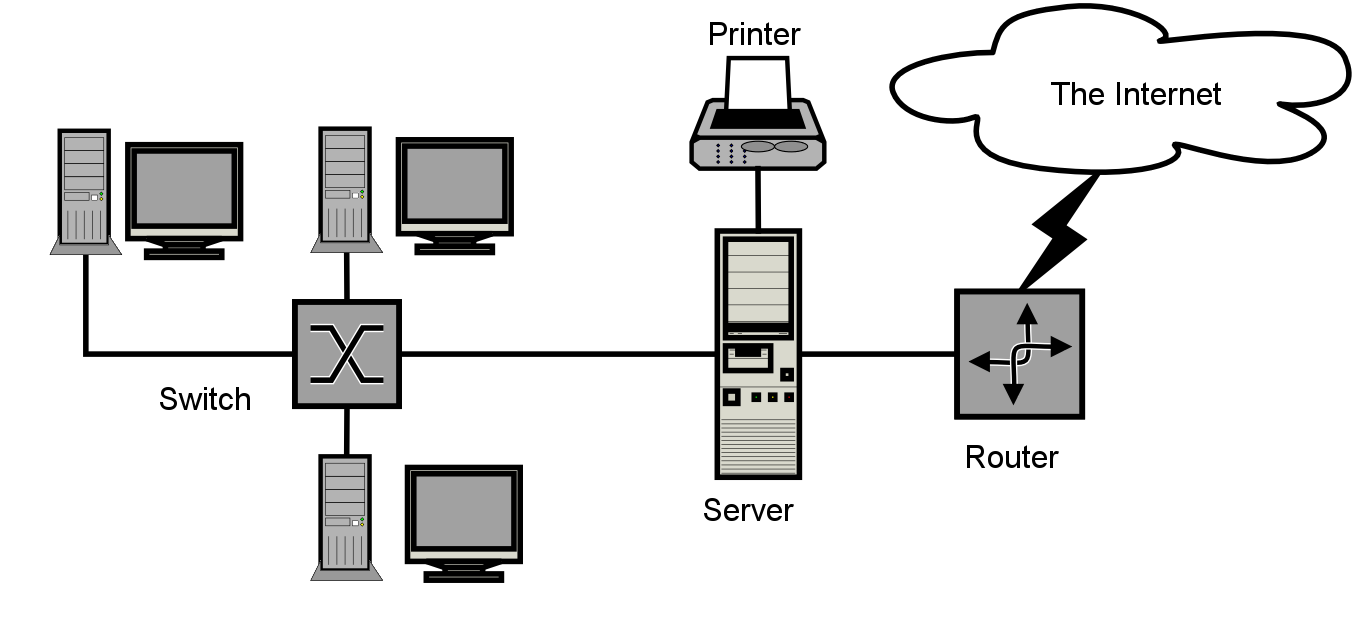
**EXPERIMENT NO : 1A**

**AIM:** Study of various network devices

**THEORY:**

1)Define Computer Networks.

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.

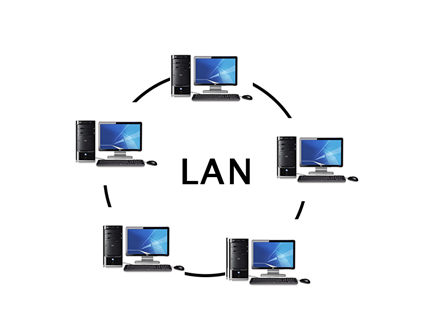


**Figure 1: A Computer Network**

2)Types of Networks:

* Local Area Network(LAN)
* Wide Area Network(WAN)
* Metropolitan Area Network(MAN)
* Personal Area Network(PAN)
* **Local Area Network(LAN):**

