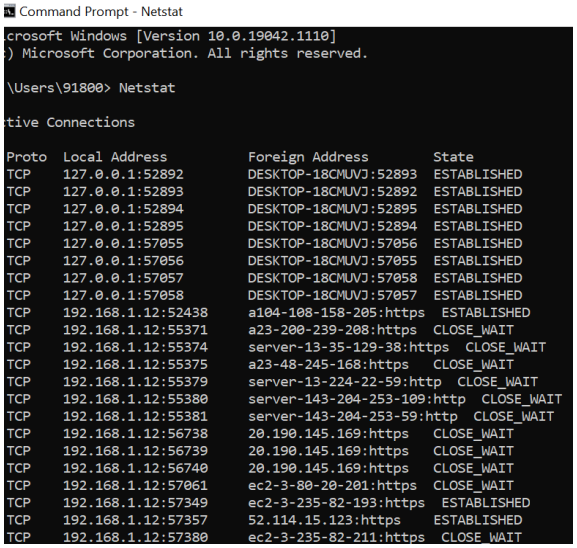

To run the basic command, at the prompt type:

tracert [host]

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

### 6) what is Netstat command

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

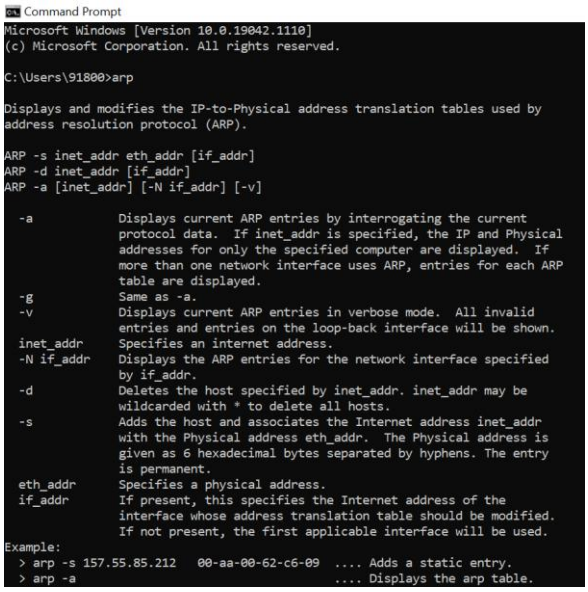
Check out Microsoft Docs for a more advanced look at the Netstat command and its variables and switches.

### 7) what is 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:

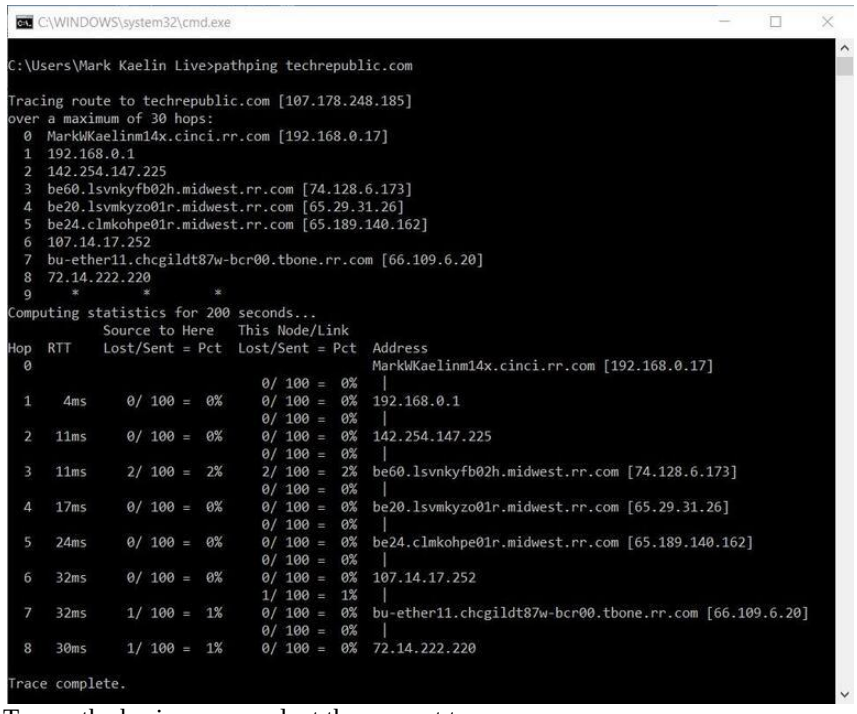
arp /a




Check out Microsoft Docs for a more advanced look at the Arp command and its variables and switches.

