USE AND INTERPRET BASIC NETWORKING UTILITIES

Experiment No 1

UID: 2021300126 Name: Pranay Singhvi

INTRODUCTION TO NETWORKING

Networking is the practice of connecting computers and devices together in order to share information and resources. This can be done through wired or wireless connections and can take place within a single location (such as a home or office) or across multiple locations (such as across a city or around the world).

There are several types of networks, including:

- Local Area Networks (LANs): Connects devices in a small area, such as a home or office.
- Wide Area Networks (WANs): Connects devices over a larger area, such as across a city or across multiple locations.
- Metropolitan Area Networks (MANs): Connects devices within a metropolitan area, such as a city.
- Virtual Private Networks (VPNs): Allows devices to connect to a network remotely, as if they were physically connected.
- The Internet: The global network of interconnected devices and networks.

Networks allow devices to share resources such as printers, files, and internet connections. They also enable communication between devices through email, instant messaging, and other means.

Networking protocols such as TCP/IP and Ethernet govern the communication between devices on a network. These protocols provide a standardized way for devices to share information, ensuring that data is transmitted correctly and securely.

Network topologies, such as bus, star, and ring, describe the layout of the devices on a network. Each topology has its own advantages and disadvantages and is suited to different types of network.

In summary, networking is the practice of connecting devices together in order to share resources and communicate. This can be done through wired or wireless connections and can take place within a single location or across multiple locations. It uses protocols, topologies, and other standard technologies to govern the communication between devices on a network.

WHY IS NETWORKING NEEDED??

Networking is essential for the efficient sharing of information and resources between devices, which can greatly improve productivity and communication. There are several key reasons why networking is important:

1. Resource sharing: Networking allows devices to share resources such as printers, files, and internet connections. This can greatly improve productivity and reduce costs by eliminating the need for multiple devices for each individual.
2. Communication: Networking enables communication between devices through email, instant messaging, and other means, making it easy to collaborate and share information.
3. Remote access: Networking allows users to access resources and communicate with other devices remotely. This can be done

through virtual private networks (VPNs) and other remote access technologies, enabling employees to work from anywhere.

4. Scalability: Networking allows for the easy expansion of a network as new devices are added or removed.
5. Efficient use of resources: A network can centralize resources and services, allowing them to be shared among multiple devices, making the use of resources more efficient.
6. Data Backup and Recovery: Networking allows for the backup of data across multiple devices or servers, which can greatly reduce the risk of data loss.
7. Internet access: Networking makes it possible for devices to connect to the internet, providing access to a vast array of information and resources.
8. Security: Networking allows for the implementation of security measures such as firewalls, intrusion detection systems, and encryption to protect against unauthorized access and data loss.

In summary, Networking is important because it enables the sharing of resources, communication, remote access, scalability, efficient use of resources, data backup and recovery, internet access and security.

WHY IS NETWORKING NEEDED??

The history of networking can be traced back to the early days of computer development in the 1950s. At that time, computers were large, expensive, and primarily used by government and research institutions. The need for computers to share information and resources led to the development of the first networks.

1. In the 1960s, the US Department of Defense's Advanced Research Projects Agency Network (ARPANET) was created, which was one of the first wide-area networks (WANs). ARPANET was designed to link government and academic researchers to facilitate the sharing of information and resources.

2. In the 1970s, the Transmission Control Protocol/Internet Protocol (TCP/IP) was developed, which became the foundation for all modern networks. TCP/IP is a set of protocols that govern how data is transmitted over networks and the internet.
3. In the 1980s, the use of local area networks (LANs) and personal computers (PCs) began to increase in popularity. This led to the development of Ethernet, a networking protocol that allowed PCs to communicate with each other and share resources.
4. In the 1990s, the World Wide Web (WWW) and the first web browsers were introduced, which made the internet more accessible to the general public. This led to a rapid increase in the number of users and the amount of information available on the internet.
5. In the 2000s, wireless networking technologies such as Wi-Fi became widely adopted, making it possible to connect to networks without the need for physical cables. This led to the increasing popularity of mobile devices such as smartphones and tablets, and the emergence of the Internet of Things (IoT).
6. Today, networking continues to evolve, with the development of new technologies such as 5G, which promises faster internet speeds and more reliable connections, and the increasing use of cloud computing, which allows users to access data and applications remotely.

In summary, the history of networking is a story of how people developed and adopted the various technologies to connect computers and devices together. From the earliest days of large, centralized systems, to the global network of connected devices we have today, the evolution of networking is ongoing and continues to shape the way we live and work.