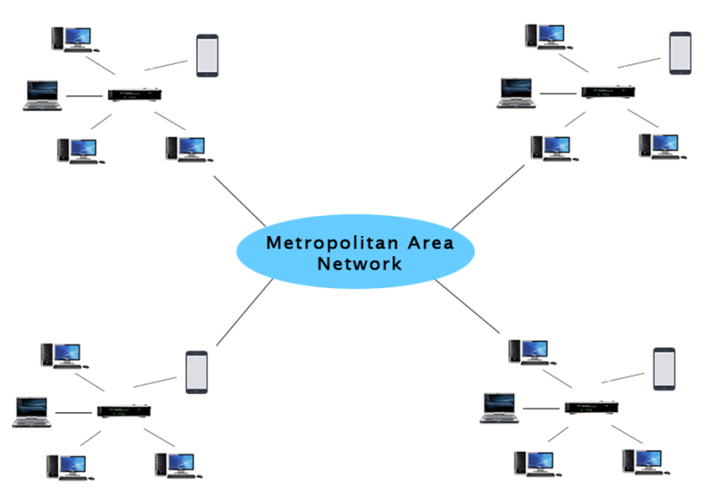
Local Area Network is a group of computers connected to each other in a small area such as building, office.LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.The data is transferred at an extremely faster rate in Local Area Network.Local Area Network provides higher security.



**Figure 2: Local Area Network**

* **Metropolitan Area Network(MAN):**

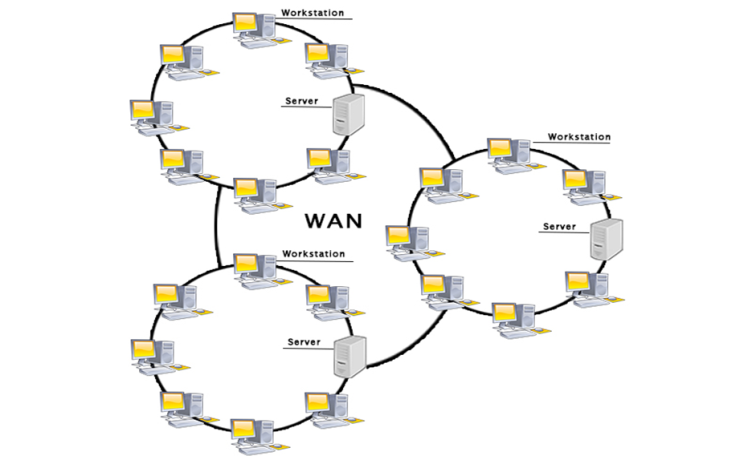
A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.Government agencies use MAN to connect to the citizens and private industries.In MAN, various LANs are connected to each other through a telephone exchange line.The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.It has a higher range than Local Area Network(LAN).



**Figure 3: Metropolitan Area Network**

* **Wide Area Network(WAN):**

A Wide Area Network is a network that extends over a large geographical area such as states or countries.A Wide Area Network is quite bigger network than the LAN.A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.The internet is one of the biggest WAN in the world.A Wide Area Network is widely used in the field of Business, government, and education.



**Figure 4: Wide Area Network**

Other type of computer network is Personal Area Network(PAN)

3) Computer Networks Hardware:

* **Router:**

A router is a [networking device](https://en.wikipedia.org/wiki/Networking_device) that forwards [data packets](https://en.wikipedia.org/wiki/Data_packet) between [computer networks](https://en.wikipedia.org/wiki/Computer_network). Routers perform the traffic directing functions on the [Internet](https://en.wikipedia.org/wiki/Internet). Data sent through the internet, such as a [web page](https://en.wikipedia.org/wiki/Web_page) or [email](https://en.wikipedia.org/wiki/Email), is in the form of data packets. A packet is typically [forwarded](https://en.wikipedia.org/wiki/Packet_forwarding) from one router to another router through the networks that constitute an [internetwork](https://en.wikipedia.org/wiki/Internetwork) (e.g. the Internet) until it reaches its destination [node](https://en.wikipedia.org/wiki/Node_(networking)). A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the [network address](https://en.wikipedia.org/wiki/Network_address) information in the packet to determine the ultimate destination.