### 8) what is 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 **Figure E**, the PathPing command provides more detail than either ping or tracert can provide, such as latency reports and statistics on packet loss.



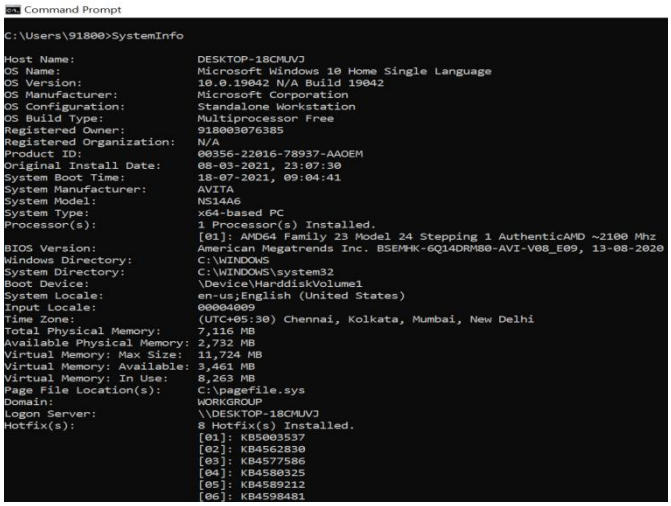

To run the basic command, at the prompt type:

pathping [host]

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

Check out Microsoft Docs for a more advanced look at the PathPing command and its variables and switches.

**9) what is SystemInfo**




The last command on our list is the SystemInfo command, which displays a detailed list of configuration information about your Windows 10 PC. The information listed by this command is too lengthy to mention in full but includes the installed version of Windows 10, the host name, the Product ID, the type and number of CPUs, RAM configuration, network card details and installed hotfixes.

To run the basic command, at the prompt type:

systeminfo

10) **What is RIP?**

RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.

11) **What are proxy servers, and how do they protect computer networks?**

Proxy servers primarily prevent external users who are identifying the IP addresses of an internal network. Without knowledge of the correct IP address, even the physical location of the network cannot be identified. Proxy servers can make a network virtually invisible to external users.

12) **What is NOS?**

NOS, or Network Operating System, is specialized software. The main task of this software is to provide network connectivity to a computer in order to communicate with other computers and connected devices

13) **What are firewalls?**

Firewalls serve to protect an internal network from external attacks. These external threats can be hackers who want to steal data or computer viruses that can wipe out data in an instant. It also prevents other users from external networks from gaining access to the private network.

14) **What is SLIP?**

SLIP, or Serial Line Interface Protocol, is an old protocol developed during the early UNIX days. This is one of the protocols that are used for remote access.

15) **What is a Hybrid Network?**

A hybrid network is a network setup that makes use of both client-server and peer-to-peer architecture.

16) **What advantages does fiber optics have over other media?**

One major advantage of fiber optics is that it is less susceptible to electrical interference. It also supports higher bandwidth, meaning more data can be transmitted and received. Signal degrading is also very minimal over long distances.

17) **What are the maximum networks and hosts in class A, B, and C network?**

For Class A, there are 126 possible networks and 16,777,214 hosts. For Class B, there are 16,384 possible networks and 65,534 hosts. For Class C, there are 2,097,152 possible networks and 254 hosts

18) **What is the standard color sequence of a straight-through cable?**

Orange/white, orange, green/white, blue, blue/white, green, brown/white, brown.

19) **You need to connect two computers for file sharing. Is it possible to do this without using a hub or a router?**

Yes, you can connect two computers, using only one cable. A crossover type cable can be used in this scenario. In this setup, the data transmit pin of one cable is connected to the data receive pin of the other cable, and vice versa

20) **What is the difference between a straight-through and crossover cable?**

A straight-through cable is used to connect computers to a switch, hub, or router. A crossover cable is used to connect two similar devices, such as a PC to PC or Hub, to the Hub.

21) **When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?**

Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when another one replaced the NIC card.

22) **What is sneakernet?**

Sneakernet is believed to be the earliest form of networking wherein data is physically transported using removable media, such as disk, tapes.

