COMPUTER ENGINEERING

THIRD YEAR (5TH SEM)

COMPUTER NETWORK:

CONTENTS:

1.Introduction-

Network needs & goals, Application of networks, network topologies, need of protocols, protocol and interfaces, networks services and service access points.

2. OSI and TCP/IP-

OSI reference model**,** TCP/IP reference model, Comparison between OSI & TCP/IP reference model.

3.Transmission media-

Analog transmission media, digital transmission media, switching techniques.

4.Data link layer-

Functions, protocols - stop & wait, sliding window.

5.IEEE standards-

802.3, 802.4, 802.5 fast Ethernet, FDDI, fiber Optics.

6.Network Layer-

Functions, routing algorithms, Inter-networking. Familiarization with repeater, hubs switch bridge, routers, and gateways.

7.Transport Layer-

Functions and services, transport service primitive, sockets, elements of transport protocols, UDP.

8.Broad Band network-

ISDN, ATM, Introduction to VSAT, ADSL.

9.Network security-

Levels of security, introduction to cryptography, Data Encryption Standard (DES) public key cryptography, firewalls.

UNIT – 1 INTRODUCTION

A network consists of two or more nodes (e.g., computers) that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

NETWORK GOALS:

The main goal of networking is "Resource sharing", and it is to make all programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user.

• A second goal is to provide high reliability by having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable, the other copies could be available.

• Another goal is saving money. Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more. This imbalance has caused many system designers to build systems consisting of powerful personal computers, one per user, with data kept on one or more shared file server machines. This goal leads to networks with many computers located in the same building. Such a network is called a LAN (local area network).

• Another closely related goal is to increase the systems performance as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.

• Computer networks provide a powerful communication medium. A file that was updated or modified on a network can be seen by the other users on the network immediately.

NETWORK APPLICATIONS:

- Access to remote programs.
- Access to remote databases.
- Value-added communication facilities.

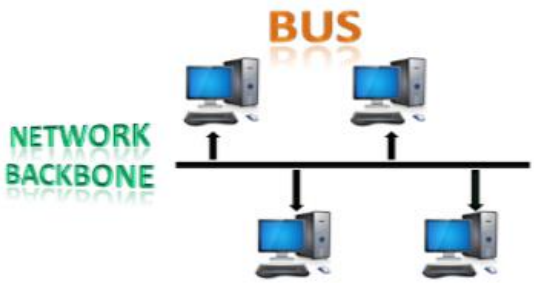
NETWORK TOPOLOGY:

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **network topology.** The various network topologies are:

Types of Topologies:

1.Bus Topology:

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.



- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:**(**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA:(Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

2.Ring Topology:

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.

- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.

- **Token passing:** It is a network access method in which token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

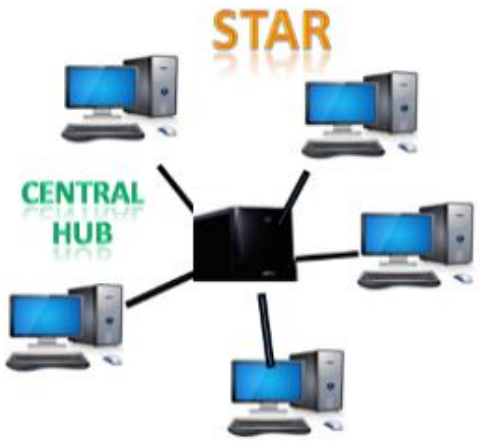
Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

3.Star Topology:



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

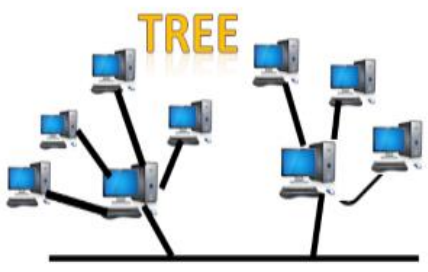
Advantages of Star topology:

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometres of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **High data speeds:** It supports a bandwidth of approx. 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology:

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

3.Tree topology:



- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree topology:

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.

Disadvantages of Tree topology:

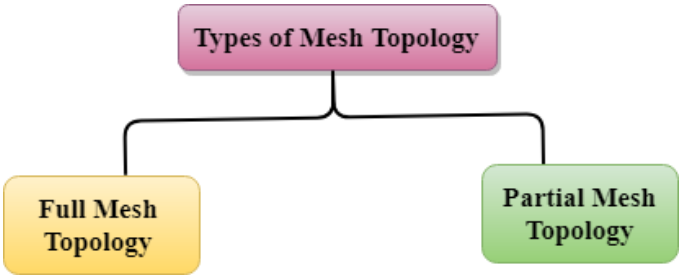
- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

4.Mesh topology:

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.

- Mesh topology can be formed by using the formula:
  Number of cables = (n*(n-1))/2;
- Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:



- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

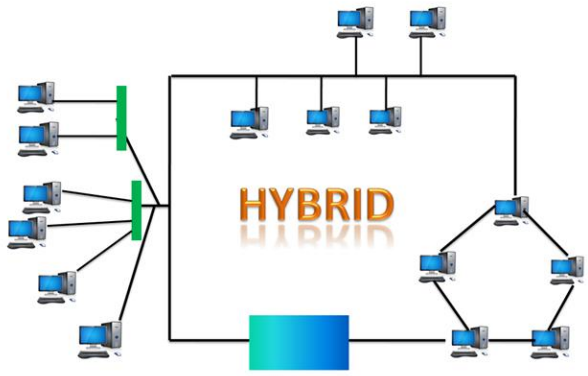
- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology:

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.

- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

5.Hybrid Topology:



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology:

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology:

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.

- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

NEED OF PROTOCOLS:

Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used to transmit and receive data over a network, we need to understand how a network is logically organized or designed.

Protocols is set of Rules which is used to communicate. Protocols provide us with a medium and set of rules to establish communication between different devices for the exchange of data and other services. Protocols are needed in every field like society, science & technology, Data Communication, media, etc.

Types of Protocols:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- Post office Protocol (POP)
- Simple mail transport Protocol (SMTP)
- File Transfer Protocol (FTP)
- Hyper Text Transfer Protocol (HTTP)
- Hyper Text Transfer Protocol Secure (HTTPS)

NETWORK INTERFACE:

A network interface can refer to any kind of software interface to networking hardware. For instance, if you have two network cards in your computer, you can control and configure each network interface associated with them individually.

Question: Is interface same as protocol?

Ans: An interface refers to the connecting point between two adjacent entities. A protocol defines rules to be complied with for exchanging information on the connecting point. An interface protocol is a specification that defines how data is delivered and interpreted.

NETWORK SERVICES:

A capability that facilitates a network operation. It typically is provided by a server (which can be running one or more services), based on network protocols running at the application layer in the Open Systems Interconnection (OSI) model of the network.

There are four types of network services:

- Personal Area Network (PAN) ...
- Local Area Network (LAN) ...
- Metropolitan Area Network (MAN) ...
- Wide Area Network (WAN) ...

SERVICE ACCESS POINT(SAP):

Service Access Point (SAP) A Service Access Point (SAP) is an identifying label for network endpoints used in Open Systems Interconnection (OSI) networking. The SAP is a conceptual location at which one OSI layer can request the services of another OSI layer.

As an example, PD-SAP or PLME-SAP in IEEE 802.15.4 can be mentioned, where the medium access control (MAC) layer requests certain services from the physical layer. Service access points are also used in IEEE 802.2 Logical Link Control in Ethernet and similar data link layer protocols.

When using the OSI Network system (CONS or CLNS), the base for constructing an address for a network element is an NSAP address, similar in concept to an IP address. OSI protocols as well as Asynchronous Transfer Mode (ATM) can use Transport (TSAP), Session (SSAP) or Presentation (PSAP) Service Access Points to specify a destination address for a connection. These SAPs consist of NSAP addresses combined with optional transport, session and presentation selectors, which can differentiate at any of the three layers between multiple services at that layer provided by a network element.

UNIT – 2 OSI & TCP/IP

OSI MODEL:

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:

- The OSI model is divided into two layers: upper layers and lower layers.

- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

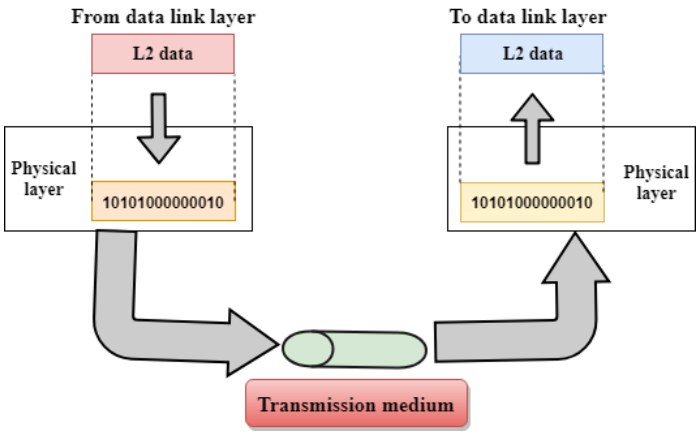
OSI Layers:

There are the seven OSI layers. Each layer has different functions. A list of seven layers is given below:

- Physical Layer
- Data-Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Physical layer:

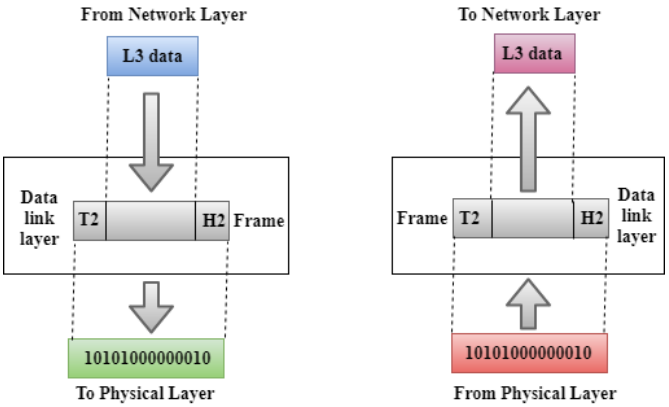
- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.



- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Data-Link Layer:

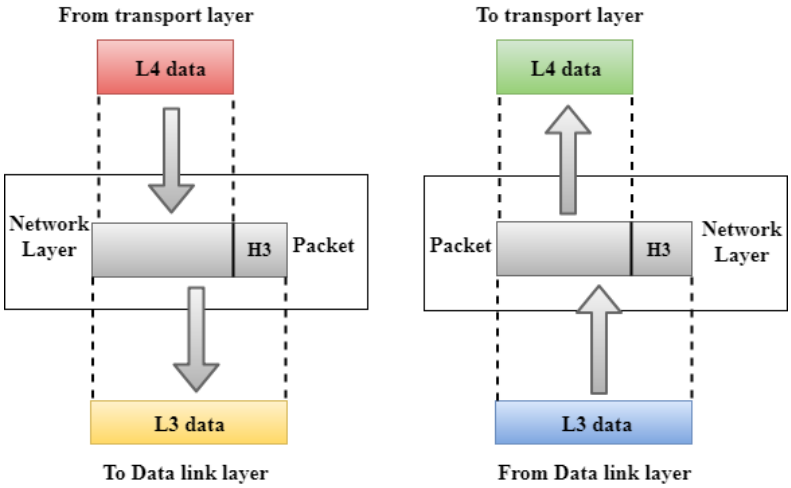
- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.



- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.

Network Layer:

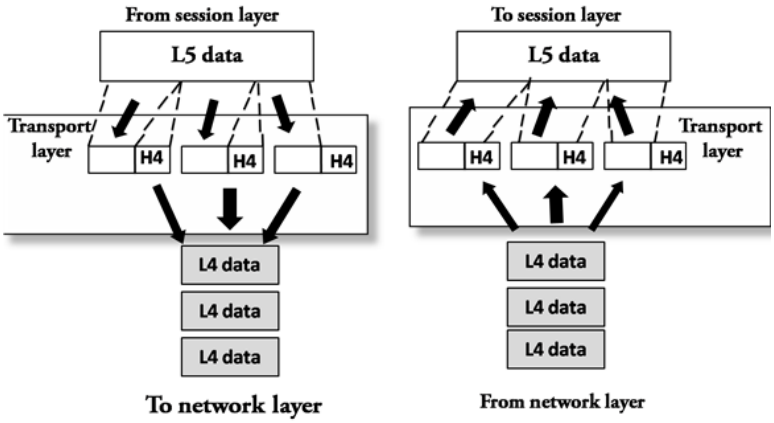
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.



- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Transport Layer:

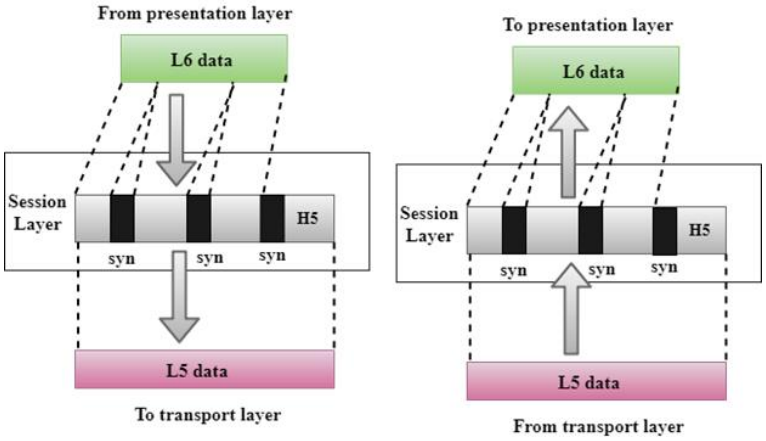
- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.



- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

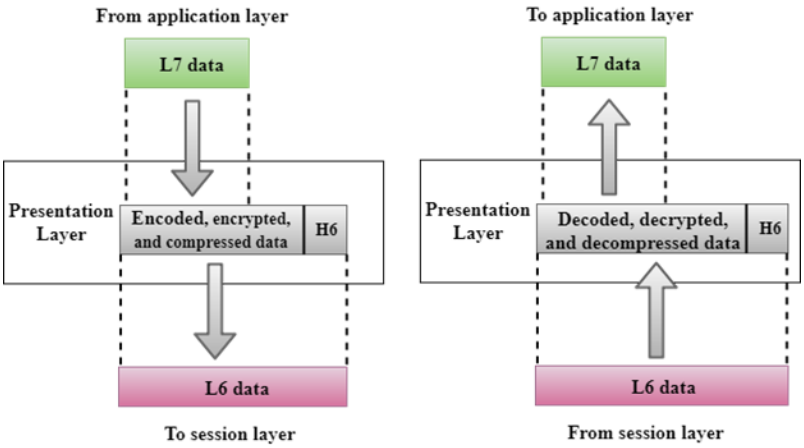
Session Layer:

- This layer is responsible to establish and terminate connections between two communicating machines. This connection is known as a session, hence the name.
- It establishes full-duplex, half-duplex and simplex connection for communication. The sessions are also used to keep a track of the connections to the web server.



Presentation Layer:

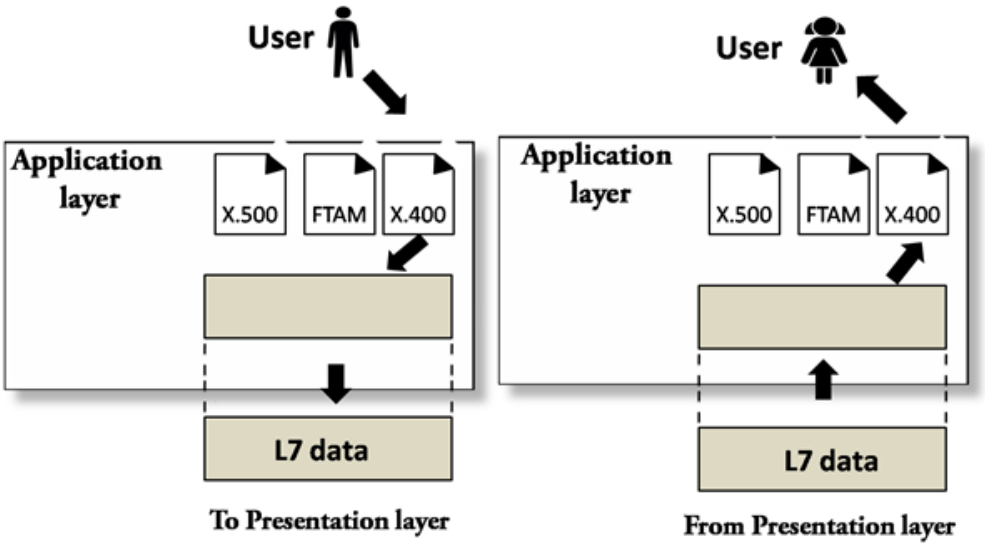
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.



- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Application Layer:

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.



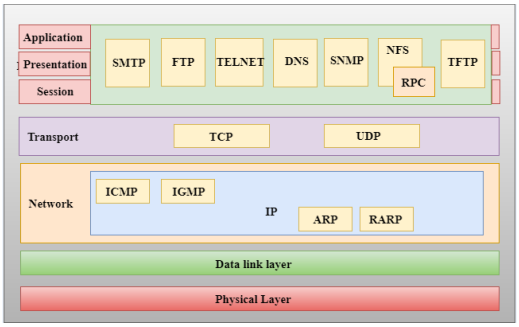
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

TCP/IP MODEL:

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.

- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

FUNCTIONS OF TCP/IP MODEL:



Network Access Layer:

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer:

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Transport Layer:

- This layer is responsible for providing datagram services to the Application layer.

