PRACTICAL-2

AIM: NETWORKING COMMANDS

1. What are networking commands?

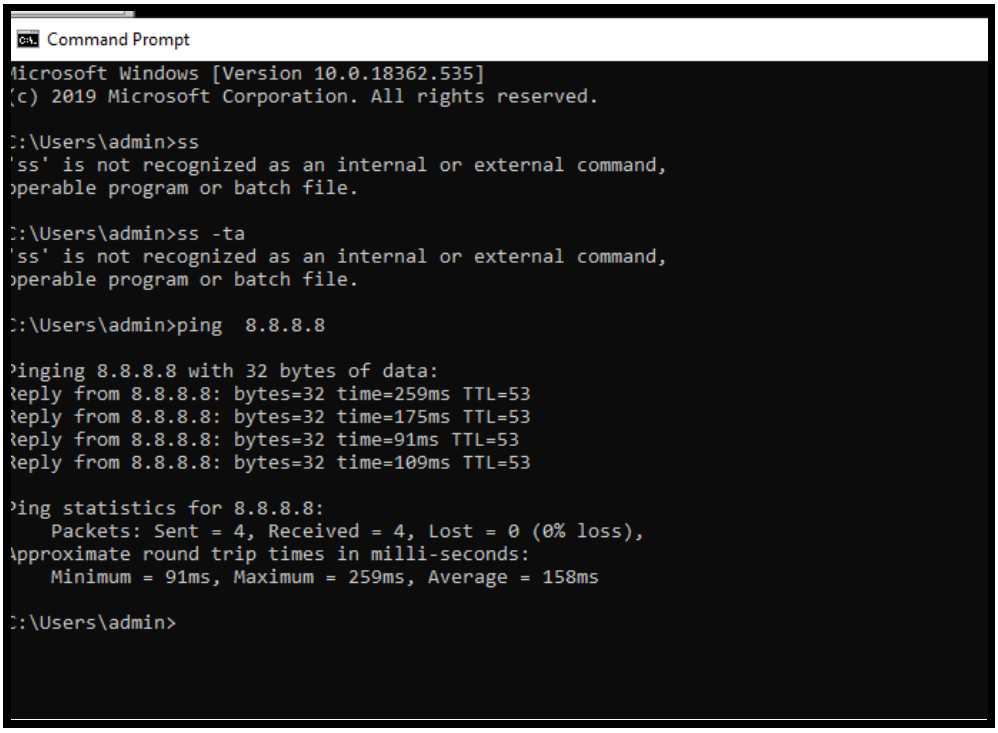
- The **commands** (such as tracert, traceroute, ping, arp, netstat, nbstat, NetBIOS, ipconfig, winipcfg and nslookup) and their arguments, options and parameters used to troubleshoot the computer **network**.

2. Why we require networking commands?

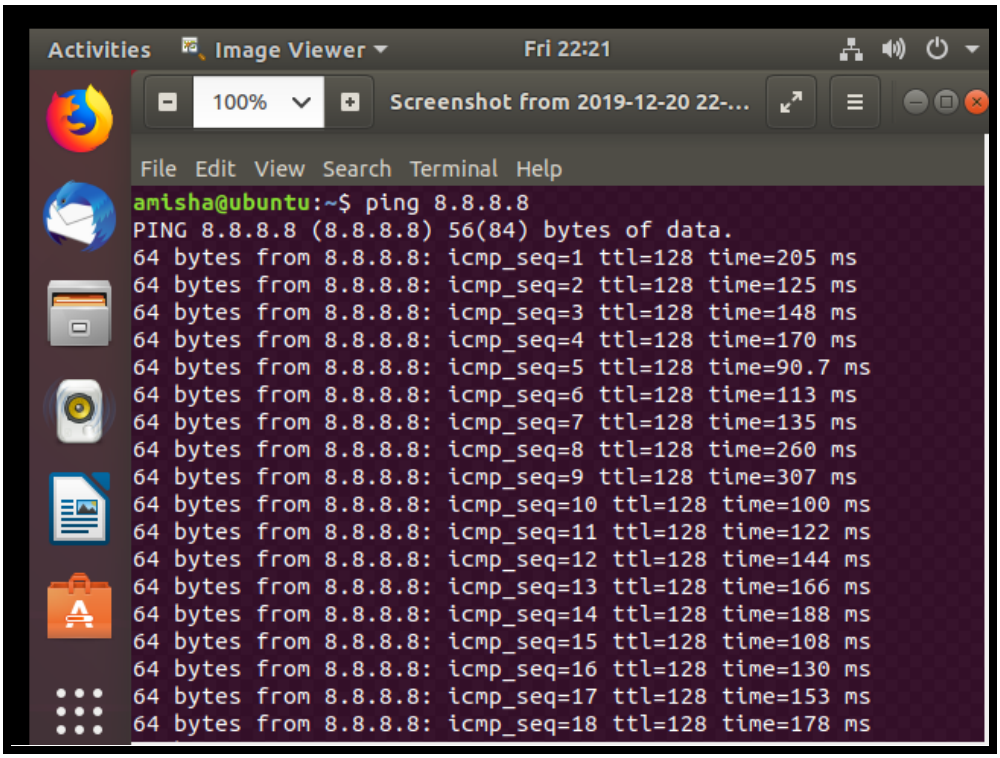
- For trouble shooting and reassuring network activity

