Dr. MGR GOVT. ARTS AND SCIENCE COLLEGE FOR WOMEN.,

VILLUPURAM - 605602

STUDY METERIALS

DATA COMMUNICATION & NETWORK

B.Sc., Computer Science

(III YEAR – V SEM)

Prepared by:

S. MURUGAN

Department of Computer Science
Dr. MGR GOVT. ARTS AND SCIENCE COLLEGE FOR WOMEN.,
VILLUPURAM – 605602.

SYLLABUS

UNIT I

Introductory Concepts - Network hardware - Network software – Network Architecture - Physical layer - Guided transmission media - Cable television.

UNIT II

Data Link Layer - Design issues - Channel allocation problem - Multiple access protocols - Ethernet - Wireless LAN - 802.11 architecture.

UNIT III

Network Layer: Design issues, Routing Algorithms, Shortest path routing, Flooding, Broadcast & Multicast routing congestion, Control & internetworking.

UNIT IV

Transport Layer - Transport service - Elements of transport protocols - User Datagram Protocol - Transmission Control Protocol.

UNIT V

Application Layer - DNS - Electronic mail - World Wide Web - Multimedia - Network security.

Unit - I

INTRODUCTION TO DATA COMMUNICATIONS:

In Data Communications, ***data*** generally are defined as **information** that is stored in **digital form**. *Data communications* is the **process of transferring digital information** between two or more points (two or more computers). *Information* is defined as the **knowledge** or **intelligence**.

Data communications can be summarized as the transmission, reception, and processing of digital information.

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

The effectiveness of a data communications system depends on four fundamental characteristics: **delivery, accuracy, timeliness, and jitter**.

A data communications system has five components:

1. **Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. **Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. **Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. **Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. **Protocol**: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

Standards Organizations for Data Communications

An association of organizations, governments, manufacturers and users form the standards organizations and are responsible for developing, coordinating and maintaining the standards. The intent is that all data communications equipment manufacturers and users comply with these standards.

The primary standards organizations for data communication are:

1. International Standard Organization (ISO)
2. International Telecommunications Union-Telecommunication Sector (ITU-T)
3. Institute of Electrical and Electronics Engineers (IEEE)
4. American National Standards Institute (ANSI)
5. Electronics Industry Association (EIA)
6. Telecommunications Industry Association (TIA)
7. Internet Architecture Board (IAB)
8. Internet Engineering Task Force (IETF)
9. Internet Research Task Force (IRTF)

DATA COMMUNICATIONS NETWORKS:

Any group of computers connected together can be called a ***data communications network***, *and* the process of sharing resources between computers over a data communications network is called ***networking*****.** The most important considerations of a data communications network are *performance, transmission rate, reliability and security.*

Network Components, Functions, and Features

Computer networks all share common devices, functions, and features, including servers, clients, transmission media, shared data, shared printers and other peripherals, hardware and software resources, network interface card (NIC), local operating system (LOS) and the network operating system (NOS).

Servers: Servers are computers that hold shared files, programs and the network operating system. Servers provide access to network resources to all the users of the network and different kinds of servers are present. Examples include file servers, print servers, mail servers, communication servers etc.

Clients: Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive service from the servers.

Shared Data: Shared data are data that file servers provide to clients, such as data files, printer access programs, and e-mail.

Shared Printers and other peripherals: these are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by the clients on the network.

Network interface card: Every computer in the network has a special expansion card called network interface card (NIS), which prepares and sends data, receives data, and controls data flow between the computer and the network. While transmitting, NIC passes frames of data on to the physical layer and on the receiver side, the NIC processes bits received from the physical layer and processes the message based on its contents.

Local operating system: A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, PC-DOS, UNIX, Macintosh, OS/2, Windows 95, 98, XP and Linux.

Network operating system: the NOS are a program that runs on computers and servers that allows the computers to communicate over a network. The NOS provides services to clients such as log-in features, password authentication, printer access, network administration functions and data file sharing.

LAYERED NETWORK ARCHITECTURE

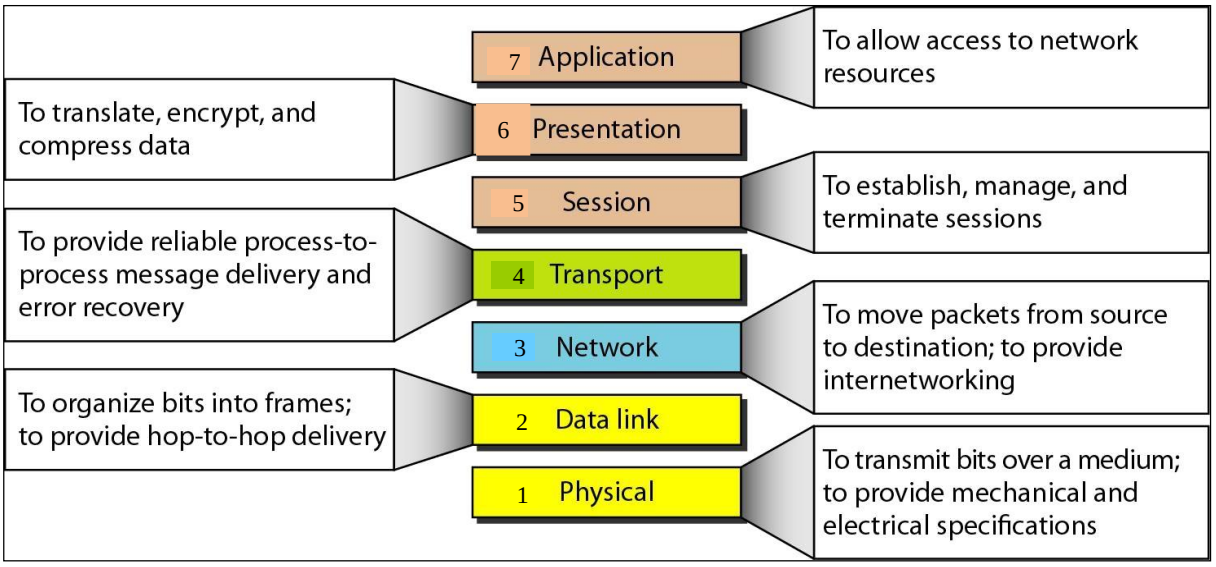
To reduce the design complexity, most of the networks are organized as a series of layers or **levels**, each one build upon one below it. The basic idea of a layered architecture is to *divide the design into small pieces*.

The benefits of the layered models are **modularity** and **clear interfaces**, i.e. open architecture and comparability between the different providers' components. The basic elements of a layered model are services, protocols and interfaces. A ***service*** is a set of actions that a layer offers to another (higher) layer. ***Protocol*** is a set of rules that a layer

uses to exchange information with a peer entity. The messages from one layer to another are sent through those **interfaces**.

Open Systems Interconnection (OSI)

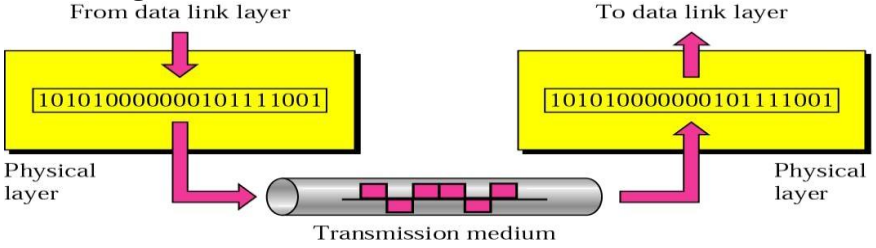
International standard organization (ISO) established a committee in 1977 to develop architecture for computer communication and the OSI model is the result of this effort. **In 1984**, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture. The term —*open*‖ denotes the ability to connect any two systems which conform to the reference model and associated standards. The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network. The OSI reference model divides the problem of moving information between computers over a network medium into **SEVEN** smaller and more manageable problems. The seven layers are:



The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network. The upper three layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications. Data is encapsulated with the necessary protocol information as it moves down the layers before network transit.

1.* Physical Layer** {the physical layer is responsible for transmitting individual bits from one node to the next***}

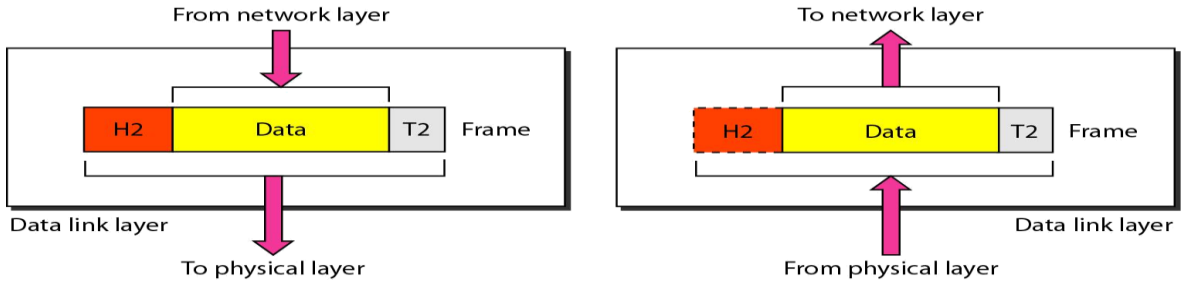
The physical layer is the lowest layer of the OSI hierarchy and coordinates the functions required to transmit a bit stream over a physical medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission occur. The physical layer specifies the type of transmission medium and the transmission mode (simplex, half duplex or full duplex) and the physical, electrical, functional and procedural standards for accessing data communication networks.



Transmission media defined by the physical layer include metallic cable, optical fiber cable or wireless radio-wave propagation. The physical layer also includes the *carrier system* used

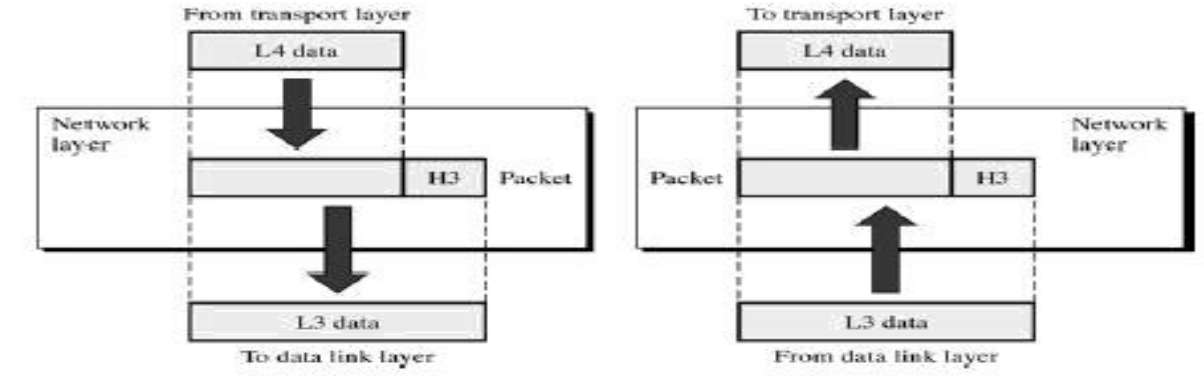
to propagate the data signals between points in the network. The carrier systems are simply communication systems that carry data through a system using either metallic or optical fiber cables or wireless arrangements such as microwave, satellites and cellular radio systems.

2.* Data-link Layer** {the data link layer is responsible for transmitting frames from one node to the next***}
The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery. It makes the physical layer appear error free to the upper layer (network layer).



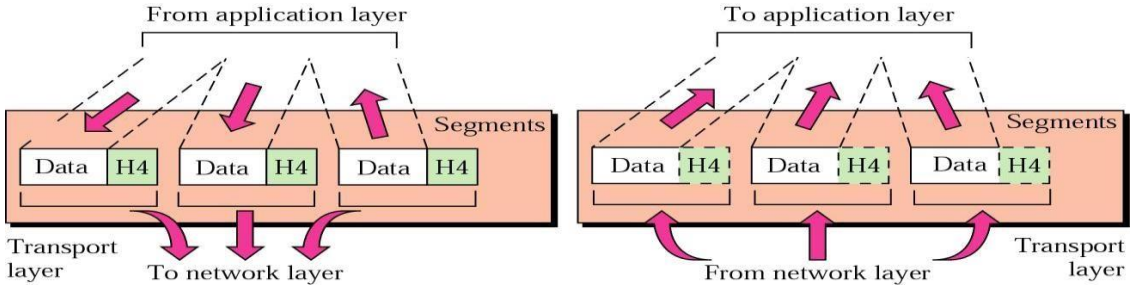
The data link layer packages data from the physical layer into groups called blocks, frames or packets. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender (source address) and/or receiver (destination address) of the frame. The data-link layer provides flow-control, access-control, and error-control.

3. Network Layer {**is responsible for the delivery of individual packets from the source host to the destination host**}
The network layer provides details that enable data to be routed between devices in an environment using multiple networks, subnetworks or both. This is responsible for addressing messages and data so they are sent to the correct destination, and for translating logical addresses and names (like a machine name FLAME) into physical addresses. This layer is also responsible for finding a path through the network to the destination computer.



The network layer provides the upper layers of the hierarchy with independence from the data transmission and switching technologies used to interconnect systems. Networking components that operate at the network layer include routers and their software.

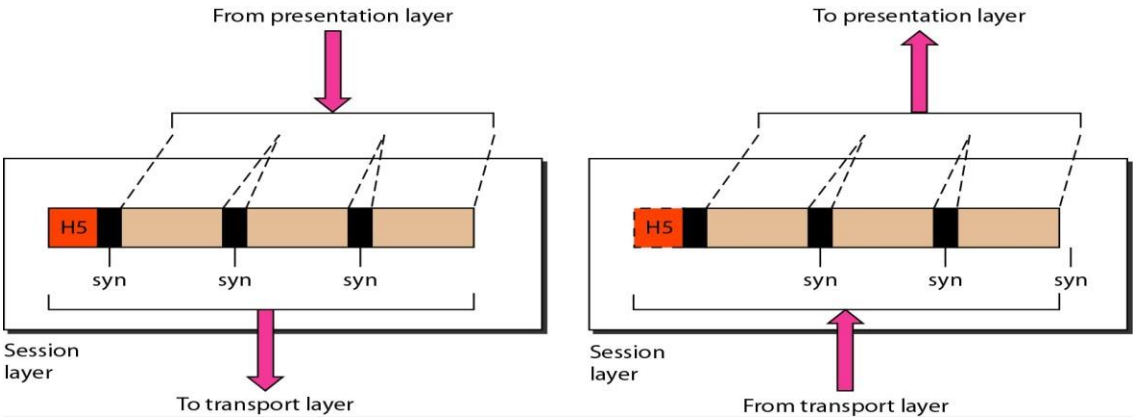
4.* Transport Layer** {is responsible for delivery of a message from one process to another***}
The transport layer controls and ensures the end-to-end integrity of the data message propagated through the network between two devices, providing the reliable, transparent transfer of data between two endpoints.



Transport layer responsibilities include message routing, segmenting, error recovery and two types of basic services to an upper-layer protocol: connection oriented and connectionless. The transport layer is the highest layer in the OSI hierarchy in terms of communicatons and may provide data tracking, connection flow control, sequencing of data, error checking, and application addressing and identification.