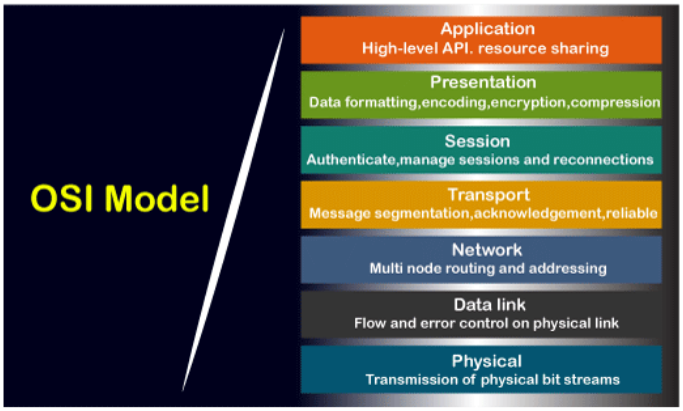
- This layer allows the host and the destination devices to communicate with each other for exchanging messages, irrespective of the underlying network type.
- Error control, congestion control, flow control, etc., are handled by the transport layer. The protocol that this layer uses is TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- TCP gives a reliable, end-to-end, connection-oriented data transfer, while UDP provides unreliable, connectionless data transfer between two computers.

Application Layer:

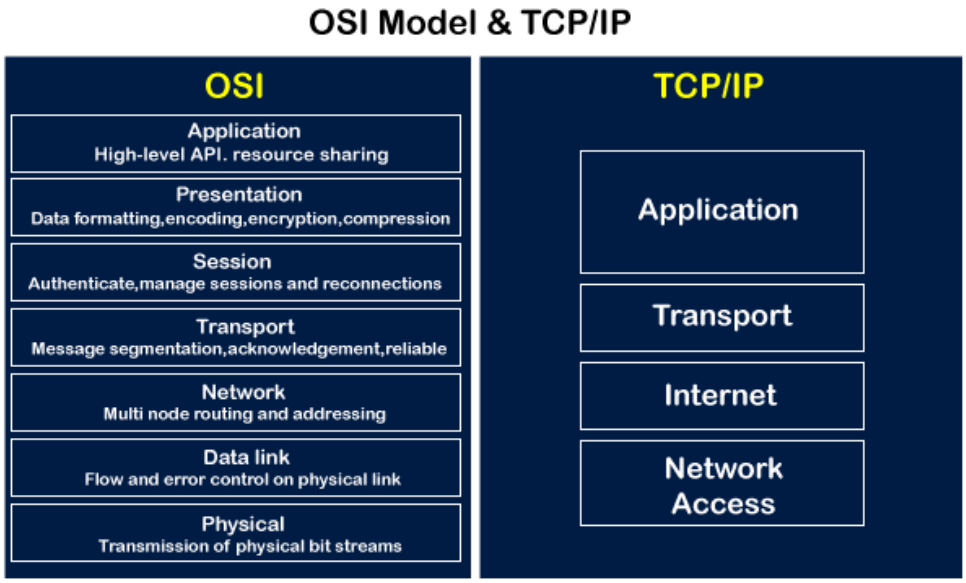
- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

COMPARISON BETWEEN OSI & TCP/IP REFERENCE MODEL:

The **OSI stands for Open System Interconnection**, which was developed in 1980s. It is a conceptual model used for network communication. It is not implemented entirely, but it is still referenced today. This OSI model consists of seven layers, and each layer is connected to each other. The data moves down the OSI model, and each layer adds additional information. The data moves down until it reaches the last layer of the OSI model. When the data is received at the last layer of the OSI model, then the data is transmitted over the network. Once the data is reached on the other side, then the process will get reversed.



The TCP model stands for **Transmission Control Protocol,** whereas IP stands for **Internet Protocol**. A number of protocols that make the internet possibly comes under the TCP/IP model. Nowadays, we do not hear the name of the TCP/IP model much, we generally hear the name of the IPv4 or IPv6, but it is still valid. This model consists of 4 layers.



Similarities between the OSI and TCP/IP model: d Nth Highest Salary in SQL

- **Share common architecture**: Both the models are the logical models and having similar architectures as both the models are constructed with the layers.
- **Define standards**: Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.
- **Simplified troubleshooting process:** Both models have simplified the troubleshooting process by breaking the complex function into simpler components.
- **Pre-defined standards**: The standards and protocols which are already pre-defined; these models do not redefine them; they just reference or use them. For example, the Ethernet standards were already defined by the IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.
- **Both have similar functionality of 'transport' and 'network' layers**: The function which is performed between the **'presentation'** and the **'network'** layer is similar to the function performed at the **transport** layer.

Differences between the OSI and TCP/IP model:

OSI Model	TCP/IP Model
It stands for Open System Interconnection.	It stands for **Transmission Control Protocol.**
OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).

It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts.
In the OSI model, the transport layer provides a guarantee for the delivery of the packets.	The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.
This model is based on a vertical approach.	This model is based on a horizontal approach.
In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool.	It is an implemented model of an OSI model.
In this model, the network layer provides both connection-oriented and connectionless service.	The network layer provides only connectionless service.
Protocols in the OSI model are hidden and can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.
It consists of 7 layers.	It consists of 4 layers.
OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.	In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.
The usage of this model is very low.	This model is highly used.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.

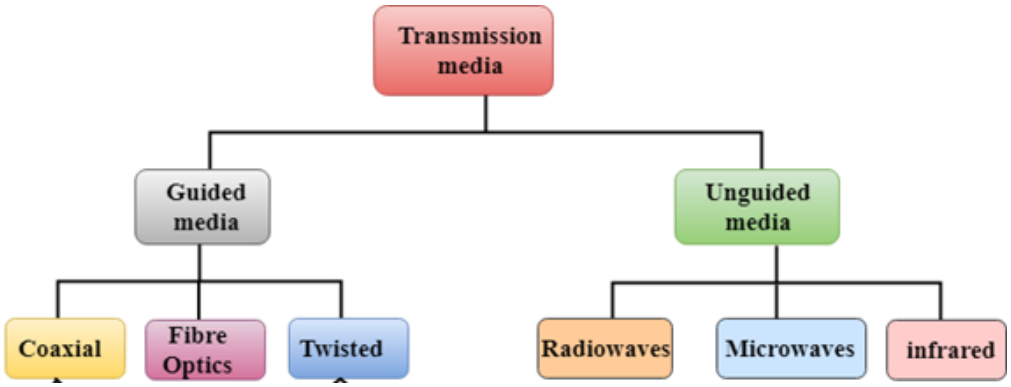
UNIT – 3 TRANSMISSION MEDIA

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals. The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network). It is a physical path between transmitter and receiver in data communication.

Some factors need to be considered for designing the transmission media:

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Classification Of Transmission Media:

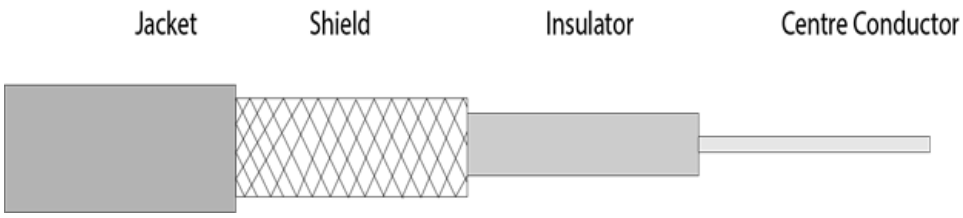


Guided Media:

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features: High Speed, Secure, Used for comparatively shorter distances.

1.Coaxial cable: 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).



Coaxial cable is of two types:

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

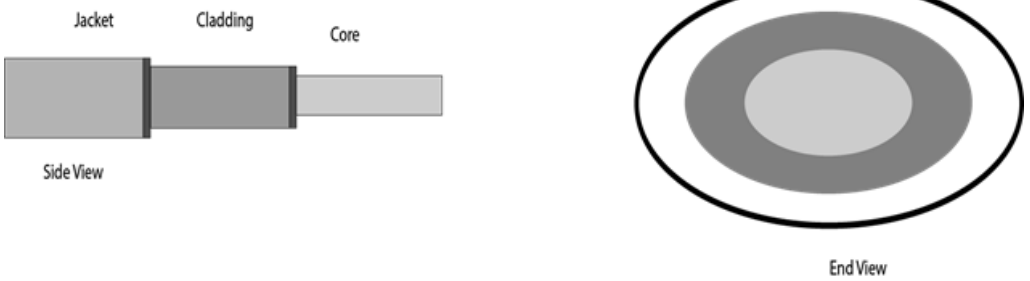
Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

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



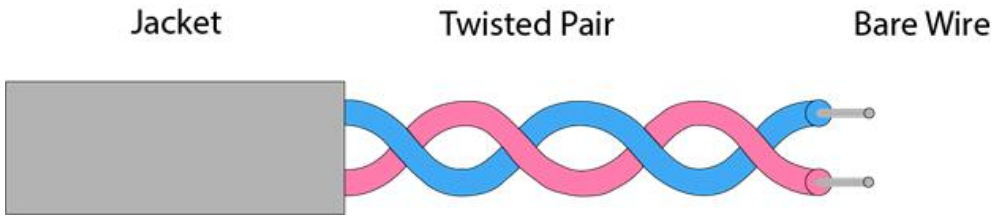
Advantages Of Optical fibre cable:

- Increased capacity and bandwidth
- Light weight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages Of Optical fibre cable:

- Difficult to install and maintain
- High cost
- Fragile
- unidirectional, i.e., will need another fibre, if we need bidirectional communication.