3. Where to perform those commands?

- On compiler for windows cmd and for linux, ubantu or cent-os terminal



```
Command Prompt
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\admin>ss
'ss' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\admin>ss -ta
'ss' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\admin>ping  8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=259ms TTL=53
Reply from 8.8.8.8: bytes=32 time=175ms TTL=53
Reply from 8.8.8.8: bytes=32 time=91ms TTL=53
Reply from 8.8.8.8: bytes=32 time=109ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 91ms, Maximum = 259ms, Average = 158ms

C:\Users\admin>
```



4. What is default gateway and subnet mask?

- **Default Gateway** is IP of your Router. In simple words, 192.168.0.1 and **Subnet** mask will be automatically deduced by operating system. 255.255.255.0.

5. Why we need default gateway?

- A default gateway makes it possible for devices in one network to communicate with devices in another network. If a computer, for example, requests a web page, the request goes through the default gateway before exiting the local network to reach the internet. Think of a default gateway as an intermediate device between the local network and the internet. The default gateway transfers internal data to the internet and back again.

6. Types of default gateways

- Broadband-Routers
- Dial-up
- Network-adaptors

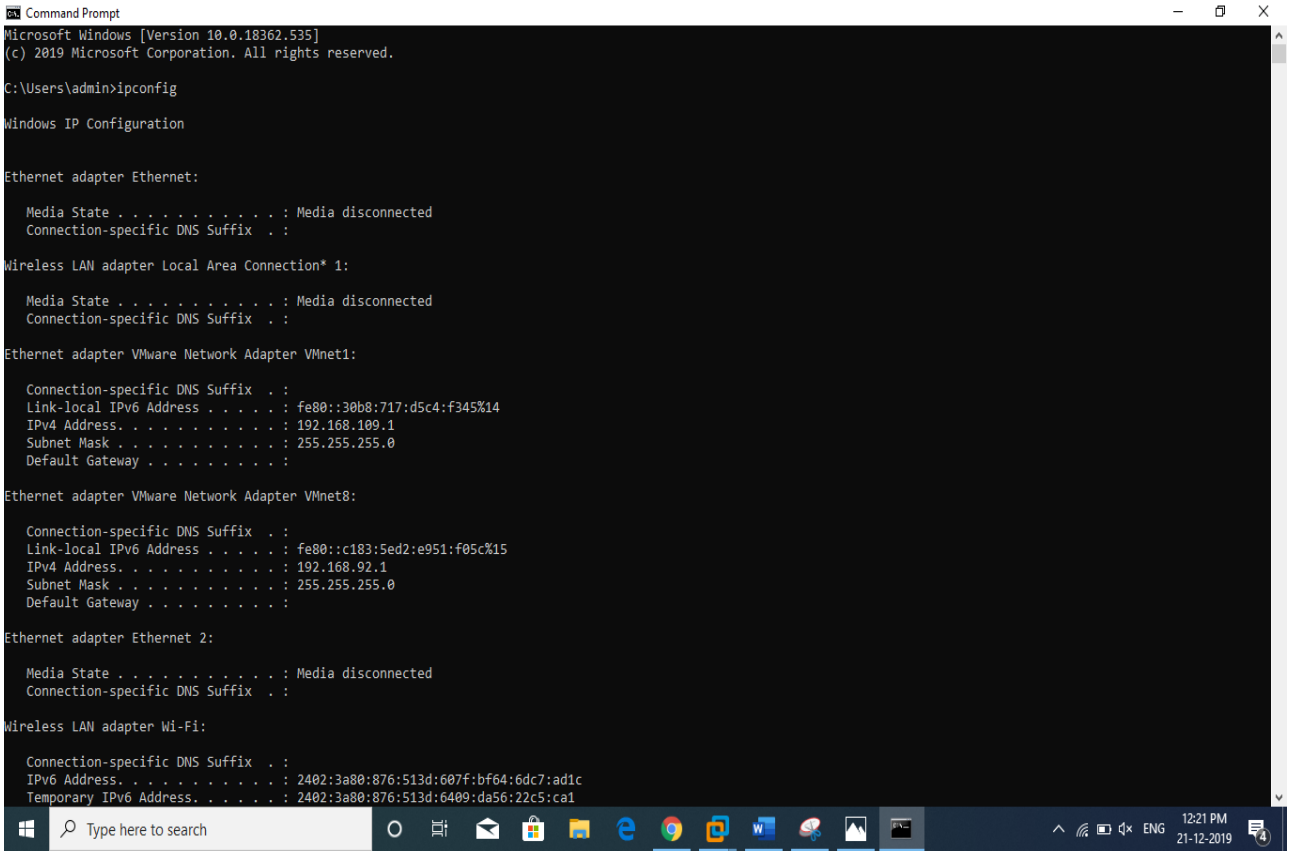
SCENARIOS AND LIST OF COMMANDS

CASE 1:
Consider a situation, where you need to set a default gateway then how you will find your default gateway ip address?

For windows: ipconfig

For linux : netstat and iproute

CMD OUTPUT OF :ipconfig



```
Command Prompt
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\admin>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  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::30b8:717:d5c4:f345%14
   IPv4 Address. . . . . . . . . . . : 192.168.109.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c183:5ed2:e951:f05c%15
   IPv4 Address. . . . . . . . . . . : 192.168.92.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:3a80:876:513d:607f:bf64:6dc7:ad1c
   Temporary IPv6 Address. . . . . . : 2402:3a80:876:513d:6409:da56:22c5:ca1
Type here to search
ENG 12:21 PM 21-12-2019
```

1. Ethernet adapter Ethernet: enables a computer to access an **Ethernet network** (**LAN**). Currently it is not connected so, media disconnected is showing.

