Network And Internet

Computer Network:

A **computer network** is a set of connected computers. Computers on a network are called **nodes**. The connection between computers can be done via cabling.

Connected computers can share resources like access to the Internet, printers, file servers, and others between different nodes connected within it. A network is a multipurpose connection, which allows a single computer to do more than it could without any connection

A network compromises of four basic elements.

All data **networks** are comprised of these **elements**, and cannot function without them.

1) Software
2) Hardware
3) Protocols
4) Connection medium

Hardware

Hardware is the backbone of network

Network hardware's includes network cards, routers or network switches, modems or ethernet repeaters

Without this hardware computer has no means of accessing a network.

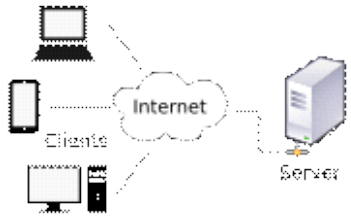
Network cards give computers direct access to other media and enable them to connect to other equipment including routers, switches, modems and repeaters

Routers and switches allow a single network connection from a modem to be divided between several computers

Client Devices:

a **client** is a piece of computer hardware or software that accesses a service made available by a server.

The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network.



In computing a **server** is a piece of computer hardware or software (computer program) that provides functionality for other programs or devices, called "client".

Computer and mobile devices connected to the network are called client devices

Client devices are vital components of networks since without clients requiring access the network is essentially pointless

In order to classify as a client device a computer or mobile must be able to connect to the network and utilize it.

Depending on the network a client device may even require a specialized software to establish a connection.

internet:

Series of network owned by two or more organisations and setup to communicate with each other.

Network of computer that are able to exchange information using Internet protocols

Internet:

Most commonly used internet

Worldwide network compromising of all other networks interconnected and communicating on the open web

Largest internet that we have in this world which compromises of trillions of computers being connected to each other

The **Internet** (or internet) is the global system of interconnected computer networks communicating between networks and devices. It is a *network of networks*

It was originated from research projects going back to the early 1960s. The goal was to develop the ability to link a variety of computer networks so That they could function as a connected system that would not be disrupted by local disasters.

Elements Of Network:

Modern data network has become a critical asset for many industries

Most basic data networks are designed to connect users and enable them to access various resources at the internet and other computers connected to network

Connection Media:

Without connections a network cannot function
The means through which we send our data from one place to another is known as connection medium.
Transmission medium is of two types:

- **(i) Wired** --------> Twisted Pair Cable , Coaxial Cable and Optical Fiber Cable
- **(ii) Wireless** --------> Radio waves, Microwaves and Infrared

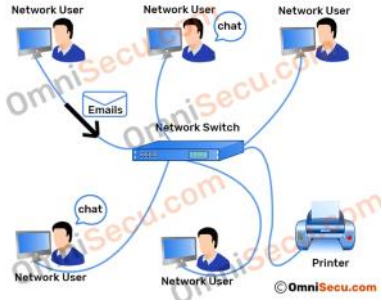
Software:

Network software is a foundational element for any network
In order for hardware to interact with the network it needs software to issue commands
The primary form of networking software is protocols (software that instructs network devices on how to connect to the network and how to interact with each other.
Other examples of networking software includes connection monitoring software, networking clients and other tools designed to further facilitate Your computer's ability to connect to the network

Protocols:

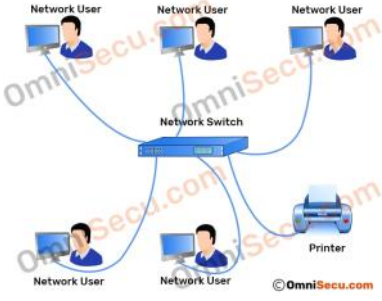
There are some defined rules and conventions for communication between network devices.
These are called Protocols. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into sent and received messages.
Set of rules governing particular aspects
Established set of rules that determine how data is transmitted between different devices in the same network
In order for two computers to talk to each other they must be speaking the same language.
Network protocols are like common language for computers-----> can have different hardware and software make hem to communicate

Why make network?