**Figure 5: Router**

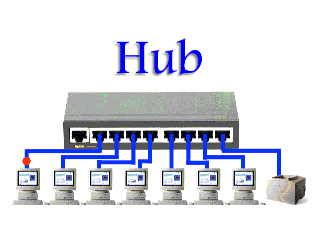
* **Network Switch:**

A network switch (also called switching hub, bridging hub, officially MAC bridge) is a [computer networking device](https://en.wikipedia.org/wiki/Computer_networking_device) that connects devices on a [computer network](https://en.wikipedia.org/wiki/Computer_network) by using [packet switching](https://en.wikipedia.org/wiki/Packet_switching) to receive, process, and forward data to the destination device.A network switch is a multiport [network bridge](https://en.wikipedia.org/wiki/Network_bridge) that uses [hardware addresses](https://en.wikipedia.org/wiki/Hardware_address) to process and forward data at the [data link layer](https://en.wikipedia.org/wiki/Data_link_layer)(layer 2) of the [OSI model](https://en.wikipedia.org/wiki/OSI_model). Some switches can also process data at the [network layer](https://en.wikipedia.org/wiki/Network_layer) (layer 3) by incorporating [routing](https://en.wikipedia.org/wiki/Routing) functionality. Such switches are commonly known as layer-3 switches or [multilayer switches](https://en.wikipedia.org/wiki/Multilayer_switch).

**Figure 6: Network Switch**

* **Hub:**

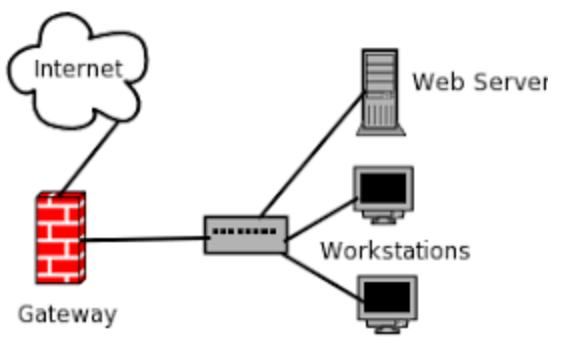
An Ethernet hub, active hub, network hub, repeater hub, multiport repeater, or simply hub is a [network hardware](https://en.wikipedia.org/wiki/Network_hardware) device for connecting multiple [Ethernet](https://en.wikipedia.org/wiki/Ethernet) devices together and making them act as a single [network segment](https://en.wikipedia.org/wiki/Network_segment). It has multiple [input/output](https://en.wikipedia.org/wiki/Input/output) (I/O) ports, in which a [signal](https://en.wikipedia.org/wiki/Signalling_(telecommunication)) introduced at the input of any [port](https://en.wikipedia.org/wiki/Computer_port_(hardware)) appears at the output of every port except the original incoming. A hub works at the [physical layer](https://en.wikipedia.org/wiki/Physical_layer) (layer 1) of the [OSI model](https://en.wikipedia.org/wiki/OSI_model). A repeater hub also participates in collision detection, forwarding a [jam signal](https://en.wikipedia.org/wiki/Jam_signal) to all ports if it detects a [collision](https://en.wikipedia.org/wiki/Collision_(telecommunications)).



**Figure 7: Hub**

* **Gateway:**

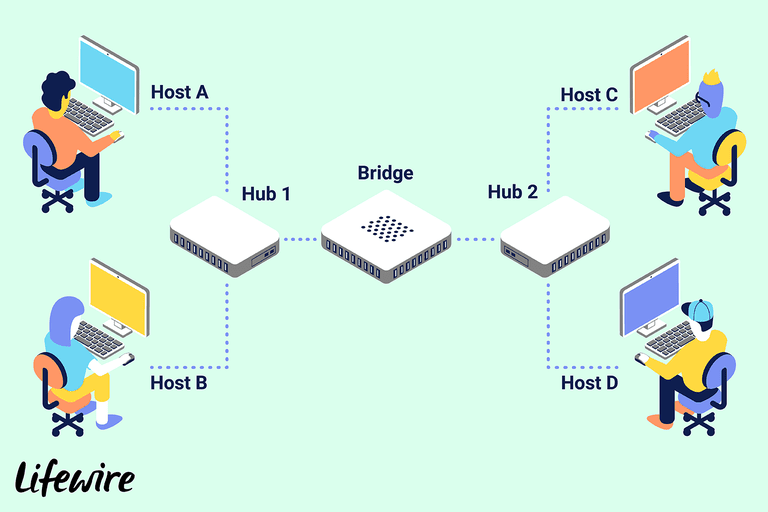
A network gateway joins two networks so the devices on one network can communicate with the devices on another network. Without gateways, you couldn't be able to access the internet, communicate and send data back and forth. A gateway can be implemented completely in software, hardware, or a combination of both. Because a network gateway by definition appears at the edge of a network, related capabilities such as [firewalls](https://www.lifewire.com/definition-of-firewall-817568) and proxy servers tend to be integrated with it.