2. Wireless LAN adapter is also not connected.

3. and 4. for VMware: let us focus on 1st DNS suffix

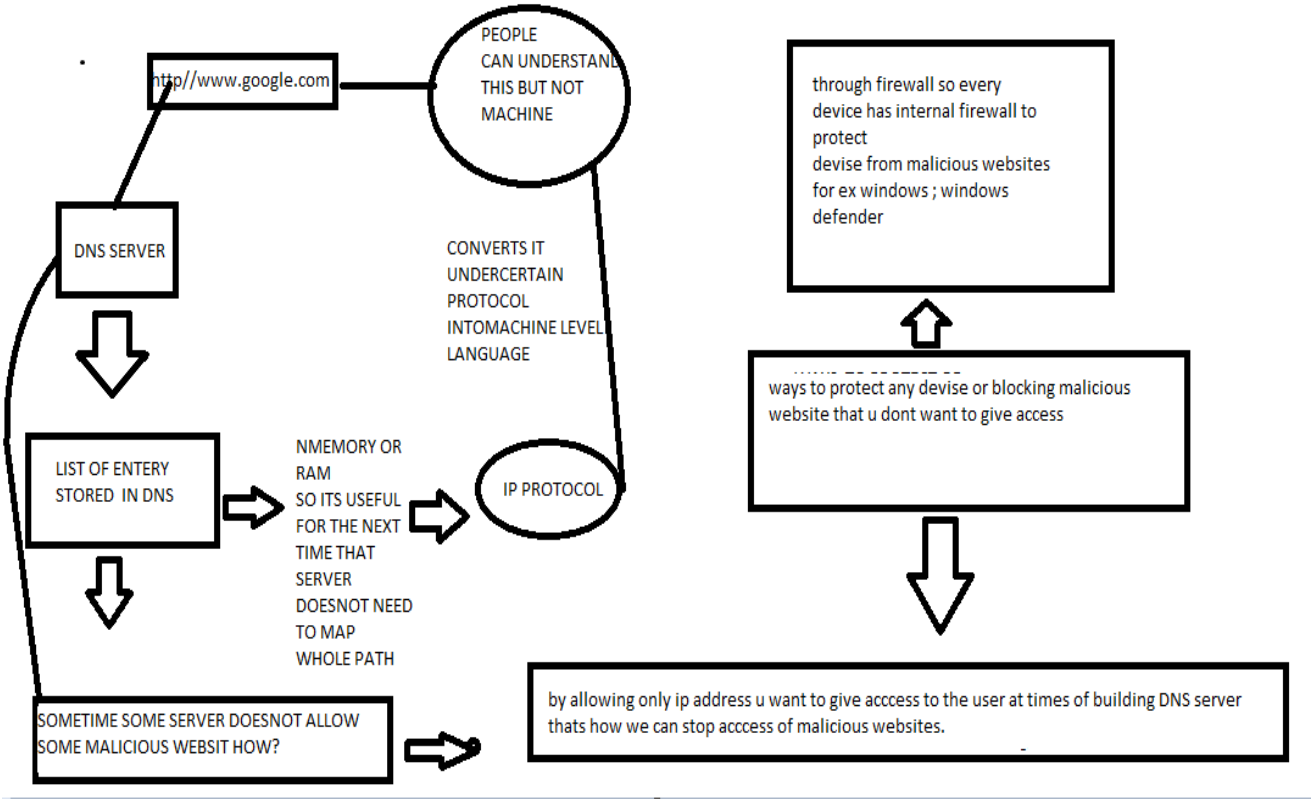
DOMAIN NAME SERVER.

For-example https://www.google.com
When a user request it this URL is : A directory (list)of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses.

Scenario1: you don't want to give access to students particular to some websites but how to do?

Scenario 2: How DNS server exactly works?

DNS SERVER:



4. Wifi for ipconfig that wifi adapter currently wifi is on so, Here it indicates details of wifi currently XYZ phone is having this ip and ipv4 and subnet mask it is used to get default gateway information in this case xyz is default gateway

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:3a80:876:513d:607f:bf64:6dc7:ad1c
   Temporary IPv6 Address. . . . . . : 2402:3a80:876:513d:6409:da56:22c5:ca1
   Link-local IPv6 Address . . . . . : fe80::607f:bf64:6dc7:ad1c%21
   IPv4 Address. . . . . . . . . . . : 192.168.43.235
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::22a6:cff:fe94:cbb2%21
                                       192.168.43.1

C:\Users\admin>
```

5. ipconfig all : to get all details of ipv4 and 6

```
USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                      ... Show information
    > ipconfig /all                 ... Show detailed information
    > ipconfig /renew               ... renew all adapters
    > ipconfig /renew EL*           ... renew any connection that has its
                                        name starting with EL
```

Scenario 3: consider a situation where I want to change or flush my old DHCP ip so for ipv4: release

Ipv6: release6

And then renew

```
C:\Users\admin>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 Ethernet 2 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  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::30b8:717:d5c4:f345%14
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c183:5ed2:e951:f05c%15
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:3a80:876:513d:607f:bf64:6dc7:ad1c
   Temporary IPv6 Address. . . . . . : 2402:3a80:876:513d:6409:da56:22c5:ca1
   Link-local IPv6 Address . . . . . : fe80::607f:bf64:6dc7:ad1c%21
   Default Gateway . . . . . . . . . : fe80::22a6:cff:fe94:cbb2%21
```

```
C:\Users\admin>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 Ethernet 2 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  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::30b8:717:d5c4:f345%14
   IPv4 Address. . . . . . . . . . . : 192.168.109.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c183:5ed2:e951:f05c%15
   IPv4 Address. . . . . . . . . . . : 192.168.92.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:
```