3.Twisted Cable: 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 3.5KHz. A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Twisted Pair is of two types:

Unshielded Twisted Pair (UTP): This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

- **Advantages:** Least expensive, Easy to install, High speed capacity.
- **Disadvantages:** Susceptible to external interference, Lower capacity and performance in comparison to STP, Short distance transmission due to attenuation.

Shielded Twisted Pair (STP): This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

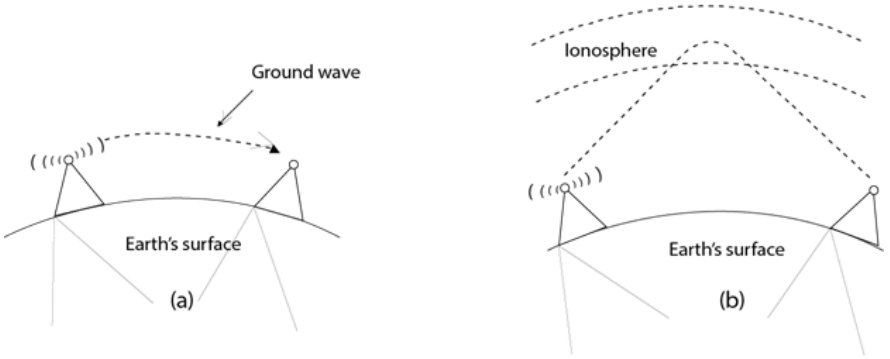
- **Advantages:** Better performance at a higher data rate in comparison to UTP, Eliminates crosstalk, comparatively faster.
- **Disadvantages:** Comparatively difficult to install and manufacture, more expensive, Bulky.

Unguided Media:

An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore, it is also known as **wireless transmission**. In unguided media, air is the media through which the electromagnetic energy can flow easily.

Features: Signal is broadcasted through air, Less Secure, Used for larger distances.

Radio waves: Radio waves are the electromagnetic waves that are transmitted in all the directions of free space. Radio waves are omnidirectional, i.e., the signals are propagated in all the directions. The range in frequencies of radio waves is from 3Khz to 1 khz. In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna. An example of the radio wave is **FM radio**.



Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves: It is a line-of-sight transmission i.e., the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

Advantages Of Microwaves:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

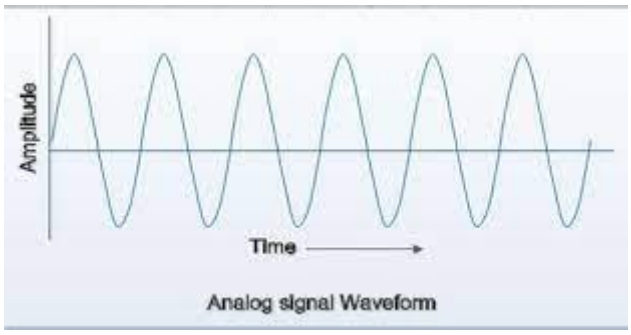
Infrared waves: An infrared transmission is a wireless technology used for communication over short ranges. The frequency of the infrared in the range from 300 GHz to 400 THz. It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Advantages Of Infrared waves:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

ANALOG TRANSMISSION MEDIA:

An analog wave form (or signal) is characterized by being continuously variable along amplitude and frequency. In the case of telephony, for instance, when you speak into a handset, there are changes in the air pressure around your mouth. Those changes in air pressure fall onto the handset, where they are amplified and then converted into current, or voltage fluctuations. Those fluctuations in current are an analog of the actual voice pattern—hence the use of the term analog to describe these signals.



When it comes to an analog circuit—what we also refer to as a voice-grade line—we need to also define the frequency band in which it operates. The human voice, for example, can typically generate frequencies from 100Hz to 10,000Hz, for a bandwidth of 9,900Hz. But the ear does not require a vast range of frequencies to elicit meaning from ordinary speech; the vast majority of sounds we make that constitute intelligible speech fall between 250Hz and 3,400Hz. So, the phone company typically allotted a total bandwidth of 4,000Hz for voice transmission. Remember that the total frequency spectrum of twisted-pair is 1MHz. To provision a voice-grade analog circuit, bandwidth-limiting filters are put on that circuit to filter out all frequencies above 4,000Hz. That's why analog circuits can conduct only fairly low-speed data communications. The maximum data rate over an analog facility is 33.6Kbps when there are analog loops at either end.

Analog facilities have limited bandwidth, which means they cannot support high-speed data. Another characteristic of analog is that noise is accumulated as the signal traverses the network. As the signal moves across the distance, it loses power and becomes impaired by factors such as moisture in the cable, dirt on a contact, and critters chewing on the cable somewhere in the network. By the time the signal arrives at the amplifier, it is not only attenuated, it is also impaired and noisy. One of the problems with a basic amplifier is that it is a dumb device. All it knows how to do is to add power, so it takes a weak and impaired

signal, adds power to it, and brings it back up to its original power level. But along with an increased signal, the amplifier passes along an increased noise level. So, in an analog network, each time a signal goes through an amplifier, it accumulates noise. After you mix together coffee and cream, you can no longer separate them. The same concept applies in analog networks: After you mix the signal and the noise, you can no longer separate the two, and, as a result, you end up with very high error rates.

DIGITAL TRANSMISSION MEDIA:

Digital transmission is quite different from analog transmission. For one thing, the signal is much simpler. Rather than being a continuously variable wave form, it is a series of discrete pulses, representing one bit and zero bits (see Figure 2.10). Each computer uses a coding scheme that defines what combinations of ones and zeros constitute all the characters in a character set (that is, lowercase letters, uppercase letters, punctuation marks, digits, keyboard control functions).

How the ones and zeros are physically carried through the network depends on whether the network is electrical or optical. In electrical networks, one bit is represented as high voltage, and zero bits are represented as null, or low voltage. In optical networks, one bit is represented by the presence of light, and zero bits are represented by the absence of light. The ones and zeros—the on/off conditions—are carried through the network, and the receiving device repackages the ones and zeros to determine what character is being represented. Because a digital signal is easier to reproduce than an analog signal, we can treat it with a little less care in the network. Rather than use dumb amplifiers, digital networks use regenerative repeaters, also referred to as signal regenerators. As a strong, clean, digital pulse travels over a distance, it loses power, similar to an analog signal. The digital pulse, like an analog signal, is eroded by impairments in the network. But the weakened and impaired signal enters the regenerative repeater, where the repeater examines the signal to determine what was supposed to be a one and what was supposed to be a zero. The repeater regenerates a new signal to pass on to the next point in the network, in essence eliminating noise and thus vastly improving the error rate.

SWITCHING TECHNIQUES:

When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**. Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN). Switching is transparent to the user and does not require any configuration in the home network. It is operated in full duplex mode.

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

There are two popular switching techniques – **circuit switching** and **packet switching.**

Circuit Switching:

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Packet Switching:

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

UNIT – 4 DATA LINK LAYER

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

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

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

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.

FUNCTIONS OF DATA LINK LAYER:

- Framing & Link access: Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- Reliable delivery: Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- Flow control: A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and

frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.

- Error detection: Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- Error correction: Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- Half-Duplex & Full-Duplex: In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

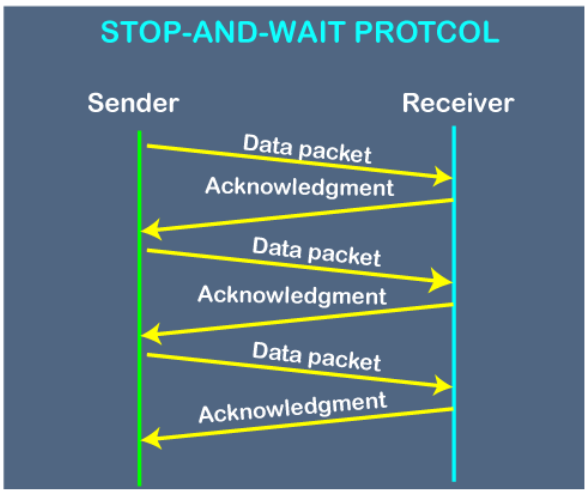
PROTOCOLS – Stop & Wait:

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Working of Stop and Wait protocol:

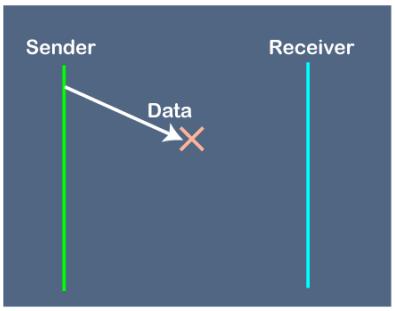


The above figure shows the working of the stop and wait protocol. If there is a sender and receiver, then sender sends the packet and that packet is known as a data packet. The sender will not send the second packet without receiving the acknowledgment of the first packet. The receiver sends the acknowledgment for the data packet that it has received. Once the acknowledgment is received, the sender sends the next packet. This process continues until all the packet are not sent. The main advantage of this protocol is its simplicity but it has some disadvantages also. For example, if there are 1000 data packets to be sent, then all the 1000 packets cannot be sent at a time as in Stop and Wait protocol, one packet is sent at a time.