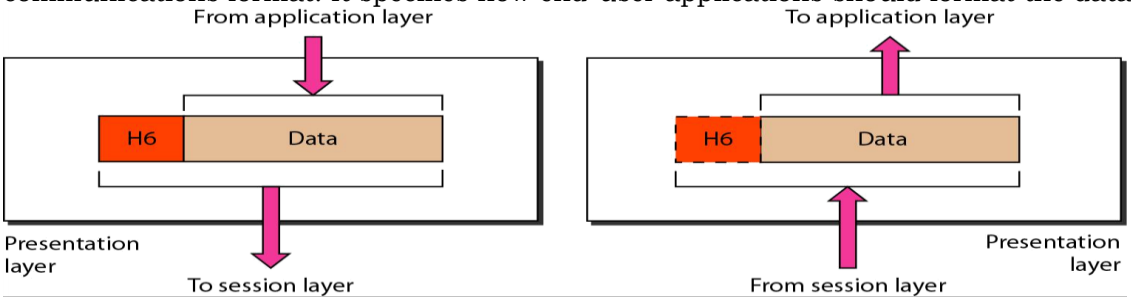
5. **Session Layer** {**responsible for dialog control and synchronization**}

Session layer, some times called the dialog controller provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.



Session layer protocols provide the logical connection entities at the application layer. These applications include file transfer protocols and sending email. Session responsibilities include network log-on and log-off procedures and user authentication. Session layer characteristics include virtual connections between applications, entities, synchronization of data flow for recovery purposes, creation of dialogue units and activity units, connection parameter negotiation, and partitioning services into functional groups.

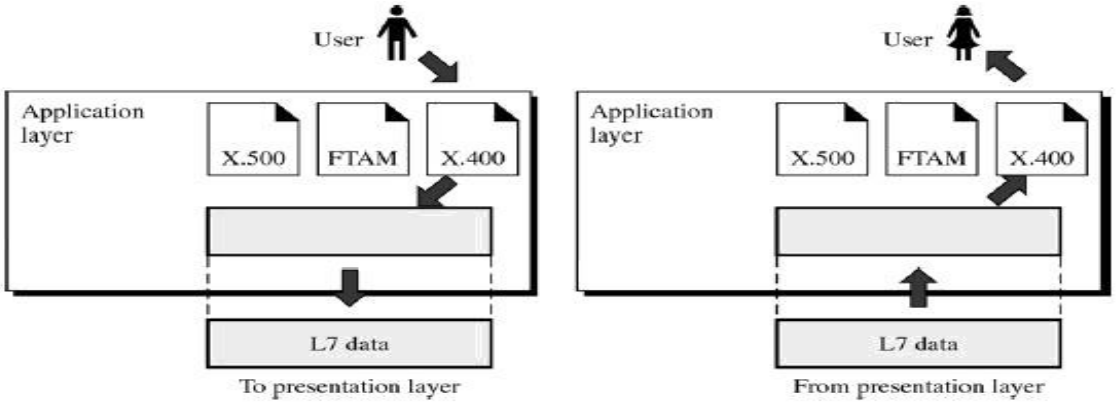
6. **Presentation Layer** {**responsible for translation, compression, and encryption**}
The presentation layer provides independence to the application processes by addressing any code or syntax conversion necessary to present the data to the network in a common communications format. It specifies how end-user applications should format the data.



The presentation layer translated between different data formats and protocols. Presentation functions include data file formatting, encoding, encryption and decryption of

data messages, dialogue procedures, data compression algorithms, synchronization, interruption, and termination.

7. **Application Layer** {**responsible for providing services to the user**}
The application layer is the highest layer in the hierarchy and is analogous to the general manager of the network by providing access to the OSI environment. The applications layer provides distributed information services and controls the sequence of activities within and application and also the sequence of events between the computer application and the user of another application.

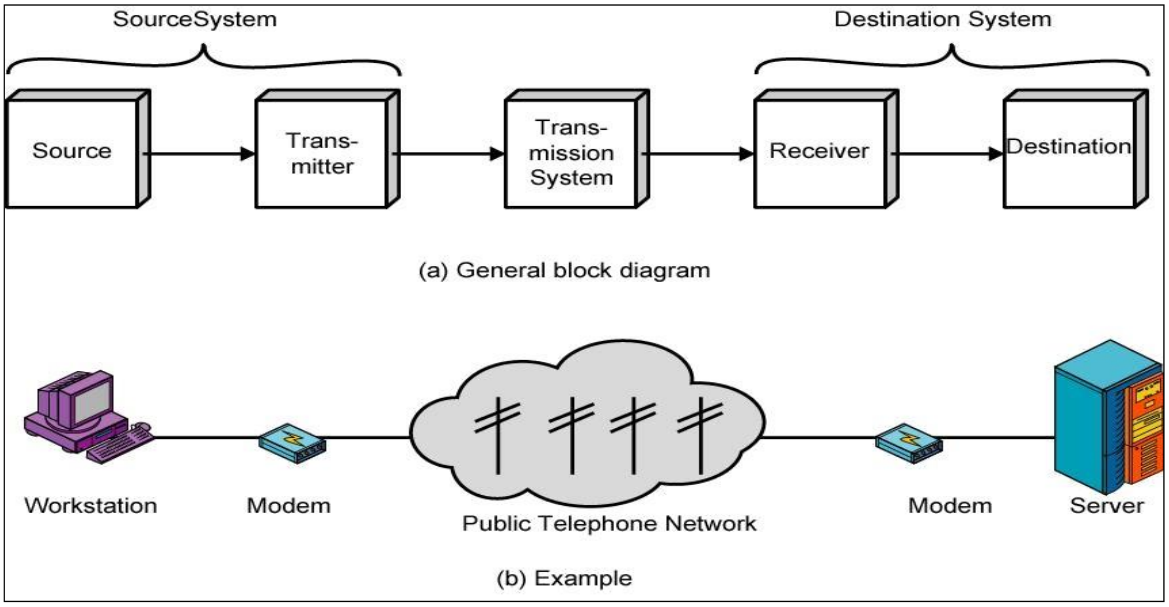


The application layer communicates directly with the user's application program. User application processes require application layer service elements to access the networking environment. The service elements are of two types: CASEs *(common application service elements)* satisfying particular needs of application processes like association control, concurrence and recovery. The second type is SASE (*specific application service elements) which* include TCP/IP stack, FTP, SNMP, Telnet and SMTP.

Data Communication Circuits/Diagram

The main purpose of a digital communications circuit is to provide a transmission path between locations and to transfer digital information from one station (node, where computers or other digital equipment are located) to another using electronic circuits. Communication facilities are physical means of interconnecting stations and are provided to data communications users through public telephone networks (PTN), public data networks (PDN.

The following figure shows a simple two-station data communications circuit/diagram.



The main components are:

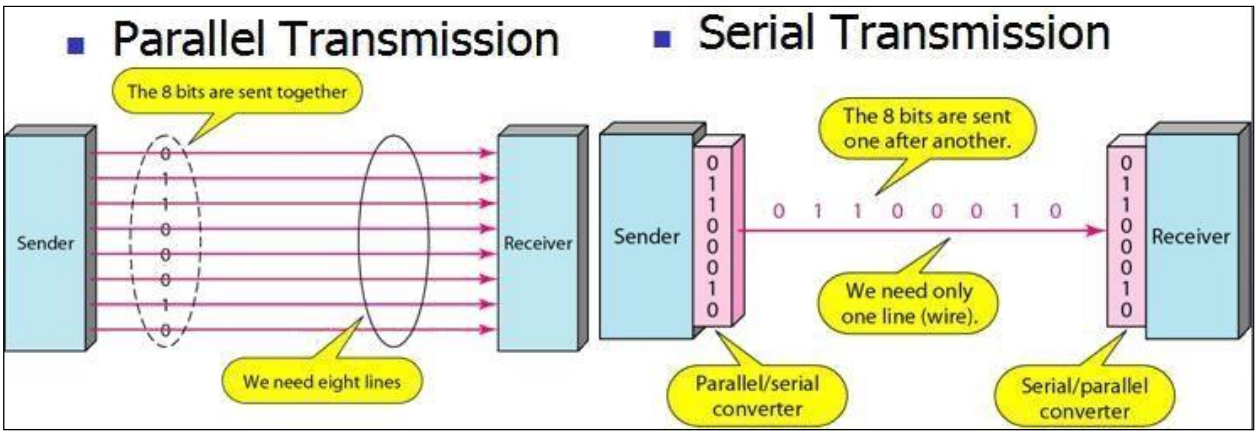
Source: - This device generates the data to be transmitted; examples are mainframe computer, personal computer, workstation etc. The source equipment provides a means for humans to enter data into system.
Transmitter: - A transmitter transforms and encodes the information in such a way as to produce electromagnetic signals that can be transmitted across some sort of transmission system. For example, a modem takes a digital bit stream from an attached device such as a personal computer and transforms that bit stream into an analog signal that can be handled by the telephone network.
Transmission medium: - The transmission medium carries the encoded signals from the transmitter to the receiver. Different types of transmission media include free-space radio transmission (i.e. all forms of wireless transmission) and physical facilities such as metallic and optical fiber cables.
Receiver: - The receiver accepts the signal from the transmission medium and converts it into a form that can be handled by the destination device. For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.
Destination: - Takes the incoming data from the receiver and can be any kind of digital equipment like the source.

SERIAL AND PARALLEL DATA TRANSMISSION:

There are two methods of transmitting digital data namely:

- ✓ Parallel Data Transmission
- ✓ Serial Data Transmission

Parallel Data Transmission: In parallel data transmission, all bits of the binary data are transmitted simultaneously. For example, to transmit an 8-bit binary number in parallel from one unit to another, eight transmission lines are required. Each bit requires its own separate data path. All bits of a word are transmitted at the same time. This method of transmission can move a significant amount of data in a given period of time. Its disadvantage is the large number of interconnecting cables between the two units. For large binary words, cabling becomes complex and expensive. This is particularly true if the distance between the two units is great. Long multi wire cables are not only expensive, but also require special interfacing to minimize noise and distortion problems.



Serial data transmission: is the process of transmitting binary words a bit at a time. Since the bits time-share the transmission medium, only one interconnecting lead is required. While serial data transmission is much simpler and less expensive because of the use of a single interconnecting line, it is a very slow method of data transmission. Serial data transmission is useful in systems where high speed is not a requirement. Parallel

communication is used for short-distance data communications and within a computer, and serial transmission is used for long-distance data communications.

COMPUTER NETWORK ARCHITECTURE

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.
Computer network architectures can be represented with two basic network models:

- ✓ Peer-to-peer network
- ✓ Dedicated client/server network

Peer-to-peer network: Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data. Here, all the computers share their resources, such as hard drives, printers and so on with all the other computers on the network. Each PC acts as both a client (information requestor) and a server (information provider).

Peer-To-Peer network is useful for small environments, usually up to 10 computers.

The advantages of peer-to-peer Network:

- No need for a network administrator
- Network is fast/inexpensive to setup & maintain
- If one computer stops working but, other computers will not stop working.
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, peer-to-peer is perfect for both home and office use.

The Disadvantages of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Dedicated client/server network: Here, one computer is designated as server and the rest of the computers are clients. The designated servers store all the networks shared files and applications programs and function only as servers and are not used as a client or workstation. Client computers can access the servers and have shared files transferred to them over the transmission medium.
Other words, the central controller is known as a server while all other computers in the network are called clients. A server performs all the major operations such as security and network management. A server is responsible for managing all the resources such as files, directories, printer, etc.
All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.
Advantages of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.

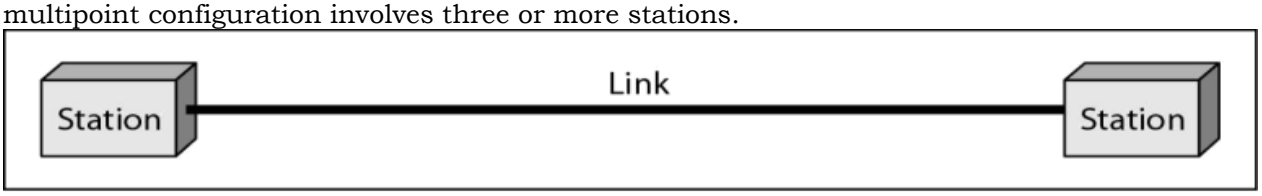
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Data Communication Circuit Arrangements

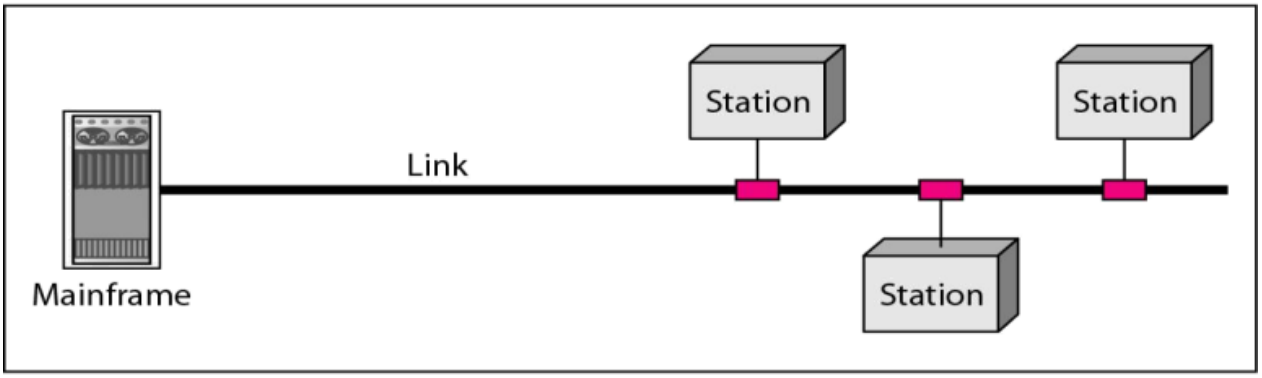
A data communications circuit can be described in terms of circuit configuration and transmission mode.