```
Wireless LAN adapter Local Area Connection* 1:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::30b8:717:d5c4:f345%14
   IPv4 Address. . . . . . . . . . . : 192.168.109.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c183:5ed2:e951:f05c%15
   IPv4 Address. . . . . . . . . . . : 192.168.92.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:3a80:876:513d:607f:bf64:6dc7:ad1c
   Temporary IPv6 Address. . . . . . : 2402:3a80:876:513d:6409:da56:22c5:ca1
   Link-local IPv6 Address . . . . . : fe80::607f:bf64:6dc7:ad1c%21
   IPv4 Address. . . . . . . . . . . : 192.168.43.235
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::22a6:cff:fe94:cbb2%21
                                       192.168.43.1
```

6. Consider a scenario when you want to cross check whether your request is being sent properly or not whether anybody is not accessing your data.

Ping:

To check whether I am connected to any website or not?

Tracert

For ex: google.com

Ping google.com

Ping 8.8.8.8

Ping 4.4.4.4

```
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=615ms TTL=53
Reply from 8.8.8.8: bytes=32 time=112ms TTL=53
Reply from 8.8.8.8: bytes=32 time=120ms TTL=53
Reply from 8.8.8.8: bytes=32 time=129ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 112ms, Maximum = 615ms, Average = 244ms

C:\Users\admin>
```

Yes, all packets are sent perfectly to transmitter and I am receiving all

Tracert command

for example : a client comes to me that my internet connectivity is not up to the mark how would I find?

Fire this command check the particular route and find out that whether a request is received by server, which route and at which point it has been showing dilemmas or whether switch/router/firewall/ISP/devices. where is the problem occurring?

```
C:\Users\admin>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     *       56 ms     3 ms  192.168.43.1
  2   278 ms   201 ms    98 ms  192.168.1.6
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9   239 ms   201 ms    98 ms  dns.google [8.8.8.8]

Trace complete.

C:\Users\admin>
```

It shows that request is going out from phone (wifi) to switch then lost somewhere and finally to the dns google server

Netstat 8.8.8.8: it is showing that these many active connections are in between to show connections are established there so

