Name: Keegan Vaz **Class:** TE CMPN B **Roll No:** 28

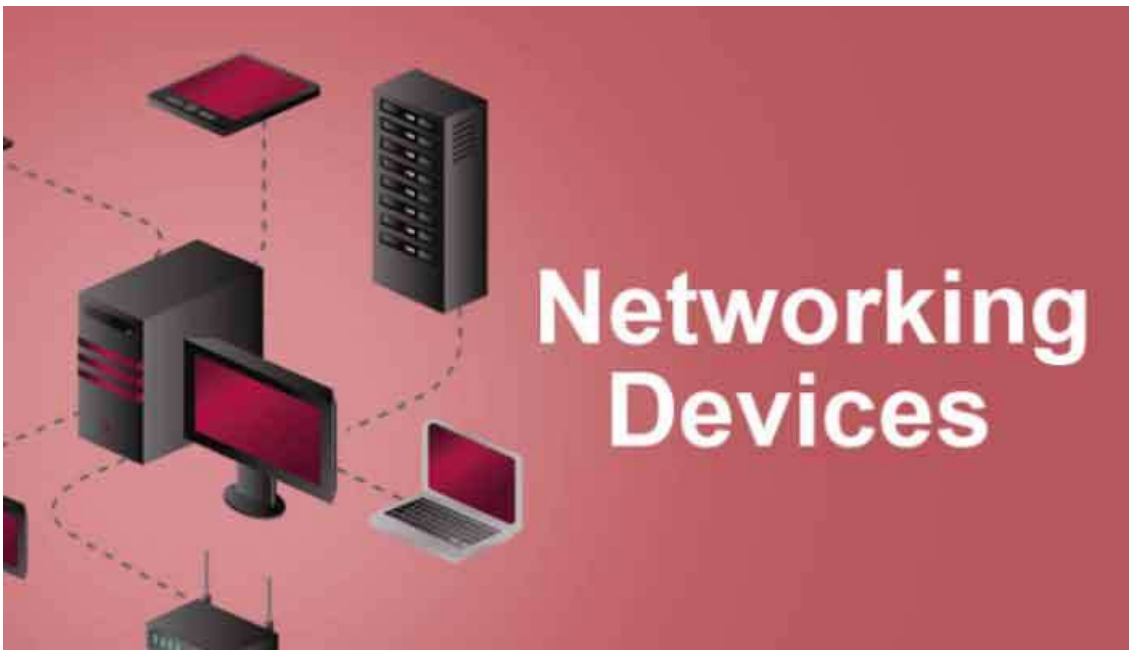
Computer Networks(Lab)

Experiment No. 2

Aim: Case Study Of Various Networking Devices and Commands.

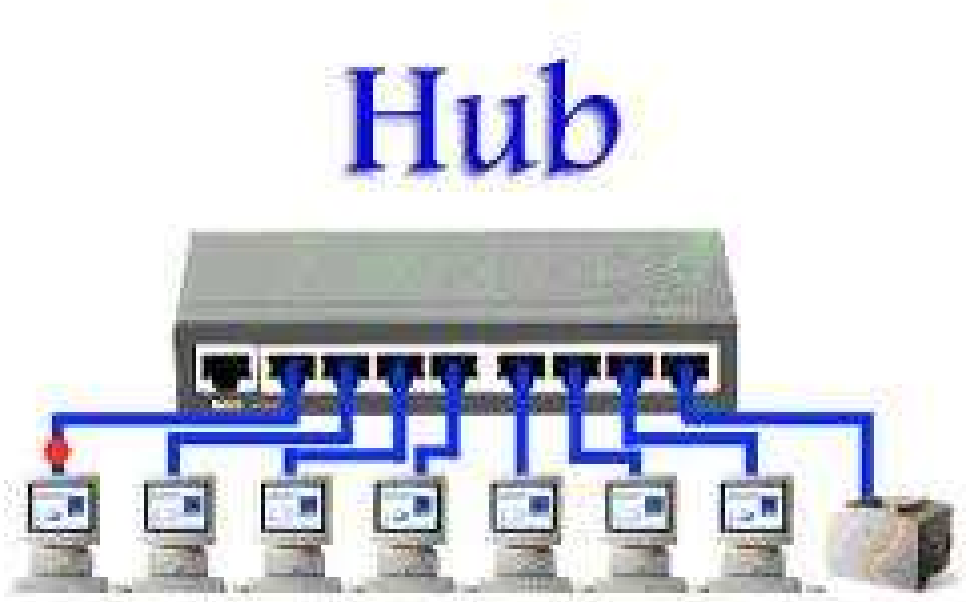
A. Networking Devices

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network. Networking devices includes a broad range of equipment which can be classified as core network components which interconnect other network components, hybrid components which can be found in the core or border of a network and hardware or software components which typically sit on the connection point of different networks. The most common kind of networking hardware today is a copper-based Ethernet adapter which is a standard inclusion on most modern computer systems. Wireless networking has become increasingly popular, especially for portable and handheld devices.