Circuit Configurations

Data communications networks can be generally categorized as either two points or multipoint. A *two-point* configuration involves only two locations or stations, whereas a multipoint configuration involves three or more stations.



a. Point-to-point

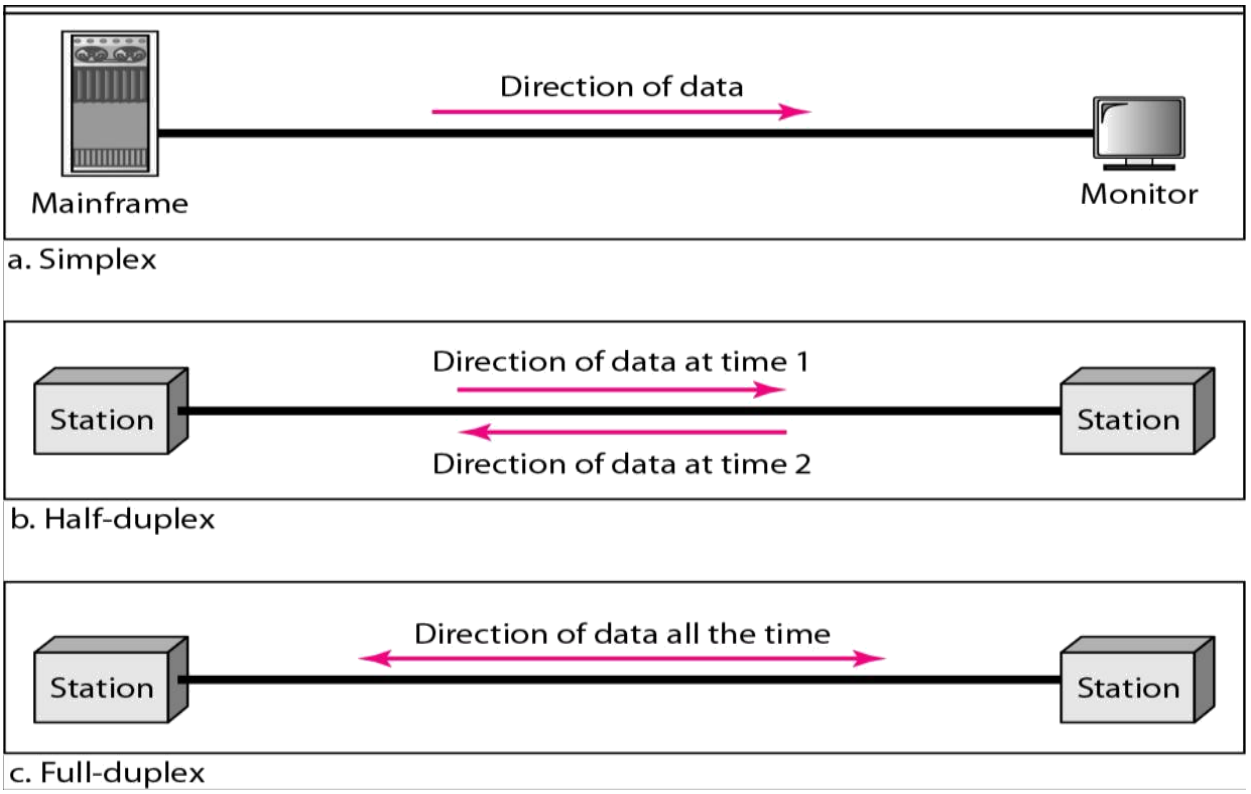


b. Multipoint

A two-point circuit involves the transfer of digital information between a mainframe computer and a personal computer, two mainframe computers or two data communications networks. A multi-point network is generally used to interconnect a single mainframe computer (host) to many personal computers or to interconnect many personal computers and capacity of the channel is either *spatially shared*: Devices can use the link simultaneously or *Timeshare*: Users take turns.

Transmission Modes

There are four modes of transmission for data communications circuits:



In ***simplex mode(SX),*** the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Commercial radio broadcasting is an example. Simplex lines are also called receive-only, transmit-only or one-way-only lines.

In **half-duplex(HDX) mode**, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction. Citizens band (CB) radio is an example where push to talk (PTT) is to be pressed or depressed while sending and transmitting.

In **full-duplex mode (FDX) (called duplex)**, both stations can transmit and receive simultaneously. One common example of full-duplex communication is the telephone network. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel must be divided between the two directions.

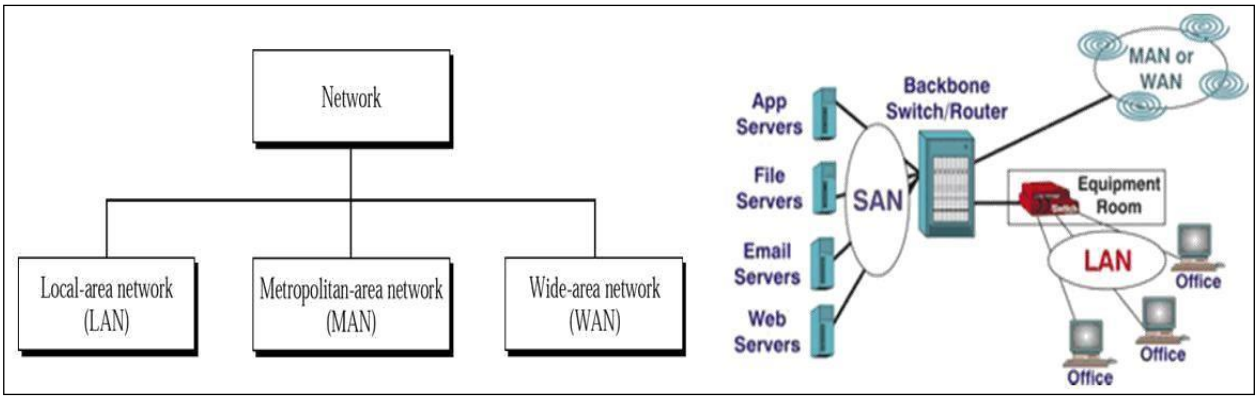
In **full/full duplex (F/FDX) mode**, transmission is possible in both directions at the same time but not between the same two stations (i.e. station 1 transmitting to station 2, while receiving from station 3). F/FDX is possible only on multipoint circuits. Postal system can be given as a person can be sending a letter to one address and receive a letter from another address at the same time.

TYPES OF NETWORKS

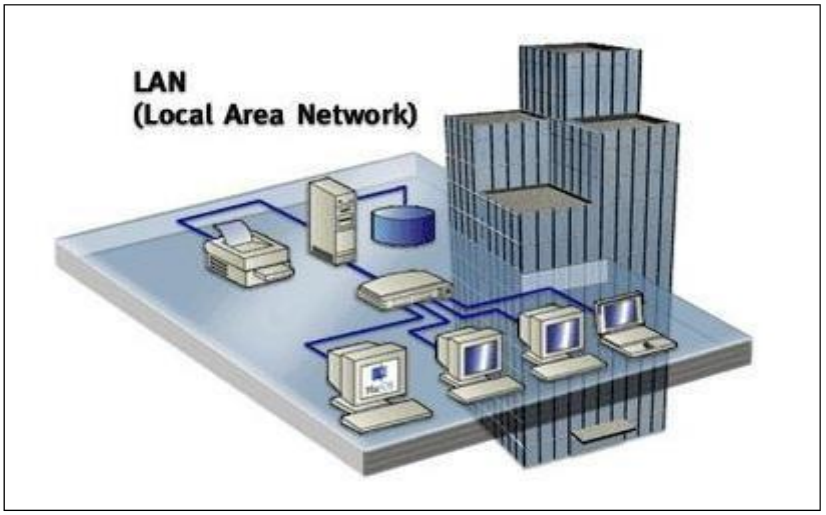
- **LAN – Local Area Network**.
- WLAN – Wireless Local Area Network.
- **WAN – Wide Area Network**.
- **MAN – Metropolitan Area Network**.
- SAN – Storage Area Network, System Area Network, Server Area Network or sometimes Small Area Network.

- CAN – Campus Area Network, Controller Area Network, or sometimes Cluster Area Network.
- PAN – Personal Area Network.
- DAN – Desk Area Network.
- HAN – Home Area Netwok

One way to categorize the different types of computer network designs is by their scope or scale. Common examples of area network types are:



LAN (Local area network): A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. LANs use a network operating system to provide two-way communications at bit rates in the range of 10 Mbps to 100 Mbps. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

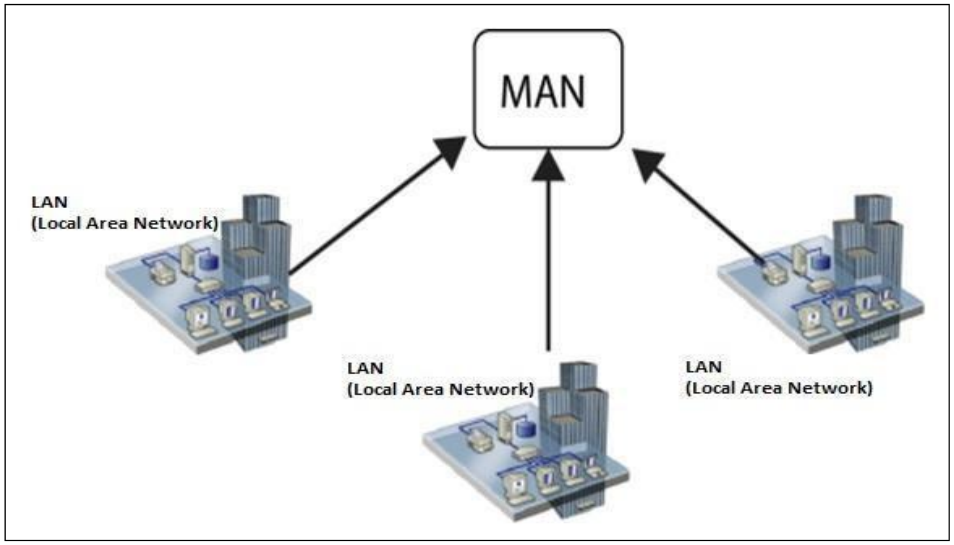


Advantages of LAN:

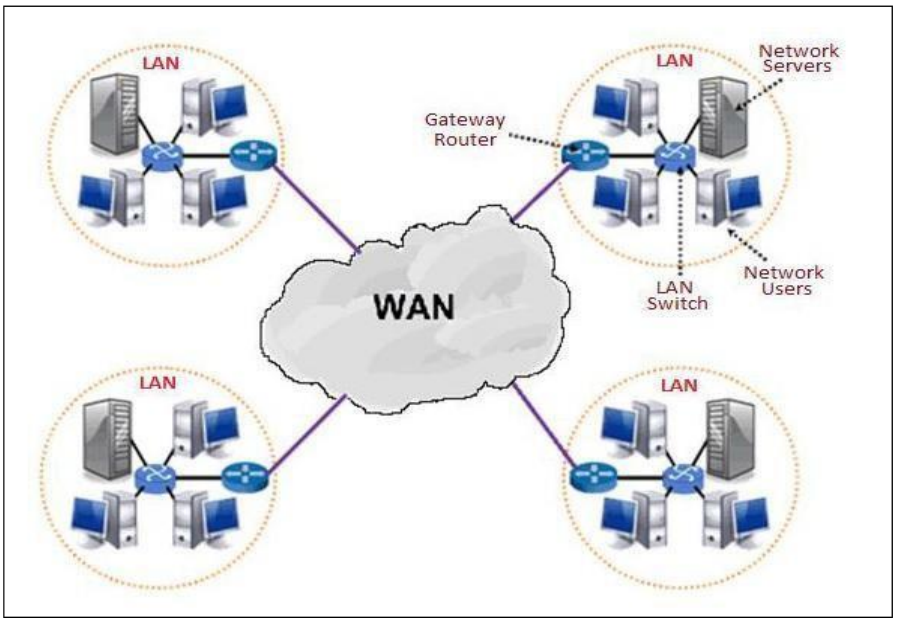
- Share resources efficiently.
- Individual workstation might survive network failure if it doesn‘t rely upon others.
- Component evolution independent of system evolution.
- Support heterogeneous hardware/software Access to other LANs and WANs.
- High transfer rates with low error rates.

MAN (Metropolitan Area Network):

- A data network designed for a town or city



WAN (Wide area network): Wide area networks are the oldest type of data communications network that provide relatively slow-speed, long-distance transmission of data, voice and video information over relatively large and widely dispersed geographical areas, such as country or entire continent. **WANs interconnect routers in different locations**. A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.



Global area network: A GAN provides connections between countries around the entire globe. Internet is a good example and is essentially a network comprised of other networks that interconnect virtually every country in the world. GANs operate from 1.5 Mbps to 100 Gbps and cover thousands of miles.

Campus Area Network: - a network spanning multiple LANs but smaller than a MAN, such as on a university or local business campus.

Storage Area Network: - connects servers to data storage devices through a technology like Fibre Channel.
System Area Network: - Links high-performance computers with high-speed connections in a cluster configuration. Also known as Cluster Area Network.

Building backbone: - It is a network connection that normally carries traffic between departmental LANs within a single company. It consists of a switch or router to provide connectivity to other networks such as campus backbones, enterprise backbones, MANs, WANs etc.

Camus backbone: - **It** is a network connection used to carry traffic to and from LANs located in various buildings on campus. It normally uses optical fiber cables for the transmission media between buildings and operates at relatively high transmission rates.

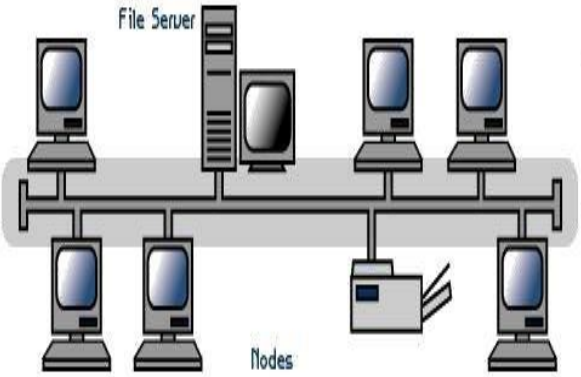
Enterprise networks: - It includes some or all of the above networks and components connected in a cohesive and manageable fashion.

Network Topologies:

In computer networking, *topology* refers to the layout of connected devices, i.e. how the computers, cables, and other components within a data communications network are interconnected, both physically and logically. The physical topology describes how the network is actually laid out, and the logical topology describes how the data actually flow through the network. Two most basic topologies are point-to-point and multipoint. A point-to-point topology usually connects two mainframe computers for high-speed digital information. A multipoint topology connects three or more stations through a single transmission medium and some examples are *star, bus, ring, mesh and hybrid.*

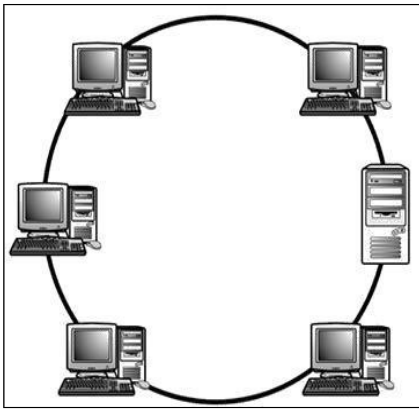
Star topology: A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator. Data on a star network passes through the hub, switch, or concentrator before continuing to its destination. The hub, switch, or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow.

Bus topology: Bus networks use a common backbone to connect all devices. A single cable, (the backbone) functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. The bus topology is the simplest and most common method of interconnecting computers. The two ends of the transmission line never touch to form a complete loop. A bus topology is also known as multidrop or linear bus or a horizontal bus.



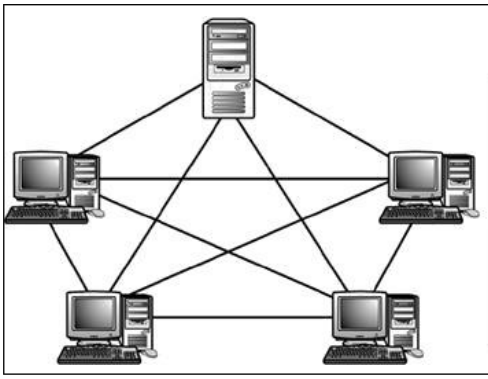
Advantages	Disadvantages
Cheap and easy to implement	Network disruption when computers are added or removed
Require less cable	A break in the cable will prevent all systems from accessing the network.
Does not use any specialized network equipment.	Difficult to troubleshoot.

Ring topology: In a ring network (sometimes called a loop), every device has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counter clockwise"). All the stations are interconnected in tandem (series) to form a closed loop or circle. Transmissions are unidirectional and must propagate through all the stations in the loop. Each computer acts like a repeater and the ring topology is similar to bus or star topologies.



