

Name : Khushi Nitinkumar Patel, PRN:2020BTECS00037, Batch : S3

Q. Use of networking commands, windows / Linux Study and demonstrate basic networking command of windows and linux operating system. Prepare a document showing output of each command (screenshot), write down importance of each command and explain the output too. Note: Linux is installed in ASEL & PL lab , utilize those PC's for study of Linux command if needed.

The networking commands are mainly used for getting system information and troubleshooting networking problems.

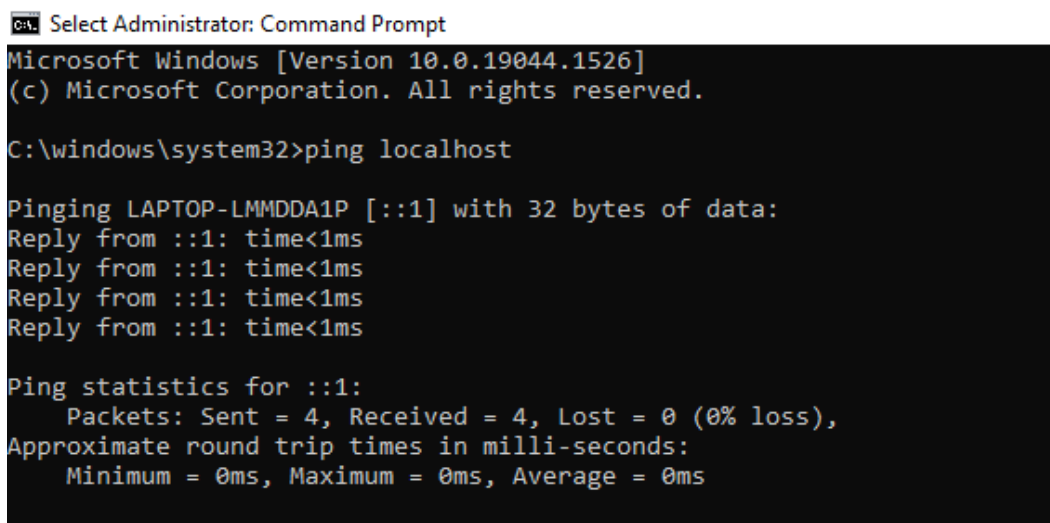
On Windows.

1. ping command

- ping in networking means a signal sent from one computer to another across a network for usually determining network speed or the status of the target computer.

-when you ping a device ,you send that device a short message,which is then sent back.

-it is one of the most often used networking utilities for detecting devices on a network and for troubleshooting network problems.



```

C:\> Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>ping localhost

Pinging LAPTOP-LMMDDA1P [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

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

```

2. ipconfig command.

-it is used for finding network information about your local machine like IP addresses, DNS addresses,etc.

-basic use : finding the default gateway (A default gateway is part of how computers and different networks communicate. On the internet, a computer sends a request for information to another network's website, and a default gateway helps route the information.)

```
C:\windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

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

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::c11:f387:ce43:1840%17
    IPv4 Address. . . . . : 10.30.1.154
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.30.0.2

Ethernet adapter Bluetooth Network Connection:

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

ipconfig /all – displays more information about the network setup on your systems including the MAC address.

```

Select Administrator: Command Prompt
C:\windows\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LAPTOP-LMMDDA1P
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : ExpressVPN TAP Adapter
Physical Address. . . . . : 00-FF-34-93-81-ED
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 4A-E7-DA-49-A1-6D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : CA-E7-DA-49-A1-6D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
Physical Address. . . . . : 48-E7-DA-49-A1-6D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter  
Physical Address. . . . . : 48-E7-DA-49-A1-6D  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::c11:f387:ce43:1840%17(Preferred)  
IPv4 Address. . . . . : 10.30.1.154(Preferred)  
Subnet Mask . . . . . : 255.255.254.0  
Lease Obtained. . . . . : 03 March 2022 15:48:59  
Lease Expires . . . . . : 03 March 2022 18:49:21  
Default Gateway . . . . . : 10.30.0.2  
DHCP Server . . . . . : 10.30.0.2  
DHCPv6 IAID . . . . . : 172550106  
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-8A-C5-08-00-E0-4C-68-CA-DF  
DNS Servers . . . . . : 192.168.1.8  
NetBIOS over Tcpip. . . . . : Enabled
```

Ethernet adapter Bluetooth Network Connection:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
Description . . . . . : Bluetooth Device (Personal Area Network)  
Physical Address. . . . . : 48-E7-DA-49-A1-6C  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes
```