Name: Keegan Vaz **Class:** TE CMPN B **Roll No:** 28

1. **Hubs:**
   A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

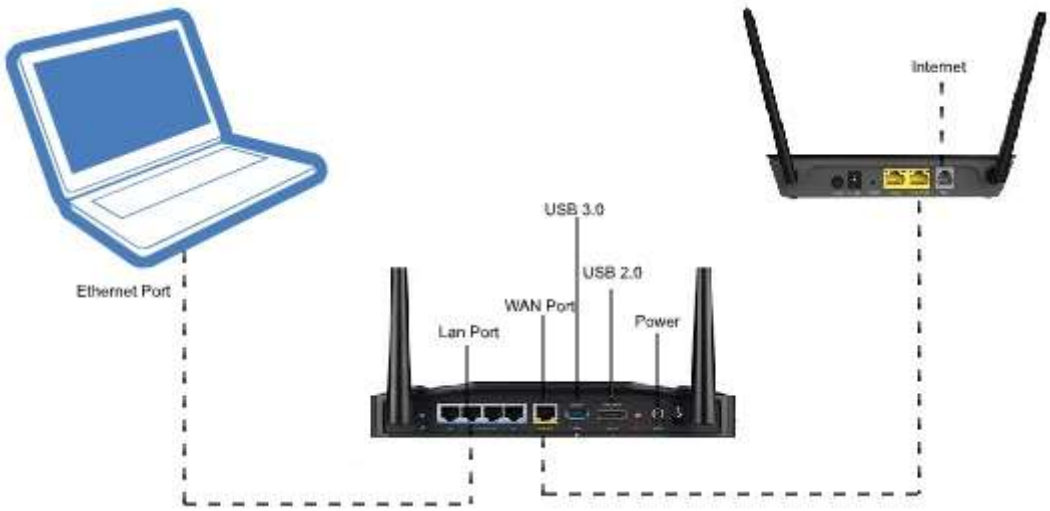


Types of Hub

1. **Active Hub:-** These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
2. **Passive Hub :-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
3. **Intelligent Hub :-** It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

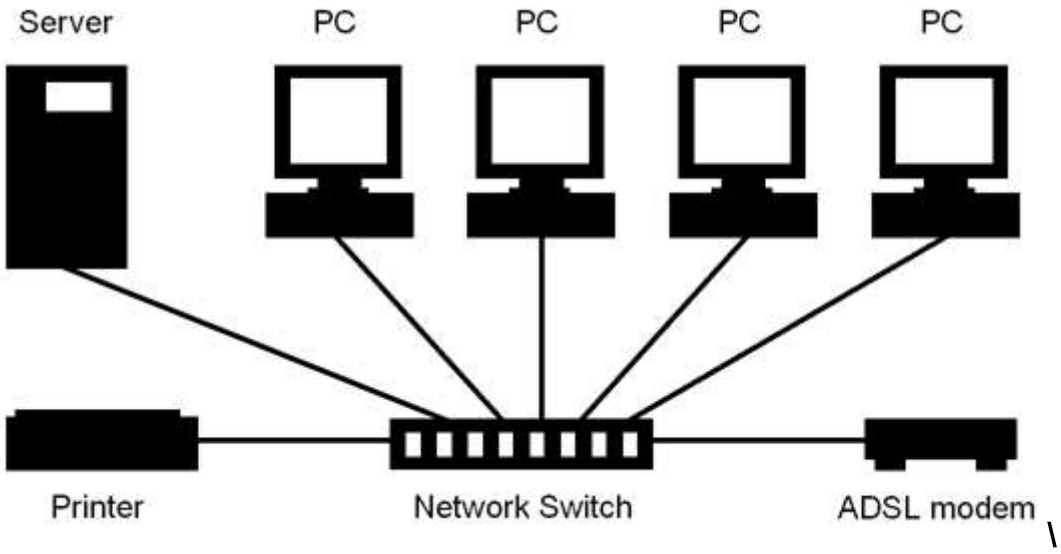
2. Routers:

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

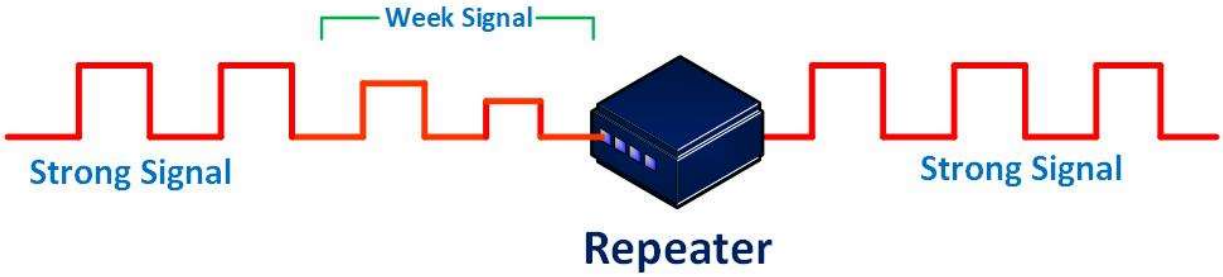


3. Switches:

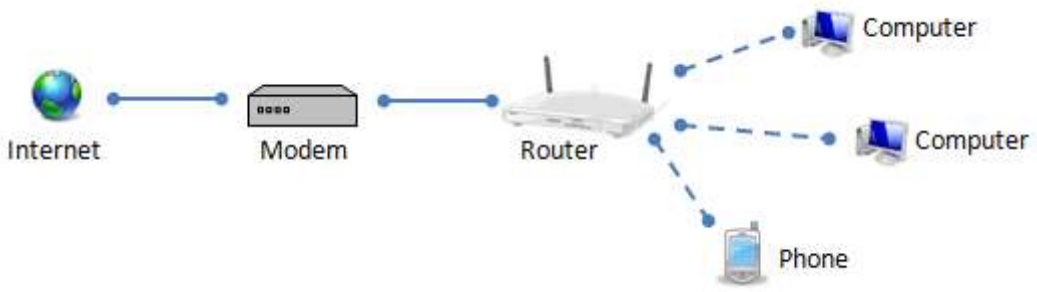
Switches generally have a more intelligent role than hubs. A switch is a multiport device that improves network efficiency. The switch maintains limited routing information about nodes in the internal network, and it allows connections to systems like hubs or routers. Strands of LANs are usually connected using switches. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination. Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors.A switch can work at either the Data Link layer or the Network layer of the OSI model.



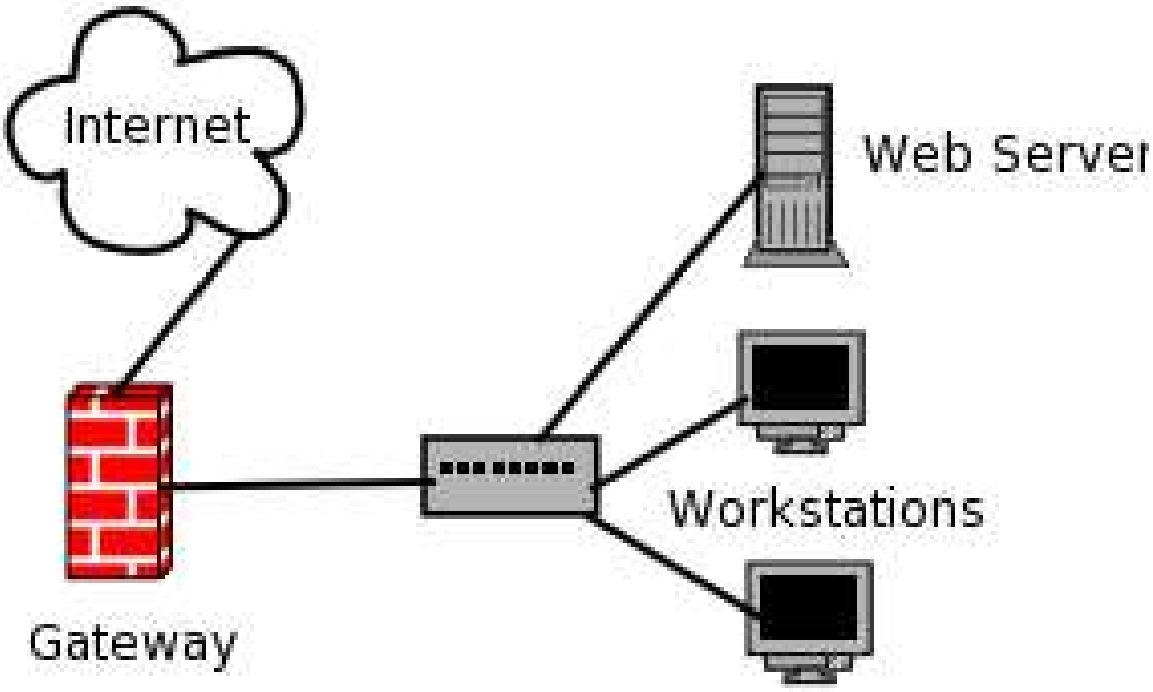
4. **Repeaters:**
   A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.