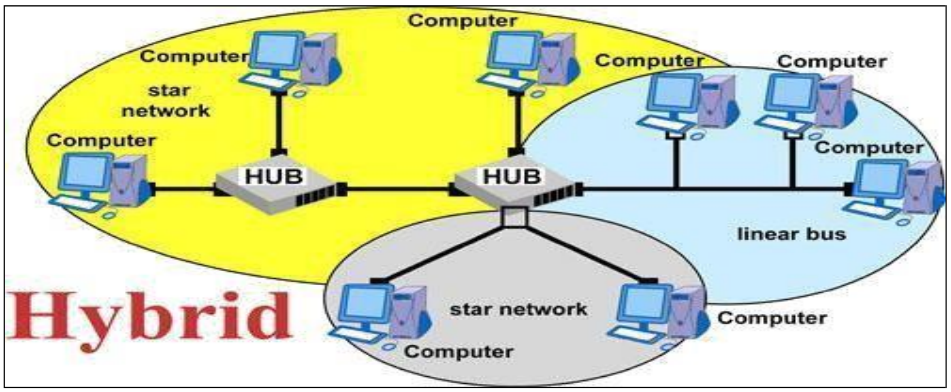
Advantages	Disadvantages
Cable faults are easily located, making troubleshooting easier	Expansion to the network can cause network disruption
Ring networks are moderately easy to install	A single break in the cable can disrupt the entire network.

Mesh topology: The *mesh* topology incorporates a unique network design in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. A mesh network in which every device connects to every other is called a full mesh. A disadvantage is that, a mesh network with *n* nodes must have *n (n-1)/ 2* links and each node must have *n-1* I/O ports (links).



Advantages	Disadvantages
Provides redundant paths between devices	Requires more cable than the other LAN topologies
The network can be expanded without disruption to current uses	Complicated implementation

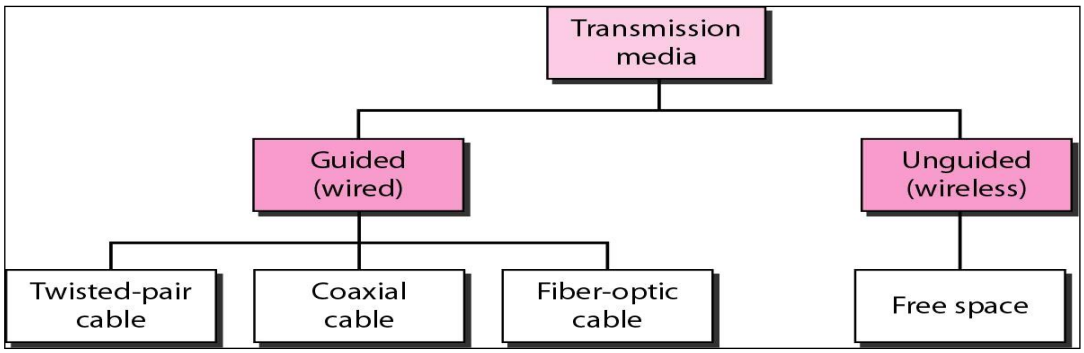
Hybrid topology: This topology (sometimes called mixed topology) is simply combining two or more of the traditional topologies to form a larger, more complex topology. Main aim is being able to share the advantages of different topologies.



Classification of Transmission Media:

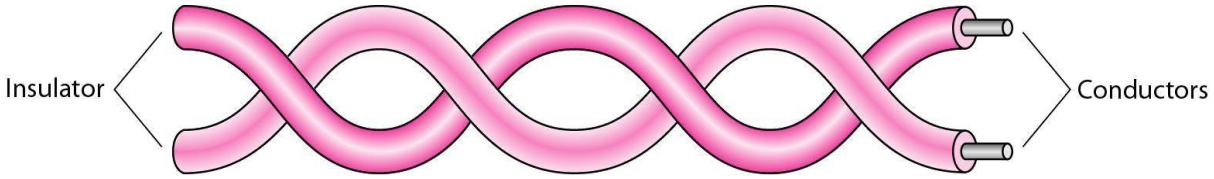
The ***transmission medium*** is the physical path between transmitter and receiver in a data transmission system. It is included in the physical layer of the OSI protocol hierarchy. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

Transmission media can be generally categorized as either *unguided or guided.* Guided Transmission Media uses a "cabling" system (or some sort of conductor) that guides the data signals along a specific path. The data signals are bound by the "cabling" system. Guided Media is also known as Bound Media. The conductor directs the signal propagating down it. Only devices physically connected to the medium can receive signals propagating down a guided transmission medium. Examples of guided transmission media are copper wire and optical fiber.



Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not bound to a cabling media and as such are often called Unbound Media. Unguided transmission media are wireless systems. Signals propagating down an unguided transmission medium are available to anyone who has a device capable of receiving them.

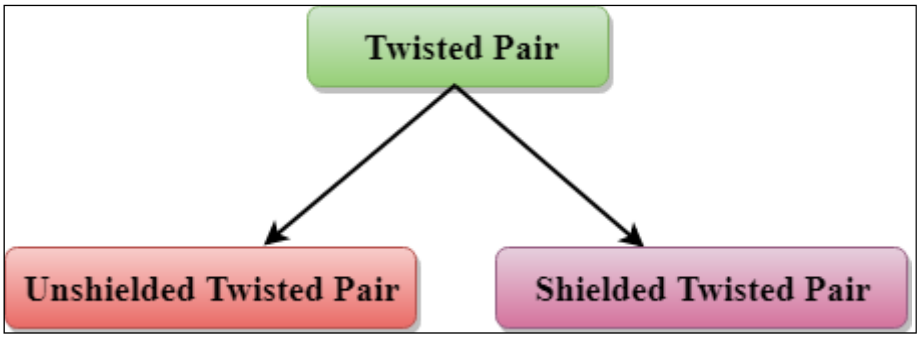
1. **Twisted pair:** Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5 KHz. A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
Twisted-pair wires are the most common media in a telephone network. These wires support both analog and digital signals and can transmit the signal at a speed of 10 Mbps over a short distance. The twisting of wires with different twisting lengths reduces the effect of cross talk and low-frequency interference.



Twisted-pair cable

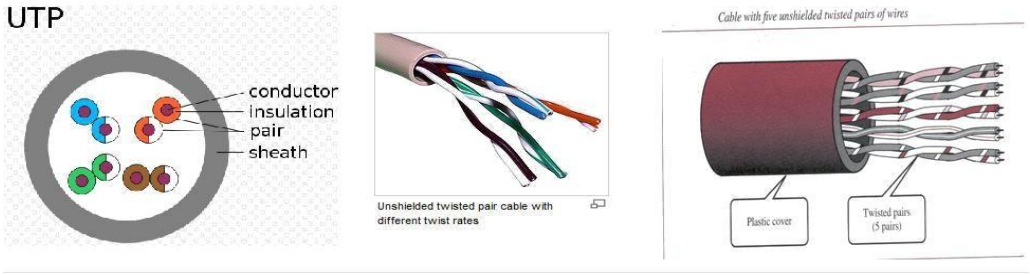
Twisted-pair transmission lines are also the transmission medium of choice for most local area networks because twisted-pair cable is simple to install and relatively independent when compared to coaxial and optical fiber cables.

The two basic types of twisted-pair transmission lines specified are unshielded twisted pair (UTP) and shielded twisted pair (STP).



Unshielded twisted-pair: An UTP cable consists of two copper wires where each wire is seperately encapsulated in PVC (polyvinyl chloride) insulation. An unshielded twisted pair is widely used in telecommunication.

UTPs are cheaper, more flexible, and easier to install. They provide enough support for telephone systems and are not covered by metal insulation. They offer acceptable performance for a long-distance signal transmission, but as they are uninsulated, they are affected by cross talk, atmospheric conditions, electromagnetic interference, and adjacent twisted pairs, as well as by any noise generated nearby. The majorities of the telephone twisted pairs are unshielded and can transmit signals at a speed of 10 Mbps.



The Electronic Industries Association (EIA) has developed standard to grade UTP cable by quality; Category 1 as the lowest quality and category 6 as the highest quality.

1. Category 1: The basic twisted-pair cabling used in telephone systems. This level of quality is fine for voice but inadequate for data transmission.
2. Category 2: This category is suitable for voice and data transmission of up to 2Mbps.
3. Category 3: This category is suitable for data transmission of up to 10 Mbps. It is now the standard cable for most telephone systems. At least three twist per feet
4. Category 4: This category is suitable for data transmission of up to 20 Mbps.
5. Category 5: This category is suitable for data transmission of up to 100 Mbps.
6. Category 6: CAT- 6 is recently proposed cable type comprised of four pairs of wire capable of operating at transmission rates of up to 400Mbps.

Advantages of UTP

- It's easy to terminate.
- Installation costs are less and more lines can be run through the same wiring ducts.

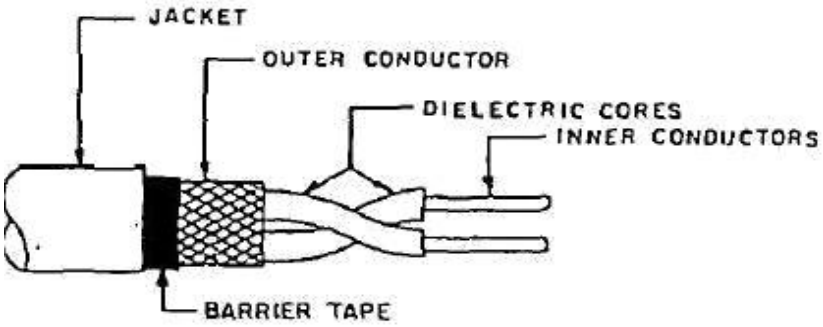
Disadvantages of UTP

UTP are its a bit noisy and prone to interference.

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Table: Categories of unshielded twisted-pair cables

Shielded Twisted Pair (STP) Cable: STP cable is a parallel two-wire transmission line consisting of two copper conductors separated by a solid dielectric material. The wires and dielectric are enclosed in a conductive-metal sleeve called a foil.



The metal casing prevents the penetration of electromagnetic noise. Materials and manufacturing requirements make STP more expensive than UTP but less susceptible to noise.

Characteristics of Shielded Twisted Pair:

•The cost of the shielded twisted pair cable is not very high and not very low.
•An installation of STP is easy.
•It has higher capacity as compared to unshielded twisted pair cable.
•It has a higher attenuation.
•It is shielded that provides the higher data transmission rate.

Coaxial (Concentric) Transmission Lines: Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable. The name of the cable is coaxial as it contains two conductors parallel to each other. It has a higher frequency as compared to twisted pair cable.
The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI** (Electromagnetic interference).

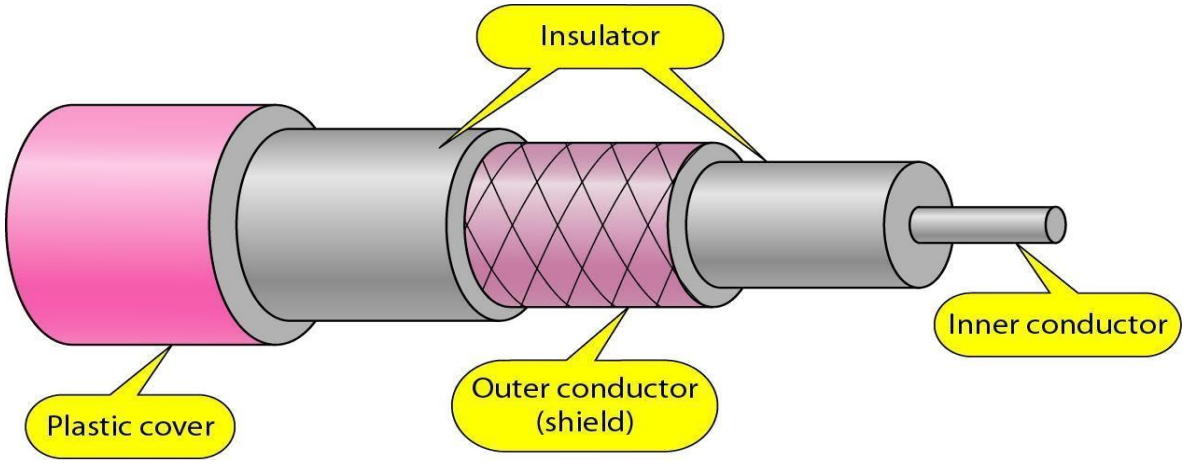


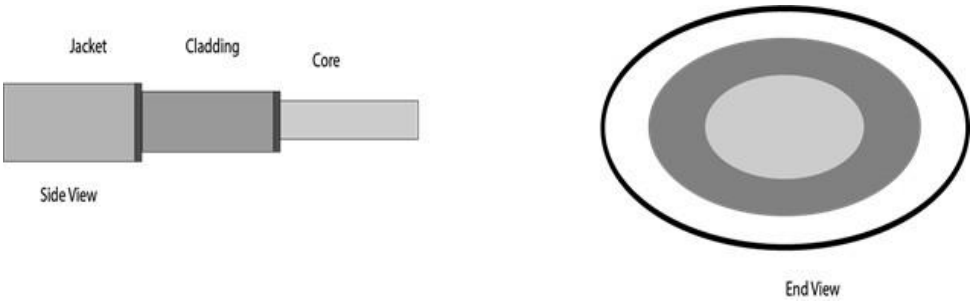
Fig: Coaxial Cables

Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Fiber Optical Cables: An optical communications system is one that uses light as the carrier of information. They use glass or plastic fiber cables to contain the light waves and guide them in a manner similar to the way EM waves are guided through a metallic transmission media.

Fiber Optical cable is a cable that uses electrical signals for communication. Fiber Optical is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light. The plastic coating protects the optical fibers from heat, cold, electromagnetic interference from other types of wiring. Fiber optics provides faster data transmission than copper wires.



Basic

elements of Fiber optic cable:

Core: The optical fiber consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fiber. The more the area of the core, the lighter will be transmitted into the fiber.

Cladding: The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fiber.

Jacket: The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fiber strength, absorb shock and extra fiber protection.

Advantages of Optical Fiber Cables

Wider bandwidth and greater information capacity: The light wave occupies the frequency range between 2×10^{12} Hz to 37×10^{12} Hz. This makes the information carrying capability of fiber optic cables is much higher.

Immunity to crosstalk: Since fiber optic cables use glass and plastic fibers, which are non-conductors of electrical current, no magnetic field is present. No magnetic induction means no crosstalk.

Immunity to static interference: As optical fiber cables are non-conductors, they are immune to electromagnetic interference (EMI) caused by lightning, electric motors, relays, fluorescent lights and other electrical noise sources.

Environmental immunity: Optical fibers are more immune to environmental extremes. They can operate over large temperature variations and are also not affected by corrosive liquids and gases.

Safety and convenience: As only glass and plastic fibers are present, no electrical currents or voltages are associated with them. Also they can be used around any volatile liquids and gasses without worrying about their causing explosions or fires.

Lower transmission loss: Fiber optic cables offers less signal attenuation over long distances. Typically, it is less than 1 dB/km

Security: Optical fibers are more secure as they are almost impossible to tap into because they do not radiate signals. No ground loops exist between optical fibers hence they are more secure.

Durability and reliability: Optical cables last longer and are more reliable than metallic facilities because fiber cables have a higher tolerance to changes in environmental conditions and are immune to corrosive materials.

Economics: Cost of optical fiber cables is same as metallic cables. Fiber cables have less loss and require fewer repeaters, which in turn needs lower installation and overall system costs.