```
C:\Users\admin>netstat 8.8.8.8

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:443          DESKTOP-DD143JG:54237  ESTABLISHED
  TCP    127.0.0.1:49670        DESKTOP-DD143JG:49671  ESTABLISHED
  TCP    127.0.0.1:49671        DESKTOP-DD143JG:49670  ESTABLISHED
  TCP    127.0.0.1:49672        DESKTOP-DD143JG:49673  ESTABLISHED
  TCP    127.0.0.1:49673        DESKTOP-DD143JG:49672  ESTABLISHED
  TCP    127.0.0.1:49674        DESKTOP-DD143JG:49675  ESTABLISHED
  TCP    127.0.0.1:49675        DESKTOP-DD143JG:49674  ESTABLISHED
  TCP    127.0.0.1:49676        DESKTOP-DD143JG:49677  ESTABLISHED
  TCP    127.0.0.1:49677        DESKTOP-DD143JG:49676  ESTABLISHED
  TCP    127.0.0.1:53387        DESKTOP-DD143JG:53388  ESTABLISHED
  TCP    127.0.0.1:53388        DESKTOP-DD143JG:53387  ESTABLISHED
  TCP    127.0.0.1:54235        DESKTOP-DD143JG:https  TIME_WAIT
  TCP    127.0.0.1:54237        DESKTOP-DD143JG:https  ESTABLISHED
  TCP    [::1]:8307             DESKTOP-DD143JG:54236  CLOSE_WAIT
  TCP    [::1]:8307             DESKTOP-DD143JG:54238  ESTABLISHED
  TCP    [::1]:53367            DESKTOP-DD143JG:53368  ESTABLISHED
  TCP    [::1]:53368            DESKTOP-DD143JG:53367  ESTABLISHED
