

COLLEGE OF COMPUTER APPLICATION(04)

Program Name: Bachelor of Computer Application

Department Name:  BCA                   Department Code: 023

Subject Name: Computer Network Subject Code: 2040233212

Academic Year: 2023-24

UNIT-1

1. Network Definition:

A network is a collection of interconnected devices or nodes that can communicate with each other to share resources, information, and services. Networks can be as small as a local area network (LAN) within a single building or as vast as the internet, connecting devices globally.

2. Network Topologies:

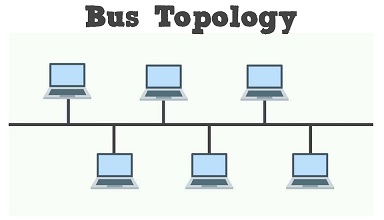
* Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.
* Network Topology is the arrangement with which computer systems or network devices are connected to each other.

Types of network topologies:-

1. Bus 2. Star 3. Ring 4. Mesh 5. Hybrid

Bus Topology:

It is a network type in which every computer and network device is connected to a single cable.



Features:

* It transmits data only in one direction.
* Every device is connected to a single cable.

Advantage

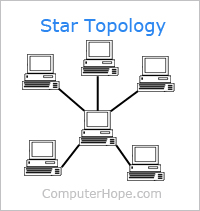
* It is cost effective (cheaper).
* Cable required is least as compared to other network topology.
* Used in small networks.
* It is easy to understand.
* Easy to expand joining two cables together.

Disadvantage

* Cables fail than the whole network fails.
* If network traffic is heavy or nodes are more the performance of network decreases.
* Cable has a limited length.

Star Topology:

* In this type of topol+ogy, all the computers are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.



Features:

* Every node has its own dedicated connection to the hub.
* Acts as a repeater for data flow.
* Can be used with twisted pair, Optical Fibre or coaxial cable.

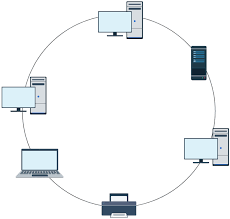
Advantages:

* Fast performance with few nodes and low network traffic.
* Hub can be upgraded easily.
* Easy to troubleshoot.
* Easy to set up and modify.
* Only that node is affected which has failed rest of the nodes can work smoothly.

Disadvantage:

* Cost of installation is high.
* Expensive to use.
* If the hub is affected than the whole network is stopped because all the nodes depend on the hub.

Ring Topology: Each device is connected to exactly two other devices, forming a ring.



Features:-

* A number of repeaters are used and the transmission is unidirectional.
* A data is transferred in a sequential manner that is bitten by bit.

Advantages:

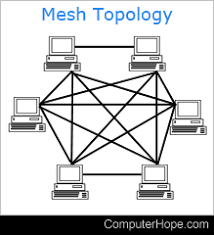
* Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
* Cheap to install and expand.

Disadvantage

* Troubleshooting is difficult in a ring topology.
* Adding or deleting the computer can disturb the network activity.

Mesh Topology:

* It is a point-to-point connection to other nodes and devices.
* Traffic is carried out between two devices or nodes to which it is connected.



Features:

* Fully connected
* Robust
* Not flexible

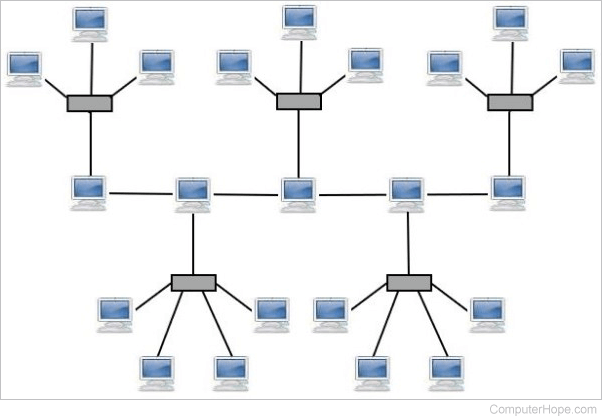
Advantages:

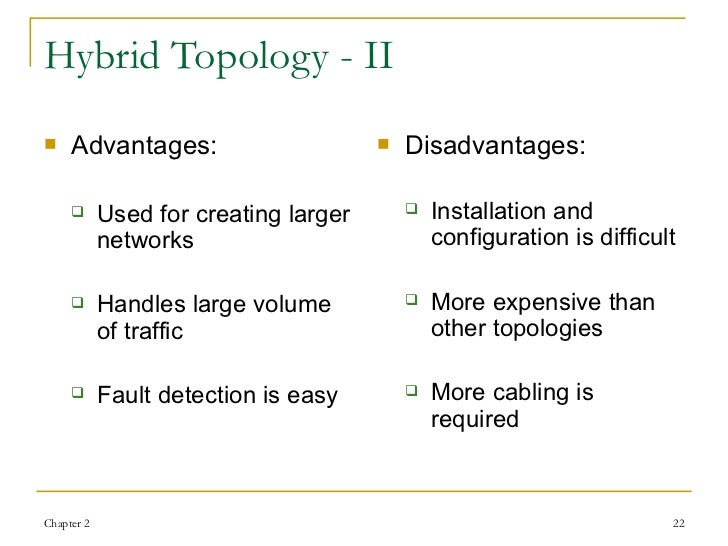
* Each connection can carry its own data load.
* It is robust.
* A fault is diagnosed easily.
* Provides security and privacy.

Disadvantage:

* Installation and configuration are difficult.
* Cabling cost is more.
* Bulk wiring is required.

Hybrid Topology: Combination of two or more different topologies.



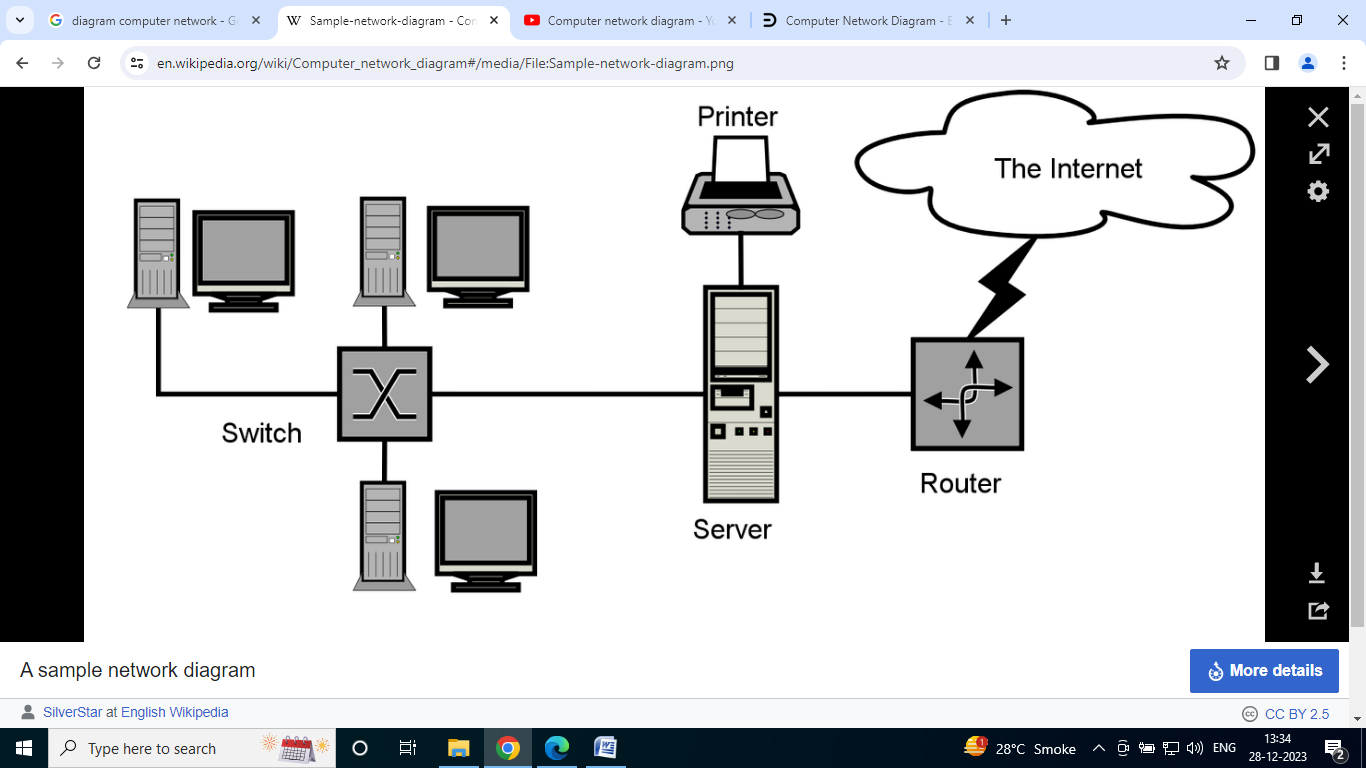


3. Computer Network:

A Computer Network is a system in which multiple computers are connected to each other to share information and resources.

The physical connection between networked computing devices is established using either cable media or wireless media.

The best known computer network is the internet.



Advantages of Computer Network

1. File Sharing

Major advantage of computer network is that allows file sharing and remote file access.

A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so.