NETWORK UTILITIES USED:

1. ‘Ifconfig ’:

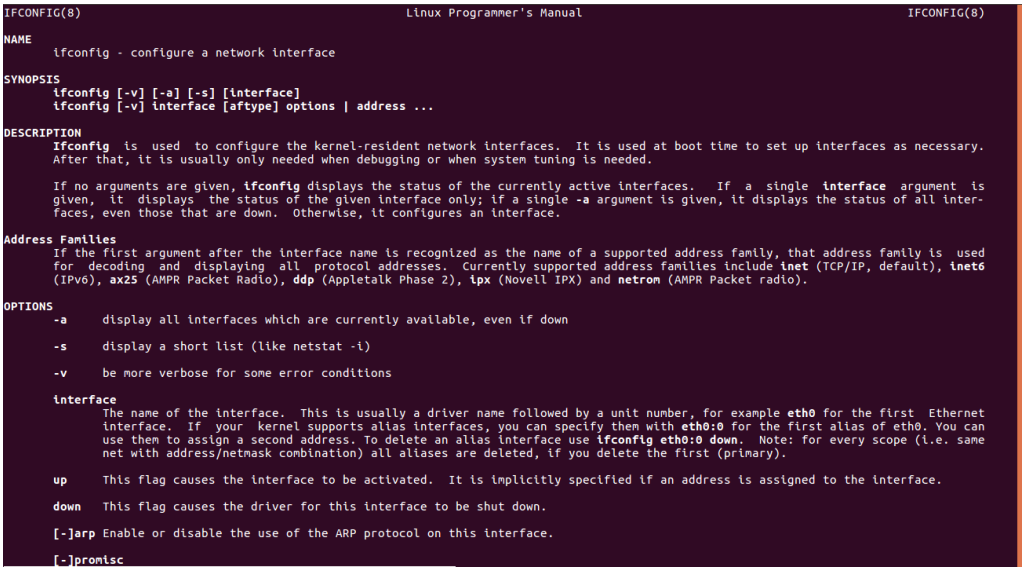
ifconfig (short for "interface configuration") is a command-line utility in Unix-like operating systems, such as Linux and macOS, for displaying and configuring network interface parameters. It is used to view and configure the IP addresses, netmasks, and other settings of network interfaces.

```
students@students-HP-Pro-3330-MT:~$ ifconfig
enp8s0    Link encap:Ethernet  HWaddr 24:be:05:0e:32:5c
          inet addr:172.16.31.222  Bcast:172.16.31.255  Mask:255.255.255.0
          inet6 addr: fe80::4a78:59b8:1095:182f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:65507 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26032 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43006147 (43.0 MB)  TX bytes:4335987 (4.3 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:2109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:355549 (355.5 KB)  TX bytes:355549 (355.5 KB)
```

2. ‘man ifconfig ‘:

The man command in Unix-like operating systems is used to display the manual pages for a command or utility. When you type man ifconfig, it will display the manual pages for the ifconfig command.



```
IFCONFIG(8)                                Linux Programmer's Manual                                IFCONFIG(8)

NAME
       ifconfig - configure a network interface

SYNOPSIS
       ifconfig [-v] [-a] [-s] [interface]
       ifconfig [-v] interface [aftype] options | address ...

DESCRIPTION
       Ifconfig  is  used  to configure the kernel-resident network interfaces.  It is used at boot time to set up interfaces as necessary.
       After that, it is usually only needed when debugging or when system tuning is needed.

       If no arguments are given, ifconfig displays the status of the currently active interfaces.  If  a  single  interface  argument  is
       given,  it  displays  the status of the given interface only; if a single -a argument is given, it displays the status of all inter-
       faces, even those that are down.  Otherwise, it configures an interface.

Address Families
       If the first argument after the interface name is recognized as the name of a supported address family, that address family is  used
       for  decoding  and  displaying  all  protocol addresses.  Currently supported address families include inet (TCP/IP, default), inet6
       (IPv6), ax25 (AMPR Packet Radio), ddp (Appletalk Phase 2), ipx (Novell IPX) and netrom (AMPR Packet radio).

OPTIONS
       -a     display all interfaces which are currently available, even if down

       -s     display a short list (like netstat -i)

       -v     be more verbose for some error conditions

       interface
              The name of the interface.  This is usually a driver name followed by a unit number, for example eth0 for the first  Ethernet
              interface.  If  your  kernel supports alias interfaces, you can specify them with eth0:0 for the first alias of eth0. You can
              use them to assign a second address. To delete an alias interface use ifconfig eth0:0 down.  Note: for every scope (i.e. same
              net with address/netmask combination) all aliases are deleted, if you delete the first (primary).

       up     This flag causes the interface to be activated.  It is implicitly specified if an address is assigned to the interface.

       down   This flag causes the driver for this interface to be shut down.

       [-]arp Enable or disable the use of the ARP protocol on this interface.

       [-]promisc
```

3. ‘Ping ‘:

ping is a command-line utility in Unix-like operating systems, such as Linux and macOS, and in Windows, that is used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for packets sent from the source host to a destination host. It is used to determine if a particular host is reachable and to measure the time it takes for packets to travel to the host and back.

```
students@students-HP-Pro-3330-MT:~$ ping 172.16.31.55
PING 172.16.31.55 (172.16.31.55) 56(84) bytes of data.
64 bytes from 172.16.31.55: icmp_seq=1 ttl=64 time=0.492 ms
64 bytes from 172.16.31.55: icmp_seq=2 ttl=64 time=0.397 ms
64 bytes from 172.16.31.55: icmp_seq=3 ttl=64 time=0.417 ms
64 bytes from 172.16.31.55: icmp_seq=4 ttl=64 time=0.398 ms
64 bytes from 172.16.31.55: icmp_seq=5 ttl=64 time=0.433 ms
64 bytes from 172.16.31.55: icmp_seq=6 ttl=64 time=0.417 ms
64 bytes from 172.16.31.55: icmp_seq=7 ttl=64 time=0.416 ms
64 bytes from 172.16.31.55: icmp_seq=8 ttl=64 time=0.427 ms
64 bytes from 172.16.31.55: icmp_seq=9 ttl=64 time=0.429 ms
64 bytes from 172.16.31.55: icmp_seq=10 ttl=64 time=0.428 ms
^C
--- 172.16.31.55 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9220ms
rtt min/avg/max/mdev = 0.397/0.425/0.492/0.031 ms
```

Connected

```
students@students-HP-Pro-3330-MT:~$ ping 172.16.31.600
ping: unknown host 172.16.31.600
```

Not Connected

4. ‘Netstat’:

netstat is a command-line utility that displays information about

```
students@students-HP-Pro-3330-MT:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        4      0 172.16.31.222:47650     172.16.31.8:netbios-ssn ESTABLISHED
tcp        0      0 172.16.31.222:41526     any-in-2678.1e100:https ESTABLISHED
tcp        0      0 172.16.31.222:41680     ec2-52-89-241-77.:https ESTABLISHED
tcp        0      0 172.16.31.222:53382     bom07s37-in-f5.1e:https ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    27843    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    14105    /run/systemd/cgroups-agent
unix  8      [ ]         DGRAM                    14114    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    14115    /run/systemd/journal/syslog
unix  14     [ ]         DGRAM                    14126    /run/systemd/journal/dev-log
unix  3      [ ]         DGRAM                    14104    /run/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     29026    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     28388
unix  3      [ ]         STREAM     CONNECTED     28239
unix  3      [ ]         DGRAM                    47751
unix  3      [ ]         STREAM     CONNECTED     42136
unix  3      [ ]         STREAM     CONNECTED     28392
unix  3      [ ]         STREAM     CONNECTED     28825
unix  3      [ ]         STREAM     CONNECTED     26488
unix  3      [ ]         STREAM     CONNECTED     23618
unix  3      [ ]         SEQPACKET  CONNECTED     34600
unix  3      [ ]         STREAM     CONNECTED     30917
unix  3      [ ]         STREAM     CONNECTED     30820
unix  3      [ ]         STREAM     CONNECTED     27450    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     27318
unix  3      [ ]         STREAM     CONNECTED     20182
unix  3      [ ]         STREAM     CONNECTED     17316
unix  3      [ ]         STREAM     CONNECTED     28306    @/tmp/dbus-NhDKqkJdmC
unix  3      [ ]         STREAM     CONNECTED     28208
unix  3      [ ]         STREAM     CONNECTED     25483
unix  3      [ ]         STREAM     CONNECTED     42987
unix  3      [ ]         STREAM     CONNECTED     27298    @/tmp/dbus-NhDKqkJdmC
unix  3      [ ]         STREAM     CONNECTED     19828
unix  3      [ ]         STREAM     CONNECTED     42144
unix  3      [ ]         STREAM     CONNECTED     28994    @/tmp/dbus-NhDKqkJdmC
unix  3      [ ]         STREAM     CONNECTED     28356    @/tmp/dbus-DLfgbbRlU2
```

active network connections on a computer. It can be used to display

information such as the current state of TCP and UDP connections, the process ID of the program that owns a connection, and the number of packets and bytes sent and received on a connection. It can also be used to display information about network interfaces and routing tables. The information displayed by netstat is typically used for troubleshooting and performance tuning.

5. ‘Traceroute ‘:

traceroute is a command-line utility that is used to trace the path that network packets take from a source computer to a destination computer. It works by sending a series of packets to the destination with increasing Time-to-Live (TTL) values. As the packets travel through the network, routers decrement the TTL value by one. When the TTL value reaches zero, the router sends an ICMP "time exceeded" message back to the source. By measuring the time it takes for each of these messages to be returned, traceroute can determine the path that the packets took and the IP addresses of the routers along the way.

```
students@students-HP-Pro-3330-MT:~$ traceroute google.com
traceroute to google.com (216.239.38.120), 30 hops max, 60 byte packets
 1  172.16.31.1 (172.16.31.1)  0.288 ms  0.963 ms  0.944 ms
 2  125.99.120.241 (125.99.120.241)  2.817 ms  3.260 ms  2.941 ms
 3  192.168.210.29 (192.168.210.29)  1.539 ms  1.571 ms  1.752 ms
 4  192.168.44.57 (192.168.44.57)  2.723 ms  4.155 ms  4.146 ms
 5  192.168.27.34 (192.168.27.34)  3.480 ms  3.463 ms  3.444 ms
 6  125.99.55.254 (125.99.55.254)  3.332 ms  3.004 ms  3.038 ms
 7  125.99.55.253 (125.99.55.253)  3.829 ms  3.910 ms  3.912 ms
 8  * * *
 9  10.240.254.120 (10.240.254.120)  3.199 ms  3.101 ms  3.192 ms
10  * * *
11  * * *
12  125.99.55.163 (125.99.55.163)  6.623 ms  6.258 ms  6.362 ms
13  125.99.55.165 (125.99.55.165)  5.620 ms  5.612 ms  5.565 ms
14  * * *
15  any-in-2678.1e100.net (216.239.38.120)  3.550 ms  3.501 ms  3.468 ms
```

6. ‘Nslookup ‘:

nslookup is a command-line utility that is used to query the Domain Name System (DNS) to obtain information about a domain name or an IP address. It can be used to look up the IP address associated with a domain name (i.e., "forward lookup"), or to look up the domain name associated with an IP address (i.e., "reverse lookup").

```
students@students-HP-Pro-3330-MT:~$ nslookup spit.ac.in
Server:         127.0.1.1
Address:        127.0.1.1#53

Name:   spit.ac.in
Address: 172.16.10.6
Name:   spit.ac.in
Address: 172.16.10.2
Name:   spit.ac.in
Address: 172.16.10.3
```

7. ‘arp ‘:

The arp command is a command-line utility that is used to display and manipulate the Address Resolution Protocol (ARP) cache on a computer. ARP is a protocol used to map a network address, such as an IP address, to a physical (MAC) address on a local network.

```
students@students-HP-Pro-3330-MT:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.31.80             ether   18:60:24:7b:60:2e   C                     enp8s0
172.16.31.55             ether   18:60:24:7b:5f:f4   C                     enp8s0
172.16.31.225            ether   d0:67:e5:11:f3:06   C                     enp8s0
172.16.31.11                     (incomplete)                              enp8s0
172.16.31.1              ether   e0:07:1b:c2:64:60   C                     enp8s0
```

a. ‘arp -a ‘:

This command formats the output of arp in alternate BSD style

```
students@students-HP-Pro-3330-MT:~$ arp -a
? (172.16.31.80) at 18:60:24:7b:60:2e [ether] on enp8s0
? (172.16.31.55) at 18:60:24:7b:5f:f4 [ether] on enp8s0
? (172.16.31.225) at d0:67:e5:11:f3:06 [ether] on enp8s0
? (172.16.31.11) at <incomplete> on enp8s0
? (172.16.31.1) at e0:07:1b:c2:64:60 [ether] on enp8s0
```

CONCLUSION:

After performing this experiment, I learned about networking and the history behind it. I got to expand my knowledge about IP and networking commands in Linux/macOS.