Disadvantages of Stop and Wait protocol:

The following are the problems associated with a stop and wait protocol:

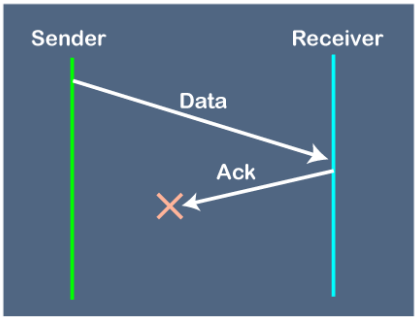
1. Problems occur due to lost data: Suppose the sender sends the data and the data is lost. The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.



In this case, two problems occur:

- Sender waits for an infinite amount of time for an acknowledgment.
- Receiver waits for an infinite amount of time for a data.

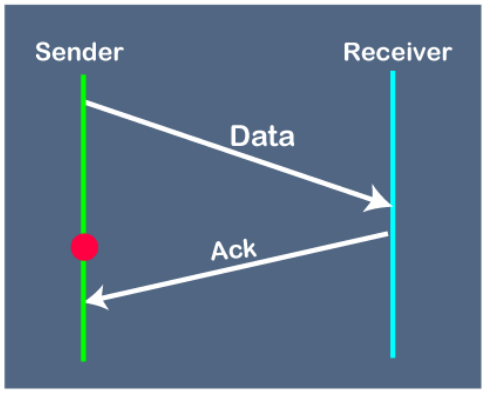
2. Problems occur due to lost acknowledgment: Suppose the sender sends the data and it has also been received by the receiver. On receiving the packet, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next packet as in stop and wait protocol, the next packet cannot be sent until the acknowledgment of the previous packet is received.



In this case, one problem occurs:

- Sender waits for an infinite amount of time for an acknowledgment.

3. Problem due to the delayed data or acknowledgment: Suppose the sender sends the data and it has also been received by the receiver. The receiver then sends the acknowledgment but the acknowledgment is received after the timeout period on the sender's side. As the acknowledgment is received late, so acknowledgment can be wrongly considered as the acknowledgment of some other data packet.



SLIDING WINDOW:

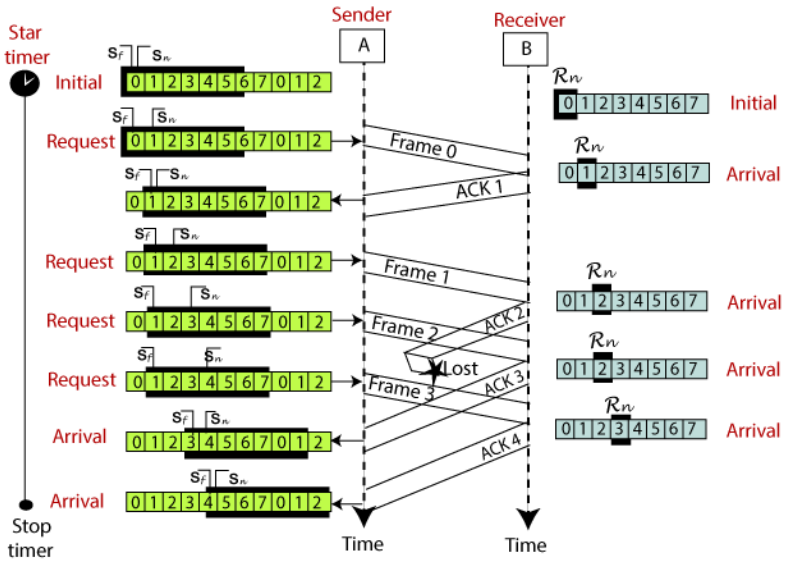
The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol). In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Sliding window protocol has two types:

- Go-Back-N ARQ
- Selective Repeat ARQ

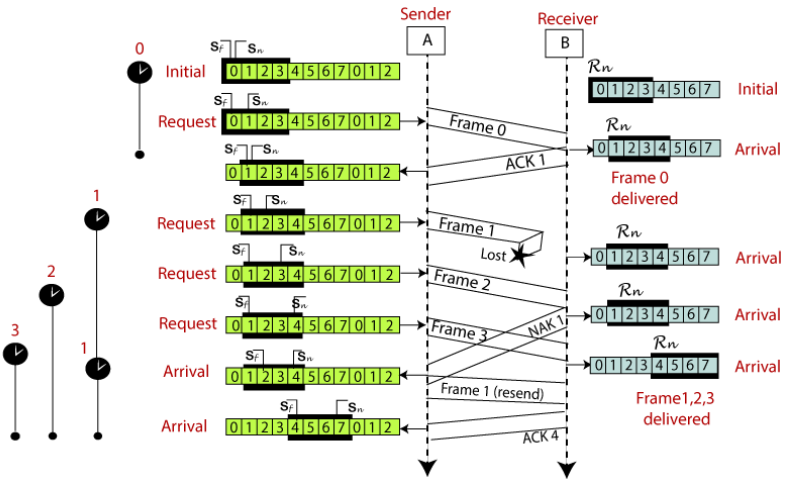
Go-Back-N ARQ:

- Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.
- The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.
- If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.
- The example of Go-Back-N ARQ is shown below in the figure.



Selective Repeat ARQ:

- Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.
- If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame. The design of the Selective Repeat ARQ protocol is shown below.
- The example of the Selective Repeat ARQ protocol is shown below in the figure.



Difference between the Go-Back-N ARQ and Selective Repeat ARQ?

Go-Back-N ARQ	Selective Repeat ARQ

If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.

UNIT – 5 IEEE STANDARDS

802.3, 802.4, 802.5 FAST ETHERNET:

- The Institute of Electrical and Electronics Engineers Standards Association is an operating unit within IEEE that develops global standards in a broad range of industries, including: power and energy.
- Essentially, the IEEE 802 standards help make sure internet services and technologies follow a set of recommended practices so network devices can all work together smoothly. IEEE 802 is divided into 22 parts that cover the physical and data-link aspects of networking.
- IEEE standards are integral to modern infrastructure. Communications networks are one example: It is estimated that 98% of all internet traffic crosses an IEEE 802 standard-based network, some of the most well-known examples being IEEE 802.3 (Ethernet™) and IEEE 802.11 (Wi-Fi™) networks.
- The IEEE 802.3 protocol standards define the physical layer and MAC sublayer of the data link layer of wired Ethernet. IEEE 802.3 uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access at a variety of speeds over a variety of physical media. The IEEE 802.3 standard covers 10 Mbps Ethernet.
- Token Bus (IEEE 802.4) is a standard for implementing token ring over the virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring.
- The IEEE 802.5 standard specifies the characteristics for Token Ring networks. ... Media Token Ring networks use unshielded twisted pair cabling or shielded twisted pair. Access method 802.5 specifies an access method known as token passing. On a Token Ring network, only one computer at a time can transmit data.

FDDI:

- FDDI stands for Fiber Distributed Data Interface. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run up to 200 km (124 miles). The FDDI convention is based on the token ring protocol.
- In expansion to being expansive geographically, an FDDI neighbourhood region arranges can support thousands of clients. FDDI is habitually utilized on the spine for a Wide Area Network (WAN).
- An FDDI network contains two token rings, one for possible backup in case the essential ring falls flat.
  The primary ring offers up to 100 Mbps capacity. In case the secondary ring isn't required for backup, it can also carry information, amplifying capacity to 200 Mbps. The single ring can amplify the most extreme remove; a double ring can expand 100 km (62 miles).

Characteristics of FDDI:

- FDDI gives 100 Mbps of information throughput.
- FDDI incorporates two interfaces.
- It is utilized to associate the equipment to the ring over long distances.
- FDDI could be a LAN with Station Management.
- Allows all stations to have broken even with the sum of time to transmit information.
- FDDI defines two classes of traffic viz. synchronous and asynchronous.