1. Resource Sharing

All computers in the network can share resources such as printer, fax machine, modems and scanner.

1. Better connectivity and Communication

It allows users to connect and communicate with each other easily. Various communication application included email and groupware are used.

1. Internet Access

Computer networks provide internet service over the entire network. Every single computer attached to the internet can experience high speed internet.

1. Entertainment

Many games and other means of entertainment are easily available on the internet. Furthermore, Local Area Networks (LANs) offers and facilitates other ways of enjoyments, such as many players are connected through LAN and play a particular game with each other from a remote location.

1. Inexpensive System

Shares resources means reduction in hardware costs. Shared files means reduction in memory requirement, which indirectly means a reduction in file storage expenses. A particular software can be installed only once on the server and made available across all connected computers at once. This saves the expense of buying and installing the same software as many times for as many users.

1. Flexible Access

A user can log on to a computer anywhere on the network and access his files. This offers flexibility to the user as to where he should be during the course of his route.

1. Instant and multiple access

Computer networks are multiple processes. Many users can access the same information at the same time. Immediate commands such as printing command can be made with the help of computer network.

Disadvantages of Computer Network

1. Lack of data security and privacy

Because there would be a huge number of people who would be using a computer networks to get and share some of their files and resources, a certain user security would be always at risk. There might even be illegal activities that would occur which you need to be careful about and aware of.

1. Presence of computer viruses and malware

If even one computer on a network gets affected by a virus, there is a possible threat for the other systems getting affected too. Viruses can spread on a network easily, because of the interconnectivity of workstations. Moreover, multiple systems with common resources are perfect breeding ground for viruses that multiply.

1. Lack of independence

Since most networks have a centralized server and dependent clients , the client user lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.

1. Lack of Robustness

As previously stated, if a computer network’s main server breaks down, the entire system would become useless. Also, if it has a bridging device or central linking server that fails, the entire network would also come to a standstill.

1. Need an efficient handler

For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly network configuration and connection is very tedious and cannot be done by a average technician who does not have advanced knowledge.

Applications of Computer Network

1. Financial Services

Nowadays almost all the financial services depend on the computer network. You can access the financial services across the world. For example, a user can transfer money from one place to another by using the electronic fund transfer feature. We can use networking in various financial areas such as ATM, foreign exchange and credit history search.

1. Business

Nowadays most of the works of businesses are done over the computers. To exchange data and ideas, you need effective data and resources sharing features. To do this, you need to connect the computer with each other through the network. For example, a person of one department of an organization can share or access the electronic data of other departments through a network.

1. Email Services

A computer network provides you the facility to send or receive emails across the globe in few seconds.

1. Mobile Applications

By using mobile applications, such as cellular or wireless phones, you can communicate (exchange your views and ideas) with one other.

1. Directory Services

It provides you the facility to store files on a centralized location to increase the speed of search operation worldwide.

1. Teleconferencing

It contains voice conferencing and video conferencing which are based on learning. In teleconferencing, the participants need not be presented at the same location.

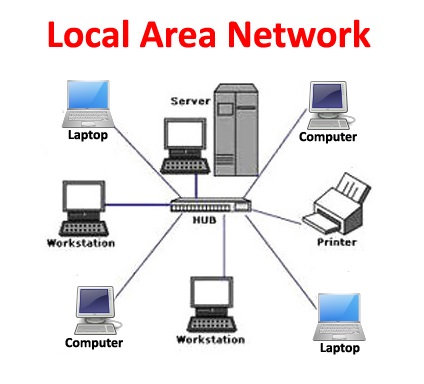
Types of Computer Network

LAN (Local Area Network)

1. It is privately-owned networks within a single building or campus of up to a few kilometers in size.
2. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
3. LANs are easy to design and troubleshoot.
4. In LAN, all the machines are connected to a single cable.
5. Different types of topologies such a Bus, Ring, Star, and Tree are used.
6. The data transfer rates for LAN is up to 10 Gbits/s.
7. They transfer data at high speeds. The high transmission rate is possible in LAN because of the short distance between various computer networks.
8. They exist in limited geographical area.