Disadvantages of Optical Fiber Cables

Interfacing costs: As optical cables need to be connected standard electronic facilities requiring expensive interfaces

Strength: Optical cables have lower tensile strength than coaxial cable. They need an extra coating of Kevlar and also a protective jacket of PVC. Glass fiber is also fragile making them less attractive in case of hardware portability is required.

Remote electrical power: Occasionally, electrical power needs to be provided to remote interfaces, which cannot be accomplished using optical cables.

Losses through bending: Bending the cable causes irregularities in the cable dimensions, resulting in loss of signal power. Also, optical cables are prone to manufacture defects causing an excessive loss of signal power.

Specialized tools, equipment and training: Special tools are required to splice and repair cables and special test equipment are needed to make routine measurements. Technicians working on optical cables need special skills and training.

Applications of Communication & Computer Network

- Resource sharing such as printers and storage devices.
- Exchange of information by means of e-Mails and FTP.
- Information sharing by using Web or Internet.
- Interaction with other users using dynamic web pages.
- IP phones.

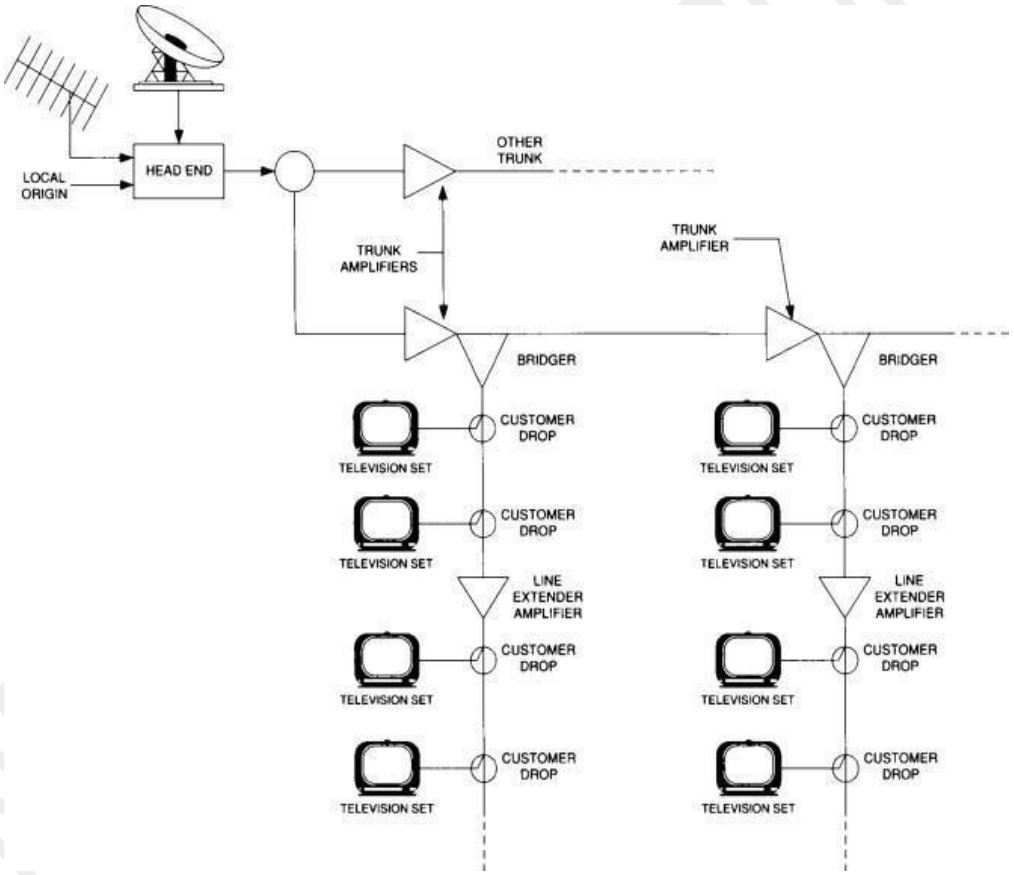
- Videoconferences.s
- Parallel computing.
- Instant messaging.

Cable television:

Cable television is a popular television system that delivers television programming services through cables. This is different from terrestrial television (where radio waves are transmitted over air and received by antennas) and satellite television (where signals are sent by communication satellites and received by satellite dish).

Types of cables used in cable TV

- coaxial cables through which radio-frequency signals are transmitted
- fiber optic cables through which light pulses are sent



Services offered by Cable TV

Originally used for broadcasting television services, the functionalities of cable TV has now been extended for providing different services of computer networks as well. Some of the most predominant services of cable TV are −

- Standard television services
- FM programming
- Cable Internet
- Telephone

NETWORK HARDWARE

Networking hardware, also known as **network** equipment or computer **networking** devices, are electronic devices which are required for communication and interaction between devices on a computer **network**. Specifically, they mediate data transmission in a computer **network**.

Following is the list of hardware's required to set up a computer network.

- Network Cables
- Distributors
- Routers
- Internal Network Cards
- External Network Cards

Network Cables

Network cables are used to connect computers. The most commonly used cable is Category 5 cable RJ-45.

Distributors

A computer can be connected to another one via a serial port but if we need to connect many computers to produce a network, this serial connection will not work.

The solution is to use a central body to which other computers, printers, scanners, etc. can be connected and then this body will manage or distribute network traffic.

Router

A router is a type of device which acts as the central point among computers and other devices that are a part of the network. It is equipped with holes called ports. Computers and other devices are connected to a router using network cables. Now-a-days router comes in wireless modes using which computers can be connected without any physical cable.

Network Card

Network card is a necessary component of a computer without which a computer cannot be connected over a network. It is also known as the network adapter or Network Interface Card (NIC). Most branded computers have network card pre-installed. Network cards are of two types:

1. Internal Network Cards
2. External Network Cards.

Internal Network Cards

Motherboard has a slot for internal network card where it is to be inserted. Internal network cards are of two types

1. Peripheral Component Interconnect (PCI) connection
2. Industry Standard Architecture (ISA).

Network cables are required to provide network access.

External Network Cards

External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network.

Universal Serial Bus (USB)

USB card is easy to use and connects via USB port. Computers automatically detect USB card and can install the drivers required to support the USB network card automatically.

NETWORK SOFTWARE

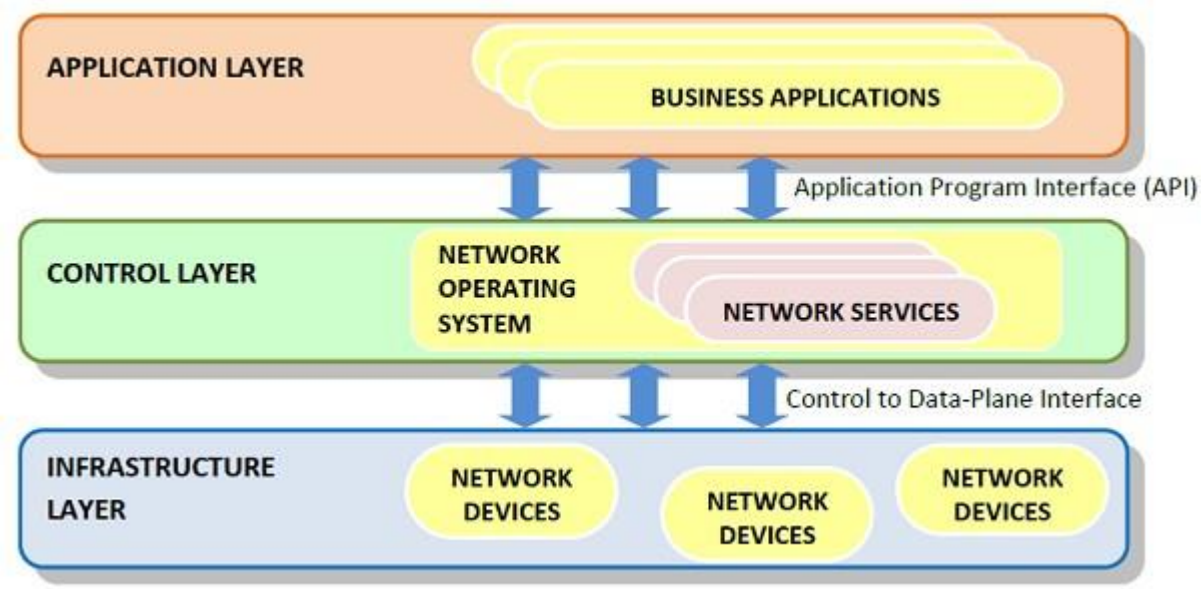
Network software encompasses a broad range of software used for design, implementation, and operation and monitoring of computer networks. Traditional networks were hardware based with software embedded. With the advent of Software – Defined Networking (SDN), software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

Functions of Network Software

- Helps to set up and install computer networks
- Enables users to have access to network resources in a seamless manner
- Allows administrations to add or remove users from the network
- Helps to define locations of data storage and allows users to access that data
- Helps administrators and security system to protect the network from data breaches, unauthorized access and attacks on a network
- Enables network virtualizations

SDN Framework

The Software Defined Networking framework has three layers as depicted in the following diagram −



- **APPLICATION LAYER** − SDN applications reside in the Application Layer. The applications convey their needs for resources and services to the control layer through APIs.
- **CONTROL LAYER** − The Network Control Software, bundled into the Network Operating System, lies in this layer. It provides an abstract view of the underlying network infrastructure. It receives the requirements of the SDN applications and relays them to the network components.
- **INFRASTRUCTURE LAYER** − Also called the Data Plane Layer, this layer contains the actual network components. The network devices reside in this layer that shows their network capabilities through the Control to data-Plane Interface.

UNIT- II

DATA LINK LAYER

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.

Data link layer has two sub-layers:

- ✓ **Logical Link Control:**It deals with protocols, flow-control, and error control
- ✓ **Media Access Control:**It deals with actual control of media

DESIGN ISSUES

The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

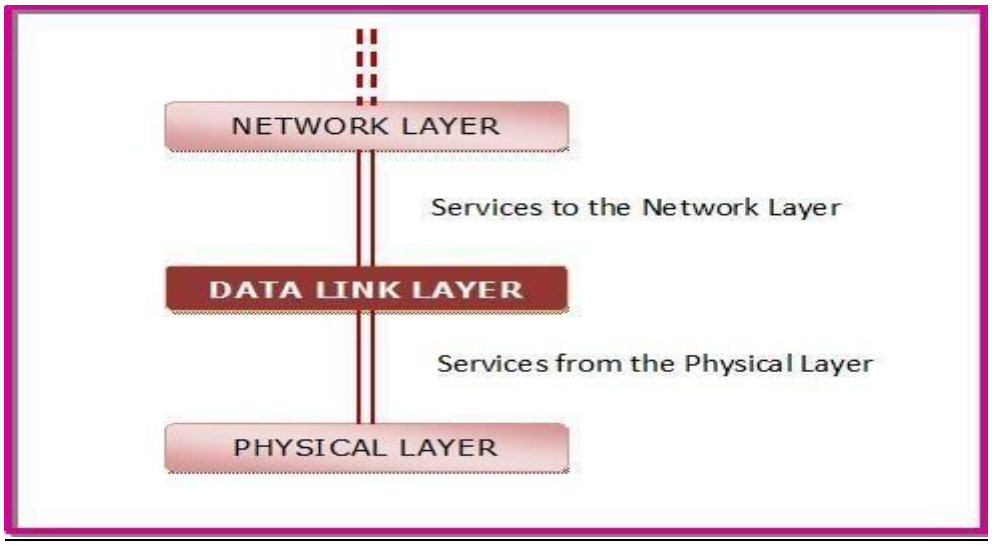
- •Providing services to the network layer
- •Framing
- •Error Control
- •Flow Control

Providing Services to the Network Layer

The data link layer uses the services offered by the physical layer. The primary function of this layer is to provide a well defined service interface to network layer above it.

The types of services provided can be of three types

- •Unacknowledged connectionless service
- •Acknowledged connectionless service
- •Acknowledged connection -oriented service



FLOW CONTROL:

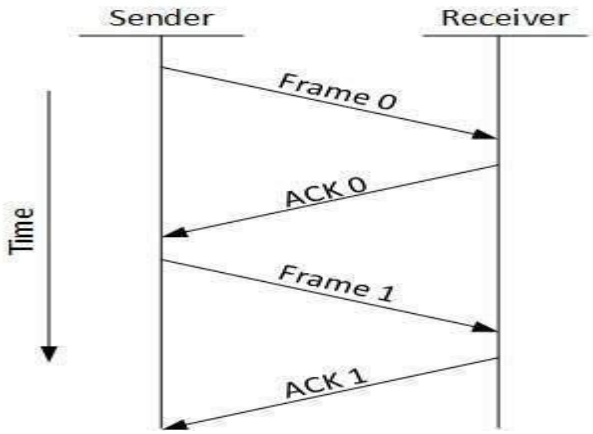
A data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

1. Stop and wait
2. Sliding window

Stop and Wait

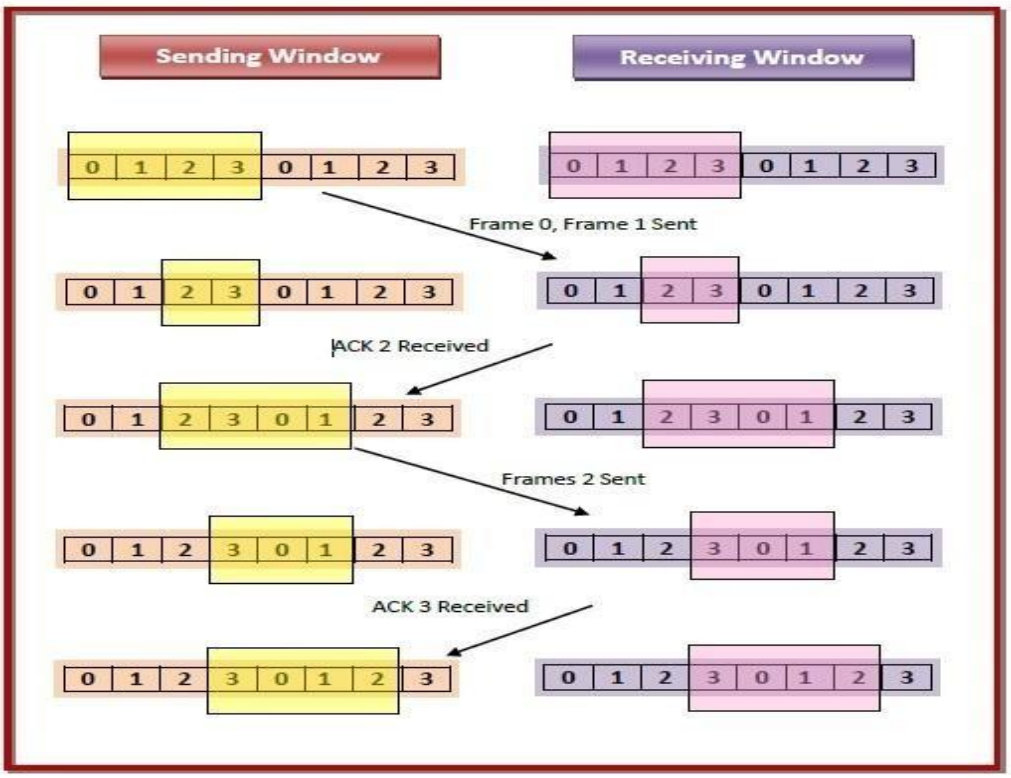
This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



Sliding Window

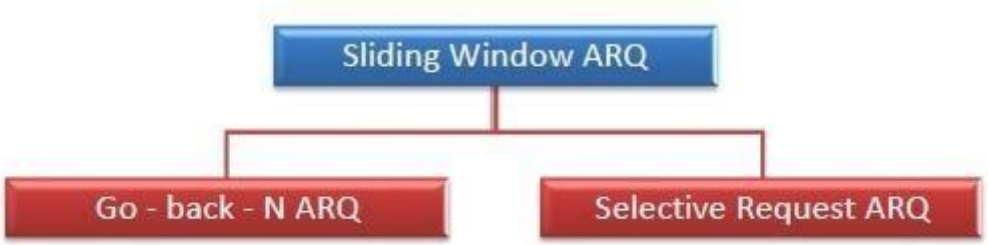
In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.