Advantages of FDDI:

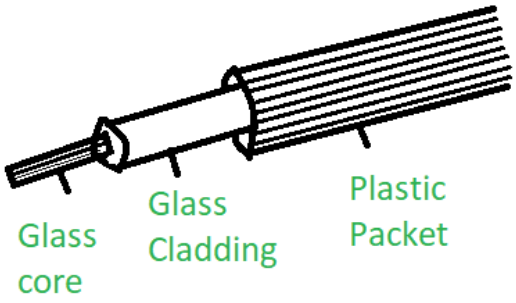
- Fiber optic cables transmit signals over more noteworthy separations of approximately 200 km.
- It is conceivable to supply the need to the work stations associated within the chain. Consequently, based on the prerequisite a few stations are bypassed to supply speedier benefit to the rest.
- FDDI employments different tokens to make strides organize speed.
- It offers a higher transmission capacity (up to 250 Gbps). Thus, it can handle information rates up to 100 Mbps.
- It offers tall security because it is troublesome to spy on the fiber-optic link.
- Fiber optic cable does not break as effectively as other sorts of cables.

Disadvantages of FDDI:

- FDDI is complex. Thus, establishment and support require an incredible bargain of expertise.
- FDDI is expensive. Typically, since fiber optic cable, connectors and concentrators are exceptionally costly.

FIBER OPTICS:

In **Optical Fiber** is a cylindrical fiber of glass which is hair thin size or any transparent dielectric medium. The fiber which is used for optical communication is waveguides made of transparent dielectrics.



Main element of Fiber Optics:

- **Core:** It is the central tube of very thin size made of optically transparent dielectric medium and carries the light transmitter to receiver and the core diameter may vary from about 5um to 100 um.
- **Cladding:** It is outer optical material surrounding the core having reflecting index lower than core and cladding helps to keep the light within the core throughout the phenomena of total internal reflection.
- **Buffer Coating:** It is a plastic coating that protects the fiber made of silicon rubber. The typical diameter of the fiber after the coating is 250-300 um.

UNIT – 6 NETWORK LAYER:

- The Network Layer is the third layer of the OSI model. It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses. It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

- Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.

- Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

ROUTING ALGORITHM:

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.

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

INTER NETWORKING:

The term Internetworking means interconnection i.e., interconnecting two or more computers. Inter means between and networking means the exchange of information or data among multiple connected devices. Internetworking means connecting two or more computer networks using devices like routers, gateways, modem, RJ-45 connector, bridge, etc. It provides a universal communication service. There are many types of physical networks like Ethernet, FDDI (Fiber Distributed Data Interface), ATM (Asynchronous Transfer Mode).

Some terms and concepts of internetworking are given below:

1. WWW (World Wide Web**)**:
    - Invented by Sir Tim Berners-Lee in 1989
    - Collection of web pages or web sites found on network of computers
    - Allow users to access web pages or documents on the net using URL (Uniform Resource Locators)
    - Allow people to share their work and documents through social networking sites, blogs, etc.
    - Web pages are formatted in HTML (Hypertext Markup Language)
    - HTTP (Hypertext Transfer Protocol) allows web pages, documents to be requested and transmitted over the Internet
    - Web servers are computers where web pages are stored and accessed by user's HTTP via internet
    - Faster communication, social networking, etc.

2. **Telnet**:

- Developed in 1969
- Stands for teletype network
- The protocol used to establish a virtual connection for text-based communication between two machines
- Follows TCP (Transmission Control Protocol) / IP (Internet Protocol) for accessing remote computers
- Protocol for remote login
- Overlapped by SSH (Security Shell) because of security issues
- Uses for modification, control over server, running various programs, supports user authentication, etc.

3. Web Browser and Web **Server**:
    - Web Browser:
        - Allows the user to access information or web pages on WWW (World Wide Web)
        - Commonly referred to as a Browser
        - Converts or translate the content of web pages and websites into human-readable content
        - Used in devices like laptops, smartphones, computers, etc.
        - Examples: Internet Explorer, Mozilla Firefox, Google chrome
        - Supports secure HTTP (Hypertext Transfer Protocol), a combination of HTML (Hypertext Markup Language) AND XHTML (Extensible Hypertext Markup Language), FTP (File Transfer Protocol)
    - Web Server:
        - A computer that runs websites
        - Uses HTTP (Hypertext Transfer Protocol) for intercommunication
        - Allows users to have access to web pages contain HTML (HyperText Markup Language) documents, includes images style sheets, etc.
        - Supports server-side scripting using ASP (Active Server Pages), PHP (Hypertext Pre-processor), or other scripting languages

4. Web Site, Web Pages and Web **Addresses**:
    - Web Site:
        - Collection of interlinked web pages identified by the common domain name
        - Examples: google.com, flipkart.com, facebook.com, etc.
        - Created and maintained by the organization, individual, group, etc.
        - It can be accessed on devices like smartphones, laptops, tablets, etc.
        - Also known as web presence
        - Stored and hosted on web servers
    - Web page:
        - Set of data or information provided by a website in a web browser identified by URL (Uniform Resource Locator)
        - Information or documents are written in HTML (HyperText Markup Language) or XHTML (Extensible HyperText Markup Language)
        - Displayed using a web browser on devices like mobile, computer, etc.
        - Easy to create and maintain
    - Web Address:

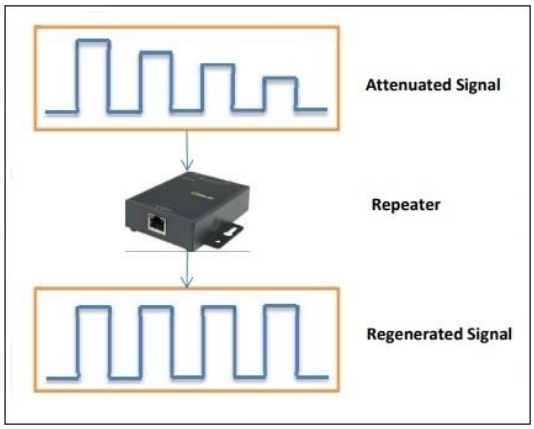
- Developed by Tim Berners-Lee in 1994 and the Internet Engineering Task Force (IETF)
- Referred to as URL (Uniform or Universal Resource Locator) or domain name
- Address of a website or document or other resources on the WWW (World Wide Web)
- Sample URL: http://www.google.com
- Uses HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) Protocol
- Makes accessing to a website very easy for users.

5. Web **Hosting**:

- Type of Internet Hosting Service
- Allows individuals and organizations to develop a web site or web page and host/post on a web server
- Wed host provides space to their users, store web pages of their websites and post them on web servers connected to the Internet
- Some types of web hosting services: Free hosting, Virtual or Shared Hosting, dedicated hosting, Co-location hosting, cloud hosting, clustered hosting, etc.
- Some Web Hosting software: Apache, Windows Server, etc.

FAMILIARIZATION FOR REPEATORS:

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters. A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.



Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at

certain intervals. Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

Advantages of Repeaters:

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don't require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Disadvantages of Repeaters:

- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

HUBS:

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

Types of Hubs:

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

Advantages of Hub:

- It provides support for different types of Network Media.
- It can be used by anyone as it is very cheap.

- It can easily connect many different media types.
- The use of a hub does not impact on the network performance.
- Additionally, it can expand the total distance of the network.

Disadvantages of Hub:

- It has no ability to choose the best path of the network.
- It does not include mechanisms such as collision detection.
- It does not operate in full-duplex mode and cannot be divided into the Segment.
- It cannot reduce the network traffic as it has no mechanism.
- It is not able to filter the information as it transmits packets to all the connected segments.
- Furthermore, it is not capable of connecting various network architectures like a ring, token, and ethernet, and more.

SWITCH:

A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.

BRIDGE:

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

Types of Bridges:

- **Transparent Bridges: -** These are the bridge in which the stations are completely unaware of the bridge's existence i.e., whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e., bridge forwarding and bridge learning.
- **Source Routing Bridges: -** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

ROUTERS:

A router is basically a device or a hardware which is responsible for receiving, analyzing and forwarding the data packets to other networks. A router actually determines the destination or the target IP address of the packet and thus the best way for transferring the packet is determined by the help of forwarding tables and headers.

The forwarding of the data packet is done from one router to the other which basically forms a network (example: internet) until it reaches the final target node. A router is mainly used in the local area network (LAN) and wide area network (WAN) domain. The data is transferred across the network by using the routing protocols. It is much more costly in comparison to other network devices like hub, switch etc.
Some of the companies that develop routers are D-Link, Cisco, Nortel etc.

GATEWAYS:

A gateway is basically a device or a hardware which acts like a "gate" among the networks. Thus, it can also be defined as a node which acts as an entrance for the other nodes in the network. It is also responsible for enabling the traffic flow within the network. Gateway uses more than one protocol for communication thus its activities are much more complex than a switch or a router.

So, a gateway is basically a device that is used for the communication among the networks which have a different set of protocols and is responsible for the conversion of one protocol into the other. For any kind of workplace, the gateway is a computer system which is responsible for routing the traffic from the main workstation to outside network. For homes, it is responsible for giving the access to the internet thus acting as an internet service provider.