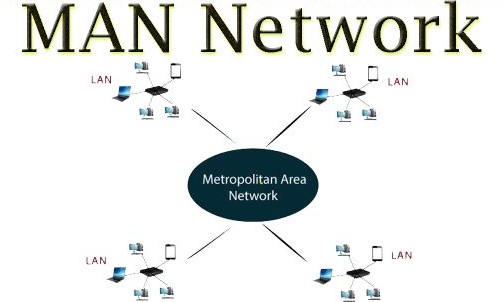
Advantages

1. LAN transfers data at high speed.
2. LAN technology is generally less expensive.



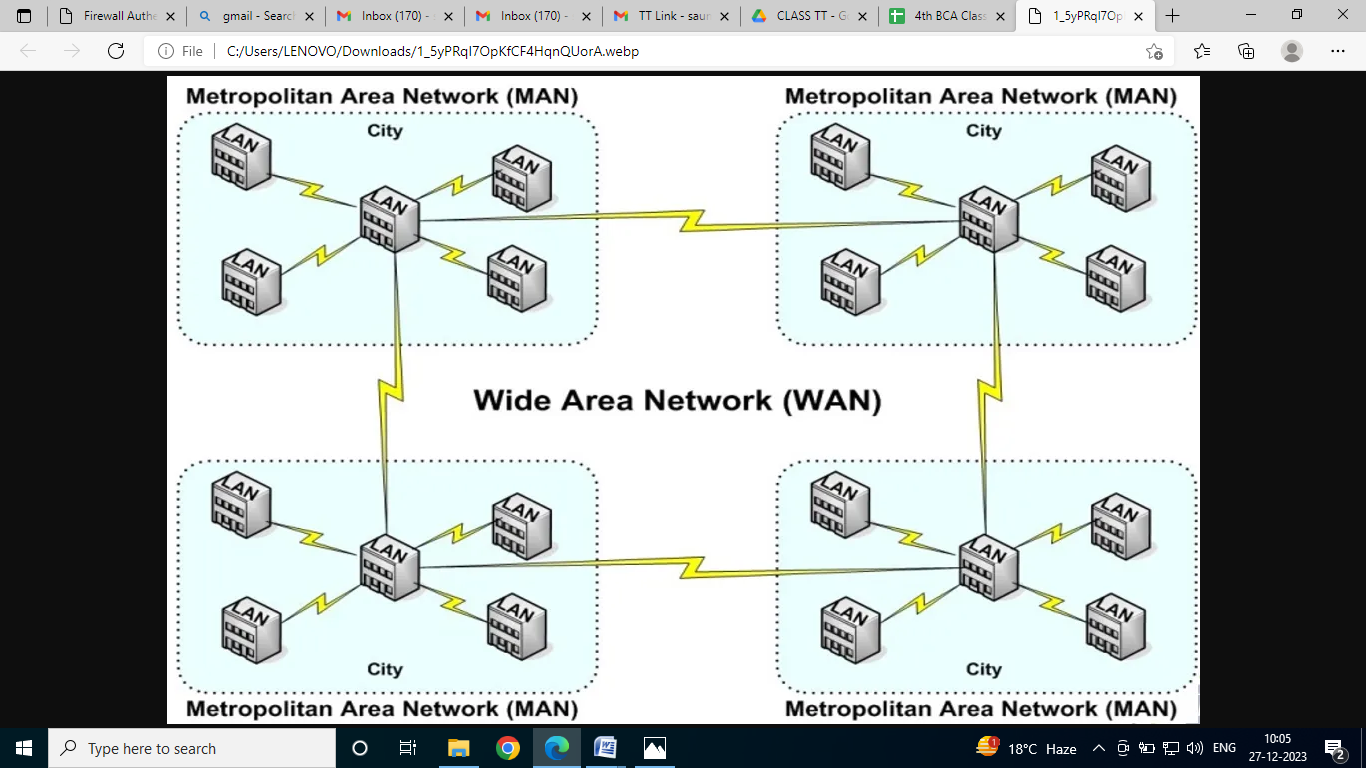
MAN (Metropolitan Area Network)