Types of Sliding Window Protocols

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories −



- **Go – Back – *N* ARQ**

  Go – Back – *N* ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

- **Selective Repeat ARQ**

  This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

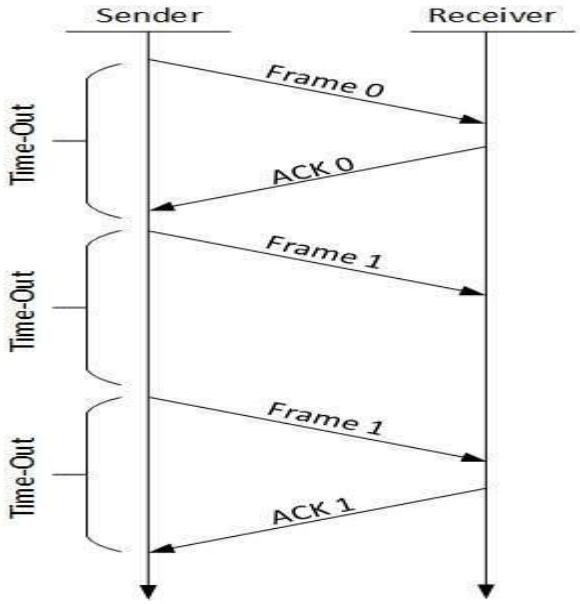
- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it‘s acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

- **Stop-and-wait ARQ**

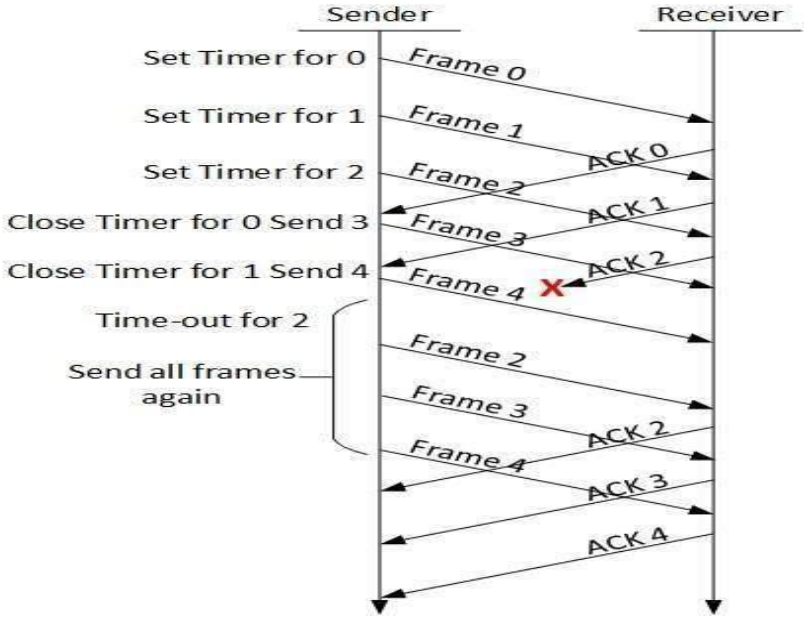
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.



- **Go-Back-N ARQ**

Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

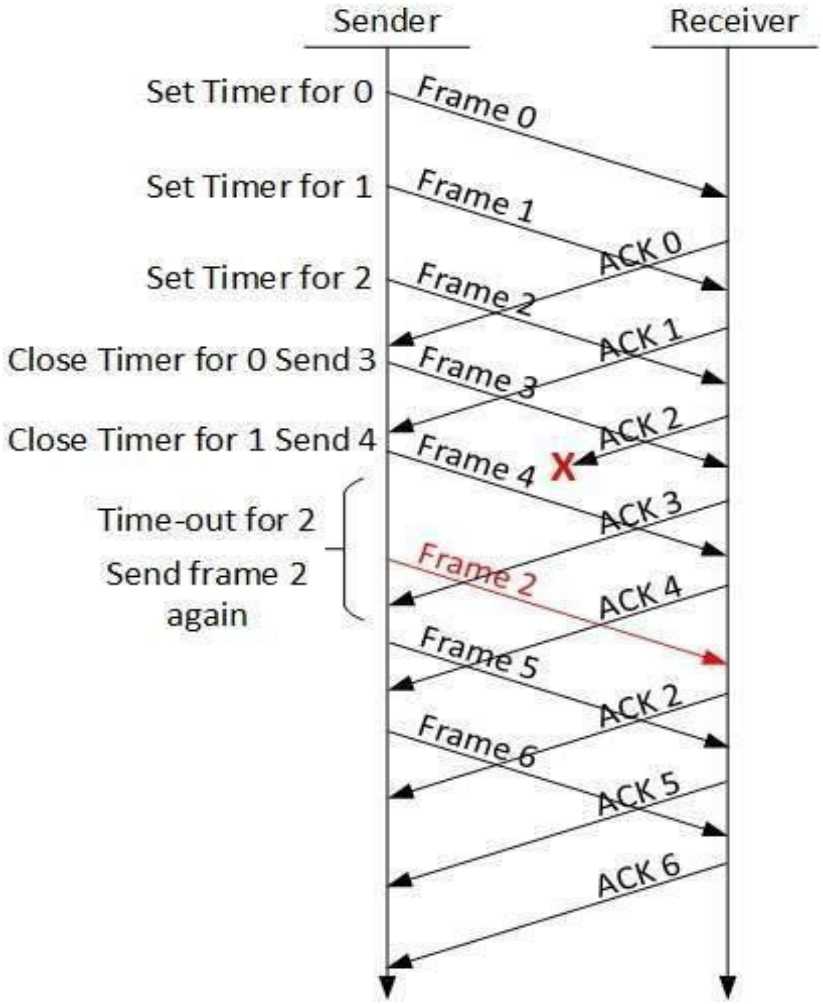


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame‘s sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

- **Selective Repeat ARQ**

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



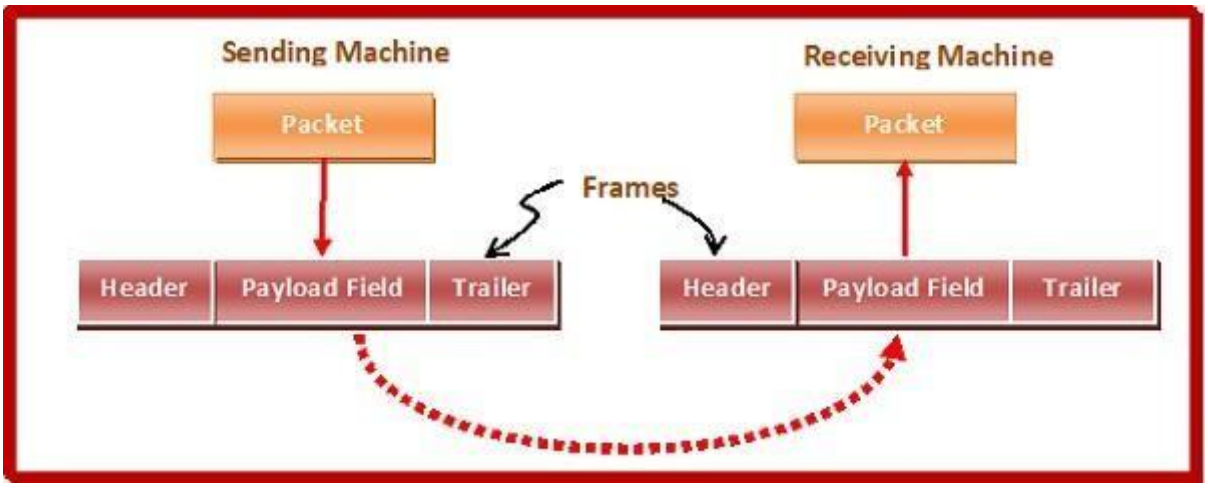
In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

Framing:

Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames makes flow control and error control more efficient.

Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.



Parts of a Frame

A frame has the following parts −

- Frame Header − It contains the source and the destination addresses of the frame.
- Payload field − It contains the message to be delivered.
- Trailer − It contains the error detection and error correction bits.
- Flag − It marks the beginning and end of the frame.

Types of Framing

Framing can be of two types, fixed sized framing and variable sized framing.

Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example − ATM cells.

Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.
Two ways to define frame delimiters in variable sized framing are −

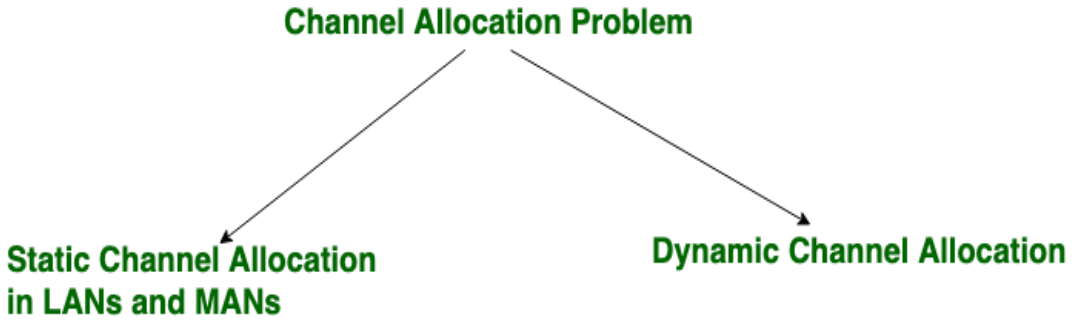
- **Length Field** − Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).
- **End Delimiter** − Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situation −
    - **Byte – Stuffing** − A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.
    - **Bit – Stuffing** − A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

Channel Allocation Problem

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes:

1. Static Channel Allocation in LANs and MANs,
2. Dynamic Channel Allocation.



1. **Static Channel Allocation in LANs and MANs:**

It is the classical or traditional approach of allocating a single channel among multiple competing users Frequency Division Multiplexing (FDM). if there are N users, the bandwidth is divided into N equal sized portions each user being assigned one portion. since each user has a private frequency band, there is no interface between users.

It is not efficient to divide into fixed number of chunks.

T = 1/(U*C-L)
T(FDM) = N*T(1/U(C/N)-L/N)
Where,

T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time

Advantages

Static channel allocation scheme is particularly suitable for situations where there are a small number of fixed users having a steady flow of uniform network traffic. The allocation technique is simple and so the additional overhead of a complex algorithm need not be incurred. Besides, there is no interference between the users since each user is assigned a fixed channel which is not shared with others.

Disadvantages

Most real-life network situations have a variable number of users, usually large in number with bursty traffic. If the value of N is very large, the bandwidth available for each user will be very less. This will reduce the throughput if the user needs to send a large volume of data once in a while.

It is very unlikely that all the users will be communicating all the time. However, since all of them are allocated fixed bandwidths, the bandwidth allocated to non-communicating users lies wasted.

If the number of users is more than N, then some of them will be denied service, even if there are unused frequencies.

2. Dynamic Channel Allocation:

In dynamic channel allocation schemes, frequency channels are not permanently allotted to any user. Channels are assigned to the user as needed depending upon the network environment. The available channels are kept in a queue or a spool. The allocation of the channels is temporary. Distribution of the channels to the contending users is based upon distribution of the users in the network and offered traffic load. The allocation is done so that transmission interference is minimized.

Dynamic Channel Allocation Schemes

The dynamic channel allocation schemes can be divided into three categories −

- Interference Adaptive Dynamic Channel Allocation (IA-DCA)
- Location Adaptive Dynamic Channel Allocation (LA-DCA)
- Traffic Adaptive Dynamic Channel Allocation (TA-DCA)

All these schemes evaluate the cost of using each available channel and allocates the channel with the optimum cost.

Advantages

Dynamic channel allocation schemes allots channels as needed. This results in optimum utilization of network resources. There are less chances of denial of services and call blocking in case of voice transmission. These schemes adjust bandwidth allotment according to traffic volume, and so are particularly suitable for bursty traffic.

Disadvantages

Dynamic channel allocation schemes increases the computational as well as storage load on the system.

Possible assumptions include:

1. **Station Model:**

   Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

2. **Single Channel Assumption:**
   In this allocation all stations are equivalent and can send and receive on that channel.
3. **Collision Assumption:**
   If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must re transmitted. Collisions are only possible error.
4. **Time** can be divided into Slotted or Continuous.
5. **Stations** can sense a channel is busy before they try it.

Protocol Assumption:

- N independent stations.
- A station is blocked untill its generated frame is transmitted.
- probability of a frame being generated in a period of length Dt is IDt where I is the arrival rate of frames.
- Only a single Channel available.
- Time can be either: Continuous or slotted.
- **Carrier Sense:** A station can sense if a channel is already busy before transmission.
- **No Carrier Sense:** Time out used to sense loss data.

Difference between Fixed and Dynamic Channel Allocations

Static channel allocation	**Dynamic channel allocation**
1. Fixed Channel Allocation is a strategy in which fixed number of channels or voice channels are allocated to the cells.Once the channels are allocated to the specific cells then they cannot be changed. 2. In FCA channels are allocated in a manner that maximize Frequency reuse 3. If all channels are occupied and user make a call then the call is blocked. Borrowing Channels handles this type of problem. In this cell borrow channels from other cells.	1. Dynamic Channel Allocation is a strategy in which channels are not permanently allocated to the cells. 2. When a User makes a call request then Base Station(BS) send that request to the Mobile Station Center(MSC) for the allocation of channels or voice channels. 3. This way the likelihood of blocking calls is reduced. As traffic increases more channels are assigned and vice-versa.