  TCP    [::1]:54236            DESKTOP-DD143JG:8307   FIN_WAIT_2
  TCP    [::1]:54238            DESKTOP-DD143JG:8307   ESTABLISHED
  TCP    [2402:3a80:876:513d:6409:da56:22c5:ca1]:53324  [64:ff9b::2877:d3cb]:https  ESTABLISHED
  TCP    [2402:3a80:876:513d:6409:da56:22c5:ca1]:53386  g2600-1417-0075-0591-0000-0000-0000-02ef:https  CLOSE_WAIT
  TCP    [2402:3a80:876:513d:6409:da56:22c5:ca1]:53932  [2402:3a80:c000:24::685e:1358]:https  CLOSE_WAIT
  TCP    [2402:3a80:876:513d:6409:da56:22c5:ca1]:54227  sc-in-xbc:https        ESTABLISHED
  TCP    [2402:3a80:876:513d:6409:da56:22c5:ca1]:54240  bom07s11-in-x0e:https  ESTABLISHED
  TCP    [2402:3a80:876:513d:6409:da56:22c5:ca1]:54241  bom07s11-in-x0e:https  ESTABLISHED
```

ARP command

ARP - Address Resolution Protocol
Short for Address Resolution Protocol, a network layer protocol **used to** convert an IP address into a physical address (called a DLC address), such as an Ethernet address. A host wishing to obtain a physical address broadcasts an **ARP** request onto the TCP/IP network.

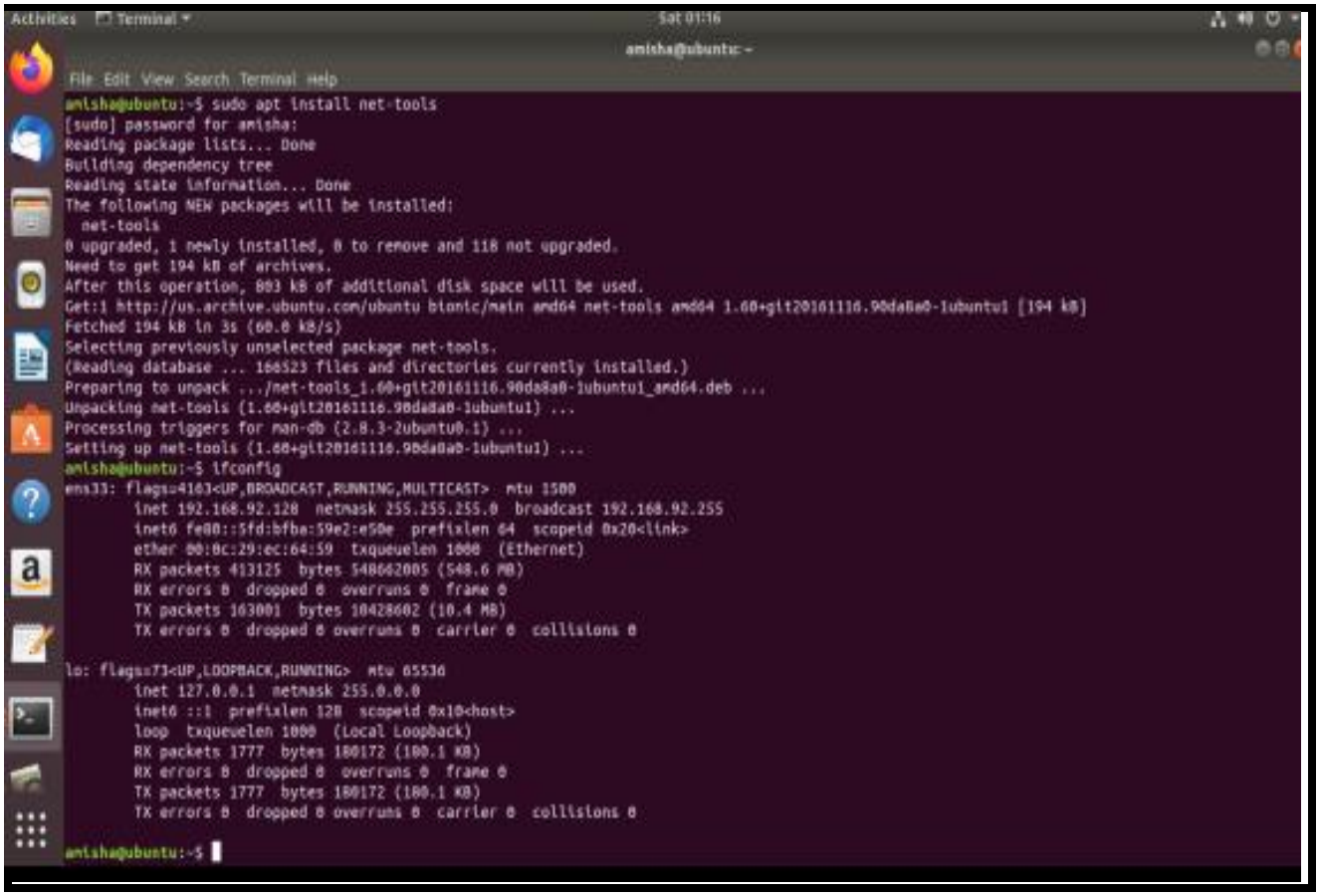
Consider a situation where ARP address that how many entries has been saved at ARP address