UNIT – 7 TRANSPORT LAYER

- The transport layer is a 4^{th} layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
- The transport layer protocols are implemented in the end systems but not in the network routers.
- A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.

- All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.
- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.

Functions of transport layer:

- **Service Point Addressing:** The system can run various programs at the equivalent time. For this reason, the header, therefore, must contain a type of address known as service point address or port. The Network layer is taken as each packet to the correct computer, whereas the transport layer receives the entire message to restore the process on that computer.
- **Segmentation and reassembly:** The message is split into several packets. Each packet has its sequence number. The transport layer reassembles the message correctly according to the order number and identifies those lost.
- **Connection Control:** This layer can be connection-oriented or connectionless. The connectionless transport layer treats each packet as independent and produces it to the destination. But, the connection-oriented transport layer first makes the connection and then provides the respective data.
- **Flow Control:** It is also responsible for flow control implemented end to end instead of across an individual link.
- **Error Control:** The transport layer can support error control. The error control at the transport layer is implemented end to end instead of across an individual link. Error correction is frequently completed by retransmission.

Services provided by the Transport Layer:

The services provided by the transport layer protocols can be divided into five categories:

End-to-end delivery: The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Addressing: According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case,

addressing is provided by the transport layer.The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity. The transport layer protocols need to know which upper-layer protocols are communicating.

Reliable delivery: The transport layer provides reliability services by retransmitting the lost and damaged packets. **The reliable delivery has four aspects:**

- **Error control:** The primary role of reliability is Error Control. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- **Sequence control:** The second aspect of the reliability is sequence control which is implemented at the transport layer. On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.
- **Loss control:** Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.
- **Duplication control:** Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow control: Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing: The transport layer uses the multiplexing to improve transmission efficiency. Multiplexing can occur in two ways:

- Upward multiplexing: Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.
- Downward multiplexing: Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the

transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

SERVICE PRIMITIVE:

Service generally includes set of various primitives. A primitive simply means Operations. A Service is specified by set of primitives that are available and given to user or other various entities to access the service. All these primitives simply tell the service to perform some action or to report on action that is taken by peer entity. Each of the protocol that communicates in layered architecture also communicates in peer-to-peer manner with some of its remote protocol entity.
Primitives are called calling functions between the layers that are used to manage communication among the adjacent protocol layers i.e., among the same communication node. The set of primitives that are available generally depends upon the nature of the service that is being provided.

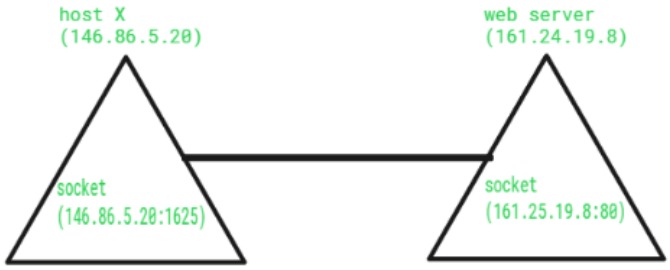
There are five types of service primitives:

- **LISTEN:** When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.
- **CONNECT:** It connects the server by establishing a connection. Response is awaited.
- **RECIEVE:** Then the RECIEVE call blocks the server.
- **SEND:** Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.
- **DISCONNECT:** This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

SOCKETS:

- A socket is one endpoint of a two-way communication link between two programs running on the network. The socket mechanism provides a means of inter-process communication (IPC) by establishing named contact points between which the communication take place.
- Like 'Pipe' is used to create pipes and sockets is created using 'socket' system call. The socket provides bidirectional FIFO Communication facility over the network. A socket connecting to the network is created at each end of the communication. Each socket has a specific address. This address is composed of an IP address and a port number.

- Socket are generally employed in client server applications. The server creates a socket, attaches it to a network port address then waits for the client to contact it. The client creates a socket and then attempts to connect to the server socket. When the connection is established, transfer of data takes place.



Types of Sockets:
There are two types of Sockets: the datagram socket and the stream socket.

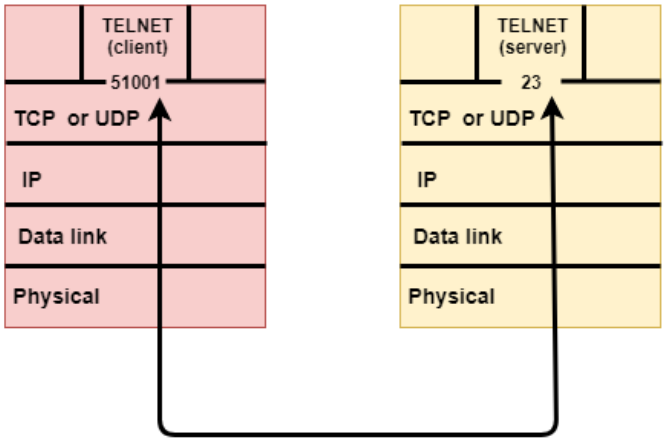
- Datagram Socket: This is a type of network which has connection less point for sending and receiving packets. It is similar to mailbox. The letters (data) posted into the box are collected and delivered (transmitted) to a letterbox (receiving socket).
- Stream Socket: A stream socket is type of interprocess communications socket or network socket which provides a connection-oriented, sequenced, and unique flow of data without record boundaries with well-defined mechanisms for creating and destroying connections and for detecting errors. It is similar to phone. A connection is established between the phones (two ends) and a conversation (transfer of data) takes place.

Function Call	Description
Create()	To create a socket
Bind()	It's a socket identification like a telephone number to contact
Listen()	Ready to receive a connection
Connect()	Ready to act as a sender
Accept()	Confirmation, it is like accepting to receive a call from a sender
Write()	To send data
Read()	To receive data
Close()	To close a connection

ELEMENTS OF TRANSPORT PROTOCOLS:

- The transport layer is represented by two protocols: TCP and UDP.

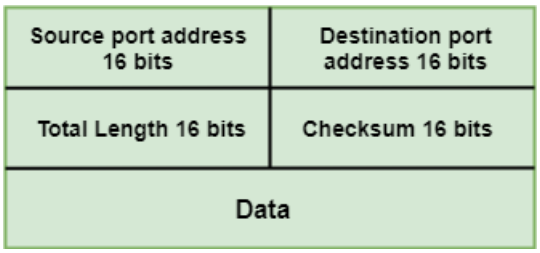
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- Each port is defined by a positive integer address, and it is of 16 bits.



UDP

- UDP stands for User Datagram Protocol.
- UDP is a simple protocol and it provides no sequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format: The user datagram has a 16-byte header which is shown below:



Disadvantages of UDP protocol:

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP:

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

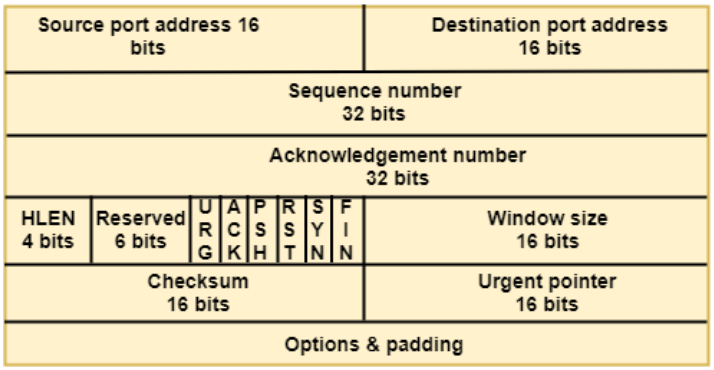
Features Of TCP protocol:

- Stream data transfer: TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- Reliability: TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- Flow Control: When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- Multiplexing: Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- Logical Connections: The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- Full Duplex: TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have

sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:

- Establish a connection between two TCPs.
- Data is exchanged in both the directions.
- The Connection is terminated.

TCP Segment Format:



Differences b/w TCP & UDP:

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retrans

UNIT – 8 BROAD BANK NETWORK

Broadband refers to various high-capacity transmission technologies used to transmit data, voice, and video across long distances and at high speeds. Common mediums of transmission include coaxial cable, fiber optic cable, and radio waves. Broadband is always connected and removes the need for dial-up. Its importance is far-reaching; it allows for

high-quality and quick access to information, teleconferencing, data transmission, and more in various capacities, from healthcare to education to technological development.

ISDN:

ISDN is a circuit-switched telephone network system, but it also provides access to packet-switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. A greater data rate was achieved through channel bonding. Generally, ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.
In the context of the OSI model, ISDN is employed as the network in data-link and physical layers but commonly ISDN is often limited to usage to Q.931 and related protocols. These protocols introduced in 1986 are a set of signalling protocols establishing and breaking circuit-switched connections, and for advanced calling features for the user. ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group videoconferencing systems.