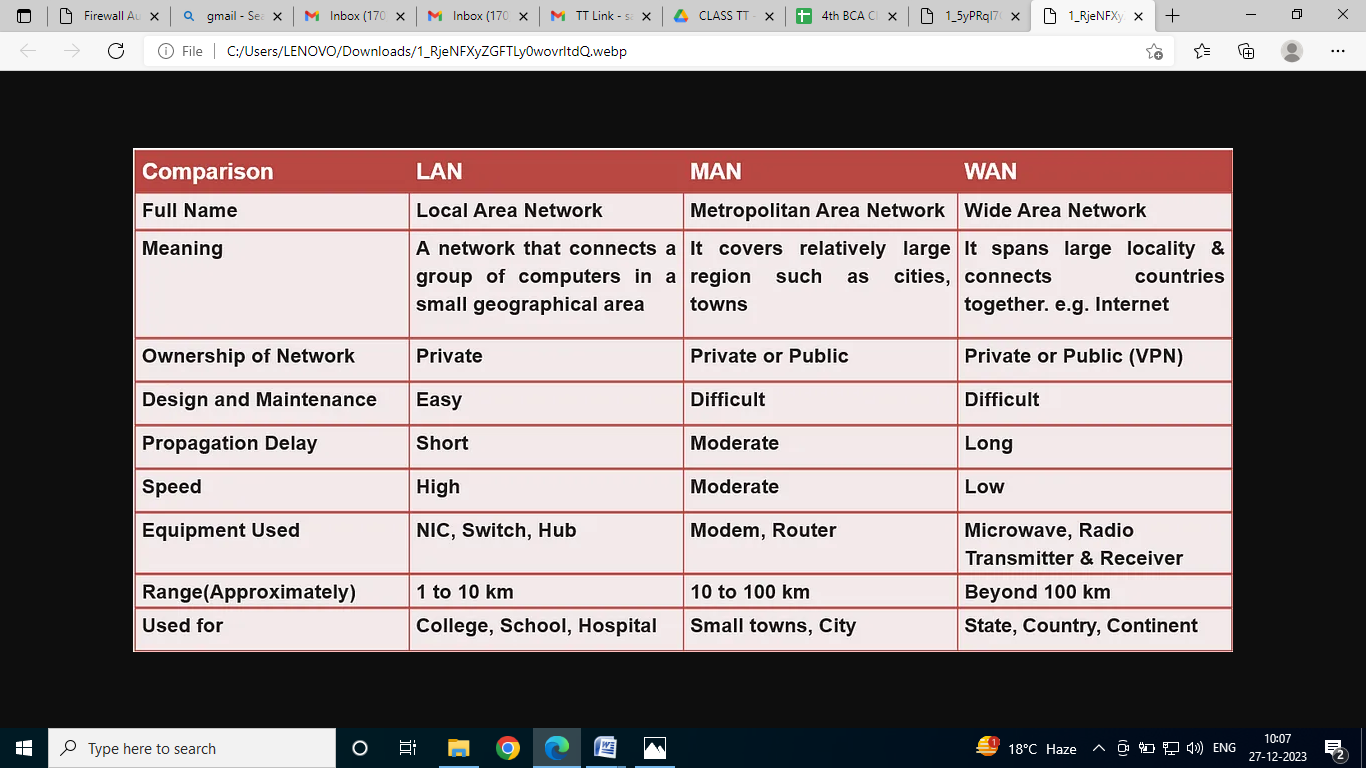
1. MAN is a larger version of LAN which covers an area that is larger than the covered by LAN but smaller than the area covered by WAN.
2. A metropolitan area network or MAN covers a city. The best-known example of MAN is the cable television network available in many cities.
3. MAN connects two or more LANs.
4. At first, the companies began jumping into the business, getting contracts from city governments to wire up an entire city.
5. The next step was television programming and even entire channels designed for cable only.



WAN (Wide Area Network)

1. It spans a large geographical area, often a country or a region.
2. WAN links different metropolitan’s countries and national boundaries thereby enabling easy communication.
3. It may be located entirely within a state or a country or it may be interconnected around the world.
4. It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
5. The communication between different users of LAN is established using leased telephone lines or satellite links and similar channels.





Internet

* The internet is a type of world-wide computer network.
* The internet is a collection of infinite numbers of connected computers that are spread across the world.
* We can also say that the Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world.
* It is established as the largest network and sometimes called a network of a network that consists of numerous academic , business and government networks, which together carry various information.
* The internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
* When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs.

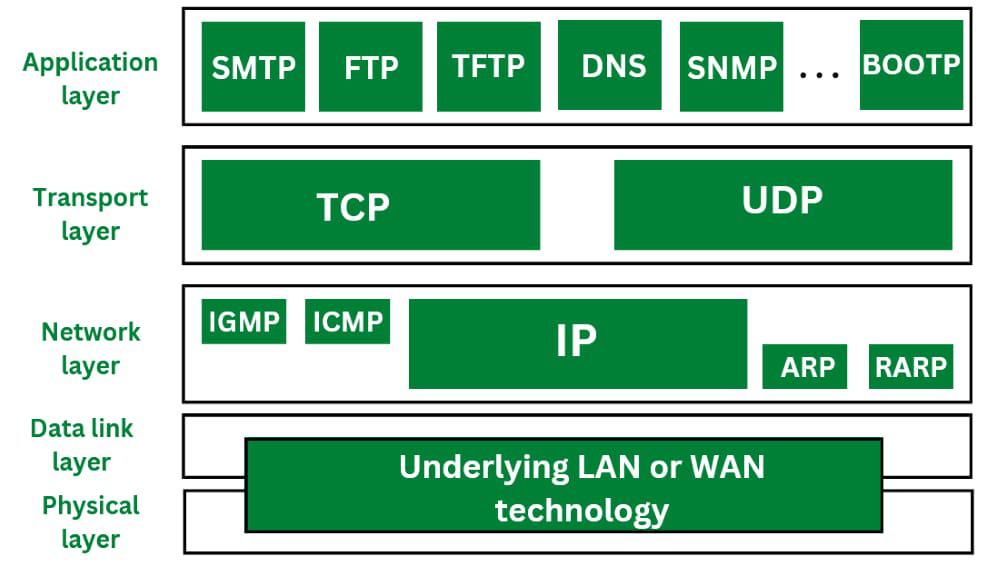
Protocol

* A protocol is a set of rules that governs (manages) data communication.
* Protocols define methods of communication, how to communicate when to communicate etc.
* A protocol is an agreement between the communicating parties on how communication is to proceed.
* Important elements of protocols are