```
                 If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.

C:\Users\admin>arp  -a

Interface: 192.168.109.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.109.255       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

Interface: 192.168.92.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.92.255        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

Interface: 192.168.43.235 --- 0x15
  Internet Address      Physical Address      Type
  192.168.43.1          20-a6-0c-94-cb-b2     dynamic
  192.168.43.255        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
```

Arp -a so these many entries are there save already if I will remove this than it will require more time as no catch memory is stored so it need to map ip address again

Looking it we come to know one is dynamic ip address that is of wifi being connected to the devise

ifconfig



```
amisha@ubuntu:~$ sudo apt install net-tools
[sudo] password for amisha:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 118 not upgraded.
Need to get 194 kB of archives.
After this operation, 803 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 net-tools amd64 1.60+git20161116.90da8a0-1ubuntu1 [194 kB]
Fetched 194 kB in 3s (60.0 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 160523 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20161116.90da8a0-1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20161116.90da8a0-1ubuntu1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Setting up net-tools (1.60+git20161116.90da8a0-1ubuntu1) ...
amisha@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.128  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::5fd:bfba:59e2:e50e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ec:64:59  txqueuelen 1000  (Ethernet)
        RX packets 413125  bytes 548662005 (548.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 163001  bytes 10428602 (10.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1777  bytes 180172 (180.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1777  bytes 180172 (180.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

amisha@ubuntu:~$
```

It shows that how many packets are being sent and how many packets are being received:

TX: TRANSMITTED: 1777 bytes

RX: RECEIVED: 1777 bytes

Interface configuration:

Consider a situation where your internet connectivity is having problem and you want to see whether all transmitted packets have been received or lost somewhere else.

Whether my ISP is better or on upto which standard so this command will help that how efficient INTERNET SERVICE PROVIDER

```
^C
amisha@ubuntu:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max
  1   192.168.92.2  0.124ms  0.292ms  0.233ms
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
```

For linux:

ss command:

It is similar to netstat utility used to display **network** connections for the TCP/UDP, **network** protocol statistics, interface statistics, routing tables, masquerade connections, multicast memberships etc. netstat program is obsolete now and its replacement is **ss**.

TCP: consider a situation where we want to acknowledge a connection-oriented request

UDP: without acknowledgement

```
amisha@ubuntu:~$ traceroute 8.8.8^C
amisha@ubuntu:~$ ss
Netid  State      Recv-Q  Send-Q   Local Address:Port                 Peer Address:Port
u_str  ESTAB      0       0                /run/user/1000/bus 58553          * 58552
u_str  ESTAB      0       0          /var/run/dbus/system_bus_socket 37271  * 37270
u_str  ESTAB      0       0                                   * 37169      * 37170
u_str  ESTAB      0       0                                   * 54331      * 54332
u_str  ESTAB      0       0                 @/tmp/dbus-yvYbFbnI 53313      * 0
u_str  ESTAB      0       0             /run/systemd/journal/stdout 36720  * 36715
u_str  ESTAB      0       0          @/dbus-vfs-daemon/socket-b9WDuNlS 57638  * 57637
u_str  ESTAB      0       0                                   * 55738      * 55739
u_str  ESTAB      0       0                                   * 55139      * 55140
u_str  ESTAB      0       0                                   * 58200      * 58201
u_str  ESTAB      0       0              @/tmp/.X11-unix/X1024 37442      * 37441
u_str  ESTAB      0       0            /run/user/121/pulse/native 36783   * 36782
u_str  ESTAB      0       0            /run/systemd/journal/stdout 31515  * 31513
u_str  ESTAB      0       0                                   * 54287      * 54288
u_str  ESTAB      0       0                 @/tmp/dbus-yvYbFbnI 53311      * 0
u_str  ESTAB      0       0            /run/systemd/journal/stdout 188613 * 188612
u_str  ESTAB      0       0                 @/tmp/dbus-B2fjI63el3 57649    * 57648
u_str  ESTAB      0       0                                   * 55710      * 55711
u_str  ESTAB      0       0          /var/run/dbus/system_bus_socket 55015 * 55014
```

Ss -ta