Multiple Access Protocols

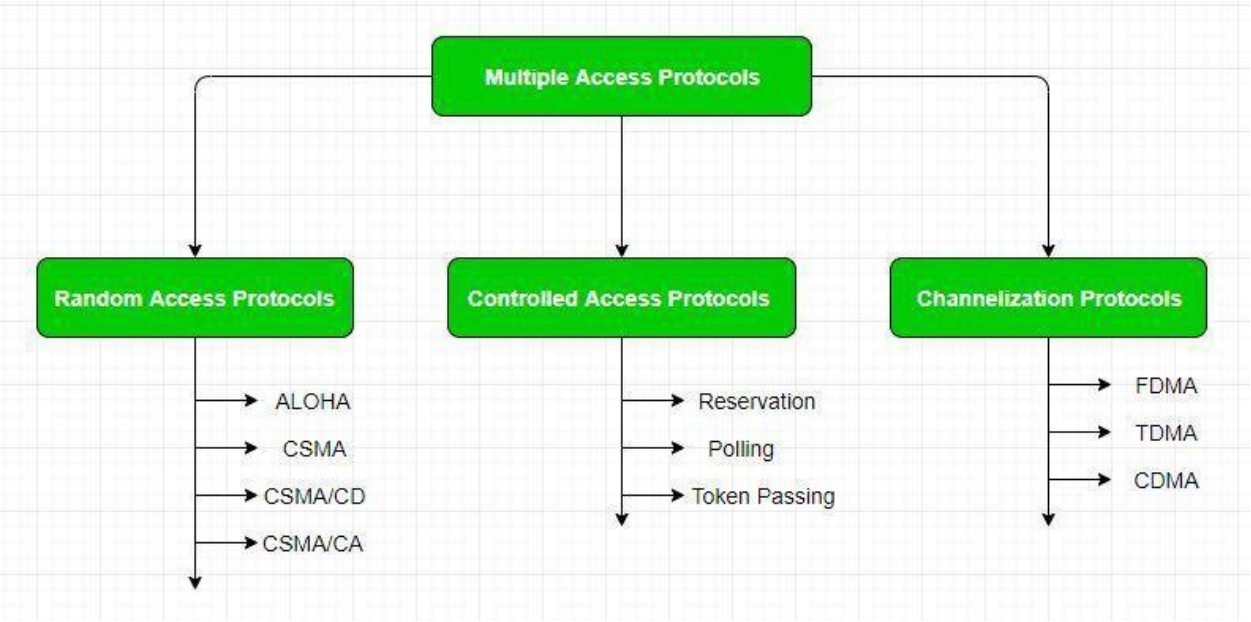
The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

1. Data Link Control
2. Multiple Access Control

Multiple Access Control

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as –



Random Access Protocol:

In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

•The Random access protocols are further subdivided as:

1. ALOHA
2. CSMA
3. CSMA/CD
4. CSMA/CA

(a) ALOHA –It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

Pure Aloha:

When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

Vulnerable Time = 2* Frame transmission time

Throughput = G exp{-2*G}

Maximum throughput = 0.184 for G=0.5

Slotted Aloha:

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Vulnerable Time = Frame transmission time

Throughput = G exp{-*G}

Maximum throughput = 0.368 for G=1

CSMA –Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.Ifit finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes:

1-persistent: The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.

Non-Persistent: The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.

P-persistent: The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifiand packet radio systems.

O-persistent: Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

CSMA/CD –Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer –Efficiency of CSMA/CD

(d) CSMA/CA –Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

•CSMA/CA avoids collision by:

Interframespace –Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframespace or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.

Contention Window –It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.

Acknowledgement –The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access:

In this, the data is sent by that station which is approved by all other stations.

3. Channelization:

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

Frequency Division Multiple Access (FDMA) –The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no to bands overlap to avoid crosstalk and noise.

Time Division Multiple Access (TDMA) –In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.

Code Division Multiple Access (CDMA) –One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly data from different stations can be transmitted simultaneously in different code languages.

Ethernet

Ethernet is the technology that is commonly used in wired local area networks (LANs). A LAN is a network of computers and other electronic devices that covers a small area such as a room, office, or building. It is used in contrast to a wide area network (WAN), which spans a large geographical area. Ethernet is a network protocol that controls how data is transmitted over a LAN and is referred to as the IEEE 802.3 protocol. The protocol has evolved and improved over time to transfer data at the speed of more than a gigabit per second.

Many people have used Ethernet technology their whole lives without knowing it. It is likely that any wired network in your office, at the bank, and at home is an Ethernet LAN. Most desktop and laptop computers come with an integrated Ethernet card and are ready to connect to an Ethernet LAN.

What You Need in an Ethernet LAN

To set up a wired Ethernet LAN, you need the following:

- **Computers and devices to connect**: Ethernet connects any computer or other electronic device to its network as long as the device has an Ethernet adapter or network card.

- **Network interface cards in the devices**: A network interface card is either integrated into the motherboard of the computer or installed separately in the device. There are also USB versions of Ethernet cards, such as external dongles. An Ethernet card is known as a network card. It has ports where you connect cables. There may be two ports, one for an RJ-45 jack that connects unshielded twisted pair (UTP) cables and one for a coaxial jack on the network card. (Coaxial connections are extremely rare, though.)

- **A router, hub, switch, or gateway to connect devices**: A hub is a device that acts as a connecting point between devices on a network. It consists of several RJ-45 ports to which you plug the cables.

- **Cables**: UTP (Unshielded Twisted Pair) cables are commonly used in Ethernet LANs. This cable is similar to the kind used for landline telephone sets but fatter, with eight twisted pairs of wires of different colors inside. The end is crimped with an RJ-45 connector, which is a larger version of the RJ-11 jack that plugs into a landline phone.
- **Software to manage the network**: Modern operating systems like recent versions of Windows, Linux and macOS are more than sufficient to manage Ethernet LANs. Third-party software that gives more features and better control is available.

How Ethernet Works

Ethernet protocol requires technical knowledge in computer science to fully understand how it works. Here is a simple explanation: When a machine on the network wants to send data to another, it senses the carrier, which is the main wire connecting the devices. If it is free, meaning no one is sending anything, it sends the data packet on the network, and the other devices check the packet to see whether they are the recipient. The recipient consumes the packet. If there is a packet on the highway, the device that wants to send holds back for some thousandths of a second to try again until it can send.

Types of LAN Technology

Ethernet

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Fast Ethernet

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks will support even higher data transfer speeds.

Gigabit Ethernet

Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as ―gigabit-Ethernet-over-copper‖ or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers. From the data link layer of the OSI model upward, the look and implementation of Gigabit Ethernet is identical to that of Ethernet. The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

10 Gigabit Ethernet

Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined.

WIRELESS LAN

Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.

Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Examples of WLANs that are available today are NCR's waveLAN and Motorola's ALTAIR.

Advantages of WLANs

- ✓ **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- ✓ **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- ✓ **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- ✓ **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- ✓ **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.
- ✓ **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.
- ✓ **Disadvantages of WLANs**
- ✓ **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
- ✓ **Proprietary Solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.
- ✓ **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
- ✓ **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
- ✓ **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
- ✓ **License free operation:** LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.
- ✓ **Robust transmission technology:** If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

802.11 ARCHITECTURE

The components of an IEEE 802.11 architecture are as follows

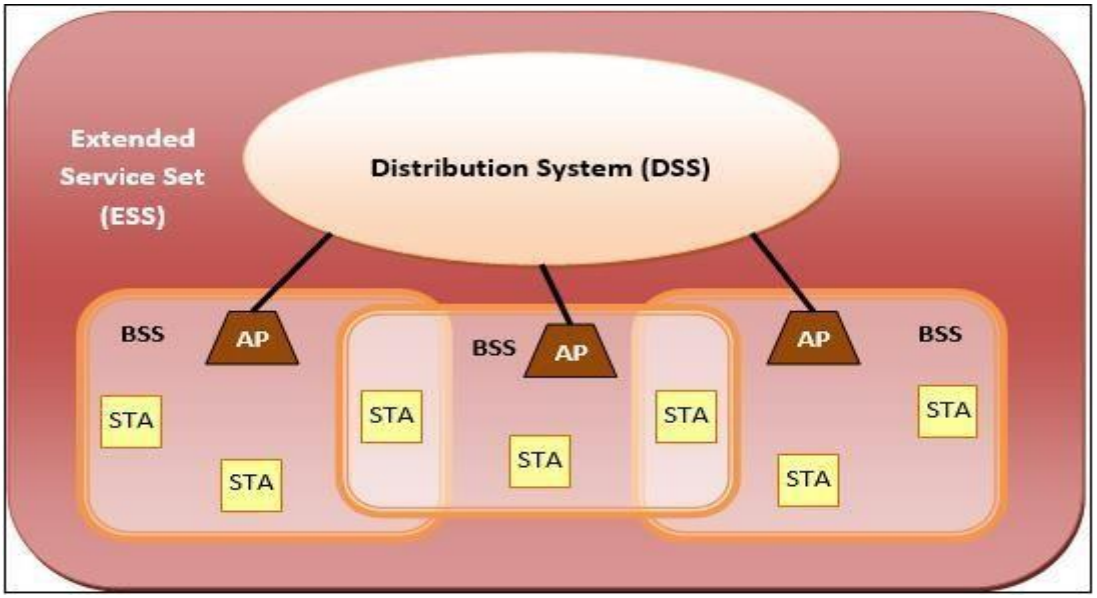
1) **Stations (STA) –** Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

- **Wireless Access Pointz (WAP) –** WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- **Client. –** Clients are workstations, computers, laptops, printers, smartphones, etc.

Each station has a wireless network interface controller.
2) **Basic Service Set (BSS) –**A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

- **Infrastructure BSS –** Here, the devices communicate with other devices through access points.
- **Independent BSS –** Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) **Extended Service Set (ESS) –** It is a set of all connected BSS.
4) **Distribution System (DS) –** It connects access points in ESS.



UNIT III

Design Issues in Network Layer

Network layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control. The various functions of network layer is

- **Addressing:**
  Maintains the address at the frame header of both source and destination and performs addressing to detect various devices in network.
- **Packeting:**
  This is performed by Internet Protocol. The network layer converts the packets from its upper layer.
- **Routing:**
  It is the most important functionality. The network layer chooses the most relevant and best path for the data transmission from source to destination.
- **Inter-networking:**
  It works to deliver a logical connection across multiple devices.

Network layer design issues:
The network layer comes with some design issues they are described as follows:

1. **Store and Forward packet switching:**

   The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called ―Store and Forward packet switching.‖

2. **Services provided to Transport Layer:**

   Through the network/transport layer interface, the network layer transfers it's services to the transport layer. These services are described below.
   But before providing these services to the transfer layer following goals must be kept in mind :-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided:

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. **Implementation of Connectionless Service:**
   Packet are termed as ―datagrams‖ and corresponding subnet as ―datagram subnets‖. When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol.Each data packet has destination address and is routed independently irrespective of the packets.

4. **Implementation of Connection Oriented service:**
   To use a connection-oriented service, first we establishes a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.

It can be done in either two ways :

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

<u>Routing algorithm</u>

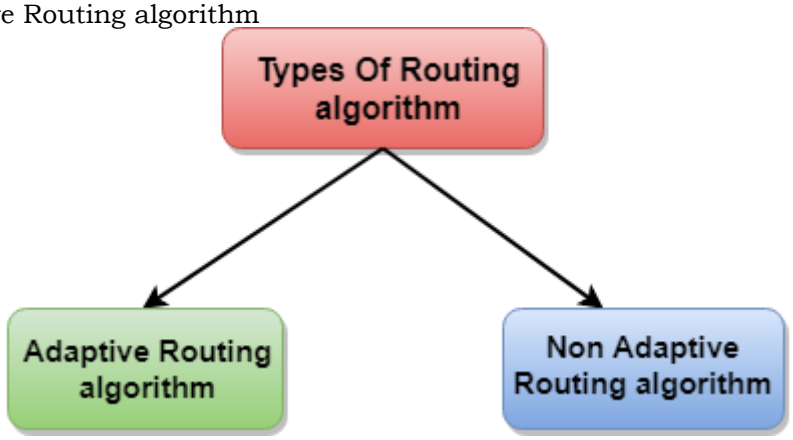
- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.

- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm



Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination; instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	**Adaptive Routing algorithm**	**Non-Adaptive Routing algorithm**
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

UNIT IV

TRANSPORT LAYER

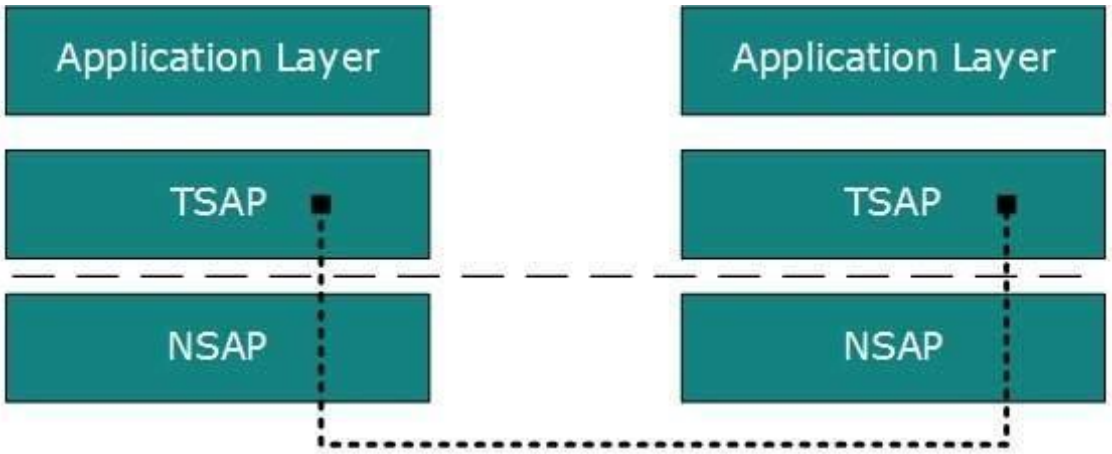
Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.

Functions

- This Layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments. It numbers every byte in the segment and maintains their accounting.
- This layer ensures that data must be received in the same sequence in which it was sent.
- This layer provides end-to-end delivery of data between hosts which may or may not belong to the same subnet.
- All server processes intend to communicate over the network are equipped with well-known Transport Service Access Points (TSAPs) also known as port numbers.

End-to-End Communication

A process on one host identifies its peer host on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.



For example, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number 67. When a DNS client wants to communicate with remote DNS server, it always requests on port number 53 (UDP).

The two main Transport layer protocols are:

- **Transmission Control Protocol**

  It provides reliable communication between two hosts.

- **User Datagram Protocol**

  It provides unreliable communication between two hosts.

TRANSMISSION CONTROL PROTOCOL (TCP)

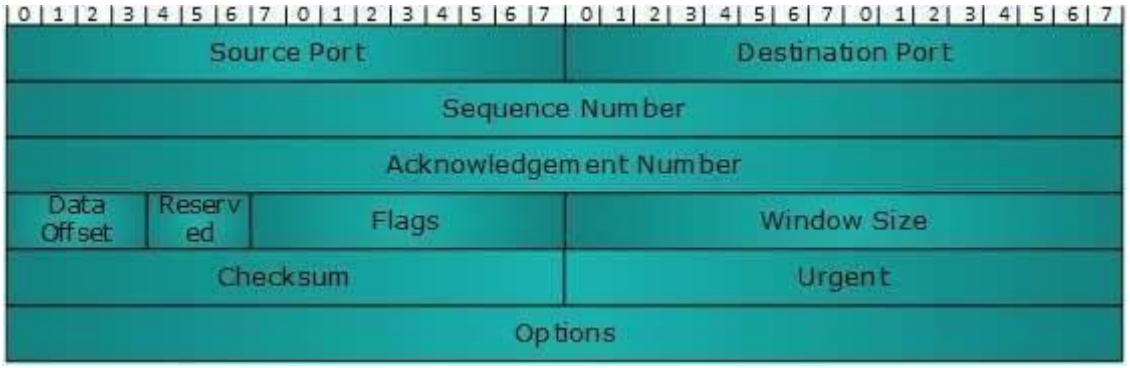
The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - **ECE** -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.

- **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
- **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
- **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
- **RST** - Reset flag has the following features:
  - It is used to refuse an incoming connection.
  - It is used to reject a segment.
  - It is used to restart a connection.
- **SYN** - This flag is used to set up a connection between hosts.
- **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Addressing

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.

Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

Bandwidth Management

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.
For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.
If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

Error Control &and Flow Control

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

Multiplexing

The technique to combine two or more data streams in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

Congestion Control

When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

Timer Management

TCP uses different types of timer to control and management various tasks:

Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

Persist timer:

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds (4 minutes).

Crash Recovery

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).
When a TCP Server crashes mid-way communication and re-starts its process it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

UDP

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

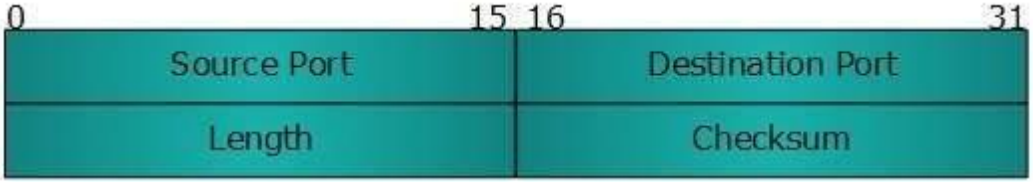
Requirement of UDP

A question may arise, why do we need an unreliable protocol to transport the data? We deploy UDP where the acknowledgement packets share significant amount of bandwidth along with the actual data. For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain huge amount of bandwidth wastage. The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not calamitous and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP header is as simple as its function.



UDP header contains four main parameters:

- **Source Port** - This 16 bits information is used to identify the source port of the packet.
- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.
- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.

UDP application

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

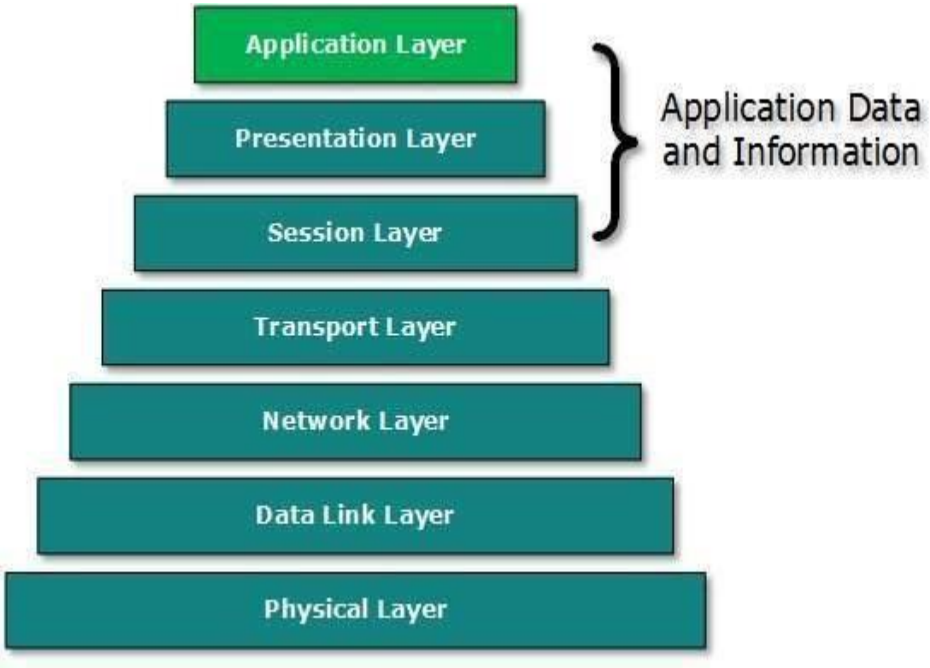
UNIT V

APPLICATION LAYER

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.



There is an ambiguity in understanding Application Layer and its protocol. Not every user application can be put into Application Layer. except those applications which interact with the communication system. For example, designing software or text-editor cannot be considered as application layer programs.

On the other hand, when we use a Web Browser, which is actually using Hyper Text Transfer Protocol (HTTP) to interact with the network. HTTP is Application Layer protocol.

Another example is File Transfer Protocol, which helps a user to transfer text based or binary files across the network. A user can use this protocol in either GUI based software like FileZilla or CuteFTP and the same user can use FTP in Command Line mode.

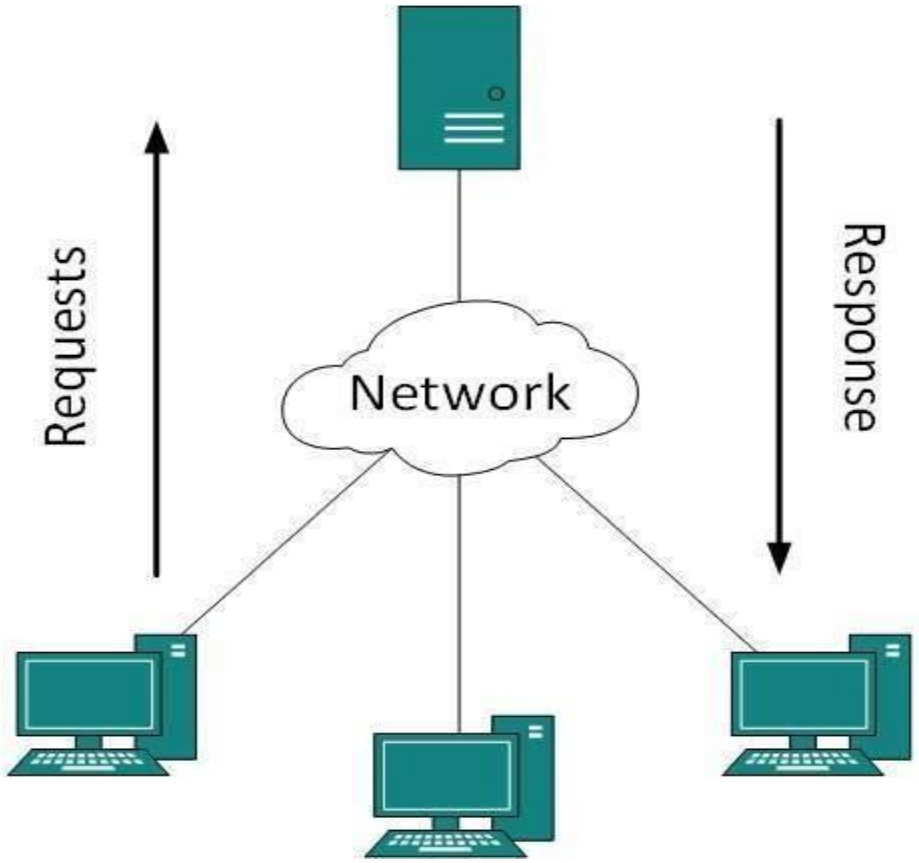
Hence, irrespective of which software you use, it is the protocol which is considered at Application Layer used by that software. DNS is a protocol which helps user application protocols such as HTTP to accomplish its work.

CLIENT SERVER MODEL

Two remote application processes can communicate mainly in two different fashions:

- **Peer-to-peer:** Both remote processes are executing at same level and they exchange data using some shared resource.
- **Client-Server:** One remote process acts as a Client and requests some resource from another application process acting as Server.

In client-server model, any process can act as Server or Client. It is not the type of machine, size of the machine, or its computing power which makes it server; it is the ability of serving request that makes a machine a server.



A system can act as Server and Client simultaneously. That is, one process is acting as Server and another is acting as a client. This may also happen that both client and server processes reside on the same machine.

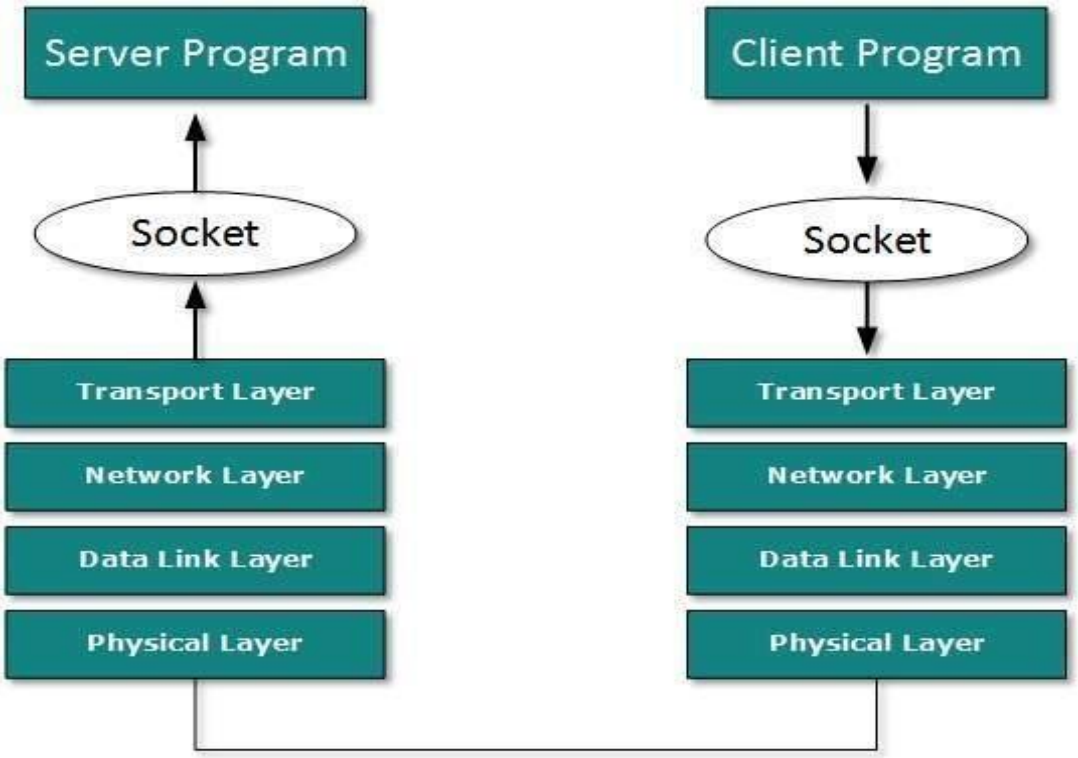
Communication

Two processes in client-server model can interact in various ways:

- Sockets
- Remote Procedure Calls (RPC)

Sockets

In this paradigm, the process acting as Server opens a socket using a well-known (or known by client) port and waits until some client request comes. The second process acting as a Client also opens a socket but instead of waiting for an incoming request, the client processes ‚requests first'.



When the request is reached to server, it is served. It can either be an information sharing or resource request.

Remote Procedure Call

This is a mechanism where one process interacts with another by means of procedure calls. One process (client) calls the procedure lying on remote host. The process on remote host is said to be Server. Both processes are allocated stubs. This communication happens in the following way:

- The client process calls the client stub. It passes all the parameters pertaining to program local to it.
- All parameters are then packed (marshaled) and a system call is made to send them to other side of the network.
- Kernel sends the data over the network and the other end receives it.
- The remote host passes data to the server stub where it is unmarshalled.

- The parameters are passed to the procedure and the procedure is then executed.
- The result is sent back to the client in the same manner.

APPLICATION PROTOCOLS

There are several protocols which work for users in Application Layer. Application layer protocols can be broadly divided into two categories:

- Protocols which are used by users. For email for example, eMail.
- Protocols which help and support protocols used by users. For example DNS.

Few of Application layer protocols are described below:

DOMAIN NAME SYSTEM

The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme. The DNS server is configured with Fully Qualified Domain Names (FQDN) and email addresses mapped with their respective Internet Protocol addresses.

DNS server is requested with FQDN and it responds back with the IP address mapped with it. DNS uses UDP port 53.

Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.

Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. SMTP uses TCP port number 25 and 587.

Software uses Internet Message Access Protocol (IMAP) or POP protocols to receive emails.

File Transfer Protocol

The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client.

FTP uses out-of-band controlling i.e. FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21.

The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

Post Office Protocol (POP)

The Post Office Protocol version 3 (POP 3) is a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server.

a client needs to retrieve mails from server, it opens a connection with the server on TCP port 110. User can then access his mails and download them to the local computer. POP3 works in two modes. The most common mode the delete mode, is to delete the emails from remote server after they are downloaded to local machines. The second

mode, the keep mode, does not delete the email from mail server and gives the user an option to access mails later on mail server.

Hyper Text Transfer Protocol (HTTP)

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

HTTP versions

- HTTP 1.0 uses non persistent HTTP. At most one object can be sent over a single TCP connection.
- HTTP 1.1 uses persistent HTTP. In this version, multiple objects can be sent over a single TCP connection.

NETWORK SERVICES

Computer systems and computerized systems help human beings to work efficiently and explore the unthinkable. When these devices are connected together to form a network, the capabilities are enhanced multiple-times. Some basic services computer network can offer are.

Directory Services

These services are mapping between name and its value, which can be variable value or fixed. This software system helps to store the information, organize it, and provides various means of accessing it.

- **Accounting**

  In an organization, a number of users have their user names and passwords mapped to them. Directory Services provide means of storing this information in cryptic form and make available when requested.

- **Authentication and Authorization**

  User credentials are checked to authenticate a user at the time of login and/or periodically. User accounts can be set into hierarchical structure and their access to resources can be controlled using authorization schemes.

- **Domain Name Services**

  DNS is widely used and one of the essential services on which internet works. This system maps IP addresses to domain names, which are easier to remember and recall than IP addresses. Because network operates with the help of IP addresses and humans tend to remember website names, the DNS provides website‘s IP address which is mapped to its name from the back-end on the request of a website name from the user.

File Services

File services include sharing and transferring files over the network.

- **File Sharing**

  One of the reason which gave birth to networking was file sharing. File sharing enables its users to share their data with other users. User can upload the file to a specific server, which is accessible by all intended users. As an alternative, user can make its file shared on its own computer and provides access to intended users.

- **File Transfer**

  This is an activity to copy or move file from one computer to another computer or to multiple computers, with help of underlying network. Network enables its user to locate other users in the network and transfers files.

Communication Services

- **Email**

  Electronic mail is a communication method and something a computer user cannot work without. This is the basis of today's internet features. Email system has one or more email servers. All its users are provided with unique IDs. When a user sends email to other user, it is actually transferred between users with help of email server.

- **Social Networking**

  Recent technologies have made technical life social. The computer savvy peoples, can find other known peoples or friends, can connect with them, and can share thoughts, pictures, and videos.

- **Internet Chat**

  Internet chat provides instant text transfer services between two hosts. Two or more people can communicate with each other using text based Internet Relay Chat services. These days, voice chat and video chat are very common.

- **Discussion Boards**

  Discussion boards provide a mechanism to connect multiple peoples with same interests.It enables the users to put queries, questions, suggestions etc. which can be seen by all other users. Other may respond as well.

- **Remote Access**

  This service enables user to access the data residing on the remote computer. This feature is known as Remote desktop. This can be done via some remote device, e.g. mobile phone or home computer.

Application Services

These are nothing but providing network based services to the users such as web services, database managing, and resource sharing.

- **Resource Sharing**

  To use resources efficiently and economically, network provides a mean to share them. This may include Servers, Printers, and Storage Media etc.

- **Databases** This application service is one of the most important services. It stores data and information, processes it, and enables the users to retrieve it efficiently by using queries. Databases help organizations to make decisions based on statistics.

- **Web Services**

  World Wide Web has become the synonym for internet.It is used to connect to the internet, and access files and information services provided by the internet servers.

NETWORK SECURITY

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.
Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Intrusion Detection Systems

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options