**Figure 8: Gateway**

* **Bridges:**

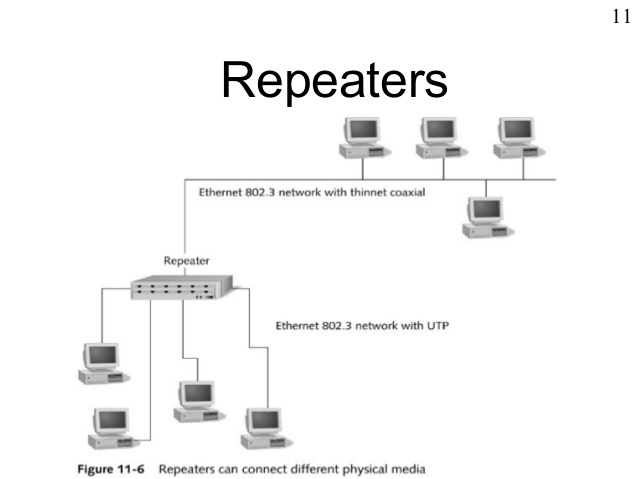
A network bridge is a [computer networking device](https://en.wikipedia.org/wiki/Networking_hardware) that creates a single aggregate network from multiple [communication networks](https://en.wikipedia.org/wiki/Communication_network) or [network segments](https://en.wikipedia.org/wiki/Network_segment). This function is called network bridging.[[1]](https://en.wikipedia.org/wiki/Bridging_(networking)#cite_note-1) Bridging is distinct from [routing](https://en.wikipedia.org/wiki/Routing). Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. In the [OSI model](https://en.wikipedia.org/wiki/OSI_model), bridging is performed in the [data link layer](https://en.wikipedia.org/wiki/Data_link_layer) (layer 2). If one or more segments of the bridged network are [wireless](https://en.wikipedia.org/wiki/Wireless_network), the device is known as a wireless bridge.