```
amisha@ubuntu:~$ ss -ta
State Recv-Q Send-Q  Local Address:Port     Peer Address:Port
LISTEN0      128     127.0.0.53%lo:domain        0.0.0.0:*
LISTEN0      5           127.0.0.1:ipp           0.0.0.0:*
LISTEN0      5               [::1]:ipp              [::]:*
amisha@ubuntu:~$
```

ss-ua

```
amisha@ubuntu:~$ ss -ua
State Recv-Q Send-Q  Local Address:Port     Peer Address:Port
UNCONN0      0             0.0.0.0:ipp           0.0.0.0:*
UNCONN0      0             0.0.0.0:41865         0.0.0.0:*
UNCONN0      0       127.0.0.53%lo:domain        0.0.0.0:*
UNCONN0      0             0.0.0.0:bootpc        0.0.0.0:*
UNCONN0      0             0.0.0.0:mdns          0.0.0.0:*
UNCONN0      0                [::]:49353            [::]:*
UNCONN0      0                [::]:mdns             [::]:*
amisha@ubuntu:~$
```

ss-xa

```
amisha@ubuntu:~$ ss -xa
Netid State   Recv-Q  Send-Q                    Local Address:Port                    Peer Address:Port
u_dgr UNCONN  0       0                 /run/user/1000/systemd/notify 53593                        * 0
u_dgr UNCONN  0       0                   /run/user/121/systemd/notify 31453                        * 0
u_seq LISTEN  0       128                          /run/udev/control 23043                          * 0
u_str LISTEN  0       128               /run/user/1000/systemd/private 53596                        * 0
u_str LISTEN  0       128                /run/user/121/systemd/private 31456                        * 0
u_str LISTEN  0       128                          /run/user/1000/bus 53600                        * 0
u_str LISTEN  0       128                       @/tmp/.ICE-unix/1031 32130                         * 0
u_str LISTEN  0       128           /run/user/121/gnupg/S.gpg-agent.ssh 31460                        * 0
u_dgr UNCONN  0       0                    /run/systemd/journal/syslog 23765                        * 0
u_str LISTEN  0       128        /run/user/1000/gnupg/S.gpg-agent.extra 53601                        * 0
u_str LISTEN  0       128          /run/user/1000/gnupg/S.gpg-agent.ssh 53602                        * 0
u_str LISTEN  0       5                    /run/user/121/pulse/native 31461                        * 0
u_str LISTEN  0       128             /run/user/1000/gnupg/S.gpg-agent 53603                        * 0
```

Nslookup

It is also one of the ways to get the ip address

Ping

Tracert

nslookup

```
amisha@ubuntu:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.166.78
Name:   google.com
Address: 2404:6800:4009:80d::200e
```

dig command in linux:

With the dig command, you can query information about various DNS records, including host addresses, mail exchanges, and name servers. It is the most

commonly used tool among system administrators for troubleshooting DNS problems because of its flexibility and ease of use.

```
amisha@ubuntu:~$ dig google.com

; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23586
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIO
NAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             5       IN      A       172.217.166.78

;; Query time: 599 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Dec 21 02:01:15 PST 2019
;; MSG SIZE  rcvd: 55
```

We can also use dig command in another form:

dig google and host id:

```
misha@ubuntu:~$ dig 127.0.0.53

 <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> 127.0.0.53
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21696
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIO
AL: 1

; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 65494
; QUESTION SECTION:
127.0.0.53.                     IN      A

; ANSWER SECTION:
27.0.0.53.              5       IN      A       127.0.0.53

; Query time: 277 msec
; SERVER: 127.0.0.53#53(127.0.0.53)
; WHEN: Sat Dec 21 02:05:22 PST 2019
; MSG SIZE  rcvd: 55
```