1. Syntax 2. Semantics 3. Timing

Network Protocol:

A network protocol is a set of rules and conventions that govern communication between devices in a network. Examples include TCP/IP, HTTP, FTP, and SMTP. Protocols ensure standardized communication and data exchange.

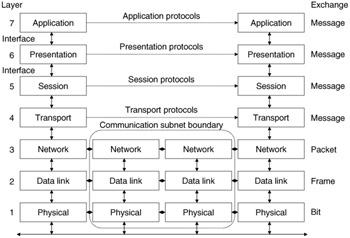


5. Layered Network Architecture:

Networks are often organized into layers, each responsible for specific functions. The OSI (Open Systems Interconnection) model and TCP/IP model are examples of layered architectures.

1. OSI Model:

* OSI model is based on a proposal developed by the International Standards Organization(ISO) as a first step towards international standardization of the protocols used in the various layers.
* It was revised in 1995.
* The model is called the OSI Reference Model because it deals with connecting open systems-that is, systems that are open for communication with other systems.



OSI MODEL

The OSI model consists of seven layers:

1. Physical Layer: Deals with the physical connection between devices.

2. Data Link Layer: Manages data transfer between devices on the same network.

3. Network Layer: Handles routing and forwarding of data packets.

4. Transport Layer: Ensures reliable data delivery.

5. Session Layer: Manages communication sessions.

6. Presentation Layer: Deals with data translation, encryption, and compression.

7. Application Layer: Provides network services directly to applications.

Physical Layer

* The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium.
* It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signal for all of the higher layers. It provides:
* Data Encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in a bit and frame synchronization.
* Transmission Technique: determines whether the encoded bits will be transmitted by baseband(digital) or broadband (analog) signaling.
* Physical medium transmission: transmits bits as electrical or optical signals appropriate for the physical medium.

Data Link Layer

* The data link layer provides error-free transfer of data frames from one-node to another over the link.
* To do this, the data link layer provides:
* Link establishment and transmission: establishes and terminates the logical link between two nodes.
* Frame traffic control: tells the transmitting node to “back-off”(stop) when no frame buffers are available.
* Frame sequencing: transmits/receives frames sequentially.
* Frame acknowledgement: provides/ expects frame acknowledgements. Detects and recovers from errors that occur in the physical layer by retransmitting non- acknowledged frames and handling duplicate frame receipt.
* Frame delimiting: creates and recognizes frame boundaries.
* Frame error Checking: checks received frame for integrity.
* Media access management: determines when the node “has the right” to use the physical medium.

Network Layer

* The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, a priority of service, and other factors.
* To do this, the data link layer provides:
* Routing: routes frames among network.
* Subnet traffic control: router (network layer intermediate systems) can instruct a sending station to “throttle back” its frame transmission when the router’s buffer fills up.
* Frame fragmentation: If it determines that a downstream router’s maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and reassembly at the destination station.
* Logical-physical address mapping translates logical addresses or names, into physical addresses.
* Subnet usage accounting: has accounting function to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Transport Layer

* The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves (release) the higher layer protocols from any concern with the transfer of data between them and their peers.
* The size and complexity of a transport protocol depend on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.
* The transport layer provides:
* Message segmentation: accepts message from the (session) layer above it, splits the message into smaller units(if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
* Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
* Message traffic control: tells the transmitting station to “back off” when no message buffers are available.
* Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.
* The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries.
* In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

Session Layer

* The session layer allows session establishment between processes running on different stations.
* It provides:
* Session establishment, maintenance, and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
* Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

Presentation Layer

* The presentation layer formats the data to be presented to the application layer. It can be viewed as a translator to the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.
* The presentation layer provides:
* Character code translation: for example, ASCII to EBCDIC.
* Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
* Data compression reduces the number of bits that need to be transmitted on the network.
* Data encryption: encrypt data for security purposes. For example, password encryption.