23) **What is the 5-4-3 rule, and in which architecture is it used?**

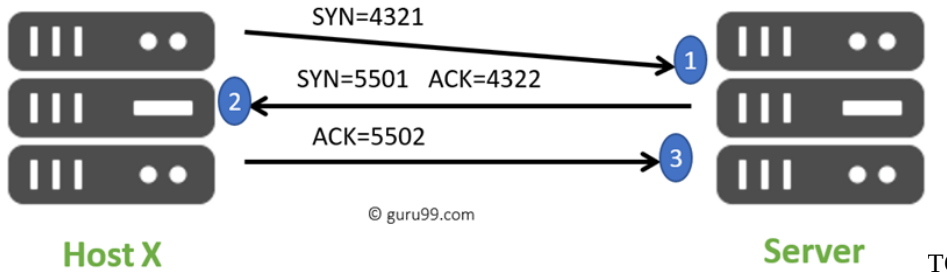
The 5-4-3 rule is used in 10Base2 and 10Base5 Ethernet architectures. In this rule, there can be a maximum of five segments in a network connected with four repeaters. Out of these five segments, only three segments can be populated with nodes.

24) **What are the benefits of the Hamming code?**

Here, are important benefits of Hamming code

- The Hamming code method is effective on networks where the data streams are given for the single-bit errors.
- Hamming code not only provides the detection of a bit error but also helps you to indent bit containing error so that it can be corrected.
- The ease of use of hamming codes makes it suitable for use in computer memory and single-error correction.
-

**25) What Is TCP Three-Way Handshake?**




TCP Three-Way Handshake

THREE-WAY handshake or a TCP 3-way handshake is a process that is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

25) **What is a Haming code?**

Hamming code is a liner code that is useful for error detection up to two immediate bit errors. It is capable of single-bit errors.

In Hamming code, the source encodes the message by adding redundant bits in the message. These redundant bits are mostly inserted and generated at certain positions in the message to accomplish the error detection and correction process.

26) **TCP Connection Establishment (Called, Three-Way Handshake)**

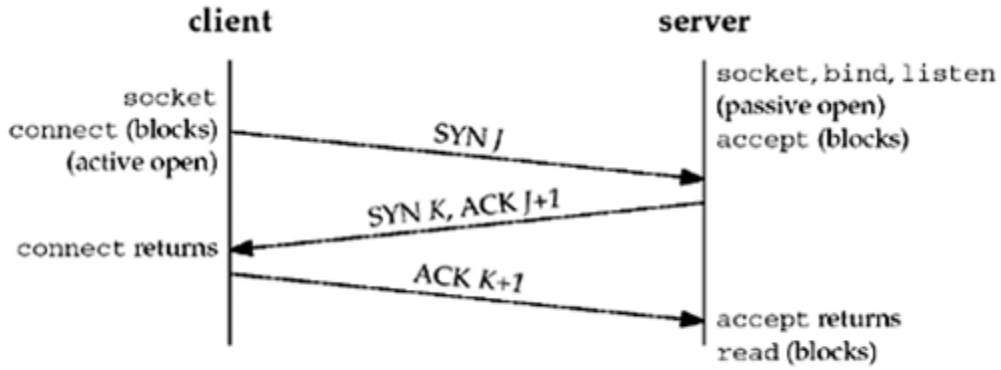
The following events happens when a TCP connection is established:

1. When a client initiate an active open by calling **connect()** function, then client TCP sends a "synchronize" (**SYN**), which includes client's initial sequence number for the data which will be send on the connection.

2. The TCP server acknowledges (**ACK**) the client's SYN along with its own SYN containing the initial sequence number for the data that the server is going to send on the active connection.

3. Finally, client TCP acknowledge the server's SYN and connection will become active.

Three packets required to make an active connection, so that it is called three-way handshake.




**TCP Connection Termination (May called, Four-Way Handshake)**

The following events happens when a TCP connection is closed:

1. When a TCP client/server close the connection first (active close), then TCP sends a **FIN** segment.

2. On the other hand who receives the FIN performs the passive close and acknowledged by TCP.

3. Later of time the application that received the end-of-file will close its socket and thus TCP to send a FIN.

4. Finally, TCP which receives this final FIN (the end which initiated the active close) acknowledges the FIN.

Four packets required to close an active connection, so that it is called four-way handshake.