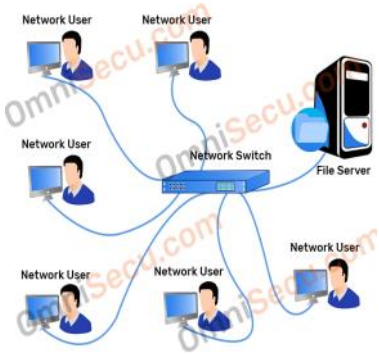


User communication: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.

Application sharing: Applications can be shared over the network, and this allows to implement client/server applications



Hardware sharing: Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc. Without computer networks, device sharing is not possible.



File sharing: Networking of computers helps the network users to share data files.
Network gaming: A lot of network games are available, which allow multi-users to play from different locations.

Improve communication
Data transfer
Collaboration facilities(like zoom, MS teams, google meet)
To group/team
Sharing resources (printer, fax, modems, scanner server etc.)
To access information
To control machines / devices remotely

High reliability -----> if there are alternate sources of supply, all files could be replicated on two or more machines. Incase one of them wasn't available because of hardware failure, other copies could be used

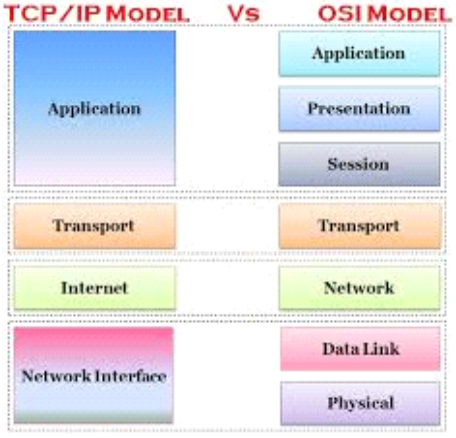
Printing Press:
Device that allows printing for mass production of uniform printed matter mainly in form of text, pamphlets and newspapers
Useful tool for efficiently communicating and disseminating written ideas and processes laid down in writing.

If there is no structure then it is impossible to the rest of the things. Dividing the works makes it easier to handle things that is why network has several layers

Open Systems Interconnection (OSI)

OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. It describes seven layers that computer systems use to communicate over a network

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium



Physical Layer :
Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations. This layer defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.
Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data. The binary data is then sent over the wired or wireless media.

Data Link Layer :

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer. The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

IP Address (Internet Protocol address):

Also known as the Logical Address, the IP Address is the network address of the system across the network.

To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^32.
Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

MAC Address (Media Access Control address):

MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card). A MAC address is assigned to the NIC at the time of manufacturing.

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. It works at Data Link Layer.

S.NO	MAC ADDRESS	IP ADDRESS
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or six byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can't be found easily by third party.	IP Address can be found by third party.

Network Layer :

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.
Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

Transport Layer :

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

All modules and procedures pertaining to transportation of data or data stream are categorized into this layer. As all other layers, this layer communicates with its peer Transport layer of the remote host.

Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.

Session Layer :

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and termined at layer 5. Session layer services also include authentication and reconnections.

Presentation Layer

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

Application Layer :

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.

Application layer is the top most layer in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

A user may or may not directly interacts with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote host.

When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.

Hops:

A hop is a computer networking term that refers to the number of routers that a packet (a portion of data) passes through from its source to its destination.

Nodes:

A node is a connection point inside a network that can receive, send, create, or store data. Each node requires you to provide some form of identification to receive access, like an IP address. A few examples of nodes include computers, printers, modems, bridges, and switches. A node is essentially any network device that can recognize, process, and transmit information to any other network node.

Routers:

A router is a physical or virtual device that sends information contained in data packets between networks. Routers analyze data within the packets to determine the best way for the information to reach its ultimate destination. Routers forward data packets until they reach their destination node.

Switches:

A switch is a device that connects other devices and manages node-to-node communication within a network, ensuring data packets reach their ultimate destination. While a router sends information between networks, a switch sends information between nodes in a single network. When discussing computer networks, 'switching' refers to how data is transferred between devices in a network.

Types of Network:

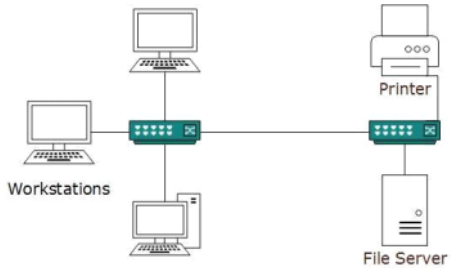
The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used

for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.
Early LAN's had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example : A bunch of students playing Counter Strike in the same room (without internet).



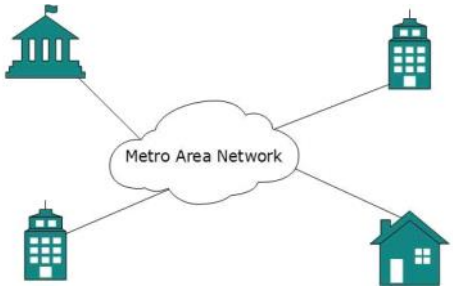
A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization' offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million. LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers.

LANs are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally.
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.
LAN can be wired, wireless, or in both forms at once.

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

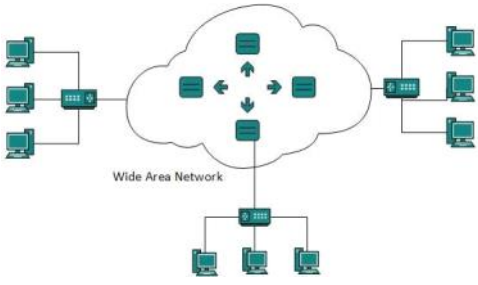


The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.

Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.
There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.
WAN's data rate is slow about a 10th LAN's speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites. Example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet.



As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment.

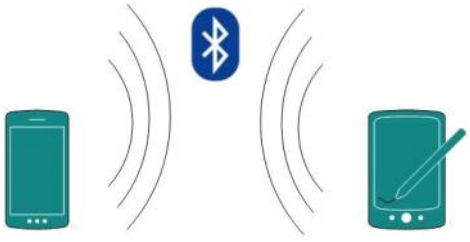
WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administration.

Conclusion –

There are many advantages of LAN over MAN and WAN, such as LAN's provide excellent reliability, high data transmission rate, they can easily be managed, and shares peripheral devices too. Local Area Network cannot cover cities or towns and for that Metropolitan Area Network is needed, which can connect city or a group of cities together. Further, for connecting Country or a group of Countries one requires Wide Area Network.

PAN (personal area network):

A PAN serves one person. For example, if you have an iPhone and a Mac, it's very likely you've set up a PAN that shares and syncs content—text messages, emails, photos, and more—across both devices.



A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.

For example, Piconet is Bluetooth-enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

WLAN (wireless local area network):

A WLAN is just like a LAN but connections between devices on the network are made wirelessly.

SAN (storage area network):

A SAN is a specialized network that provides access to block-level storage—shared network or cloud storage that, to the user, looks and works like a storage drive that's physically attached to a computer.

CAN (campus area network):

A CAN is also known as a corporate area network. A CAN is larger than a LAN but smaller than a WAN. CANs serve sites such as colleges, universities, and business campuses.

VPN (virtual private network):

A VPN is a secure, point-to-point connection between two network end points (see 'Nodes' below). A VPN establishes an encrypted channel that keeps a user's identity and access credentials, as well as any data transferred, inaccessible to hackers.

Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as **Network devices** and include things such as routers, switches, hubs, and bridges.