**Figure 9: Network Bridge**

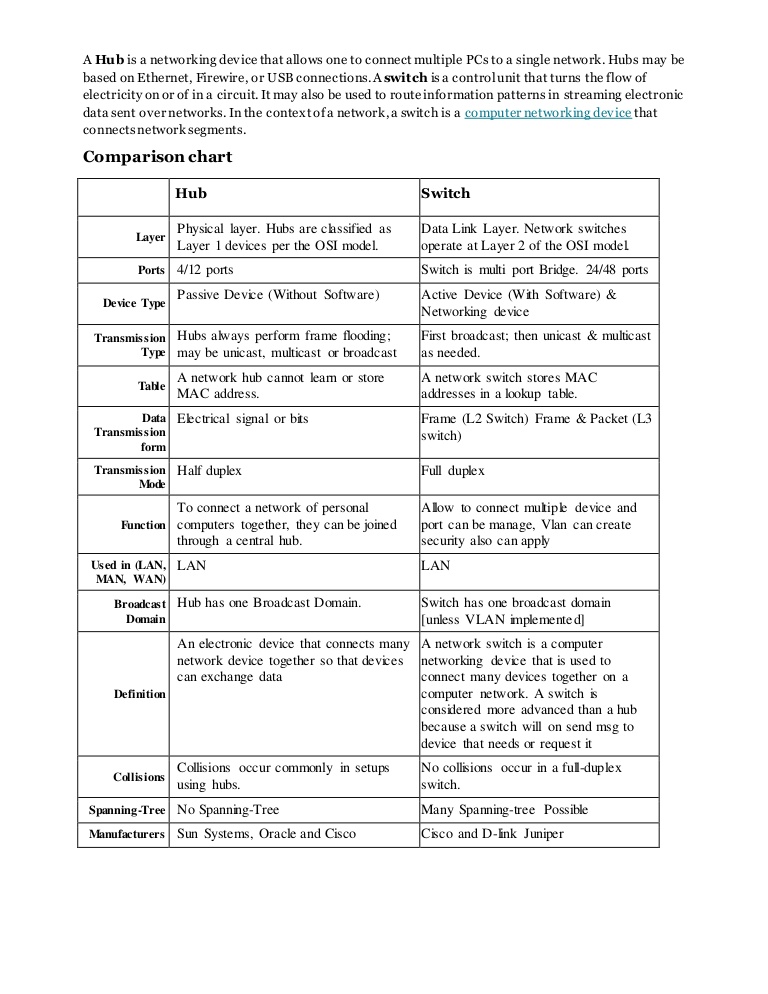
* **Repeaters:**

Network repeaters are small devices that receive and retransmit incoming electrical, wireless, and optical signals. They help bring a signal to spots where [Ethernet](https://www.lifewire.com/what-is-ethernet-3426740) and [Wi-Fi](https://www.lifewire.com/what-is-wi-fi-2377430) data transmissions, which can span only limited distances before the signal quality degrades, can't reach. Repeaters attempt to preserve signal integrity and extend the distance over which data can travel.



**Figure 10: Network Repeater**

4)Difference Between Hub and Switch:



5) Connectors:

* **Coaxial Cable:**

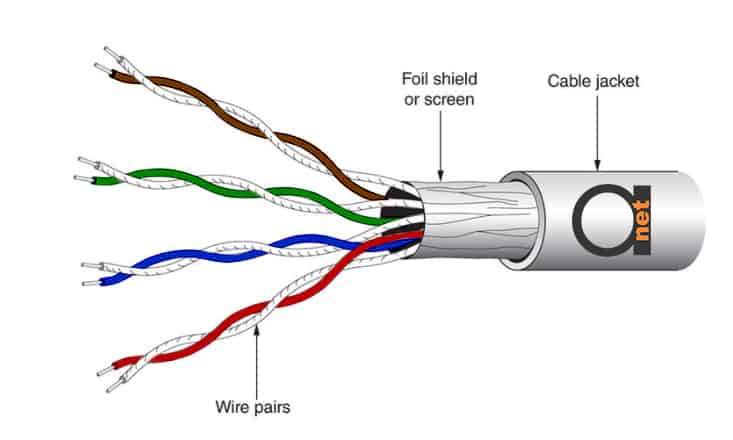
Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses. It is also sometimes used by telephone companies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



**Figure 11: Coaxial Cable**

* **Twisted Pair:**

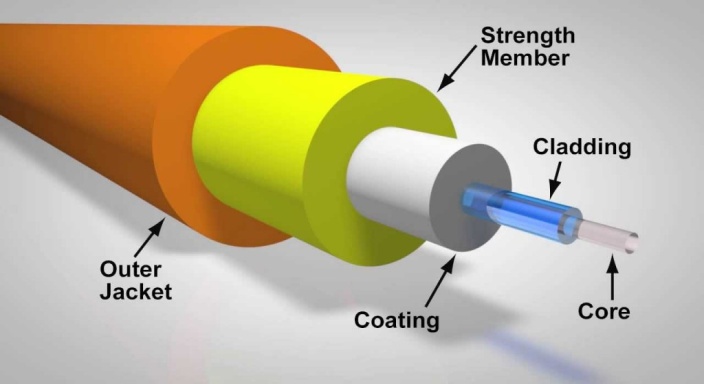
A type of cable that consists of two independently insulated wires twisted around one another. The use of two wires twisted together helps to reduce [crosstalk](https://www.webopedia.com/TERM/C/crosstalk.html) and electromagnetic induction. While twisted-pair cable is used by older telephone [networks](https://www.webopedia.com/TERM/N/network.html) and is the least expensive type of [local-area network (LAN)](https://www.webopedia.com/TERM/L/local_area_network_LAN.html) cable, most networks contain some twisted-pair cabling at some point along the network. Other types of cables used for LANs include [coaxial cables](https://www.webopedia.com/TERM/C/coaxial_cable.html)and [fiber optic](https://www.webopedia.com/TERM/F/fiber_optics.html) cables.



**Figure 12: Twisted Pair**

* **Optical Fibres:**

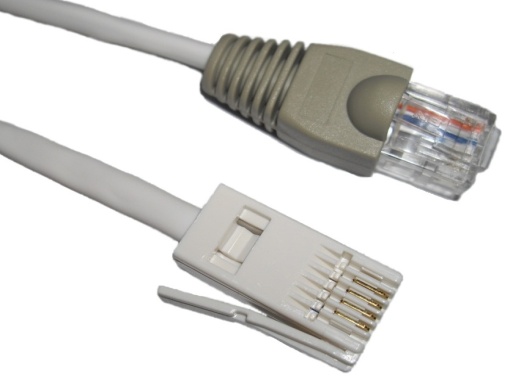
An optical fiber is a flexible, [transparent](https://en.wikipedia.org/wiki/Transparency_and_translucency) fiber made by [drawing](https://en.wikipedia.org/wiki/Drawing_(manufacturing)) [glass](https://en.wikipedia.org/wiki/Glass) ([silica](https://en.wikipedia.org/wiki/Silica)) or plastic to a diameter slightly thicker than that of a [human hair](https://en.wikipedia.org/wiki/Hair%27s_breadth). Optical fibers are used most often as a means to transmit light between the two ends of the fiber and find wide usage in [fiber-optic communications](https://en.wikipedia.org/wiki/Fiber-optic_communication), where they permit transmission over longer distances and at higher [bandwidths](https://en.wikipedia.org/wiki/Bandwidth_(computing)) (data rates) than electrical cables. Fibers are used instead of [metal](https://en.wikipedia.org/wiki/Metal) wires because signals travel along them with less [loss](https://en.wikipedia.org/wiki/Attenuation); in addition, fibers are immune to [electromagnetic interference](https://en.wikipedia.org/wiki/Electromagnetic_interference), a problem from which metal wires suffer excessively. Fibers are also used for [illumination](https://en.wikipedia.org/wiki/Illumination_(lighting)) and imaging, and are often wrapped in bundles so they may be used to carry light into, or images out of confined spaces, as in the case of a [fiberscope](https://en.wikipedia.org/wiki/Fiberscope).



**Figure 13: Optical Fibres**

* **RJ45:**

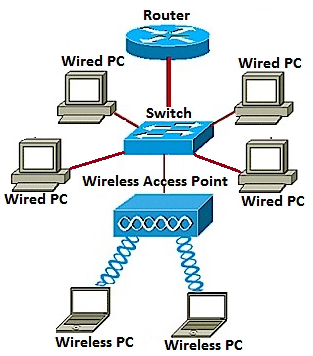
RJ45 is a type of connector commonly used for [Ethernet](https://techterms.com/definition/ethernet) networking. It looks similar to a telephone jack, but is slightly wider. Since Ethernet cables have an RJ45 connector on each end, Ethernet cables are sometimes also called RJ45 cables.The "RJ" in RJ45 stands for "registered jack," since it is a standardized networking interface. The "45" simply refers to the number of the interface standard.



**Figure 13: RJ45**

* **Access Point:**

In a wireless local area network ([WLAN](https://searchmobilecomputing.techtarget.com/definition/wireless-LAN)), an access point is a station that transmits and receives data (sometimes referred to as a [transceiver](https://searchnetworking.techtarget.com/definition/transceiver)). An access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each access point can serve multiple users within a defined network area; as people move beyond the range of one access point, they are automatically handed over to the next one. A small WLAN may only require a single access point; the number required increases as a function of the number of network users and the physical size of the [network](https://searchnetworking.techtarget.com/definition/network).



**Figure 14: Access Points**

**EXPERIMENT NO. 1B**

**Aim:** Study of various network commands

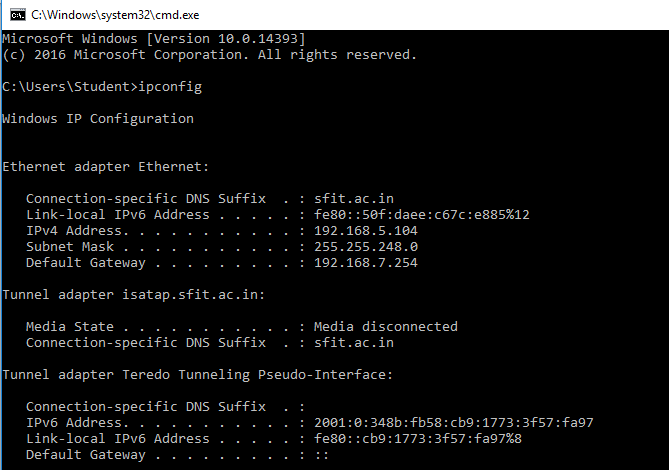
**Theory:**

1) ipconfig:

Ipconfig is a DOS utility that can be used from MS-DOS and the Windows command line to display the network settings currently assigned and given by a network. This command can be utilized to verify a network connection as well as to verify your network settings. Syntax:

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

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



**FIGURE 1: IPCONFIG**

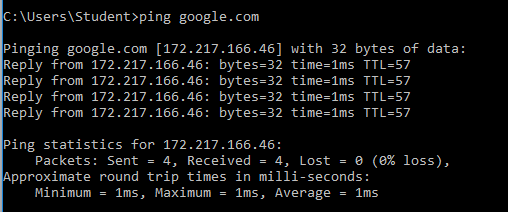
2) ping:

The ping command helps determine TCP/IP networks IP address, as well as issues with the network and assists in resolving them. See the ping definition for a full description.

Syntax:

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] [-4] [-6 target\_name

Ping supports the ability to ping an Internet address. In the example above, we pinged "google.com" and as can be seen, received four responses back. If we couldn't reach the server or the server was blocking our request, we would have lost all four packets.



**FIGURE 2: PING**

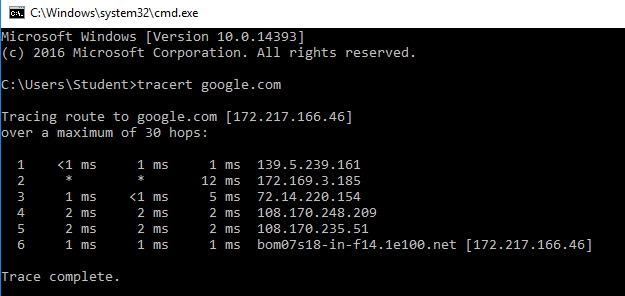
3) Tracert:

The tracert command is used to see a network packet being sent and received, as well as the number hops required for that packet to get to its destination. Users with Microsoft Windows 2000 and Windows XP who need additional network latency and loss information should also consider using the pathping command.

Syntax:

tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target\_name

Below is an example of the result when we used the tracert command on www.google.com. As you can see, the packet had very few hops and short reply times on its way to its destination due to our close location.



**FIGURE 3: TRACERT**

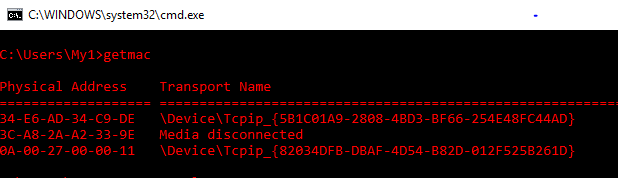
4) getmac:

Getmac is a Windows command used to display the Media Access Control (MAC) addresses for each network adapter in the computer. getmac can be useful either when you want to enter the MAC address into a network analyzer or when you need to know what protocols are currently in use on each network adapter in a computer.

Syntax:

getmac[.exe][/s <computer> [/u <Domain\<User> [/p <Password>]]][/fo {TABLE | list | CSV}][/nh][/v]

A media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC). For communications within a network segment, it is used as a network address for most IEEE 802 network technologies, including Ethernet, Wi-Fi, and Bluetooth.



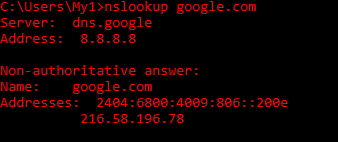
**FIGURE 4:GETMAC**

5)nslookup:

nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records. The name "nslookup" means "name server lookup".

Syntax:

nslookup [-opt ...] [{Host| [Server]}]



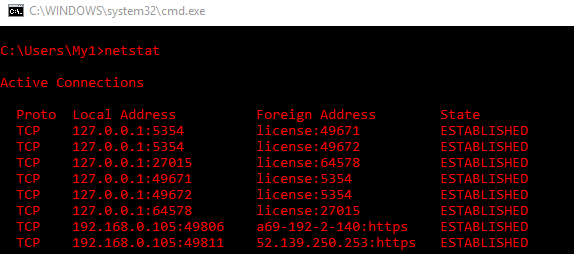
**FIGURE 5:NSLOOKUP**

6)Netstat:

Netstat is a common command line TCP/IP networking utility available in most versions of Windows, Linux, UNIX and other operating systems. In computing, netstat (network statistics) is a command-line network utility tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics.

Syntax:

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p protocol] [-r] [-s] [-t] [-x] [-y] [time\_interval] [/?]



**FIGURE 5:NETSTAT**