C:\windows\system32>

ipconfig /release – release the current IP address

```
C:\windows\system32>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet 2 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 Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet 2:

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

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::c11:f387:ce43:1840%17
    Default Gateway . . . . . :

Ethernet adapter Bluetooth Network Connection:

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

C:\windows\system32>
```

ipconfig /renew – renew IP address

```
C:\windows\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 2 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 Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet 2:

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

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::c11:f387:ce43:1840%17
    IPv4 Address. . . . . : 10.30.1.154
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.30.0.2

Ethernet adapter Bluetooth Network Connection:

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

C:\windows\system32>
```

ipconfig /? -shows help

Administrator: Command Prompt

```
C:\windows\system32>ipconfig /?
```

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.
```

Administrator: Command Prompt

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  
> ipconfig /release *Con* ... release all matching connections,  
                      eg. "Wired Ethernet Connection 1" or  
                      "Wired Ethernet Connection 2"  
> ipconfig /allcompartments ... Show information about all  
                      compartments  
> ipconfig /allcompartments /all ... Show detailed information about all  
                      compartments
```

ipconfig/flushdns – flush the dns cache

```
C:\windows\system32>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\windows\system32>
```

3. Hostname command

-a simple command that displays the hostname of your machine.

```
C:\windows\system32>hostname
LAPTOP-LMMDDA1P

C:\windows\system32>
```

4. getmac command

-it shows the MAC address of your network interfaces.

```
C:\windows\system32>getmac

Physical Address      Transport Name
=====
48-E7-DA-49-A1-6D    \Device\Tcpip_{C64A5278-D1B9-4172-841F-FD251C390E6A}
48-E7-DA-49-A1-6C    Media disconnected
00-FF-34-93-81-ED    Media disconnected

C:\windows\system32>_
```


5. arp command

- This is used for showing the address resolution cache.
- used with a command line switch arp -a is the most common.
- it's function is to translate IP address to physical address.

```
C:\windows\system32>arp -a

Interface: 10.30.1.154 --- 0x11
    Internet Address      Physical Address         Type
    10.30.0.2             00-04-96-a1-fb-0b       dynamic
    10.30.1.255           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
    224.0.0.251           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
    239.255.102.18        01-00-5e-7f-66-12       static
    239.255.255.250       01-00-5e-7f-ff-fa       static
    255.255.255.255       ff-ff-ff-ff-ff-ff       static
```

- ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.

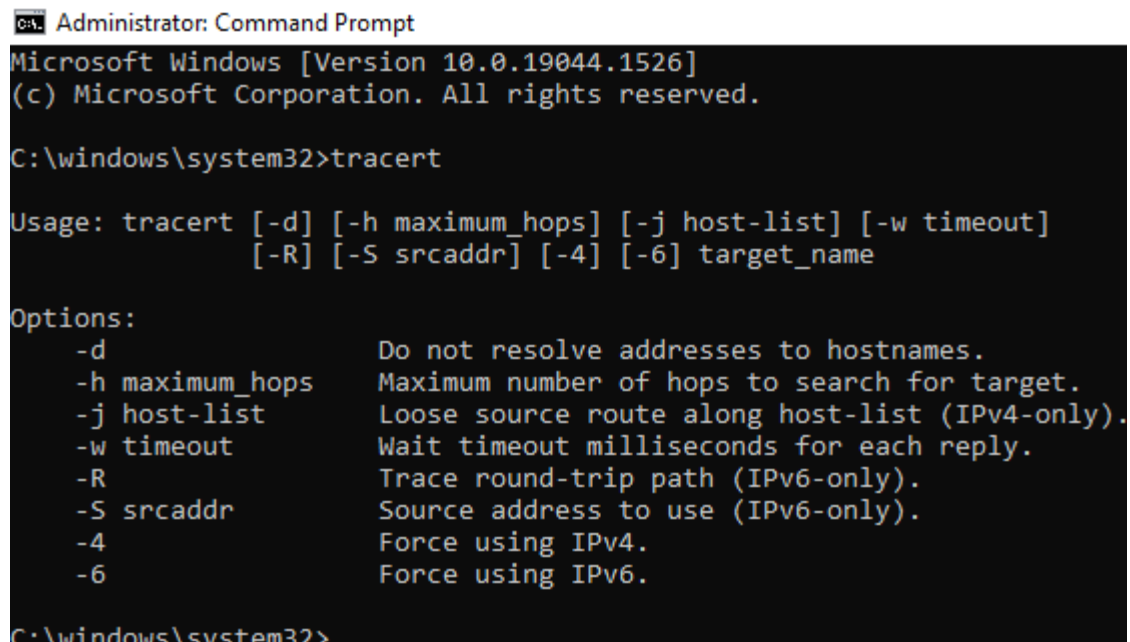
6. nslookup command

- Used for checking DNS record entries.

```
C:\windows\system32>NSlookup
Default Server:  UnKnown
Address:  192.168.1.8
```

7. tracert command

- Used for troubleshooting network connections.
- 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



```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                Do not resolve addresses to hostnames.
    -h maximum_hops   Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                Force using IPv4.
    -6                Force using IPv6.

C:\windows\system32>
```

8. Netstat command

-This command displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics, and IPv6 statistics.

-It allows you to understand open and connected ports to monitor and troubleshoot networking problems for systems or applications.

Administrator: Command Prompt - netstat

```
C:\windows\system32>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:58176	LAPTOP-LMMDDA1P:58177	ESTABLISHED
TCP	127.0.0.1:58177	LAPTOP-LMMDDA1P:58176	ESTABLISHED
TCP	127.0.0.1:58181	LAPTOP-LMMDDA1P:58184	ESTABLISHED
TCP	127.0.0.1:58184	LAPTOP-LMMDDA1P:58181	ESTABLISHED
TCP	127.0.0.1:58555	LAPTOP-LMMDDA1P:58557	ESTABLISHED
TCP	127.0.0.1:58557	LAPTOP-LMMDDA1P:58555	ESTABLISHED
TCP	192.168.45.96:49507	20.197.71.89:https	ESTABLISHED
TCP	192.168.45.96:49961	52.182.143.211:https	ESTABLISHED
TCP	192.168.45.96:50912	ec2-13-214-98-78:https	ESTABLISHED
TCP	192.168.45.96:51088	20.44.229.112:https	TIME_WAIT
TCP	192.168.45.96:51146	maa05s05-in-f3:https	ESTABLISHED
TCP	192.168.45.96:51281	ec2-54-205-140-90:https	ESTABLISHED
TCP	192.168.45.96:51328	20.197.71.89:https	ESTABLISHED
TCP	192.168.45.96:51353	1drv:https	TIME_WAIT
TCP	192.168.45.96:51546	ip-81-11-235-181:6881	TIME_WAIT
TCP	192.168.45.96:51720	241:https	ESTABLISHED
TCP	192.168.45.96:51829	ec2-65-0-236-111:8080	CLOSE_WAIT
TCP	192.168.45.96:51937	20.44.229.112:https	ESTABLISHED
TCP	192.168.45.96:52254	vsy89-1_migr-88-122-193-247:53302	SYN_SENT
TCP	192.168.45.96:52257	112.134.142.243:6881	SYN_SENT
TCP	192.168.45.96:52281	125.167.60.226:6881	SYN_SENT
TCP	192.168.45.96:52283	157.47.106.90:6881	SYN_SENT
TCP	192.168.45.96:52285	112.134.216.27:6881	SYN_SENT
TCP	192.168.45.96:52287	118.99.83.89:6881	SYN_SENT
TCP	192.168.45.96:52289	177-64-230-154:6881	SYN_SENT
TCP	192.168.45.96:52291	135:6881	SYN_SENT
TCP	192.168.45.96:52295	160.238.74.89:6881	SYN_SENT
TCP	192.168.45.96:52297	abts-ap-dynamic-154:6881	SYN_SENT
TCP	192.168.45.96:52298	176.105.216.52:6881	SYN_SENT
TCP	192.168.45.96:52300	178.159.28.110:6881	SYN_SENT

9. pathping command

-It is used to locate spots that have network latency and network loss.

```
Administrator: Command Prompt
C:\windows\system32>pathping google.com

Tracing route to google.com [2404:6800:4007:822::200e]
over a maximum of 30 hops:
  0  LAPTOP-LMMDDA1P [2401:4900:5021:443a:24c9:91a1:e08c:4caf]
  1  2401:4900:5021:443a::6d
  2  * * *
Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
    0                               0/ 100 = 0%      LAPTOP-LMMDDA1P [2401:4900:5021:443a:24c9:91a1:e08c:4caf]
    1  18ms     0/ 100 = 0%     0/ 100 = 0%      2401:4900:5021:443a::6d

Trace complete.

C:\windows\system32>
```

10. systeminfo command

-displays a list of details about your operating system, computer hardware and software components.

```
C:\windows\system32>systeminfo

Host Name:                LAPTOP-LMMDDA1P
OS Name:                  Microsoft Windows 10 Home Single Language
OS Version:               10.0.19044 N/A Build 19044
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         khushi.patel22@outlook.com
Registered Organization:   HP
Product ID:               00327-36308-59986-AAOEM
Original Install Date:     06-08-2021, 19:17:21
System Boot Time:         02-03-2022, 20:46:13
System Manufacturer:      HP
System Model:              HP Laptop 14s-dq2xxx
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2419 Mhz
BIOS Version:              AMI F.18, 12-01-2022
Windows Directory:         C:\windows
System Directory:          C:\windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,835 MB
Available Physical Memory: 2,198 MB
Virtual Memory: Max Size:  9,627 MB
Virtual Memory: Available: 2,533 MB
Virtual Memory: In Use:    7,094 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:               \\LAPTOP-LMMDDA1P
Hotfix(s):                 15 Hotfix(s) Installed.
                           [01]: KB5010472
                           [02]: KB4534170
                           [03]: KB4537759
                           [04]: KB4545706
                           [05]: KB4562830
                           [06]: KB4577586
                           [07]: KB4586864
                           [08]: KB5003791
                           [09]: KB5008575
                           [10]: KB5010342
```

```
[11]: KB5006753
[12]: KB5007273
[13]: KB5009636
[14]: KB5011352
[15]: KB5005699
Network Card(s): 2 NIC(s) Installed.
                  [01]: Realtek RTL8822CE 802.11ac PCIe Adapter
                     Connection Name: Wi-Fi
                     DHCP Enabled:    Yes
                     DHCP Server:    192.168.45.176
                     IP address(es)
                     [01]: 192.168.45.96
                     [02]: fe80::c11:f387:ce43:1840
                     [03]: 2401:4900:5021:443a:24c9:91a1:e08c:4caf
                     [04]: 2401:4900:5021:443a:c11:f387:ce43:1840
                  [02]: ExpressVPN TAP Adapter
                     Connection Name: Ethernet 2
                     Status:          Media disconnected
Hyper-V Requirements: VM Monitor Mode Extensions: Yes
                     Virtualization Enabled In Firmware: Yes
                     Second Level Address Translation: Yes
                     Data Execution Prevention Available: Yes
C:\windows\system32>_
```

On Linux.

1. ping command

-The Linux ping command is a simple utility used to check whether a network is available and if a host is reachable.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ ping
Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
          [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
          [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
          [-w deadline] [-W timeout] [hop1 ...] destination
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

2. ifconfig command

-The “ifconfig” command is used for displaying current network configuration information, setting up an ip address, netmask, or broadcast address to a network interface, creating an alias for the network interface, setting up hardware address, and enable or disable network interfaces.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ ifconfig
ens3      Link encap:Ethernet  HWaddr 52:54:00:12:34:56
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::ae8:44ad:baf7:10fd/64  Scope:Link
          inet6 addr: fec0::794a:6ae2:1411:54a5/64  Scope:Site
          inet6 addr: fec0::e319:1b8b:5ce5:c3e1/64  Scope:Site
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195397 errors:182 dropped:0 overruns:0 frame:182
          TX packets:33351 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:290468427 (290.4 MB)  TX bytes:2058414 (2.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:332 errors:0 dropped:0 overruns:0 frame:0
          TX packets:332 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29730 (29.7 KB)  TX bytes:29730 (29.7 KB)

onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

3. Ifconfig -a command

-It displays MAC address of your PC.

-HWaddr or ether or lladdr is the device's MAC address.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ ifconfig -a
ens3      Link encap:Ethernet  HWaddr 52:54:00:12:34:56
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::ae8:44ad:baf7:10fd/64 Scope:Link
          inet6 addr: fec0::794a:6ae2:1411:54a5/64 Scope:Site
          inet6 addr: fec0::e319:1b8b:5ce5:c3e1/64 Scope:Site
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195524 errors:191 dropped:0 overruns:0 frame:191
          TX packets:33420 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:290481674 (290.4 MB)  TX bytes:2061690 (2.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:336 errors:0 dropped:0 overruns:0 frame:0
          TX packets:336 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30348 (30.3 KB)  TX bytes:30348 (30.3 KB)

onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```


4. traceroute command

-traceroute command in Linux prints the route that a packet takes to reach the host.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ traceroute
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squerl
es ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [ -q nqueries ] [ -s src_addr ] [ -z sendwa
it ] [ --fwmark=num ] host [ packetlen ]
Options:
  -4                               Use IPv4
  -6                               Use IPv6
  -d --debug                       Enable socket level debugging
  -F --dont-fragment              Do not fragment packets
  -f first_ttl --first=first_ttl   Start from the first_ttl hop (instead from 1)
  -g gate,... --gateway=gate,...  Route packets through the specified gateway
                                  (maximum 8 for IPv4 and 127 for IPv6)
  -I --icmp                       Use ICMP ECHO for tracerouting
  -T --tcp                        Use TCP SYN for tracerouting (default port is 80)
  -i device --interface=device    Specify a network interface to operate with
  -m max_ttl --max-hops=max_ttl   Set the max number of hops (max TTL to be
                                  reached). Default is 30
  -N squeries --sin-queries=squeries Set the number of probes to be tried
                                  simultaneously (default is 16)
  -n                               Do not resolve IP addresses to their domain names
  -p port --port=port             Set the destination port to use. It is either
                                  initial udp port value for "default" method
                                  (incremented by each probe, default is 33434), or
                                  initial seq for "icmp" (incremented as well,
                                  default from 1), or some constant destination
                                  port for other methods (with default of 80 for
                                  "tcp", 53 for "udp", etc.)
  -t tos --tos=tos               Set the TOS (IPv4 type of service) or TC (IPv6
                                  traffic class) value for outgoing packets
  -l flow_label --flowlabel=flow_label Use specified flow_label for IPv6 packets
  -w waittime --wait=waittime    Set the number of seconds to wait for response to
                                  a probe (default is 5.0). Non-integer (float
                                  point) values allowed too
  -q nqueries --queries=nqueries Set the number of probes per each hop. Default is
```

5. arp command

-On Linux operating systems, the arp command manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one, or display the current content.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.3         ether   52:55:0a:00:02:03 C          ens3
10.0.2.2         ether   52:55:0a:00:02:02 C          ens3
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

6. netstat command

-Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type        State         I-Node  Path
unix  14      [ ]         DGRAM       12787         /run/systemd/journal/dev-log
unix  2      [ ]         DGRAM       18518         /run/user/1000/systemd/notify
unix  7      [ ]         DGRAM       12789         /run/systemd/journal/socket
unix  2      [ ]         DGRAM       12803         /run/systemd/journal/syslog
unix  3      [ ]         DGRAM       12782         /run/systemd/notify
unix  3      [ ]         STREAM      CONNECTED     22109         @/tmp/dbus-pQQgmRubwm
unix  3      [ ]         STREAM      CONNECTED     20867         I
unix  3      [ ]         STREAM      CONNECTED     18785
unix  3      [ ]         STREAM      CONNECTED     16880         /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM      CONNECTED     23993         @onworks-com.canonical.Unity.Scope.scopes.T163
1847529218
unix  3      [ ]         STREAM      CONNECTED     23972         @onworks-com.canonical.Unity.Master.Scope.appl
ications.T1627579743492
unix  3      [ ]         STREAM      CONNECTED     23084         /run/systemd/journal/stdout
unix  3      [ ]         STREAM      CONNECTED     22885         /run/systemd/journal/stdout
unix  3      [ ]         STREAM      CONNECTED     22630         @/tmp/dbus-pQQgmRubwm
unix  3      [ ]         STREAM      CONNECTED     19385         @/tmp/dbus-pQQgmRubwm
unix  3      [ ]         STREAM      CONNECTED     18805         @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM      CONNECTED     18068         /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM      CONNECTED     35147         /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM      CONNECTED     22064
unix  3      [ ]         STREAM      CONNECTED     21107         @/tmp/dbus-pQQgmRubwm
unix  3      [ ]         STREAM      CONNECTED     20863         /run/systemd/journal/stdout
unix  3      [ ]         STREAM      CONNECTED     16854
unix  3      [ ]         STREAM      CONNECTED     19717
unix  3      [ ]         STREAM      CONNECTED     23978         /run/systemd/journal/stdout
unix  3      [ ]         STREAM      CONNECTED     18812         @/tmp/dbus-pQQgmRubwm
unix  3      [ ]         STREAM      CONNECTED     18500         /run/systemd/journal/stdout
unix  3      [ ]         STREAM      CONNECTED     51388         @/tmp/dbus-3tK6Wf7F4K
unix  3      [ ]         STREAM      CONNECTED     23085         /run/systemd/journal/stdout
unix  3      [ ]         STREAM      CONNECTED     19627         @/tmp/dbus-pQQgmRubwm
unix  3      [ ]         STREAM      CONNECTED     21094         /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM      CONNECTED     20862
```

7. dig command

-The dig command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data about Domain Name Servers. The dig command is helpful for troubleshooting DNS problems, but is also used to display DNS information.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ dig

; <<>> DiG 9.10.3-P4-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53058
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;
; IN NS
;; ANSWER SECTION:
. 56937 IN NS m.root-servers.net.
. 56937 IN NS a.root-servers.net.
. 56937 IN NS b.root-servers.net.
. 56937 IN NS c.root-servers.net.
. 56937 IN NS d.root-servers.net.
. 56937 IN NS e.root-servers.net.
. 56937 IN NS f.root-servers.net.
. 56937 IN NS g.root-servers.net.
. 56937 IN NS h.root-servers.net.
. 56937 IN NS i.root-servers.net.
. 56937 IN NS j.root-servers.net.
. 56937 IN NS k.root-servers.net.
. 56937 IN NS l.root-servers.net.

;; Query time: 1 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Sun Mar 06 11:48:10 CET 2022
;; MSG SIZE rcvd: 239

onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

8. route

-route command in Linux is used when you want to work with the IP/kernel routing table.

-It is mainly used to set up static routes to specific hosts or networks via an interface.

- It is used for showing or update the IP/kernel routing table.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 10.0.2.2 0.0.0.0 UG 100 0 0 ens3
10.0.2.0 * 255.255.255.0 U 100 0 0 ens3
link-local * 255.255.0.0 U 1000 0 0 ens3

onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

9. nslookup command

-nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server.

-It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ nslookup
> ^Conworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ nslookup google.com
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.186.78

onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

10. sudo lshw command

-this command displays the device's hardware configuration information.

-While using this command in a terminal, you will get a print of CPU version, memory configuration, cache information, bus speed, and other PowerPC machines running on the backend.

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo lshw
onworks-standard-pc-i440fx-piix-1996
  description: Computer
  product: Standard PC (i440FX + PIIX, 1996)
  vendor: QEMU
  version: pc-i440fx-4.0
  width: 32 bits
  capabilities: smbios-2.8 dmi-2.8 smp-1.4 smp
  configuration: boot=normal cpus=2
*-core
  description: Motherboard
  physical id: 0
*-firmware
  description: BIOS
  vendor: SeaBIOS
  physical id: 0
  version: rel-1.12.1-0-ga5cab58e9a3f-prebuilt.qemu.org
  date: 04/01/2014
  size: 96KiB
*-cpu:0
  description: CPU
  product: Common KVM processor
  vendor: Intel Corp.
  physical id: 400
  bus info: cpu@0
  version: 15.6.1
  serial: 0000-0F61-0000-0000-0000-0000
  slot: CPU 0
  size: 2GHz
  capacity: 2GHz
  width: 64 bits
  capabilities: boot fpu fpu_exception wp vme de pse tsc msr pae mce cx8 apic sep ntrr pge mca cm
ov pat pse36 clflush mmx fxsr sse sse2 syscall nx x86-64 constant_tsc xtopology cpuid tsc_known_freq pni
cx16 x2apic hypervisor ptl
  configuration: cores=1 enabledcores=1 threads=1
*-cpu:1
  description: CPU
  product: Common KVM processor
  vendor: Intel Corp.
  physical id: 401
  bus info: cpu@1
```