Application Layer

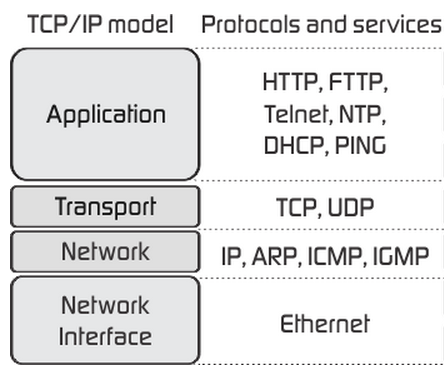
* The application layer serves as the window for users and application processes to access network services.
* This layer contains a variety of commonly needed functions:

1. Resource sharing and device redirection
2. Remote file access.
3. Remote printer access.
4. Inter-process communication
5. Network management
6. Directory Services
7. Electronic messaging(such as mail)
8. Network virtual terminals

7. TCP/IP Protocol Suite:

The TCP/IP model is a conceptual model used for the internet and consists of four layers:

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Link Layer
5. Physical Network



* As we can see from the above figure, the presentation and session layers are not there in the TCP/IP model. Also, note that the Network Access Layer in the TCP/IP model combines the functions of Data link Layer and Physical Layer.

Application Layer

* The application layer is the topmost layer of the four-layer TCP/IP model.
* The application layer is present on the top of the Transport layer.
* Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.
* Application layer includes all the higher-level protocols like DNS (Domain Name System), HTTP(Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File transfer Protocol), SNMP (Simple Network Management Protocol), SMTP(Simple Mail Transfer Protocol), DHCP(Dynamic Host Configuration Protocol), X Windows, RDP(Remote Desktop Protocol) etc.

Transport Layer

* The purpose of the Transport layer is to permit devices on the source and destination hosts to carry on a conversation.
* Transport layer defines the level of service and status of the connection used when transporting data.
* The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer.
* The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
  + - Reliable data delivery
    - Duplicate data suppression
    - Congestion Control
    - Flow Control
* Another transport layer protocol is the User Datagram Protocol (UDP), which provides:
  + - Connectionless
    - Unreliable
    - Best-effort service
* UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

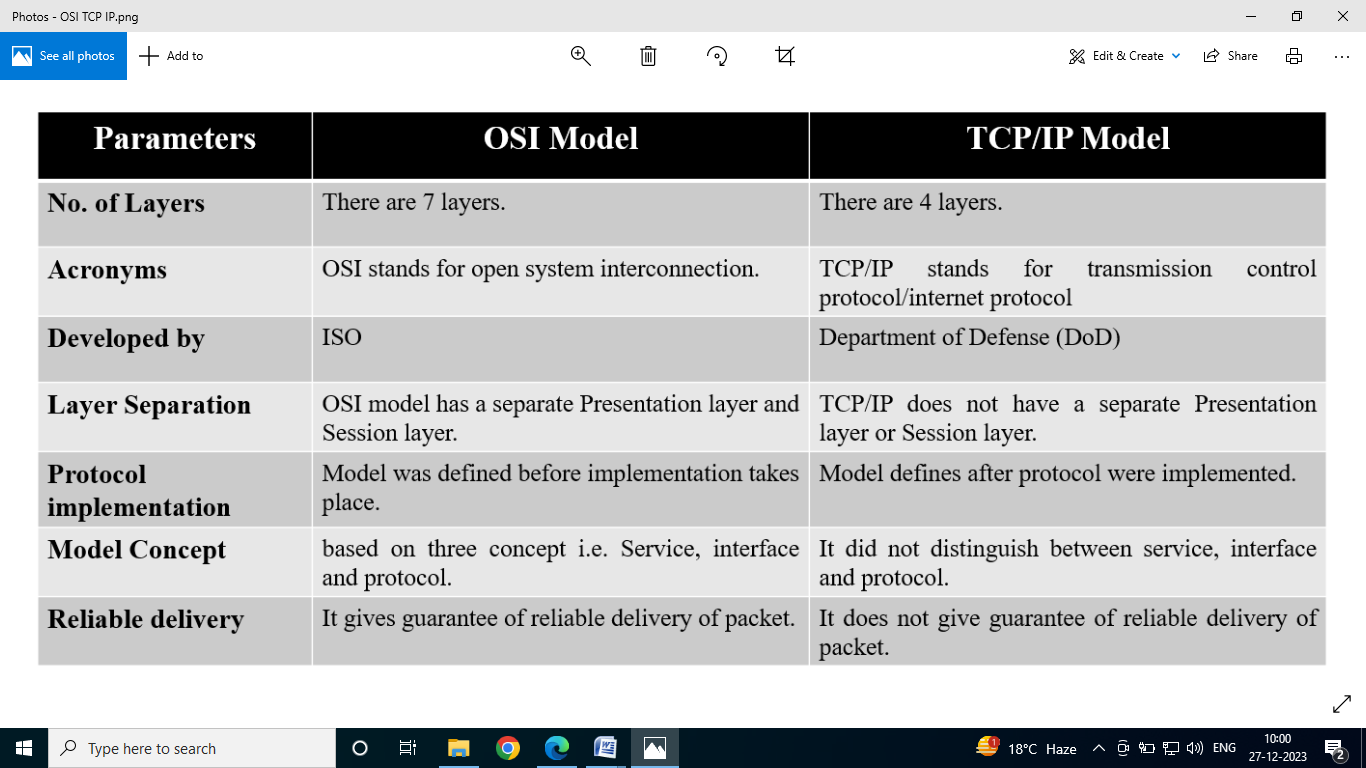
Network layer (Internet layer)

* The internet layer also called the network layer.
* Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.
* The Internet layer is also responsible for the routing of IP datagrams.
* Internet Protocol (IP) is the most important protocols in this layer.
* It is connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control or error recovery.
* IP provides a routing function that attempts to deliver transmitted messages to their destination.
* These messages units in an IP network are called as IP datagrams.
* Example: IP, ICMP, IGMP, ARP and RARP.

Network Interface Layer (Network Access Layer)

* It defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.
* The protocols included in Network Access layer are Ethernet, Token Ring, FDDI, X.25, frame Relay etc.

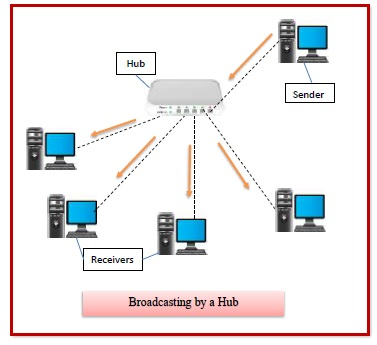
Difference between TCP/IP PROTOCOL STACK AND OSI Model-



8. Networking Devices:

Hub:

* Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.
* A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.



Features of Hubs

* A hub operates in the physical layer of the OSI model.
* A hub cannot filter data. It is a non-intelligent network device that sends message to all ports.
* It primarily broadcasts messages. So, the collision domain of all nodes connected through the hub stays one.
* Transmission mode is half duplex.
* Collisions may occurs during setup of transmission when more than one computers place data simultaneously in the corresponding ports.
* Since they lack intelligence to compute best path for transmission of data packets, inefficiencies and wastage occur.
* They are passive devices, they don’t have any software associated with it.
* They generally have fewer ports of 4/12.

Switch (Managed and Unmanaged): Forwards data to specific devices based on MAC addresses, reducing network congestion.

* The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segment is responsible for filtering and forwarding the packets between LAN segments based on [MAC address](about:blank).
* Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices. Different types of communication are supported here like unicast, multicast, and broadcast communication.

Features of Network Switches

* It operates in Data Link Layer in [OSI Model](about:blank).
* It performs error checking before forwarding data.
* It transfers the data only to the device that has been addressed.
* It operates in full duplex mode.
* It allocates each [LAN](about:blank) segment a limited bandwidth.
* It uses Unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) transmission modes.
* Packet Switching techniques are used to transfer data packets from source to destination.
* Switches have a more significant number of ports.

Router: Connects different networks, directing data between them based on IP addresses.

Routers are networking devices operating at layer 3 or a [network layer](about:blank) of the [OSI model](about:blank). They are responsible for receiving, analysing, and forwarding data packets among the connected [computer networks](about:blank). When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

* A router is a layer 3 or network layer device.
* It connects different networks together and sends data packets from one network to another.
* A router can be used both in LANs ([Local Area Networks](about:blank)) and WANs ([Wide Area Networks](about:blank)).
* It transfers data in the form of [IP packets](about:blank). In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
* Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
* In order to prepare or refresh the routing table, routers share information among each other.
* Routers provide protection against broadcast storms.
* Routers are more expensive than other networking devices like hubs, bridges, and switches.
* Routers are manufactured by some popular companies like −

Cisco

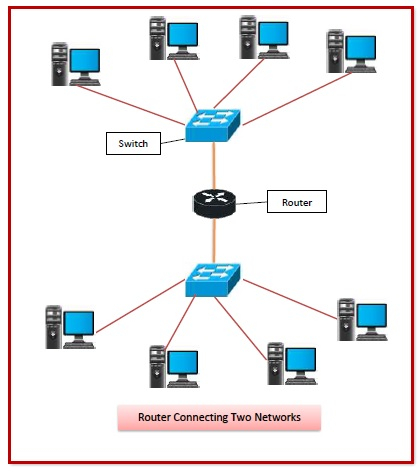
D-Link

HP

3Com

Juniper

Nortel



These elements form the fundamental building blocks of computer networks, facilitating communication and data exchange among devices in various configurations and sizes.