5. **Modems:**
   Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data. The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − modulator and demodulator. The modulator converts digital data into analog data when the data is being sent by the computer. The demodulator converts analog data signals into digital data when it is being received by the computer.



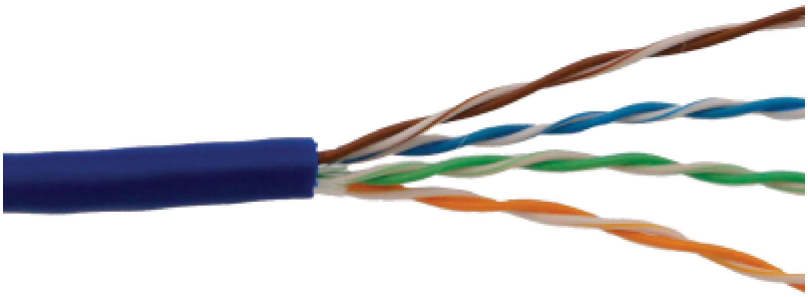
6. **Gateways:**
   Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.



7. Types of Network Cables:

a. Unshielded Twisted Pair Cable

Unshielded twisted pair (UTP) cables are widely used in the computer and telecommunications industry as Ethernet cables and telephone wires. In an UTP cable, conductors which form a single circuit are twisted around each other in order to cancel out electromagnetic interference (EMI) from external sources. Unshielded means no additional shielding like meshes or aluminum foil, which add bulk, are used. UTP cables are often groups of twisted pairs grouped together with color coded insulators, the number of which depends on the purpose.



b. Shielded Twisted Pair Cable

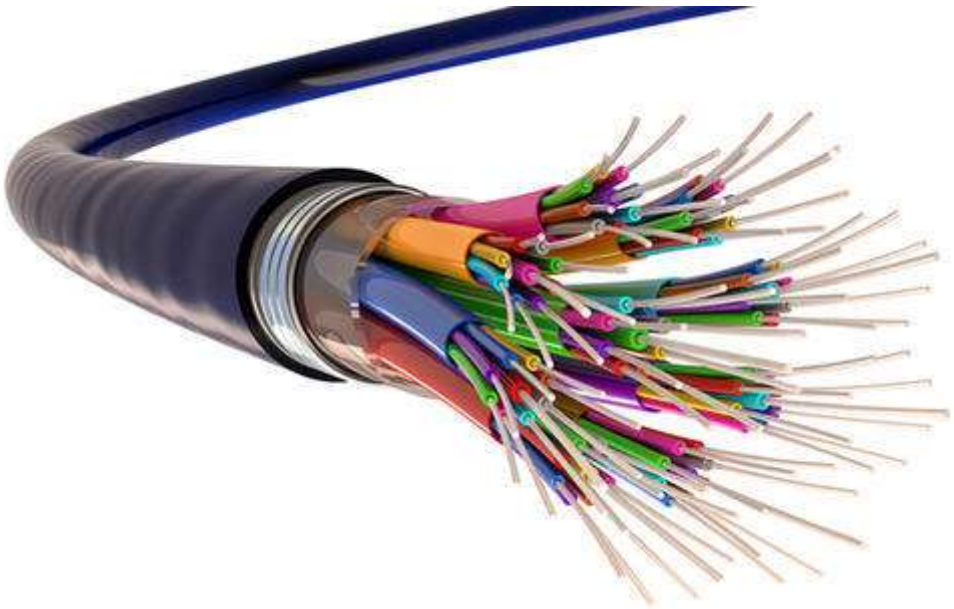
STP is similar to unshielded twisted pair (UTP); however, it contains an extra foil wrapping or copper braid jacket to help shield the cable signals from interference. STP cables are costlier when compared to UTP, but has the advantage of being capable of supporting higher transmission rates across longer distances.

c. Coaxial Cable

Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses. It is also sometimes used by telephone companies to connect central offices to telephone poles near customers. Some homes and offices use coaxial cable, too, but its widespread use as an Ethernet connectivity medium in enterprises and data centers has been supplanted by the deployment of twisted pair cabling.

d. Fibre Optic Cable

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems. A fiber optic cable consists of one or more strands of glass, each only slightly thicker than a human hair. The center of each strand is called the core, which provides the pathway for light to travel. The core is surrounded by a layer of glass called cladding that reflects light inward to avoid loss of signal and allow the light to pass through bends in the cable.



B. Commands

8 Basic Networking and Troubleshooting Commands:

1. ping

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. It's usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

```
C:\Users\keega>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

```
C:\Users\keega>ping www.google.com

Pinging www.google.com [142.250.77.36] with 32 bytes of data:
Reply from 142.250.77.36: bytes=32 time=3ms TTL=118
Reply from 142.250.77.36: bytes=32 time=3ms TTL=118
Reply from 142.250.77.36: bytes=32 time=3ms TTL=118
Reply from 142.250.77.36: bytes=32 time=2ms TTL=118

Ping statistics for 142.250.77.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

2. **tracert/traceroute**

   The tracert command (spelled traceroute in Unix/Linux implementations) is one of the key diagnostic tools for TCP/IP. It displays a list of all the routers that a packet must go through to get from the computer where tracert is run to any other computer on the Internet. Each one of these routers is called a hop.

```
C:\Users\keega>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:\Users\keega>tracert www.google.com

Tracing route to www.google.com [172.217.174.68]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     6 ms     1 ms     1 ms  100.93.152.1
  3     1 ms     2 ms     1 ms  114.79.129.57.dvois.com [114.79.129.57]
  4     3 ms     3 ms     3 ms  72.14.208.165
  5     5 ms     5 ms     4 ms  209.85.245.11
  6     3 ms     3 ms     3 ms  142.250.228.51
  7     3 ms     2 ms     2 ms  bom07s25-in-f4.1e100.net [172.217.174.68]

Trace complete.
```

3. **getmac/ifconfig**

   We can find mac address (physical address) of a computer using the command '*getmac*'. This can be used to get mac address for remote computers also.

```
C:\Users\keega>getmac

Physical Address    Transport Name
=================== ==========================================================
2C-F0-5D-DA-BC-7F   \Device\Tcpip_{FDA25F7A-12B0-4353-B623-AD9437A07EFB}
N/A                 Hardware not present
```

4. **ipconfig**

   ipconfig (standing for "Internet Protocol configuration") is a console application program of some computer operating systems that displays all current TCP/IP network configuration values.

```
C:\Users\keega>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4c37:677a:1433:323f%15
   IPv4 Address. . . . . . . . . . . : 192.168.0.108
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

5. **nslookup**

   nslookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records.

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

> www.google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:813::2004
          142.250.67.196
```

6. **netstat**

   The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information.

```
C:\Users\keega>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:49399  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:49401  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:50050  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:50725  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51312  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51315  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51316  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51323  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51327  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51330  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51332  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51336  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51338  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51340  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51343  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51347  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51351  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51356  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51365  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51368  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51371  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51373  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51378  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51382  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51386  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51389  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51393  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51395  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51400  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51402  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51405  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51409  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51413  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51415  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51417  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51422  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51425  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51428  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51431  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51439  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51440  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51441  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51449  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51454  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51458  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51463  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51469  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51470  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51476  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51481  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51486  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51490  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51494  TIME_WAIT
  TCP    127.0.0.1:1120         DESKTOP-QK5TB9G:51498  TIME_WAIT
```

7. **route**

   The route command allows you to make manual entries into the network routing tables. The route command distinguishes between routes to hosts and routes to networks by interpreting the network address of the *Destination* variable, which can be specified either by symbolic name or numeric address.

```
C:\Users\keega>route print
===========================================================================
Interface List
 15...2c f0 5d da bc 7f ......Realtek PCIe GbE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.108     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link     192.168.0.108    291
    192.168.0.108  255.255.255.255         On-link     192.168.0.108    291
    192.168.0.255  255.255.255.255         On-link     192.168.0.108    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.0.108    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.0.108    291
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0         25.0.0.1  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 15    291 fe80::/64                On-link
 15    291 fe80::4c37:677a:1433:323f/128
                                    On-link
  1    331 ff00::/8                 On-link
 15    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
 If Metric Network Destination      Gateway
  0 4294967295 2620:9b::/96             On-link
  0   9000 ::/0                      2620:9b::1900:1
===========================================================================
```

Conclusion: In this experiment, the case study about the different types of Networking Devices available in the market and their uses. We even learnt different basic and troubleshooting commands in networking.