Principle of ISDN:
The ISDN works based on the standards defined by ITU-T (formerly CCITT). The Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. The various principles of ISDN as per ITU-T recommendation are:

- To support switched and non-switched applications
- To support voice and non-voice applications
- Reliance on 64-kbps connections
- Intelligence in the network
- Layered protocol architecture
- Variety of configurations

ATM:

Why ATM networks?

- Driven by the integration of services and performance requirements of both telephony and data networking: “broadband integrated service vision” (B-ISON).
- Telephone networks support a single quality of service and are expensive to boot.
- Internet supports no quality of service but is flexible and cheap.
- ATM networks were meant to support a range of service qualities at a reasonable cost- intended to subsume both the telephone network and the Internet.

It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. *Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.
Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus, it can carry multiple types of traffic with **end-to-end** quality of service. ATM is independent of a transmission medium; they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use "Packet" or "cell" Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

ATM Applications:

- **ATM WANs –**
  It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.
- **Multimedia virtual private networks and managed services –**
  It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.
- **Frame relay backbone –**
  Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.
- **Residential broadband networks –**
  ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.
- **Carrier infrastructure for telephone and private line networks –**
  To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

INTRODUCTION TO VSAT:

A very small aperture terminal (VSAT) is a small-sized earth station used in the transmit/receive of data, voice and video signals over a satellite communication network, excluding broadcast television. The satellite sends and receives signals from a ground station computer that acts as a hub for the system.

VSAT (Very Small Aperture Terminal) consists of a terminal with very small dimensions which is able to provide bi-directional communication connectivity.

- Point-to-Point links (SCPC)
- Star Networks (TDMA)
- Point to Multi-Point (Mesh)
- Multi-Point with Multi-Point and Star

Uses of VSATs:

- In narrowband data − e.g., point – of – sale transactions using debit cards or credit cards, RFID data
- In broadband data − e.g., Internet access to remote locations, VoIP
- Mobile communications
- Maritime communication

ADSL:

ADSL stands for Asymmetric Digital Subscriber Line and is a common type of DSL communication technology designed to offer faster speeds and greater bandwidth over traditional dial-up connections. ADSL allows faster transmission and more data to be sent over existing copper telephone lines that are used for landlines when compared to traditional modem lines. The word Asymmetric in ADSL refers to the fact that it uses most of its capacity to transmit signals downstream towards the customer in order to provide faster download speed.

Advantages

- ADSL provides a greater bandwidth.
- ADSL is always ‘on’ and it doesn’t require dialing-up each time thus saving time.
- ADSL provides thirty to forty times faster speed than a dial-up connection.
- The voice quality and the browsing speeds are not affected by the fact that they use the same telephone line for transmission.
- ADSL uses the existing infrastructure, thus lowering the installation costs and making it easy to install.

Disadvantages

- Speed is dependent on the distance between your home (or office) and the ISP’s office, which sometimes results in receiving a rate considerably lower than offered.
- Slower upload speed.
- ADSL is susceptible to interference.
- ADSL is affected by the number of users using the same line in the certain area simultaneously.

UNIT – 9 NETWORK SECURITY

Network Security refers to the measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organisation that handles large amount of data, has a degree of solutions against many cyber threats.

The most basic example of Network Security is password protection where the user of the network oneself chooses. In the recent times, Network Security has become the central topic of cyber security with many organisations inviting applications of people who have

skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as:

```
Users

Locations
Data
Devices
Applications
```

Network Security: Working
The basic principle of network security is protecting huge stored data and network in layers that ensures a bedding of rules and regulations that have to be acknowledged before performing any activity on the data.
These levels are:
1. Physical
2. Technical
3. Administrative
These are explained as following below.

1. Physical Network Security:
   This is the most basic level that includes protecting the data and network though unauthorized personnel from acquiring the control over the confidentiality of the network. These includes external peripherals and routers might be used for cable connections. The same can be achieved by using devices like bio-metric systems.
2. Technical Network Security:
   It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One, protection from the unauthorized users and the other being protection from malicious activities.
3. Administrative Network Security:
   This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done over the infrastructure.

INTRODUCTION TO CRYPTOGRAPHY:

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:**
   Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:**
   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:**
   The creator/sender of information cannot deny his or her intention to send information at later stage.
4. **Authentication:**
   The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

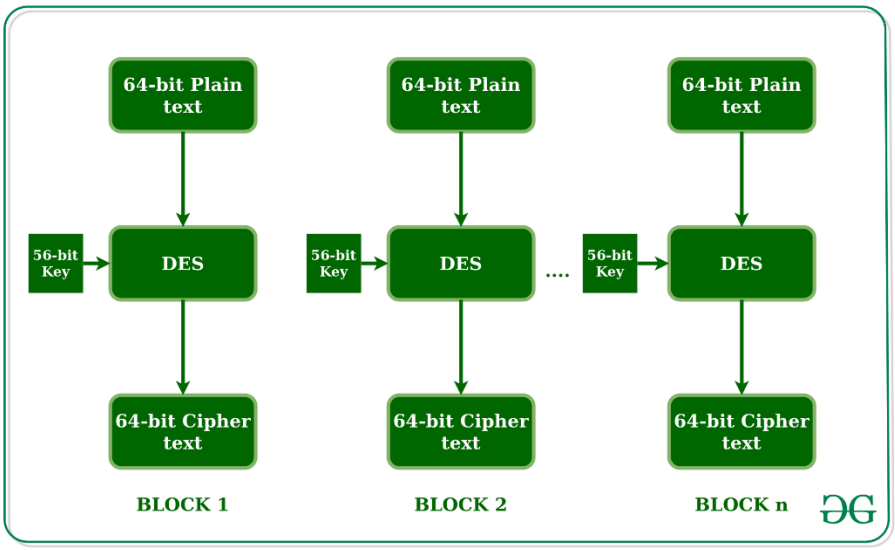
In general there are three types of cryptography:

1. **Symmetric Key Cryptography:**
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).
2. **Hash Functions:**
   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:**
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

DATA ENCRYTION STANDARD:

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on the decline.

DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text goes as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is shown in the figure.



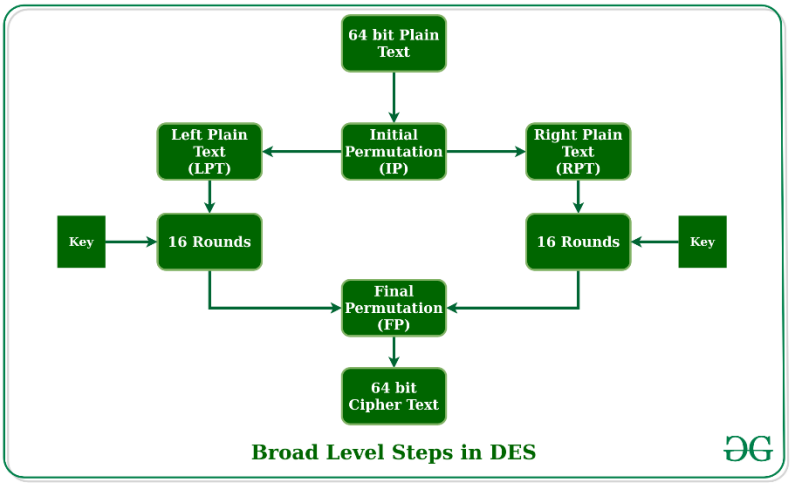
We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discording of every 8th bit of original key

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.
DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

1. In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
2. The initial permutation is performed on plain text.
3. Next, the initial permutation (IP) produces two halves of the permuted block; says Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now each LPT and RPT go through 16 rounds of the encryption process.
5. In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
6. The result of this process produces 64-bit ciphertext.



PUBLIC KEY CRYPTOGRAPHY:

Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as **Public Key Encryption.**

Characteristics of Public Encryption key:

- Public key Encryption is important because it is infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and encryption key.
- Either of the two key (Public and Private key) can be used for encryption with other key used for decryption.
- Due to Public key cryptosystem, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem is RSA (Rivest–Shamir–Ad leman). The difficulty of finding the prime factors of a composite number is the backbone of RSA.

Components of Public Key Encryption:

- **Plain Text:**
  This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **Cipher Text:**
  The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **Encryption Algorithm:**
  The encryption algorithm is used to convert plain text into cipher text.
- **Decryption Algorithm:**
  It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text
- **Public and Private Key:**
  One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption.

Applications of the Public Key Encryption:

- **Encryption/Decryption:**
  Confidentiality can be achieved using Public Key Encryption. In this the Plain text is encrypted using receiver public key. This will ensures that no one other than receiver private key can decrypt the cipher text.
- **Digital signature:**
  Digital signature is for senders authentication purpose. In this sender encrypt the plain text using his own private key. This step will make sure the authentication of the sender because receiver can decrypt the cipher text using senders pubic key only.
- **Key exchange:**
  This algorithm can use in both Key-management and securely transmission of data.

FIREWALLS:

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

Functions of Firewall:

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

Limitations of Firewall:

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected