


ANNAMALAI  **UNIVERSITY**
(Accredited with 'A' Grade by NAAC)

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE

M.Sc. (INFORMATION TECHNOLOGY)

III YEAR – VI SEMESTER

IITT64- COMPUTER NETWORKS

UNIT –I: INTRODUCTION

Computer Network is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network. The aim of the computer network is the sharing of resources among various devices.

Uses

Resource sharing: Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.

Server-Client model: Computer networking is used in the server-client model. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.

Communication medium: Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.

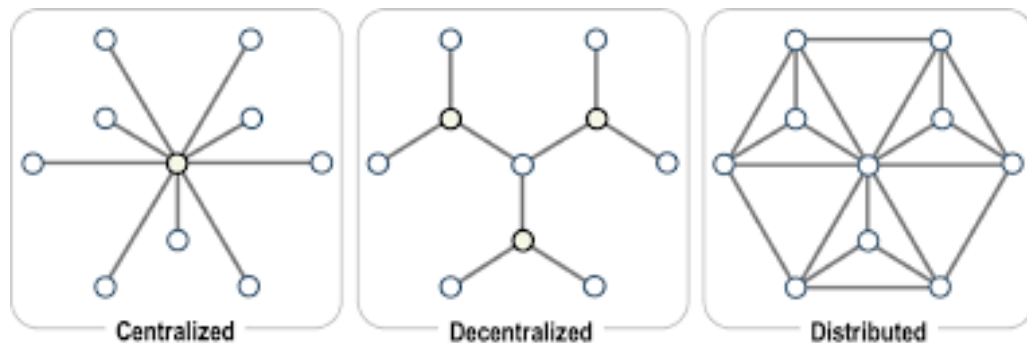
E-commerce: Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Advantages

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

Network Structure

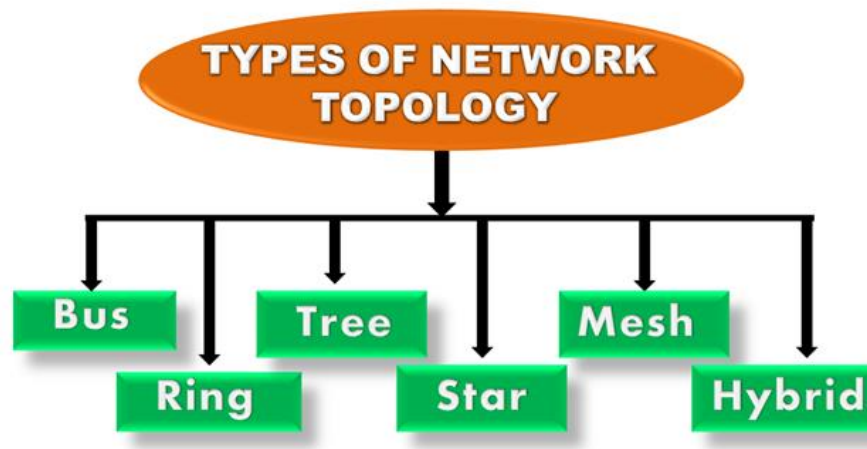
- The network structure is a newer type of organizational structure viewed as less hierarchical (i.e., more "flat"), more decentralized, and more flexible than other structures.
- In a network structure, managers coordinate and control relationships that are both internal and external to the firm.



- The concept underlying the network structure is the social network—a social structure of interactions. Open communication and reliable partners (both internally and externally) are key components of social networks.
- Proponents argue that the network structure is more agile than other structures. Because it is decentralized, a network organization has fewer tiers, a wider span of control, and a bottom-up flow of decision making and ideas.
- A disadvantage of the network structure is that this more fluid structure can lead to more complex relations in the organization.

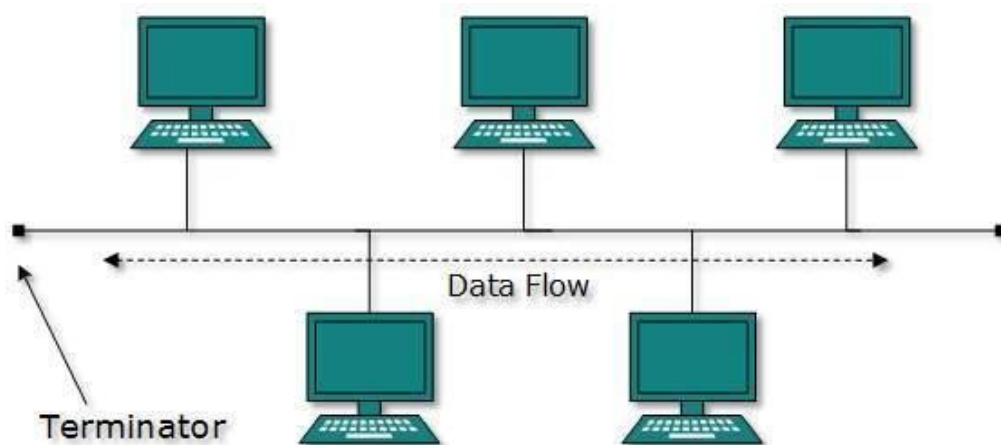
Network Topology

- Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.
- Physical topology is the geometric representation of all the nodes in a network.



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.
- 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 most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).



Advantages

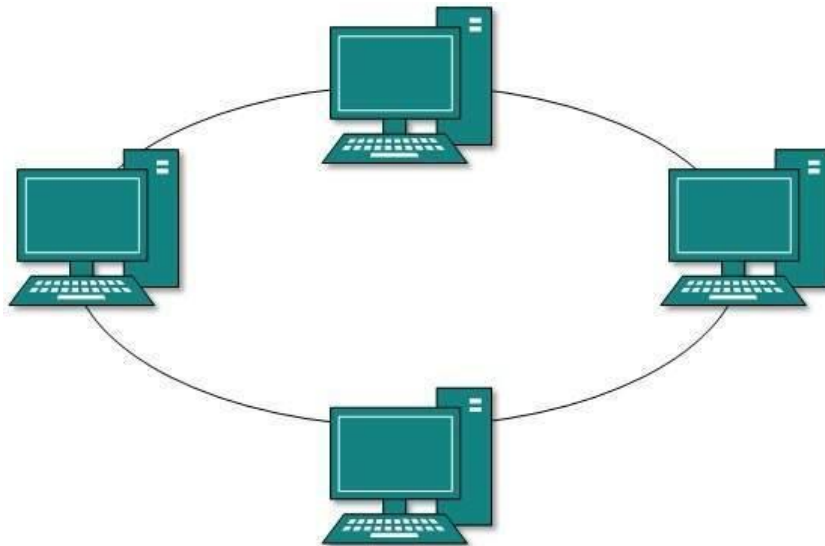
- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to built small networks.

Disadvantages

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

Ring Topology

- 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

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Disadvantages

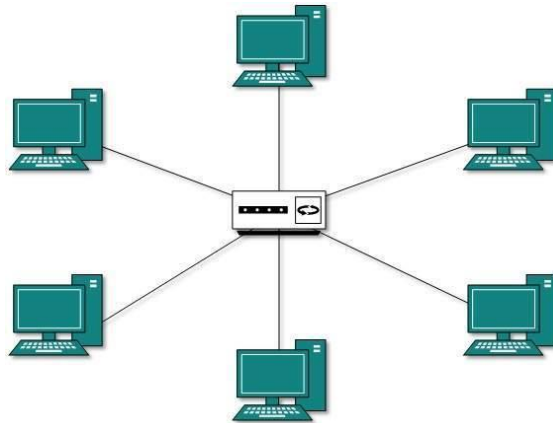
- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

Star Topology

- All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection.
- That is, there exists a point to point connection between hosts and hub.

The hub device can be any of the following:

- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway



Advantages

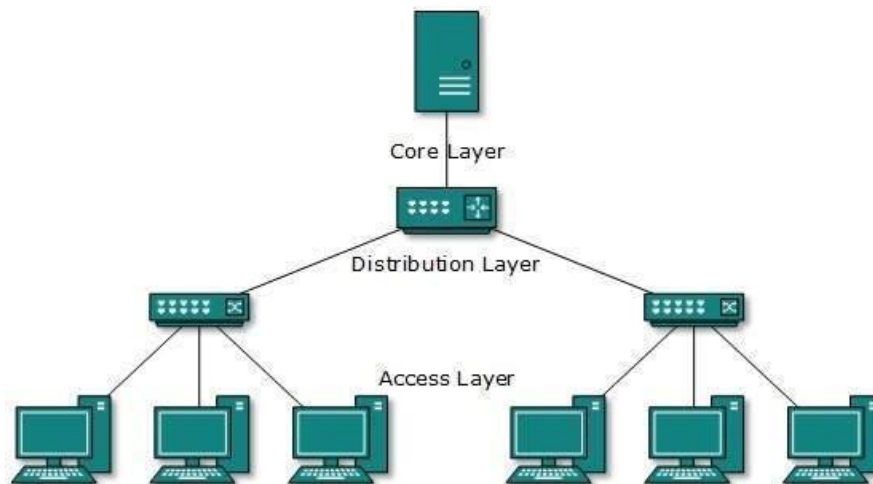
- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub.

Disadvantages

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

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

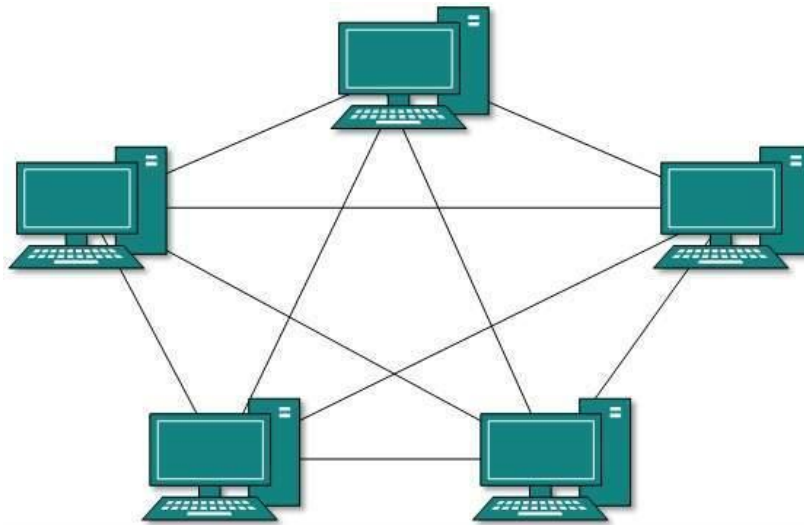
- Support for broadband transmission
- Easily manageable
- Error detection
- Point-to-point wiring

Disadvantages

- Difficult troubleshooting
- Failure
- Reconfiguration difficult
- High Cost

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.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: Number of cables = $(n*(n-1))/2$



Mesh topology is divided into two categories:

- Fully connected mesh topology :Each computer is connected to all the computers available in the network
- Partially connected mesh topology: Not all but certain computers are connected to those computers with which they communicate frequently.

Advantages

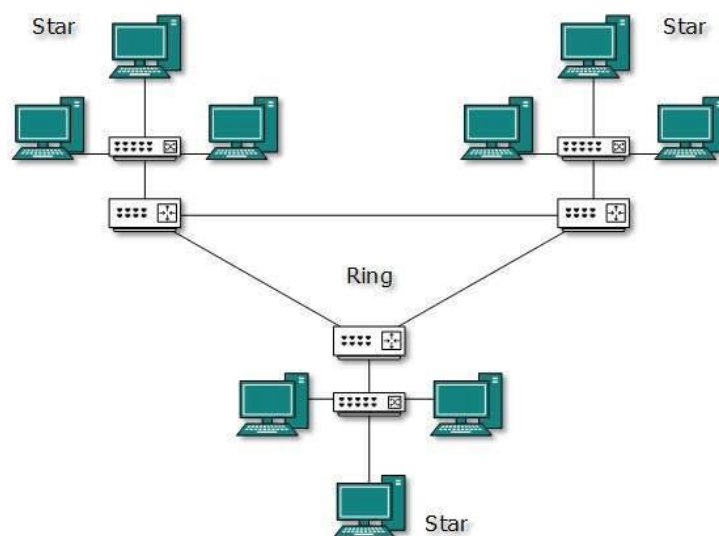
- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages

- Installation and configuration is difficult.
- Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
- Cost of maintenance is high.

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.

Network Design

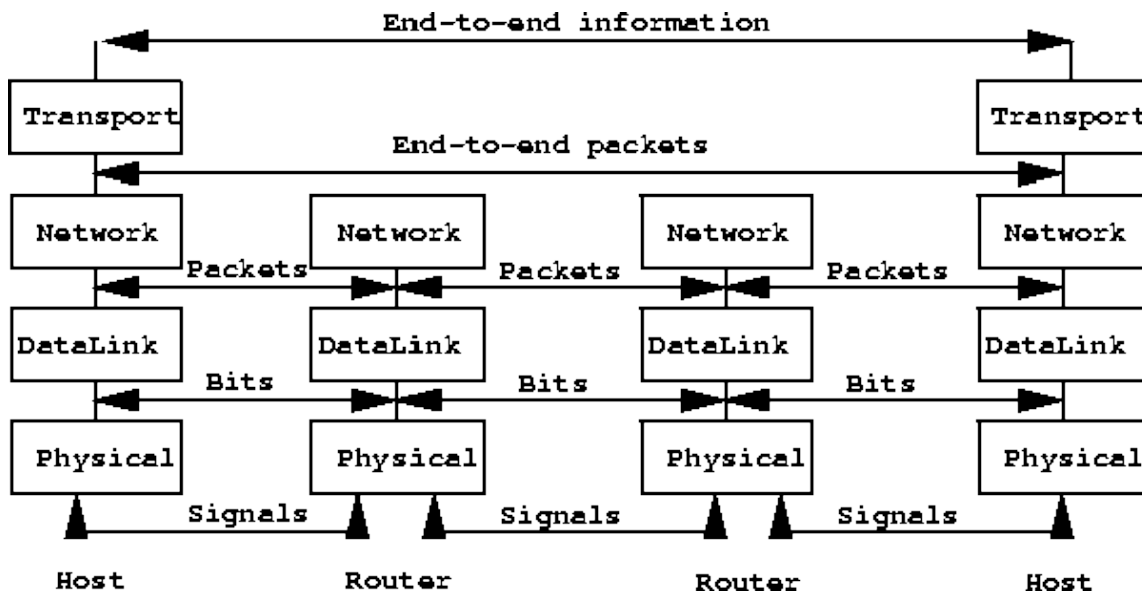
- Network design involves evaluating, understanding and scoping the network to be implemented.
- The whole network design is usually represented as a network diagram that serves as the blueprint for implementing the network physically.
- Typically, network design includes the following:
 - Logical map of the network to be designed
 - Cabling structure
 - Quantity, type and location of network devices (router, switches, servers)
 - IP addressing structure
 - Network security architecture and overall network security processes

Layered Protocols

- A layered protocol architecture provides a conceptual framework for dividing the complex task of exchanging information between remote hosts into simpler tasks.
- Each protocol layer has a narrowly defined responsibility.
- A protocol layer provides a standard interface to the next higher protocol layer.
- Consequently, it hides the details of the underlying physical network infrastructure.

Benefit: The same user-level (application) program can be used over very diverse communication networks.

Example: The same WWW browser can be used when you are connected to the internet via a LAN or a dial-up line.



Design issues for the Layers of Computer Networks

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows:

Reliability

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

Scalability

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

Addressing

At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

Error Control

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

Flow Control

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

Resource Allocation

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

Statistical Multiplexing

It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.

Routing

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

Security

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

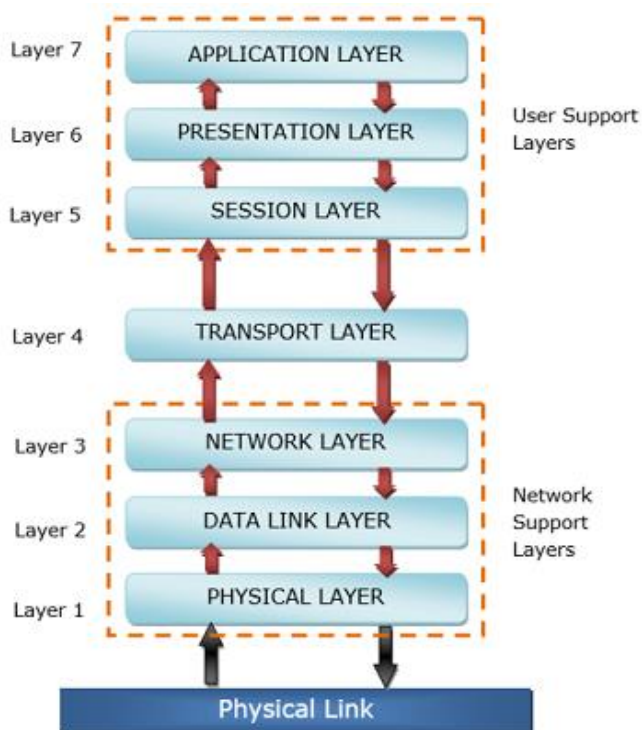
Standards Organizations

Some of the noted standards organizations are

- International Standards Organization (ISO)
- International Telecommunication Union (ITU)
- Institute of Electronics and Electrical Engineers (IEEE)
- American National Standards Institute (ANSI)
- Internet Research Task Force (IETF)
- Electronic Industries Association (EIA)

OSI Reference Model

- OSI or Open System Interconnection model was developed by International Standards Organization (ISO) in 1984.
- It gives a layered networking framework that conceptualizes how communications should be done between heterogeneous systems.
- It has seven interconnected layers.



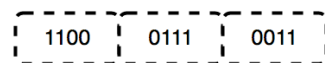
Session layer, presentation layer, and application layer are the user support layers. These layers allow communication among unrelated software in dissimilar environments.

The physical layer, data link layer and the network layer are the network support layers. The layers manage a physical transfer of data from one device to another.

Transport layer links the two groups.

1. Physical Layer (Layer 1) :

- The lowest layer of the OSI reference model is the physical layer.
- It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of bits.
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



2. Data Link Layer (DLL) (Layer 2) :

- The data link layer is responsible for the node to node delivery of the message.
- The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
- Data Link Layer is divided into two sub layers :
 - Logical Link Control (LLC)
 - Media Access Control (MAC)
- The packet received from Network layer is further divided into frames depending on the frame size of NIC (Network Interface Card).
- DLL also encapsulates Sender and Receiver's MAC address in the header.
- The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



3. Network Layer (Layer 3) :

- Network layer works for the transmission of data from one host to the other located in different networks.
- It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP address are placed in the header by the network layer.

4. Transport Layer (Layer 4) :

- Transport layer provides services to application layer and takes services from network layer.
- The data in the transport layer is referred to as *Segments*.
- It is responsible for the End to End Delivery of the complete message.
- The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

Functions: Segmentation and Reassembly, Service point Addressing

Services: Connection Oriented Service and Connection Less Service

• At sender's side:

Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission.

It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

At receiver's side:

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

5. Session Layer (Layer 5) :

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

6. Presentation Layer (Layer 6) :

- Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
- 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.

7. Application Layer (Layer 7) :

- At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications.
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

The main functions of each of the layers are as follows –

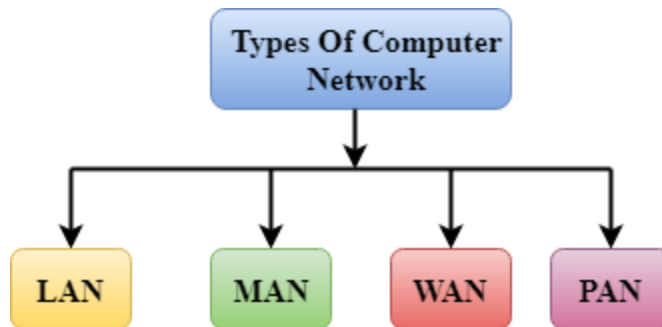
- **Physical Layer** – Its function is to transmit individual bits from one node to another over a physical medium.
- **Data Link Layer** – It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
- **Network Layer** – It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.
- **Transport Layer** –It is responsible for delivery of the entire message from the source host to destination host.

- **Session Layer** – It establishes sessions between users and offers services like dialog control and synchronization.
- **Presentation Layer** – It monitors syntax and semantics of transmitted information through translation, compression, and encryption.
- **Application Layer** – It provides high-level APIs (application program interface) to the users like
 - Network Virtual Terminal
 - FTAM-File transfer access and management
 - Mail Services
 - Directory Services

UNIT –II: COMMUNICATION BETWEEN AND AMONG COMPUTER AND TERMINALS

Networks Classification

A Computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications. A computer network can be categorized by their size. A **computer network** is mainly of **four types**.



a. LAN (Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.



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

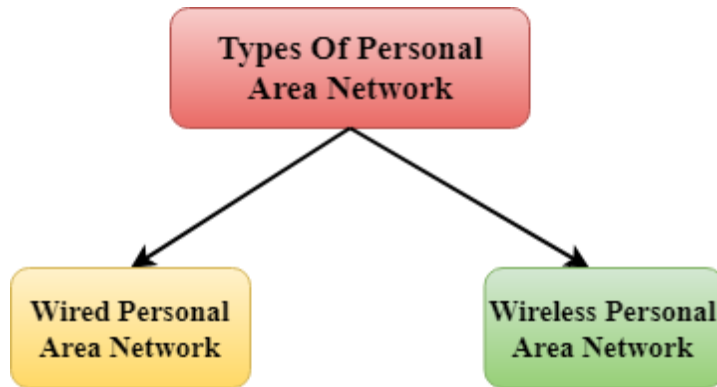
b. PAN (Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.



- Thomas Zimmerman was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of 30 feet.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of PAN.

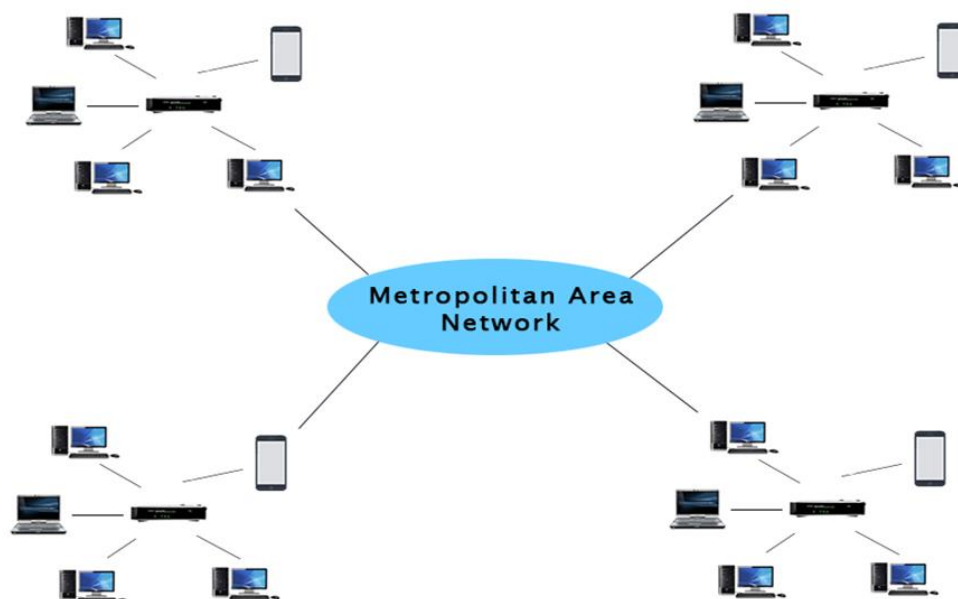


Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

c. MAN (Metropolitan Area Network)

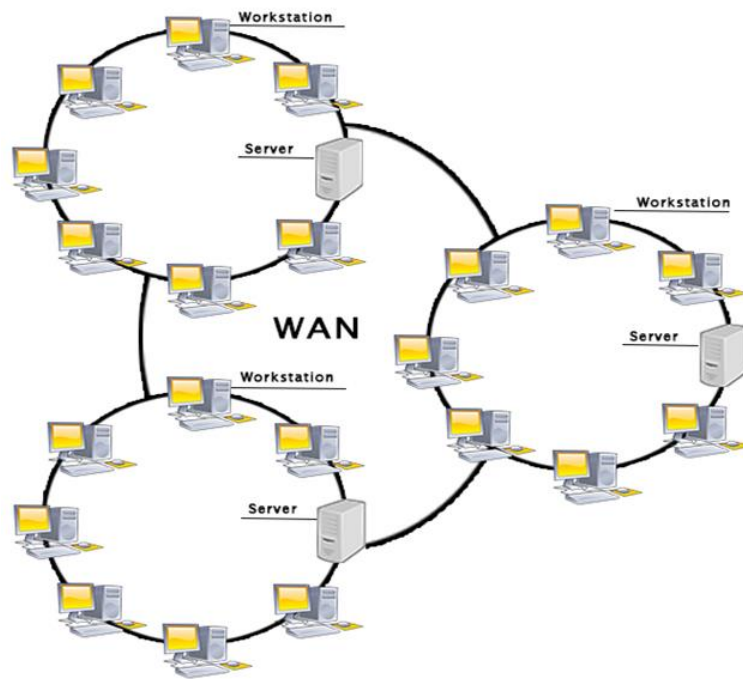
- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.



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

d. WAN (Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.



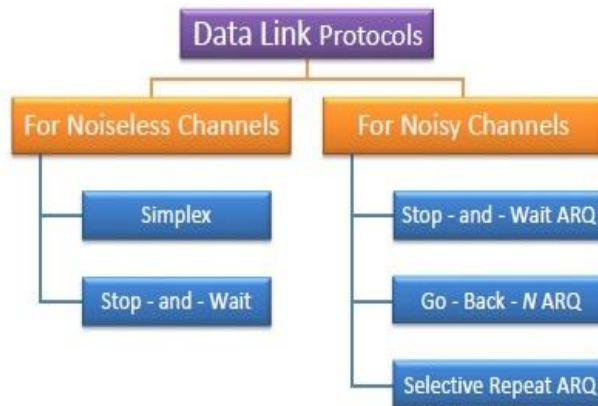
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

Simplex Protocols

The Simplex protocol is data link layer protocol for transmission of frames over computer network. The receiver is assumed to process all incoming data instantly. It does not handle flow control or error control. Since this protocol is totally unrealistic, it is often called Utopian Simplex protocol.

Types of Data Link Protocols

Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



Simplex Protocol

The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel.

i.e. a channel through which transmission can never go wrong. It has distinct procedures for sender and receiver.

The sender simply sends all its data available onto the channel as soon as they are available its buffer. The receiver is assumed to process all incoming data instantly. It is hypothetical since it does not handle flow control or error control.

Stop – and – Wait Protocol

Stop – and – Wait protocol is for noiseless channel too. It provides unidirectional data transmission without any error control facilities. However, it provides for flow control so that a fast sender does not drown a slow receiver. The receiver has a finite buffer size with finite processing speed. The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.

Stop – and – Wait ARQ

Stop – and – wait Automatic Repeat Request (Stop – and – Wait ARQ) is a variation of the above protocol with added error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires or a negative acknowledgement is received, the frame is retransmitted. If a positive acknowledgement is received then the next frame is sent.

Go – Back – N ARQ

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

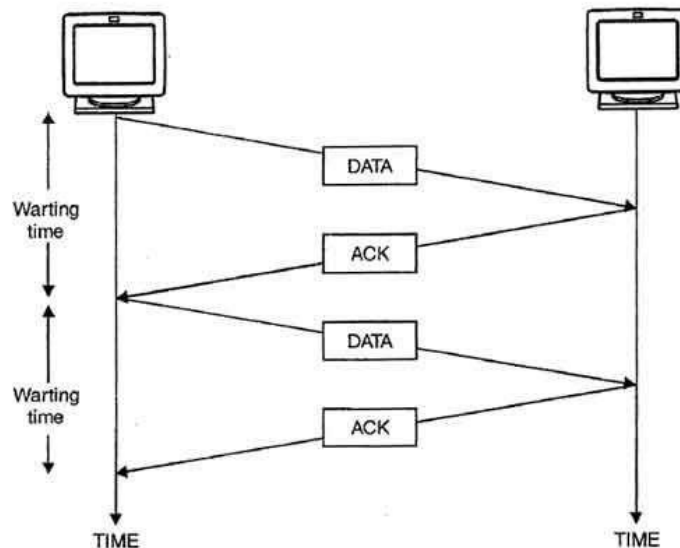
Selective Repeat ARQ

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

Stop and Wait Protocol

- In this method of flow control, the sender sends a single frame to receiver & waits for an acknowledgment.
- The next frame is sent by sender only when acknowledgment of previous frame is received.
- This process of sending a frame & waiting for an acknowledgment continues as long as the sender has data to send.
- To end up the transmission sender transmits end of transmission (EOT) frame.
- The main advantage of stop & wait protocols is its accuracy. Next frame is transmitted only when the first frame is acknowledged. So there is no chance of frame being lost.
- The main disadvantage of this method is that it is inefficient. It makes the transmission process slow. In this method single frame travels from source to destination and single

acknowledgment travels from destination to source. As a result each frame sent and received uses the entire time needed to traverse the link. Moreover, if two devices are distance apart, a lot of time is wasted waiting for ACKs that leads to increase in total transmission time.



Stop & Wait Method.

Characteristics

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop & Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1.

Sender:

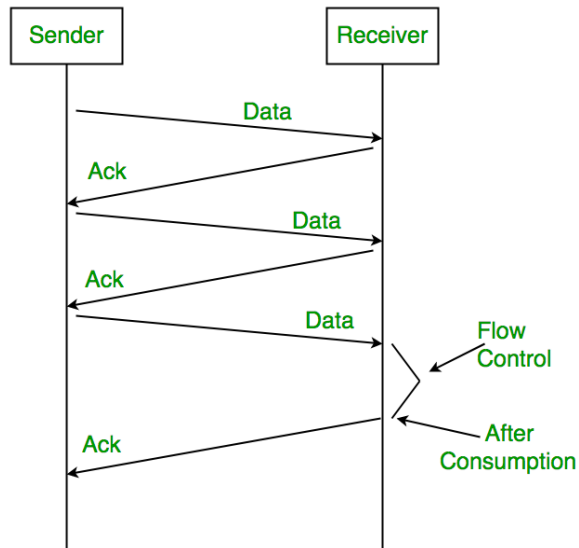
Rule-1) Send one data packet at a time.

Rule-2) Send next packet only after receiving acknowledgement for previous.

Receiver:

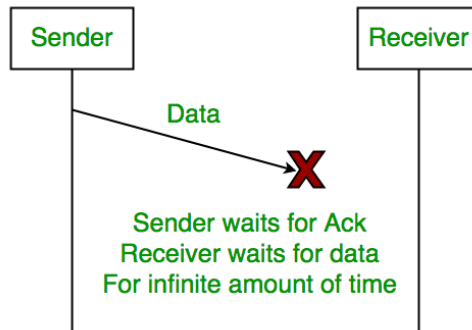
Rule-1) Send acknowledgement after receiving and consuming of data packet.

Rule -2) After consuming packet acknowledgement need to be sent (Flow Control)

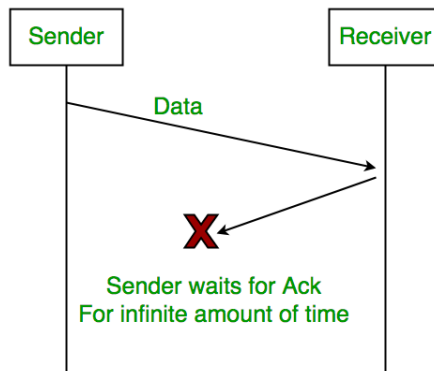


Problems:

1. Lost Data



2. Lost Acknowledgement

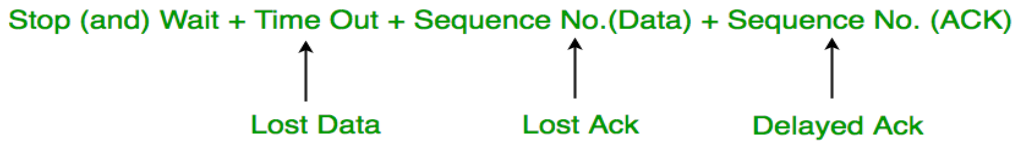


3. Delayed Acknowledgement/Data

After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

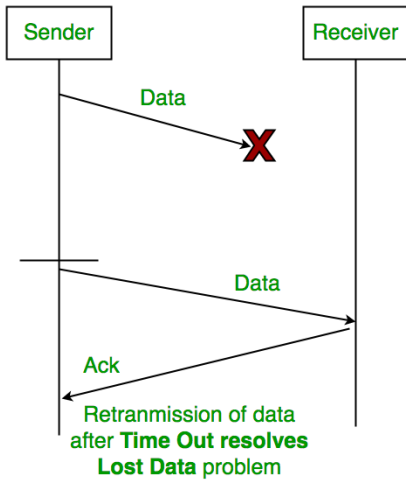
Stop and Wait ARQ (Automatic Repeat Request)

Above 3 problems are resolved by Stop and Wait ARQ that does both error control and flow

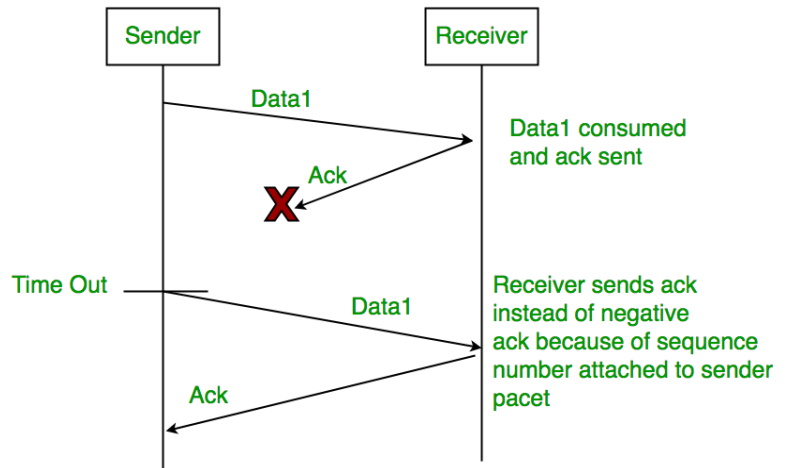


control.

1. Time out:



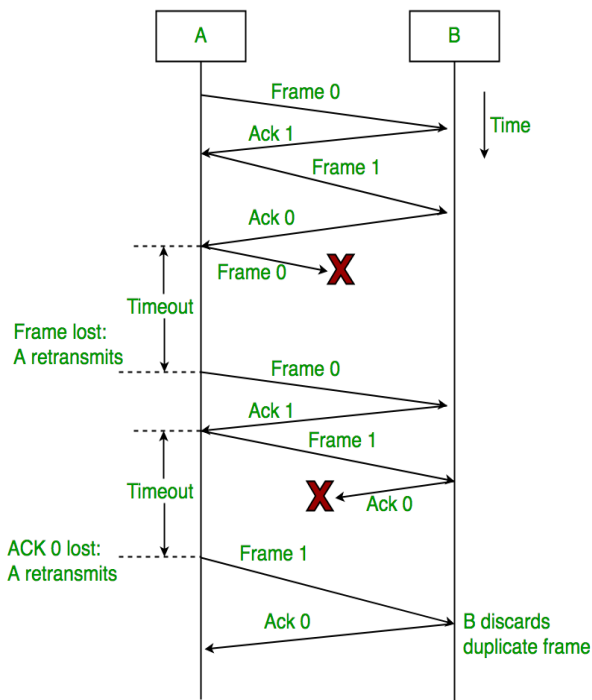
2. Sequence Number (Data)



3. Delayed Acknowledgement

This is resolved by introducing sequence number for acknowledgement also.

Working of Stop and Wait ARQ



➤ Sender A sends a data frame or packet with sequence number 0.

➤ Receiver B, after receiving data frame, sends an acknowledgement with sequence number 1 (sequence number of next expected data frame or packet). There is only one bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.

Characteristics of Stop and Wait ARQ:

- It uses the link between sender and receiver as a half duplex link.
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example for “Closed Loop or connection oriented “ protocols
- It is a special category of SWP where its window size is 1
- Irrespective of the number of packets, the sender using the stop and wait protocol requires only 2 sequence numbers, 0 and 1.

The Stop and Wait ARQ solves three main problems, but it may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high speed connection). To solve this problem, we can send more than one packet at a time with larger sequence numbers.

So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections, but performs badly for distant connections like satellite connection.

Sliding Window Protocol

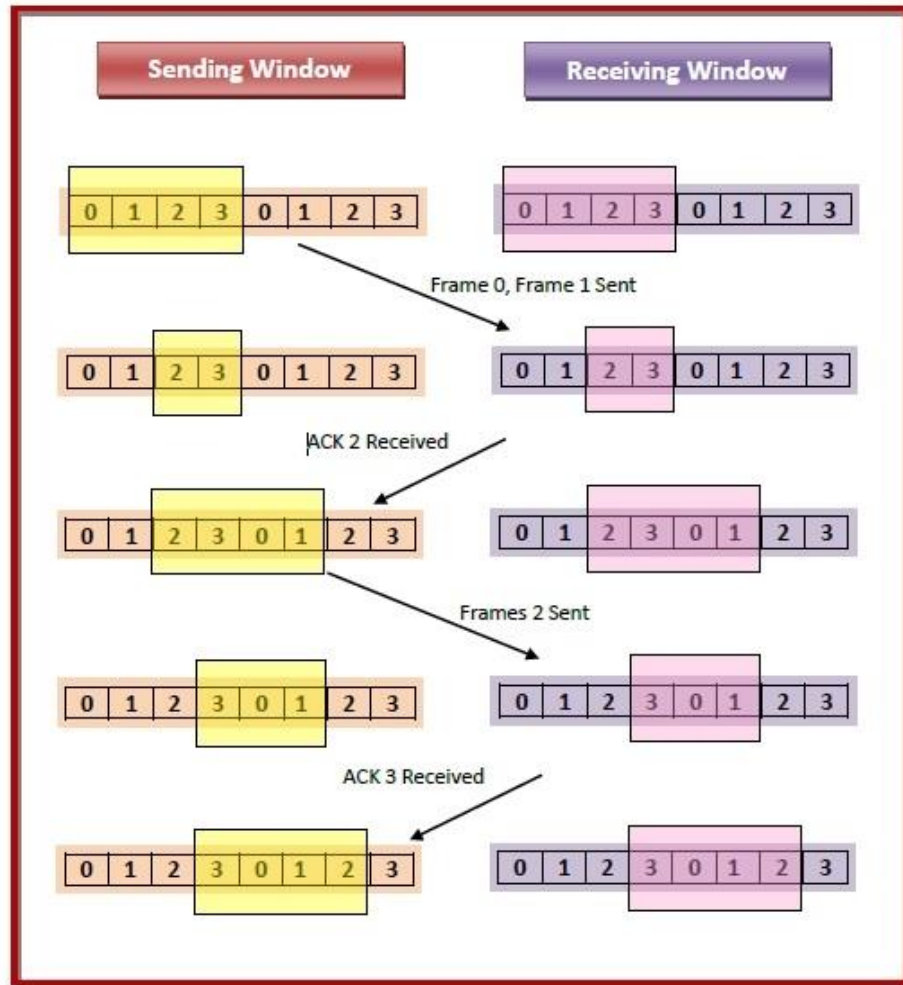
- Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.
- In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

Working Principle

- In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.
- The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n -bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1 . Consequently, the size of the sending window is 2^n-1 . Thus in order to accommodate a sending window size of 2^n-1 , a n -bit sequence number is chosen.
- The sequence numbers are numbered as modulo- n . For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.
- The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

Example

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



Sliding Window Protocol Types



Go - Back - N ARQ

Go - Back - N ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite

number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

Selective Repeat ARQ

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

Protocol Performance

It can be calculated prior to clinical use; however, the necessary information is seldom available. Thus, protocols are frequently used with limited information as to performance. The next best strategy is to base protocol design on available information combined with a thorough understanding of the factors that determine protocol performance. Unfortunately, there is limited information as to these factors and how they interact. The three factors that determine protocol performance:

- Protocol criterion
- Test correlation
- Test performance

Protocol Specification

A user's interest in a protocol lies in what kind of services it provides. Usually this involves interactions with other entities (such as users or programs) in order to get certain functions performed. For example, one user may wish to interact with another (remote) user by performing various functions such as Send Message. How these functions are actually performed by the protocol is not really of concern.

Users, then, can regard the protocol as a black box, to which one gives a series of commands in order to get certain services performed. The description of this machine is termed the service specification. One theorem we may wish to prove about a service specification is that the messages received constitute an initial subsequence of the messages sent (i.e., messages are not delivered in the wrong order, or garbled, nor are messages spontaneously delivered if they were not sent).

In general, the components used to provide the service can also be regarded as black boxes in their own right. In the case of protocols there is always more than one entity interacting (because we are dealing with distributed systems). In order to provide a given service, it is necessary to have several stations (at least one for each physical site) interacting with each other via some transmission machine (see Figure). The pattern of their interactions constitutes the protocol.

This transmission machine is just another level of protocol. Thus we can see a hierarchy of abstract machines developing. In this uses hierarchy, each protocol level makes use of the services provided by the lower level. Within each level, there is an implementation hierarchy where the service is logically implemented by the abstract protocol specification. The protocol is implemented in turn by an actual program. Thus for each protocol level N , the following information must be provided:

- a. A service specification, describing the services provided by the level to the users above, at level $N + 1$.
- b. A protocol specification, describing the interaction of the objects in this level in a precise way (assuming services provided by the level below, level $N - 1$).
- c. A program implementing each station in the level (of course, the program may vary from station to station).

This characterization follows closely the model for open system interconnection being proposed by the International Organization for Standardization

Protocol Verification

In the context of the model introduced in the previous subsection, we say that protocol verification is a formal demonstration that the logical design of the protocol (the interaction of the stations within one layer) satisfies the service specification of that layer. Note that this will depend on the assumed properties (the service specification) of the layer below.

The ultimate task in protocol verification is to demonstrate that an actual program is a valid implementation of the protocol specification. That is, when one has reached a low-enough level of abstraction in the specification, it is possible to take an actual program that purportedly implements the protocol, and show it is correct with respect to the specification. This is no different than traditional program verification.

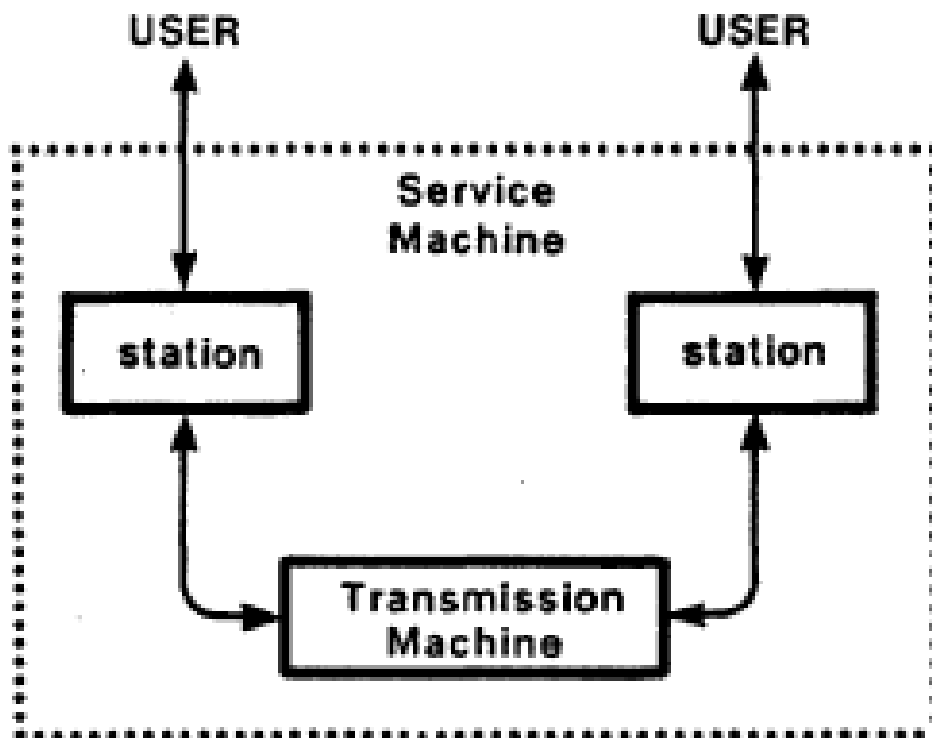


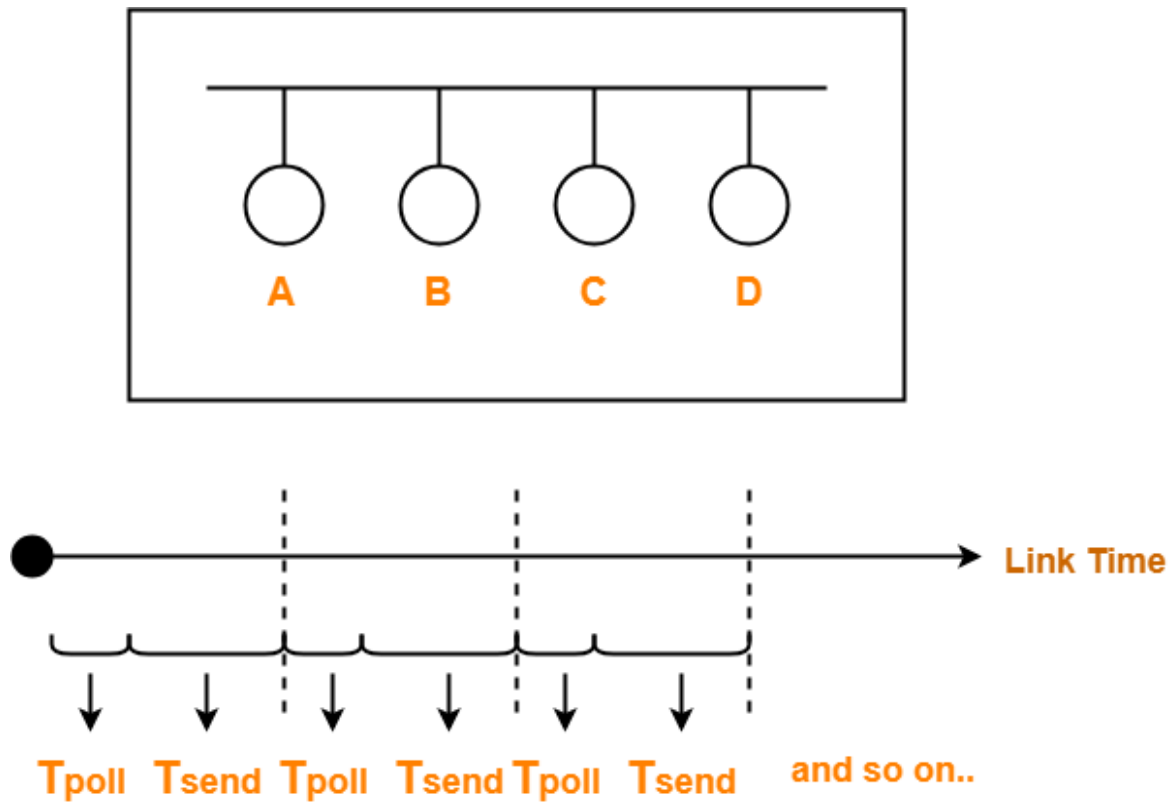
Figure: Internal structure of service machine

In order to gain greater confidence that specifications are suitable for their intended use, it is useful to prove properties of a single specification. For example, we might want to show that the sequence of messages delivered is equal to the sequence of messages sent. Liveness properties such as eventual termination are also often proved for a single specification.

Thus we have three major types of protocol verification problems in each layer of a system:

- 1) Verification of the protocol against its service
- 2) Verification of an implementation against the protocol
- 3) Verification of desired properties of the service, protocol, and program independently.

Polling



Polling Access Control Method

In this access control method,

- A polling is conducted in which all the stations willing to send data participates.
- The polling algorithm chooses one of the stations to send the data.
- The chosen station sends the data to the destination.
- After the chosen station has sent the data, the cycle repeats.

Example-

Here,

- T_{poll} = Time taken for polling
- T_{send} = Time taken for sending the data = Transmission delay + Propagation delay = $T_t + T_p$

Efficiency

$$\text{Efficiency } (\eta) = \text{Useful Time} / \text{Total Time}$$

Useful time = Transmission delay of data packet = T_t

Useless time = Time wasted during polling + Propagation delay of data packet = $T_{\text{poll}} + T_p$

Thus,

$$\text{Efficiency } (\eta) = \frac{T_t}{T_{\text{poll}} + T_t + T_p}$$

Advantages

- Unlike in Time Division Multiplexing, no slot is ever wasted.
- It leads to maximum efficiency and bandwidth utilization.

Disadvantages

- Time is wasted during polling.
- Link sharing is not fair since each station has the equal probability of winning in each round.
- Few stations might starve for sending the data.

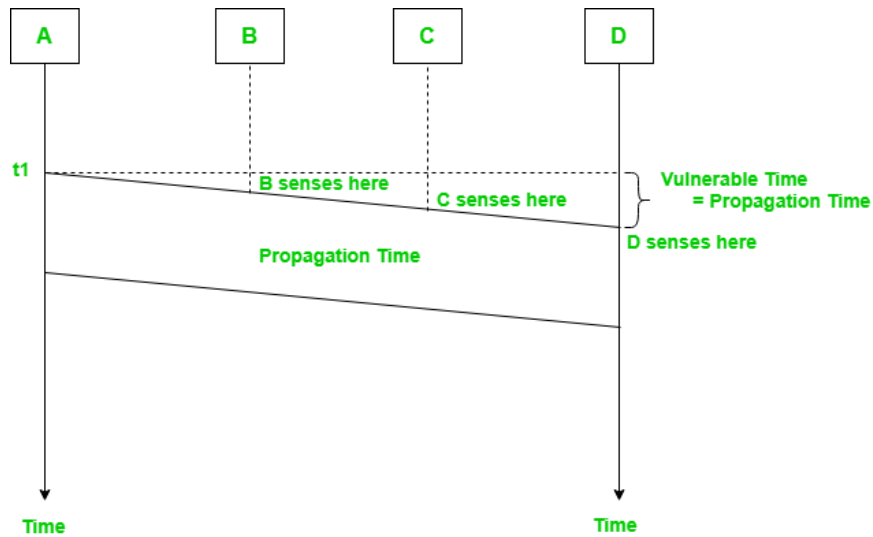
Important Formulas:

- Efficiency (η) = $T_t / (T_{\text{poll}} + T_t + T_p)$
- Effective Bandwidth / Bandwidth Utilization / Throughput = Efficiency(η) x Bandwidth
- Maximum Available Effective Bandwidth = Total number of stations x Bandwidth requirement of 1 station.

Carrier Sense Multiple Access (CSMA)

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station first check the state of the medium before sending.

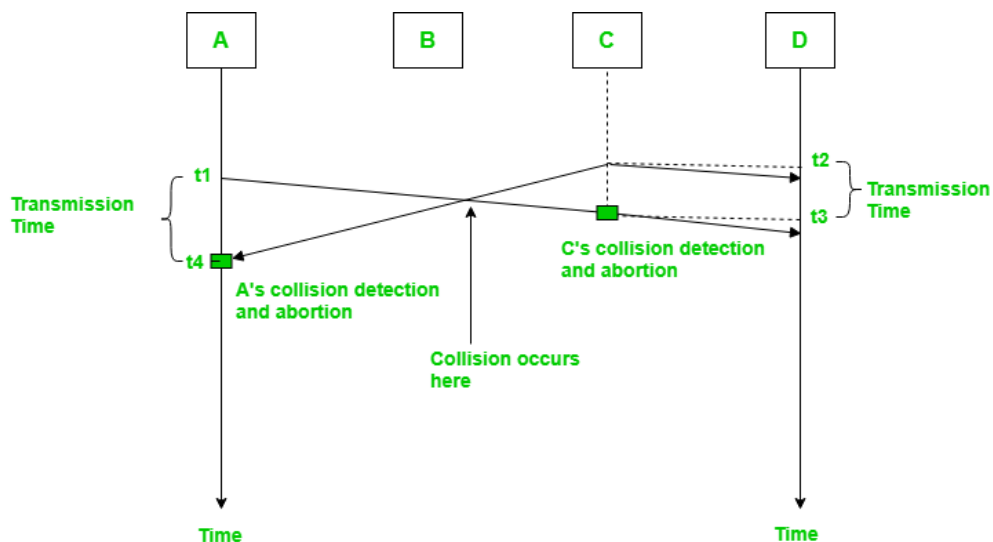
$$\text{Vulnerable Time} = \text{Propagation time (Tp)}$$



Prerequisite – Multiple Access Protocols

1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the station is finished, if not, the frame is sent again.



In the diagram, A starts send the first bit of its frame at t_1 and since C sees the channel idle at t_2 , starts sending its frame at t_2 . C detects A's frame at t_3 and aborts transmission. A detects C's frame at t_4 and aborts its transmission. Transmission time for C's frame is therefore T_{fr} and for A's frame is T_{fr} .

So, the frame transmission time (T_{fr}) should be at least twice the maximum propagation time (T_p). This can be deduced when the two stations involved in collision are maximum distance apart.

Throughput and Efficiency

The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For 1-persistent method throughput is 50% when $G=1$.
- For non-persistent method throughput can go upto 90%.

2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if collision occurs. It can't be used by station to sense collision. Therefore CSMA/CA has been specially designed for wireless networks.

These are three types of strategies:

2. Inter Frame Space (IFS) – When a station finds the channel busy, it waits for a period of time called IFS time. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
3. Contention Window – It is the amount of time divided into slots. A station which is ready to send frames chooses random number of slots as wait time.
4. Acknowledgements – The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

Binary Synchronous Control (BSC)

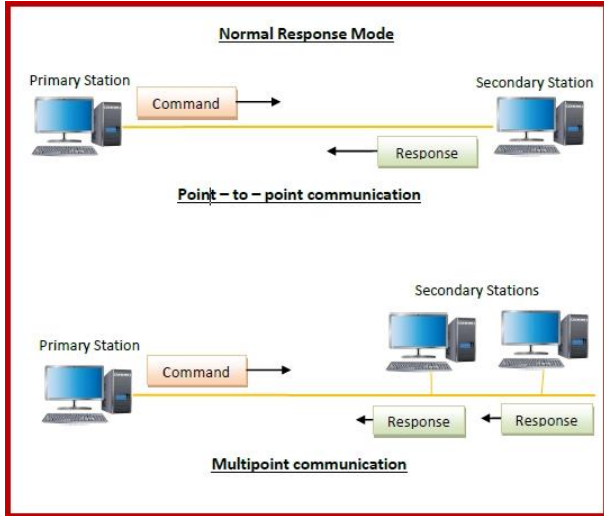
- Binary Synchronous Control (BSC; also known as BISYNC) is a widely-used synchronous, character-oriented protocol devised by IBM in the 1960s for halfduplex communication.
- To synchronize, the transmitter repeatedly sends a SYN character which the receiver looks for. Once the receiver has detected the SYN character, the two stations handshake to confirm that they are synchronized and can start exchanging data. Information is exchanged in character blocks.
- A block starts with a SYN character. SOH marks the beginning of a header which contains additional control information, such as the block sequence number, the address of the transmitter, the address of the receiver, etc. STX and ETX mark the beginning and end of user data, which is an arbitrary sequence of characters. A redundancy check concludes the block.
- Since control characters may also occur in user data, another control character, DLE (Data Link Escape), is used to avoid their being interpreted as control codes. If a control character occurs in user data, it is simply preceded by a DLE character. A literal DLE itself appears as two consecutive DLEs. The receiver treats a DLE as meaning 'accept the next character as literal'.
- Error handling in BSC is fairly simple. If the receiver receives a corrupted block, it returns a NAK block which contains the sequence number of the offending block. The transmitter then retransmits that block. Parity checking is also used on individual characters.

High-level Data Link Control (HDLC)

It is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

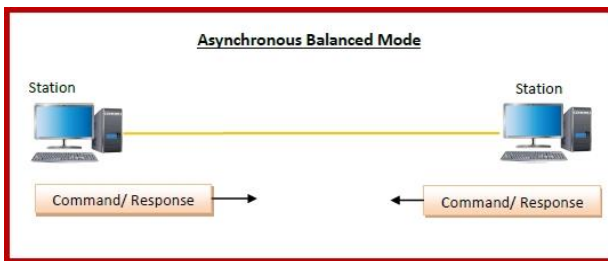
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.



Normal Response Mode (NRM)

Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



Asynchronous Balanced Mode (ABM)

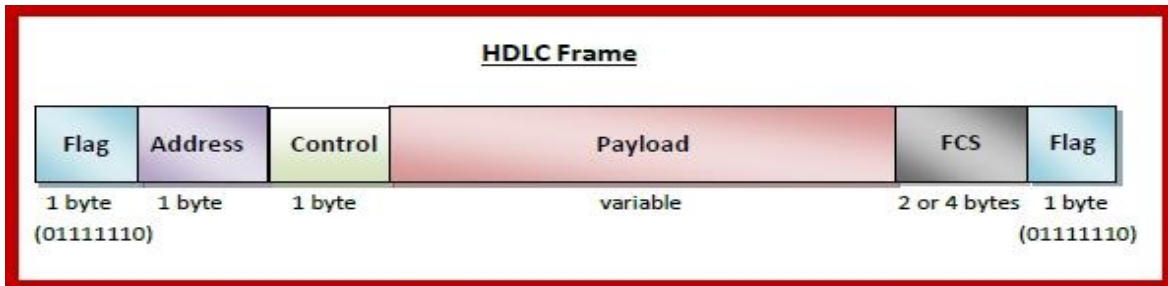
Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.

HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are,

- **Flag** – It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** – It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** – It is 1 or 2 bytes containing flow and error control information.

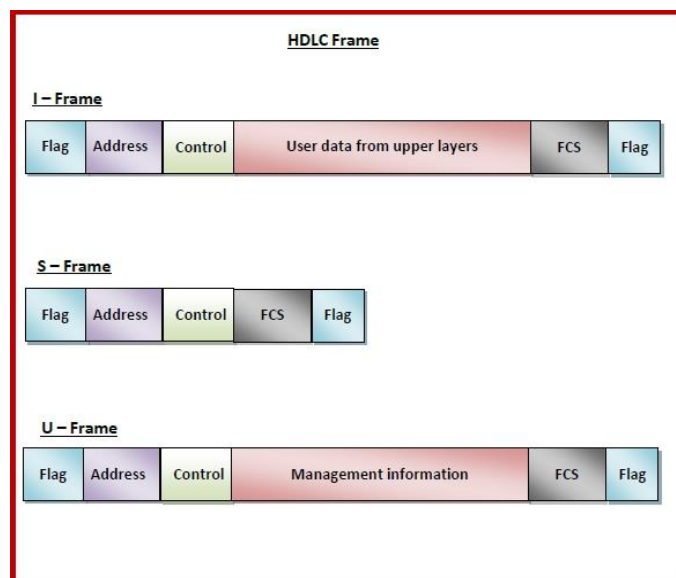
- **Payload** – This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** – It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame –

I-frame – I-frames or **Information frames** carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.



Code	Command
00	RR Receive Ready
01	REJ Reject
10	RNR Receive Not Ready
11	SREJ Selective Reject

S-frame – S-frames or **Supervisory frames** do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.

- **U-frame** – U-frames or **Un-numbered frames** are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11

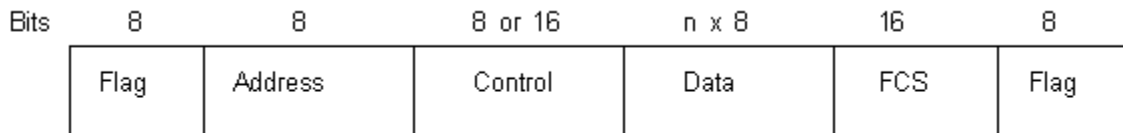
Synchronous Data Link Control (SDLC)

Although a subset of HDLC, SDLC was developed by IBM before HDLC, and was the first link layer protocol based on synchronous, bit-oriented operation. IBM defined SDLC for managing synchronous serially transmitted bits over a data link, and these links can be full/half-duplex, switched or unswitched, point-to-point, point to multipoint or even looped. SDLC is designed for carrying SNA traffic.

- In SDLC, a link station is a logical connection between adjacent nodes.
- Only one Primary Link Station is allowed on an SDLC line.
- A device can be set up as a Primary or a Secondary link station.
- A device configured as a Primary link station can communicate with both PU 2.0 nodes and PU 2.1 nodes (APPN) and controls the secondary devices.
- If the device is set up as a secondary link station then it acts as a PU 2.0 device and can communicate with Front End Processors (FEP), but only communicates with the primary device when the primary allows it.
 - i.e. the primary sets up and tears down the connections and controls the secondaries.

- In APPN configurations the device can support negotiable link stations where XID frames are exchanged to decide which station is to be secondary and which is to be primary.
- A primary station issues commands, controls the link and initiates error-recovery. A device set up as a secondary station can communicate to a FEP, exist with other secondary devices on an SDLC link and exist as a secondary PU 2.0 device.
- SDLC supports line speeds up to 64Kb/s e.g. V.24 (RS-232) at 19.2Kb/s, V.35 (up to 64Kb/s) and X.21.

The following diagram shows the frame format for SDLC, almost identical to HDLC.



SDLC Frame

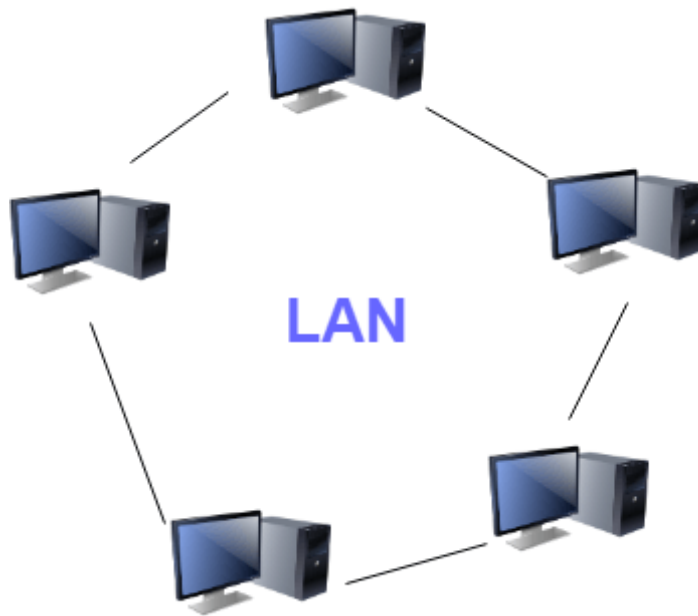
- **Flag** - Begins and ends the error checking procedure with **0x7E** which is **01111110** in binary.
- **Address** - This is only the secondary address since all communication occurs via the single primary device. The address can be an individual, group or broadcast address.
- **Control** - this identifies the frame's function and can be one of the following:
 - ❖ **Information (I)** - contains the Send Sequence Number which is the number of the next frame to be sent, and the Receive Sequence Number which is the number of the next frame expected to be received. The is also a Poll Final Bit (P/F) which performs error checking.
 - ❖ **Supervisory (S)** - this can report on status, ask for and stop transmission and acknowledge **I** frames.
 - ❖ **Unnumbered (U)** - this does not have sequence numbers (hence 'unnumbered'), it can be used to start up secondaries and can sometimes have an Information field.
- **Data** - can contain Path Information Unit (PIU) or Exchange Identification (XID).
- **Frame Check Sequence (FCS)** - this check is carried out on the sending AND receiving of the frame.

UNIT –III: LOCAL AREA NETWORKS

Local Area Network

A Local Area Network (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.

It is a network which consists of less than 5000 interconnected devices across several buildings.



Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.

- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and Ethernet.

LAN Standards

IEEE 802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers. It includes architecture, MAC sub layer, Frame format and Frame types.

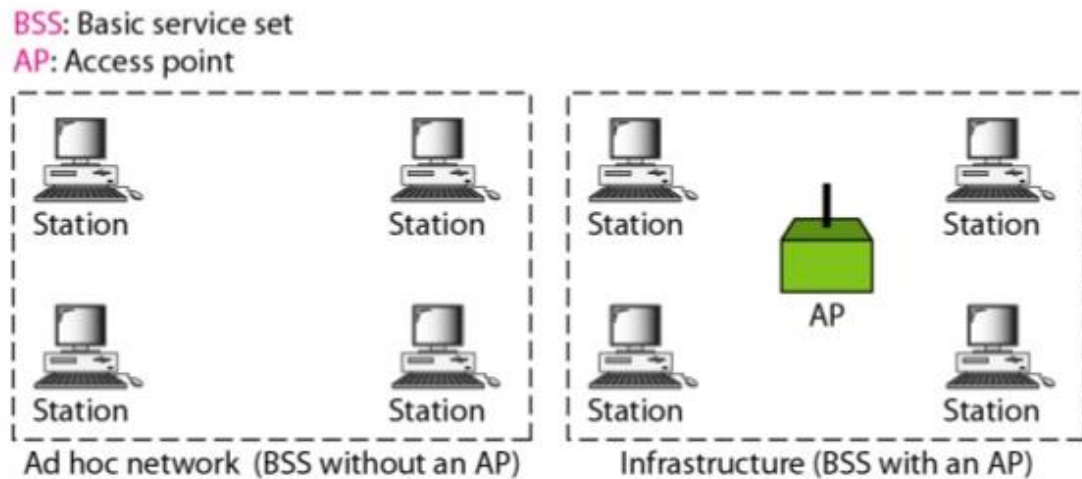
1. Architecture

The standard defines two kinds of services.

- a. Basic Service Set (BSS)
- b. Extended Service Set (ESS)

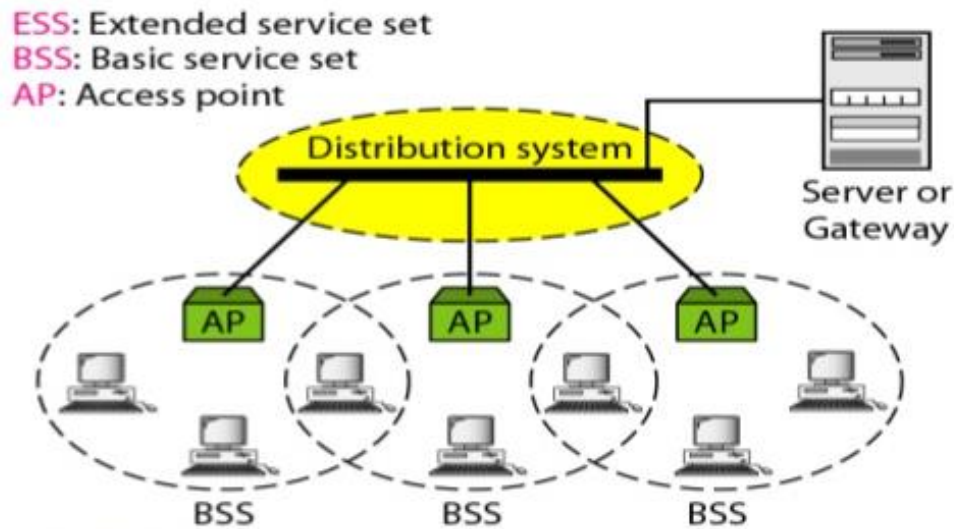
a. Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.



b. Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.



2. MAC Sub layer

IEEE 802.11 defines two MAC sub layers: the distributed coordination function (DCF) and point coordination function (PCF).

a. *Distributed Coordination Function*

One of the two protocols defined by IEEE at the MAC sub layer is called the distributed coordination function (DCF). DCF uses CSMA/CA as the access method. Wireless LANs cannot implement CSMA/CD for three reasons:

- For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.
- Collision may not be detected because of the hidden station problem.
- The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

Network Allocation Vector

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed

to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

b. Point Coordination Function (PCF)

The Point Coordination Function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission. PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

3. Frame Format

The MAC layer frame consists of nine fields

Frame control (FC): The FC field is 2 bytes long and defines the type of frame and some control information.

D: In all frame types except one, this field defines the duration of the transmission that is used to set the value of NAV. In one control frame, this field defines the ID of the frame

Addresses: There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the To DS and From DS subfields.

Sequence control: This field defines the sequence number of the frame to be used in flow control.

Frame body: This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.

FCS: The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.

4. Frame Types

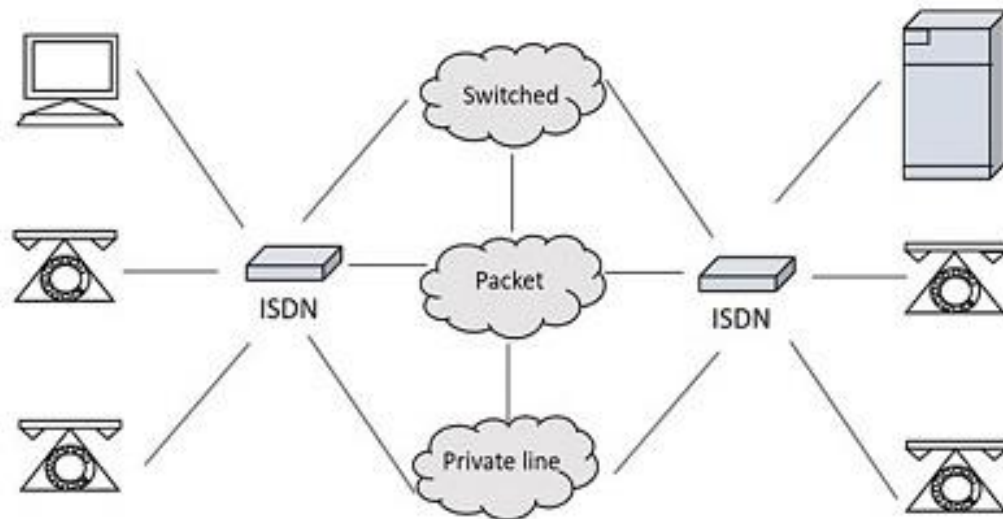
A wireless LAN defined by IEEE 802.11 have three categories of frames: Management frames, Control frames, and Data frames

- Management Frames: They are used for the initial communication between stations and access points.
- Control Frames: They are used for accessing the channel and acknowledging frames.
- Data Frames: Data frames are used for carrying data and control information.

ISDN

The Integrated Services of Digital Networking (ISDN) is a telephone network based infrastructure that allows the transmission of voice and data simultaneously at a high speed with greater efficiency. This is a circuit switched telephone network system, which also provides access to Packet switched networks.

The model of a practical ISDN is as shown below.



ISDN supports a variety of services. A few of them are listed below –

- Voice calls
- Facsimile
- Videotext
- Teletext
- Electronic Mail

- Database access
- Data transmission and voice
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer
- Audio and Video Conferencing

Types of ISDN

Among the types of several interfaces present, some of them contains channels such as the **B-Channels** or Bearer Channels that are used to transmit voice and data simultaneously; the **D-Channels** or Delta Channels that are used for signaling purpose to set up communication.

The ISDN has several kinds of access interfaces such as –

- a. Basic Rate Interface (BRI)
- b. Primary Rate Interface (PRI)
- c. Narrowband ISDN
- d. Broadband ISDN

a. Basic Rate Interface (BRI)

The Basic Rate Interface or Basic Rate Access, simply called the ISDN BRI Connection uses the existing telephone infrastructure. The BRI configuration provides two data or bearer channels at 64 Kbits/sec speed and one control or delta channel at 16 Kbits/sec. This is a standard rate.

The ISDN BRI interface is commonly used by smaller organizations or home users or within a local group, limiting a smaller area.

b. Primary Rate Interface (PRI)

The Primary Rate Interface or Primary Rate Access, simply called the ISDN PRI connection is used by enterprises and offices. The PRI configuration is based on T-carrier or T1

in the US, Canada and Japan countries consisting of 23 data or bearer channels and one control or delta channel, with 64kbps speed for a bandwidth of 1.544 M bits/sec. The PRI configuration is based on E-carrier or E1 in Europe, Australia and few Asian countries consisting of 30 data or bearer channels and two-control or delta channel with 64kbps speed for a bandwidth of 2.048 M bits/sec.

The ISDN BRI interface is used by larger organizations or enterprises and for Internet Service Providers.

c. Narrowband ISDN

The Narrowband Integrated Services Digital Network is called the N-ISDN. This can be understood as a telecommunication that carries voice information in a narrow band of frequencies. This is actually an attempt to digitize the analog voice information. This uses 64kbps circuit switching.

The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

d. Broadband ISDN

The Broadband Integrated Services Digital Network is called the B-ISDN. This integrates the digital networking services and provides digital transmission over ordinary telephone wires, as well as over other media. The CCITT defined it as, “Qualifying a service or system requiring transmission channels capable of supporting rates greater than primary rates.”

The broadband ISDN speed is around 2 MBPS to 1 GBPS and the transmission is related to ATM, i.e., Asynchronous Transfer Mode. The broadband ISDN communication is usually made using the fiber optic cables.

As the speed is greater than 1.544 Mbps, the communications based on this are called Broadband Communications. The broadband services provide a continuous flow of information, which is distributed from a central source to an unlimited number of authorized receivers connected to the network. Though a user can access this flow of information, he cannot control it.

Advantages of ISDN

ISDN is a telephone network based infrastructure, which enables the transmission of both voice and data simultaneously. There are many advantages of ISDN such as –

- As the services are digital, there is less chance for errors.
- The connection is faster.
- The bandwidth is higher.
- Voice, data and video – all of these can be sent over a single ISDN line.

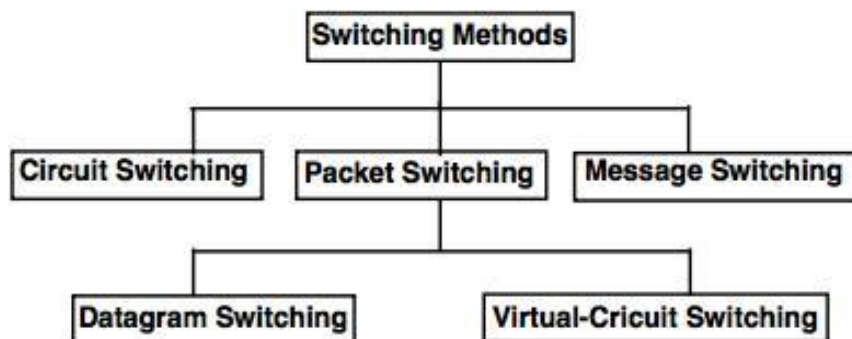
Disadvantages of ISDN

- The disadvantage of ISDN is that it requires specialized digital services and is costlier.

Switching

Network switching is the process of channeling data received from any number of input ports to another designated port that will transmit the data to its desired destination. The device through which the input data passes is called a switch.

There are three types of Switching.



I - Circuit Switching

- It consists of a set of switches connected by physical links.
- Two nodes communicate with each other over a dedicated communication path.
- There is a need of pre-specified route from which data will travel and no

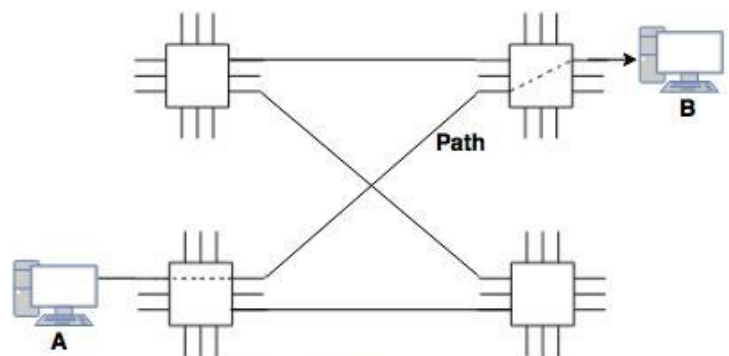


Fig: Circuit Switching

other data is permitted.

- Before starting communication, the nodes must make a reservation for the resources to be used during the communication.
- Once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- The end systems, such as telephones or computers are directly connected to a switch.
- When system A needs to communicate with system B, system A needs to request a connection to system B that must be accepted by all switches as well as by B itself.
- This is called as setup phase in which a circuit is reserved on each link, and the combination of circuits or channels defines a dedicated path.

II - Packet Switching

- Messages are divided into packets of fixed or variable size.
- The size of packet is decided by the network and the governing protocol.
- Resource allocation for a packet is not done in packet switching.
- Resources are allocated on demand.
- The resource allocation is done on first-come, first-served basis.
- Each switching node has a small amount of buffer space to hold packets temporarily.
- If the outgoing line is busy, the packet stays in queue until the line becomes available.

Packet switching method uses two routing methods:

- Datagram Packet Switching
- Virtual Circuit packet switching

a. Datagram Packet Switching

- It is normally implemented in the network layer.
- In datagram network, each packet is routed independently through the network.
- Each packet carries a header that contains the full information about the destination.

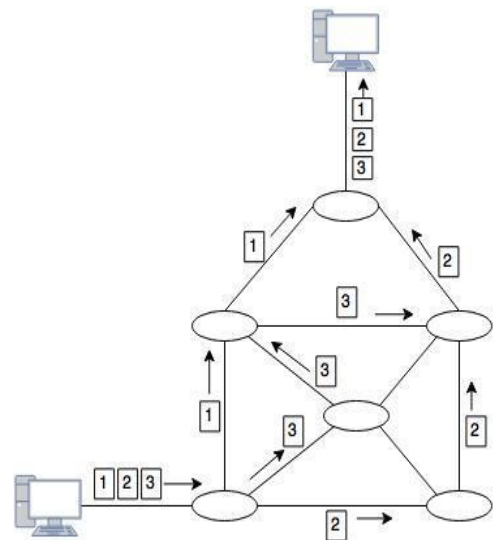


Fig: Datagram Packet Switching

- When the switch receives the packet, the destination address in the header of the packet is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

b. Virtual Circuit Packet Switching

- It is normally done at the data link layer.
- It establishes a fixed path between a source and a destination to transfer the packets.
- It is also called as connection oriented network.
- A logical connection is established when a sender sends a setup request to the receiver and the receiver sends back an acknowledgement to the sender if the receiver agree.
- All packets belonging to the same source and destination travel the same path.
- The information is delivered to the receiver in the same order as transmitted by the sender.

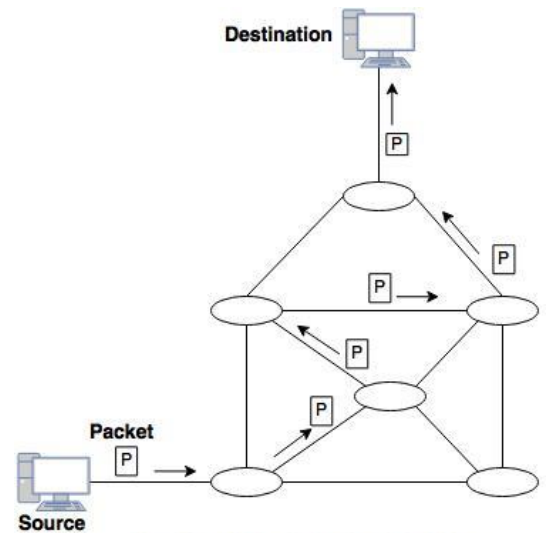


Fig: Virtual Circuit Packet Switching

III - Message Switching

- It is not necessary to establish a dedicated path between transmitter and receiver.
- Each message is routed independently through the network.
- Each message carries a header that contains the full information about the destination.

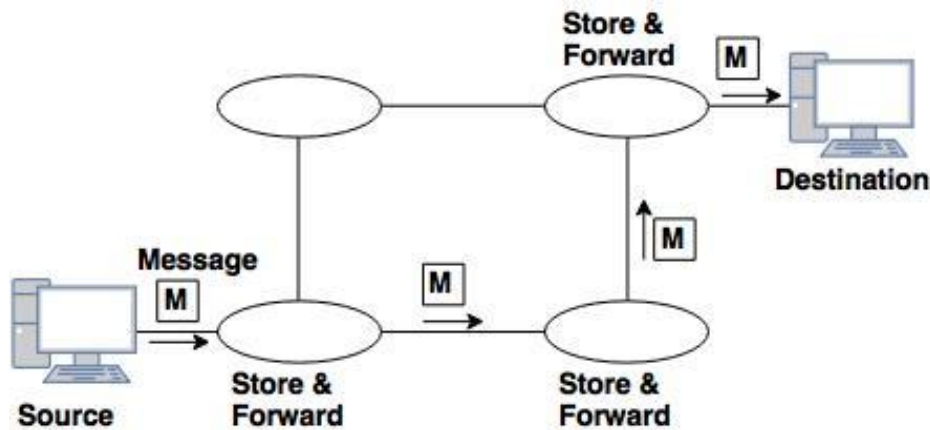


Fig: Message Switching

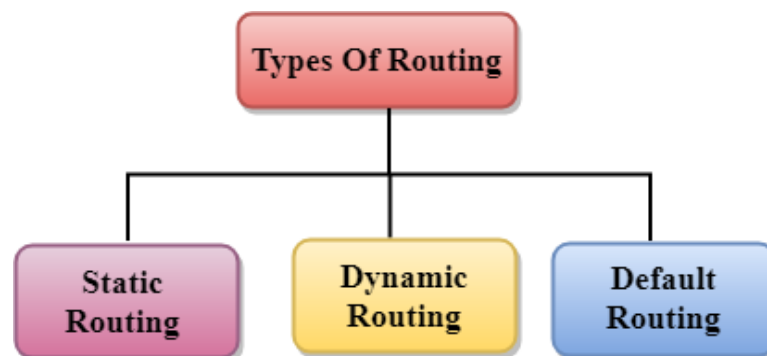
- Each intermediate device receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop does not have enough resources to accommodate large size message, the message is stored and switch waits.
- It is very slow because of store-and-forward technique.
- It is not recommended for real time applications like voice and video.

Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- It works at the network layer in the OSI model and internet layer in TCP/IP model
- It is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Types of Routing

Routing can be classified into three categories:



a. Static Routing

- Static Routing is also known as Non-adaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks.

Advantages of Static Routing

- **No Overhead:** It has no overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

b. Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

Features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

Advantages of Dynamic Routing

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

c. Default Routing

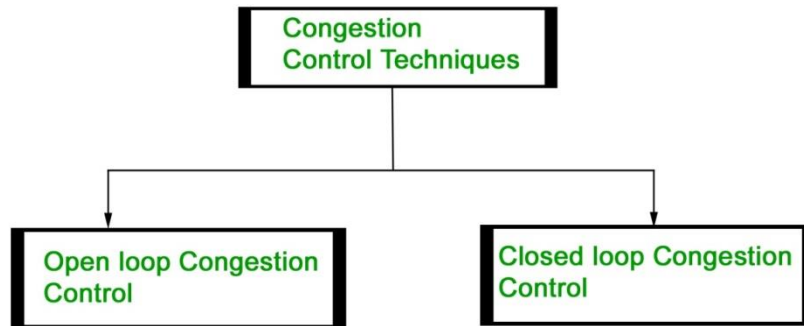
- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Congestion Control

Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity. Congestion happens in any system that involves waiting.

For example, congestion happens on a freeway because any abnormality in the flow, such as an accident during rush hour, creates blockage

Congestion control techniques can be broadly classified into two categories:



a. **Open Loop Congestion Control**

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control

1. **Retransmission Policy**

It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. **Window Policy**

The type of window at the sender side may also affect the congestion. Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and making it worse. Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

3. **Discarding Policy**

A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message. In case of audio file transmission,

routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

4. Acknowledgment Policy

Since acknowledgements are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment. The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send a acknowledgment only if it has to sent a packet or a timer expires.

5. Admission Policy

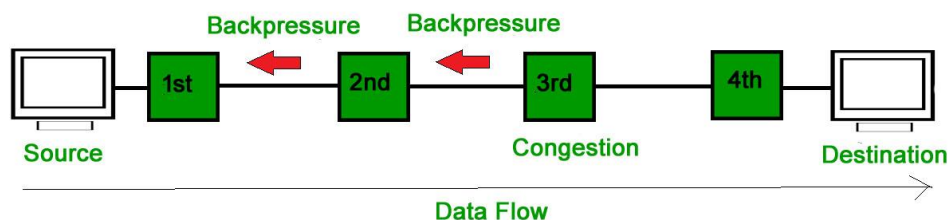
In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

b. Closed Loop Congestion Control

Closed loop congestion control technique is used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure

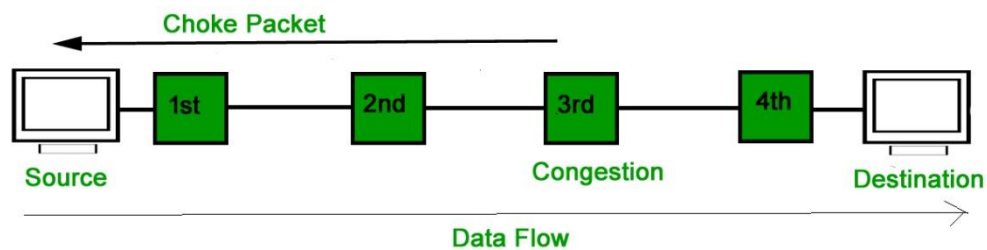
Backpressure is a technique in which a congested node stop receiving packet from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow.



The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node. In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and informs the source to slow down.

2. Choke Packet Technique

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion.



Each router monitor its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.

3. Implicit Signaling

In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is congestion.

4. Explicit Signaling

In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet

and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique. Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling:** In forward signaling signal is sent in the direction of the congestion. The destination is warned about congestion. The receivers in this case adopt policies to prevent further congestion.
- **Backward Signaling:** In backward signaling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

UNIT –IV: PERSONAL COMPUTER NETWORKS

Personal Computer (PC)

PC is an abbreviation for a Personal Computer, it is also known as a Microcomputer. Its physical characteristics and low cost are appealing and useful for its users. The capabilities of a personal computer have changed greatly since the introduction of electronic computers. By the early 1970s, people in academic or research institutions had the opportunity for single-person use of a computer system in interactive mode for extended durations, although these systems would still have been too expensive to be owned by a single individual.

The introduction of the microprocessor, a single chip with all the circuitry that formerly occupied large cabinets, led to the proliferation of personal computers after about 1975. Early personal computers, generally called microcomputers, were sold often in kit form and in limited volumes and were of interest mostly to hobbyists and technicians. By the late 1970s, mass-market pre-assembled computers allowed a wider range of people to use computers, focusing more on software applications and less on development of the processor hardware. Throughout the 1970s and 1980s, home computers were developed for household use, offering some personal productivity, programming and games, while somewhat larger and more expensive systems (although still low-cost compared with mainframes) called workstations were aimed for office and small business use.

Today a personal computer is an all rounded device that can be used as a productivity tool, a media server and a gaming machine. The modular construction of the personal computer allows components to be easily (at least for desktop units) swapped out when broken or upgraded. Although occasionally "PC" is used to refer to the family of computers descended from the original IBM-PC, it is now typically used for any general purpose computing platform available (according to price) for the home market, including laptops and Apple computers.

Characteristics

The characteristics of computers that have made them so powerful and universally useful are speed, accuracy, diligence, versatility and storage capacity.

Speed

Computers work at an incredible speed. A powerful computer is capable of performing about 3-4 million simple instructions per second.

Accuracy

In addition to being fast, computers are also accurate. Errors that may occur can almost always be attributed to human error (inaccurate data, poorly designed system or faulty instructions/programs written by the programmer)

Diligence

Unlike human beings, computers are highly consistent. They do not suffer from human traits of boredom and tiredness resulting in lack of concentration. Computers, therefore, are better than human beings in performing voluminous and repetitive jobs.

Versatility

Computers are versatile machines and are capable of performing any task as long as it can be broken down into a series of logical steps. The presence of computers can be seen in almost every sphere – Railway/Air reservation, Banks, Hotels, Weather forecasting and many more.

Storage Capacity

Today's computers can store large volumes of data. A piece of information once recorded (or stored) in the computer, can never be forgotten and can be retrieved almost instantaneously.

Error Handling

Error handling refers to the response and recovery procedures from error conditions present in a software application. In other words, it is the process comprised of anticipation, detection and resolution of application errors, programming errors or communication errors. Error handling helps in maintaining the normal flow of program execution. In fact, many applications face numerous design challenges when considering error-handling techniques.

Error handling helps in handling both hardware and software errors gracefully and helps execution to resume when interrupted. When it comes to error handling in software, either the programmer develops the necessary codes to handle errors or makes use of software tools to handle the errors. In cases where errors cannot be classified, error handling is usually done with returning special error codes. Special applications known as error handlers are available for certain applications to help in error handling. These applications can anticipate errors, thereby helping in recovering without actual termination of application.

There are four main categories of errors:

- Logical errors
- Generated errors
- Compile-time errors
- Runtime errors

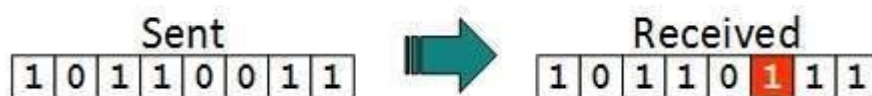
Error-handling techniques for development errors include rigorous proofreading. Error-handling techniques for logic errors or bugs is usually by meticulous application debugging or troubleshooting. Error-handling applications can resolve runtime errors or have their impact minimized by adopting reasonable countermeasures depending on the environment. Most hardware applications include an error-handling mechanism which allows them to recover gracefully from unexpected errors.

As errors could be fatal, error handling is one of the crucial areas for application designers and developers, regardless of the application developed or programming languages used. In worst-case scenarios, the error handling mechanisms force the application to log the user off and shut down the system.

Types of Errors

There may be three types of errors:

- **Single bit error**



In a frame, there is only one bit, anywhere though, which is corrupt.

➤ **Multiple bits error**



Frame is received with more than one bits in corrupted state.

➤ **Burst error**



Frame contains more than 1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- a. Error detection
- b. Error correction

a. Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity. The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

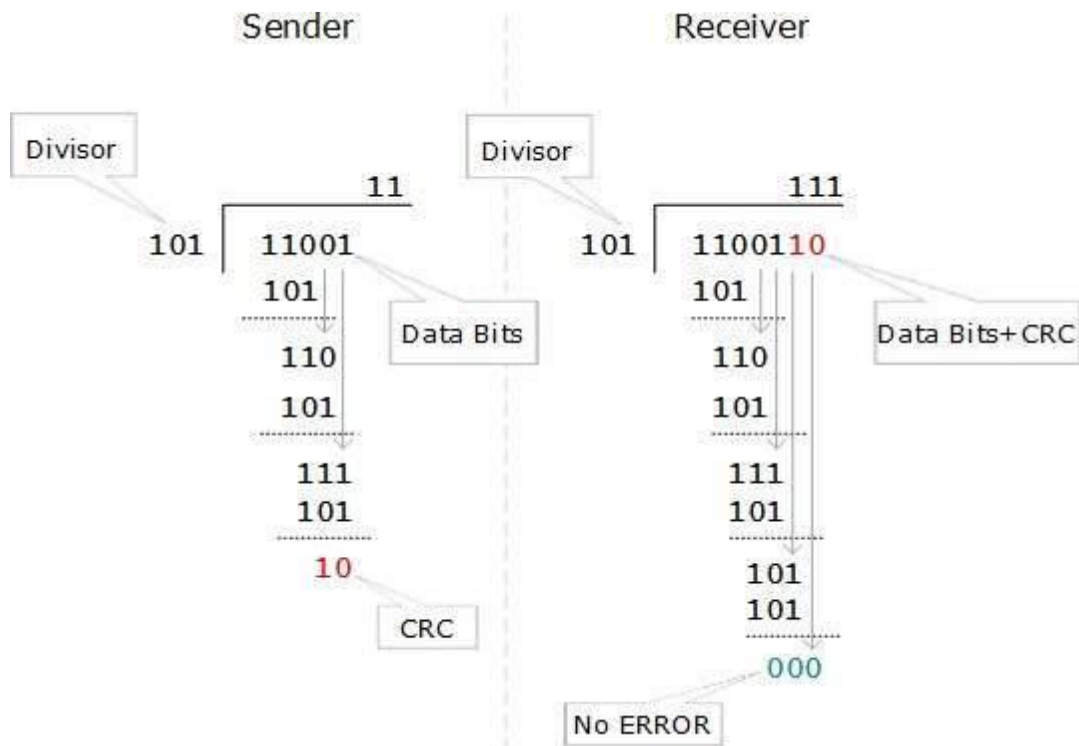


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erroneous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder.



Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as code words.

At the other end, the receiver performs division operation on code words using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

b. Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction:** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction:** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

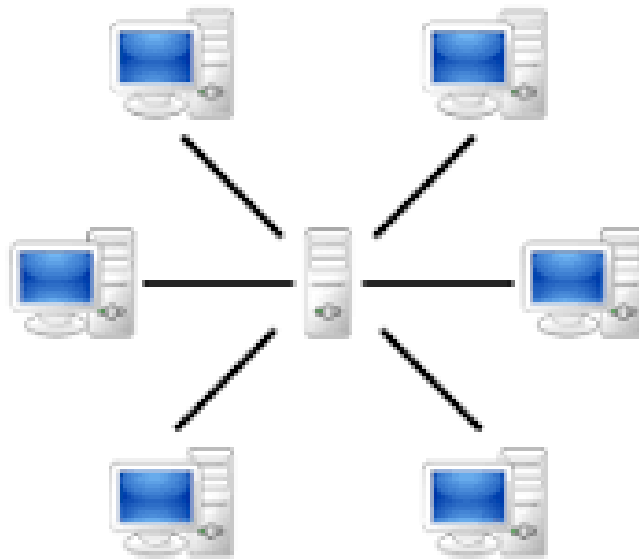
To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2^r combinations of information. In $m+r$ bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about $m+r$ bit locations plus no-error information, i.e. $m+r+1$.

PC as Server

Servers are similar to mainframes in that they serve many users with the main difference that, usually, the users (called clients) do much of their own processing. The server processes are devoted to sharing files and managing access rights.

A server is a central computer that contains collections of data and programs. Also called a network server, this system allows all connected users to share and store electronic data and applications. Two important types of servers are file servers and application servers.



An application server hosts various applications or programs that you can use without having to install them directly on your system. At SRU, once you have installed the Citrix client interface the Citrix server(s) provide access to many applications used across campus. Web apps, like Google Docs, work in essentially the same way.

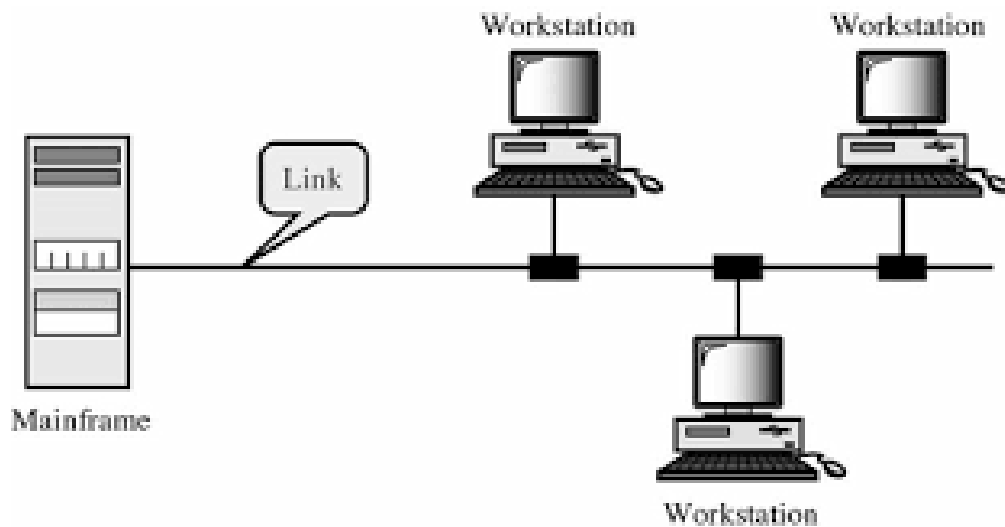
A file server manages your files, the H: (home drive) and I: (class works) drives show up on any computer you log into as "network drives". These files are not actually located on your computer's hard disk, but appear to be so.

A web server is essentially a file server located somewhere in the Internet. You request files (or web pages) by clicking on a (hyper)link or typing in a URL. The file is displayed by

your browser as a web page. Much of the web has been developed using this client-server model.
Example: client request for the SRU home page:

Linking PC with Mainframes

They are computers in which all the processing is done centrally, and the user terminals are called "dumb terminals" since they only input and output (and do not process). In modern systems, a PC or a web app often acts as the dumb terminal.



Mainframes are computers used mainly by large organizations for critical applications, typically bulk data processing such as a census. Examples: banks, airlines, insurance companies, and colleges. They support hundreds of users simultaneously.

Mainframes are computers. At their core, mainframes are high-performance computers with large memory (RAM) and processors that process billions of simple calculations and transactions in real-time.

The mainframe is critical to commercial databases, transaction servers and applications that require high reliability, scalability, compatibility and security – the core design values of the mainframe.



Figure: 360 Mainframe system

Reliability

Mainframes have 99.999% uptime, or less than 1 minute of unplanned downtime per server per year. The mainframe's "Mean Time Between Failure" is measured in decades.

Scalability

Run up to 8,000 virtual machines on a single server with 160 I/O cards 320 I/O channels. A single mainframe is equivalent to approximately 1,500 x86 servers.

Performance

IBM z14, for example, has 14 nanometer cores, 170 configurable processors, 6.8GB of cache memory, 32TB of main memory and 10 cores per chip to process up to 30 billion transactions daily.

Security

IBM z14 mainframes, for example, seamlessly encrypts 100% of application, cloud service and database data. It has 8.5 times the interception level of alternative platform solutions with 81% less effort.

File transfer

It is the process of copying or moving a file from one computer to another over a network or Internet connection. It enables sharing, transferring or transmitting a file or a logical data object between different users and/or computers both locally and remotely.

A file transfer can be an upload or download. File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Bit Torrent and Simple File Transfer Protocol are the most common file transfer protocols used in computer networks and online.

There are two main types of file transfer:

- Pull-Based: The file transfer request is initiated by the receiver.
- Push Based: The file transfer request is initiated by the sender.

Moreover, other than network or Internet, file transfer can be performed manually by copying a file to a new folder/drive in the same computer or by copying it on a USB pen drive, CD or other portable storage device to be transferred to another computer.

Pull Technology

Pull coding or client pull is a style of network communication and it requests form the foundation of network computing, where many clients request data from centralized servers. Pull is used extensively on the Internet for HTTP page requests from websites.

Push Technology

Push technology, or server push, is a style of Internet-based communication where the request for a given transaction is initiated by the publisher or central server. It is contrasted with pull/get, where the request for the transmission of information is initiated by the receiver or client.

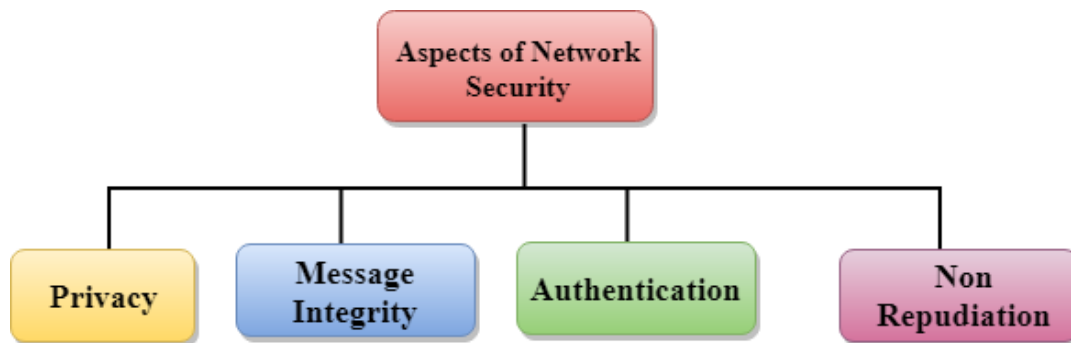
Push services are often based on information preferences expressed in advance. This is called a publish/subscribe model. A client "subscribes" to various information "channels" provided by a server; whenever new content is available on one of those channels, the server pushes that information out to the client.

UNIT –V: UPPER LEVEL PROTOCOLS

Network Security

Security in networking is based on cryptography, the science and art of transforming messages to make them secure and immune to attack. Cryptography can provide several aspects of security related to the interchange of messages through networks.

Aspects of Network Security



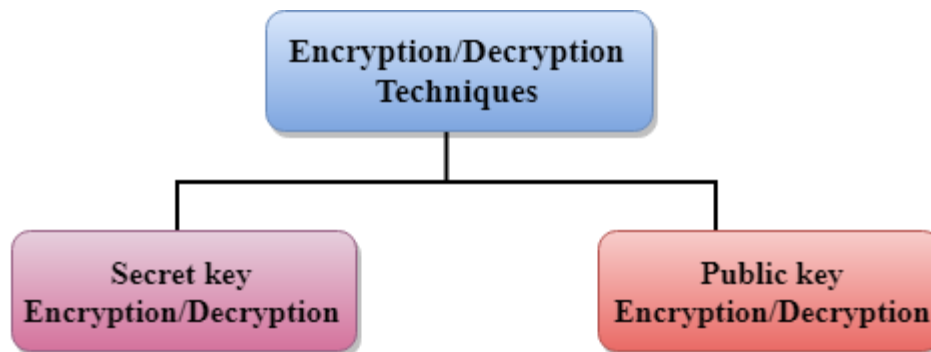
- **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
- **End-point authentication:** Authentication means that the receiver is sure of the sender's identity, i.e., no imposter has sent the message.

- **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

Encryption/Decryption

- **Encryption:** Encryption means that the sender converts the original information into another form and sends the unintelligible message over the network.
- **Decryption:** Decryption reverses the Encryption process in order to transform the message back to the original form.

The data which is to be encrypted at the sender site is known as plaintext, and the encrypted data is known as cipher text. The data is decrypted at the receiver site. There are two types of Encryption/Decryption techniques.

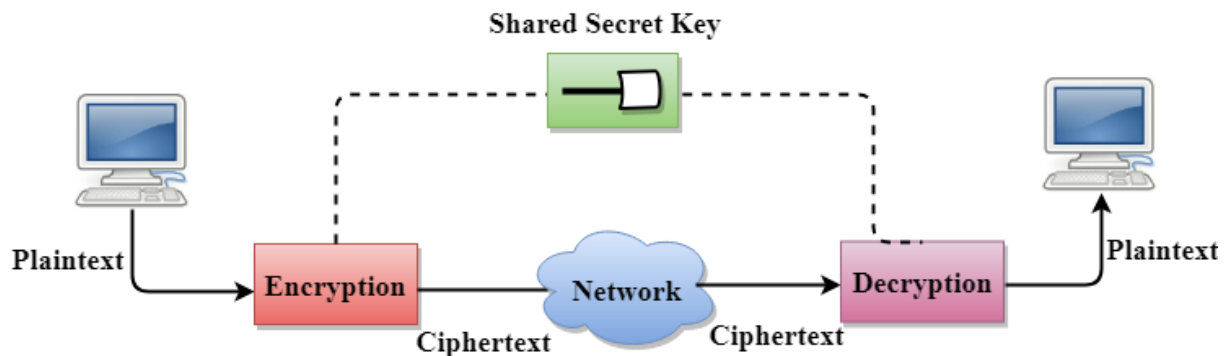


Secret Key Encryption/Decryption technique

- In Secret Key Encryption/Decryption technique, the same key is used by both the parties, i.e., the sender and receiver.
- The sender uses the secret key and encryption algorithm to encrypt the data; the receiver uses this key and decryption algorithm to decrypt the data.
- In Secret Key Encryption/Decryption technique, the algorithm used for encryption is the inverse of the algorithm used for decryption. It means that if the encryption algorithm

uses a combination of addition and multiplication, then the decryption algorithm uses a combination of subtraction and division.

- The secret key encryption algorithm is also known as symmetric encryption algorithm because the same secret key is used in bidirectional communication.



- In secret key encryption/decryption algorithm, the secret code is used by the computer to encrypt the information before it is sent over the network to another computer.
- The secret key requires that we should know which computers are talking to each other so that we can install the key on each computer.

Advantage

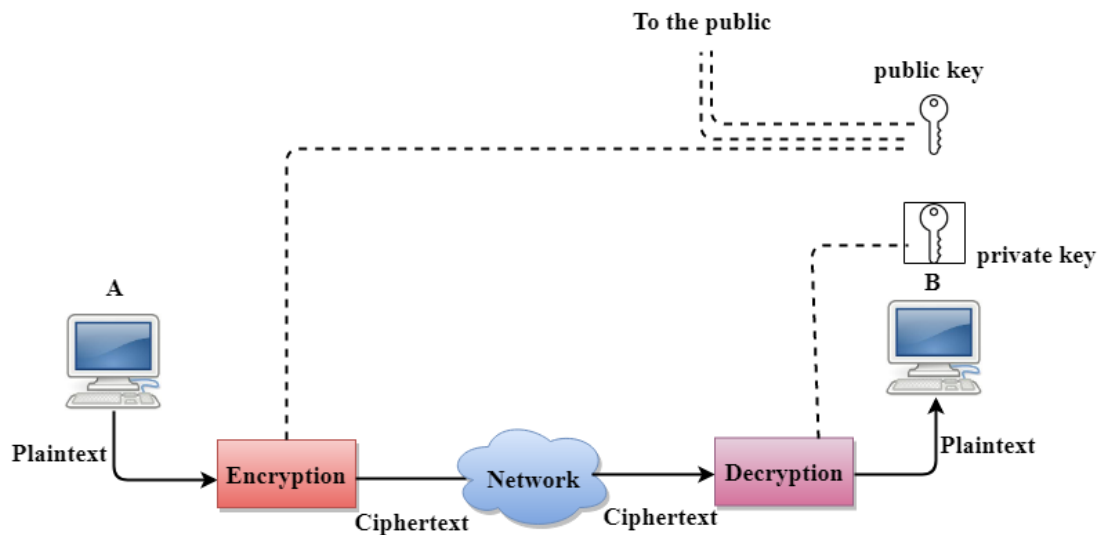
The secret key algorithms are more efficient as it takes less time to encrypt the message than to encrypt the message by using a public key encryption algorithm. The reason for this is that the size of the key is small. Due to this reason, Secret Key Algorithms are mainly used for encryption and decryption.

Disadvantages

- Each pair of users must have a secret key. If the number of people wants to use this method in the world is N , then there are $N(N-1)/2$ secret keys. For example, for one million people, then there are half billion secret keys.
- The distribution of keys among different parties can be very difficult. This problem can be resolved by combining the Secret Key Encryption/Decryption with the Public Key Encryption/Decryption algorithm.

Public Key Encryption/Decryption technique

- There are two keys in public key encryption: a private key and a public key.
- The private key is given to the receiver while the public key is provided to the public.



In the above figure, we see that A is sending the message to user B. 'A' uses the public key to encrypt the data while 'B' uses the private key to decrypt the data.

- In public key Encryption/Decryption, the public key used by the sender is different from the private key used by the receiver.
- The public key is available to the public while the private key is kept by each individual.
- The most commonly used public key algorithm is known as RSA.

Advantages

- The main restriction of private key encryption is the sharing of a secret key. A third party cannot use this key. In public key encryption, each entity creates a pair of keys, and they keep the private one and distribute the public key.
- The number of keys in public key encryption is reduced tremendously. For example, for one million users to communicate, only two million keys are required, not a half-billion keys as in the case of secret key encryption.

Disadvantages

- **Speed:** One of the major disadvantage of the public-key encryption is that it is slower than secret-key encryption. In secret key encryption, a single shared key is used to

encrypt and decrypt the message which speeds up the process while in public key encryption, different two keys are used, both related to each other by a complex mathematical process. Therefore, we can say that encryption and decryption take more time in public key encryption.

- **Authentication:** A public key encryption does not have a built-in authentication. Without authentication, the message can be interpreted or intercepted without the user's knowledge.
- **Inefficient:** The main disadvantage of the public key is its complexity. If we want the method to be effective, large numbers are needed. But in public key encryption, converting the plaintext into cipher text using long keys takes a lot of time. Therefore, the public key encryption algorithms are efficient for short messages not for long messages.

Data Encryption Standard

In 1973, NIST published a request for proposals for a national symmetric-key cryptosystem. A proposal from IBM, a modification of a project called Lucifer, was accepted as DES. DES was published in the Federal Register in March 1975 as a draft of the Federal Information Processing Standard (FIPS). After the publication, the draft was criticized severely for two reasons. First, critics questioned the small key length (only 56 bits), which could make the cipher vulnerable to brute-force attack. Second, critics were concerned about some hidden design behind the internal structure of DES. They were suspicious that some part of the structure (the S-boxes) may have some hidden trapdoor that would allow the National Security Agency (NSA) to decrypt the messages without the need for the key.

Later IBM designers mentioned that the internal structure was designed to prevent differential cryptanalysis. DES was finally published as FIPS 46 in the Federal Register in January 1977. NIST, however, defines DES as the standard for use in unclassified applications. DES has been the most widely used symmetric-key block cipher since its publication. NIST later issued a new standard that recommends the use of triple DES (repeated DES cipher three times) for future applications. At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text; at the decryption site, DES takes a 64-bit cipher text and creates a 64-bit block of plaintext. The same 56-bit cipher key is used for both encryption and decryption.

Let us concentrate on encryption; later we will discuss decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm.

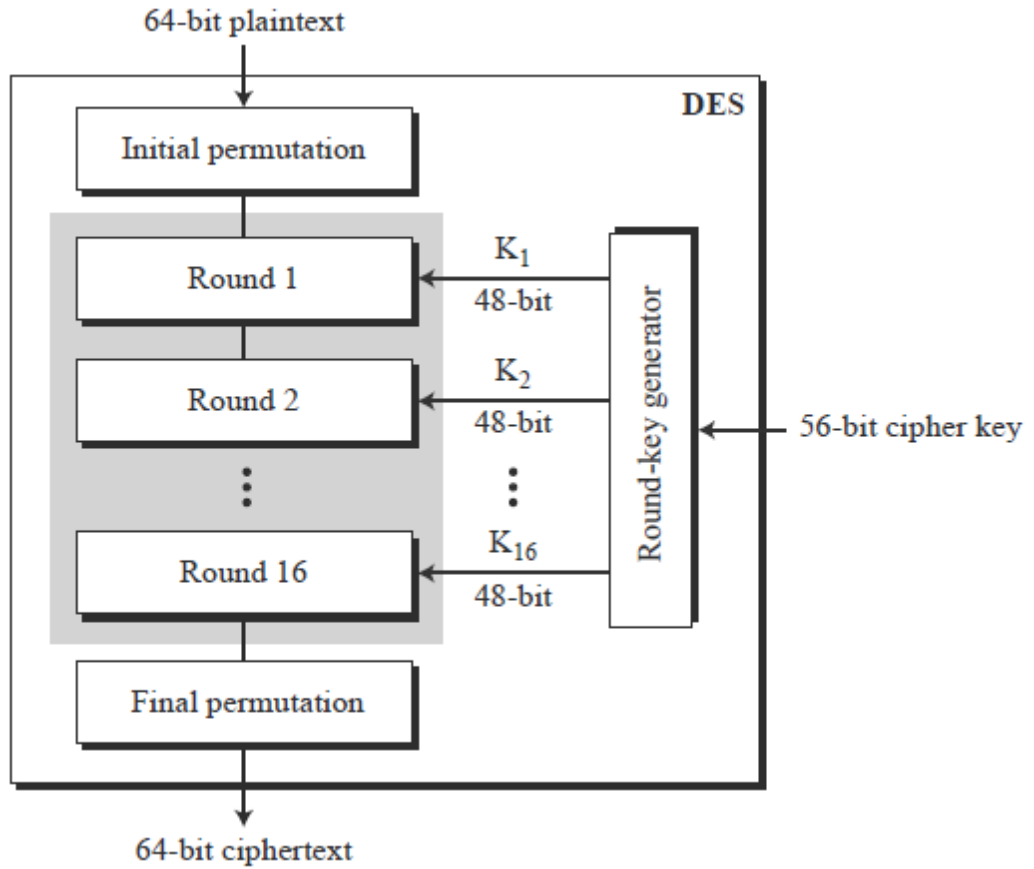


Figure-1: General Structure of DES

Initial and Final Permutations

Figure-2 shows the initial and final permutations (P-boxes). Each of these permutations takes a 64-bit input and permutes them according to a predefined rule.

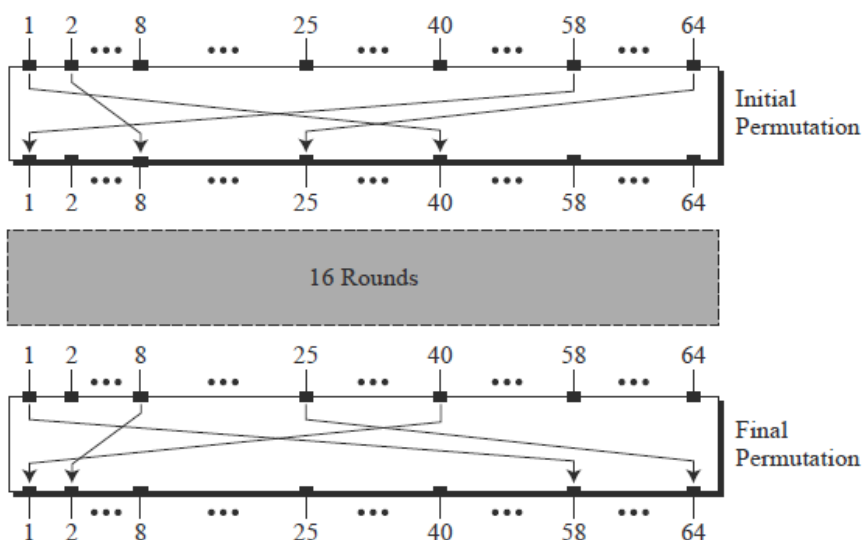


Figure-2: Initial and Final Permutation

We have shown only a few input ports and the corresponding output ports. These permutations are keyless straight permutations that are the inverse of each other.

For example, in the initial permutation, the 58th bit in the input becomes the first bit in the output. Similarly, in the final permutation, the first bit in the input becomes the 58th bit in the output. In other words, if the rounds between these two permutations do not exist, the 58th bit entering the initial permutation is the same as the 58th bit leaving the final permutation.

<i>Initial Permutation</i>	<i>Final Permutation</i>
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

Table-1

The permutation rules for these P-boxes are shown in Table 6.1. Each side of the table can be thought of as a 64-element array. Note that, as with any permutation table we have

discussed so far, the value of each element defines the input port number, and the order (index) of the element defines the output port number

These two permutations have no cryptography significance in DES. Both permutations are keyless and predetermined. The reason they are included in DES is not clear and has not been revealed by the DES designers. The guess is that DES was designed to be implemented in hardware (on chips) and that these two complex permutations may thwart a software simulation of the mechanism.

Rounds

DES uses 16 rounds. Each round of DES is a Feistel cipher, as shown in Figure-3.

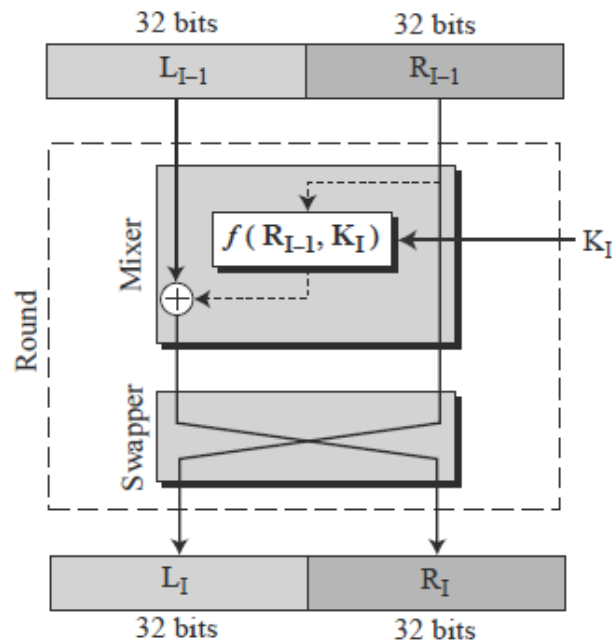


Figure-3: Single round of DES

The round takes L_{I-1} and R_{I-1} from previous round (or the initial permutation box) and creates L_I and R_I , which go to the next round (or final permutation box). Each of these elements is invertible. The swapper is obviously invertible. It swaps the left half of the text with the right half. The mixer is invertible because of the XOR operation. All noninvertible elements are collected inside the function $f(R_{I-1}, K_I)$.

DES Function

The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits (R_{I-1}) to produce a 32-bit output. This function is made up of four sections: an expansion D-box, a whitener (that adds key), a group of S-boxes, and a straight D-box as shown in Figure-4.

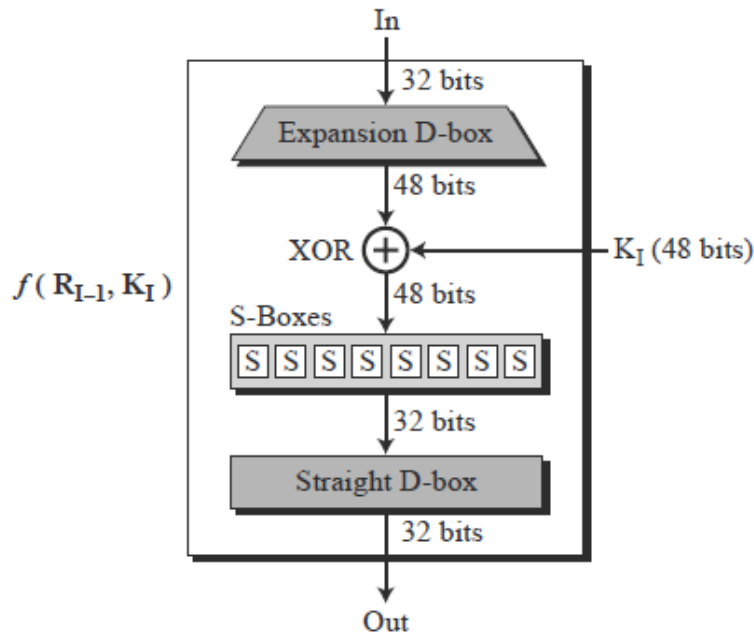


Figure-4: DES function

Expansion D-box

Since R_{I-1} is a 32-bit input and K_I is a 48-bit key, we first need to expand R_{I-1} to 48 bits. R_{I-1} is divided into 8 4-bit sections. Each 4-bit section is then expanded to 6 bits. This expansion permutation follows a predetermined rule. For each section, input bits 1, 2, 3, and 4 are copied to output bits 2, 3, 4, and 5, respectively. Output bit 1 comes from bit 4 of the previous section; output bit 6 comes from bit 1 of the next section.

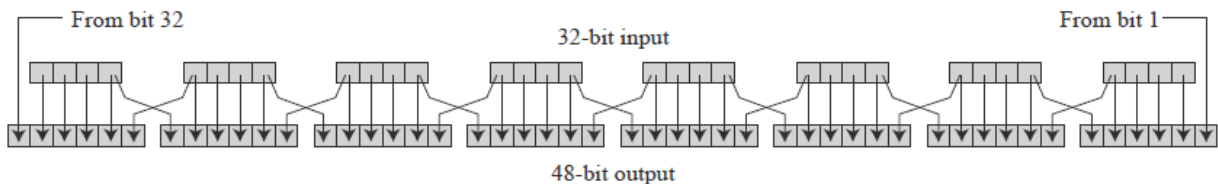


Figure-5: Expansion Permutation

If sections 1 and 8 can be considered adjacent sections, the same rule applies to bits 1 and 32. Figure-5 shows the input and output in the expansion permutation.

Although the relationship between the input and output can be defined mathematically, DES uses Table-2 to define this D-box. Note that the number of output ports is 48, but the value range is only 1 to 32. Some of the inputs go to more than one output. For example, the value of input bit 5 becomes the value of output bits 6 and 8

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Table-2

After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key. Note that both the right section and the key are 48-bits in length. Also note that the round key is used only in this operation.

The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.

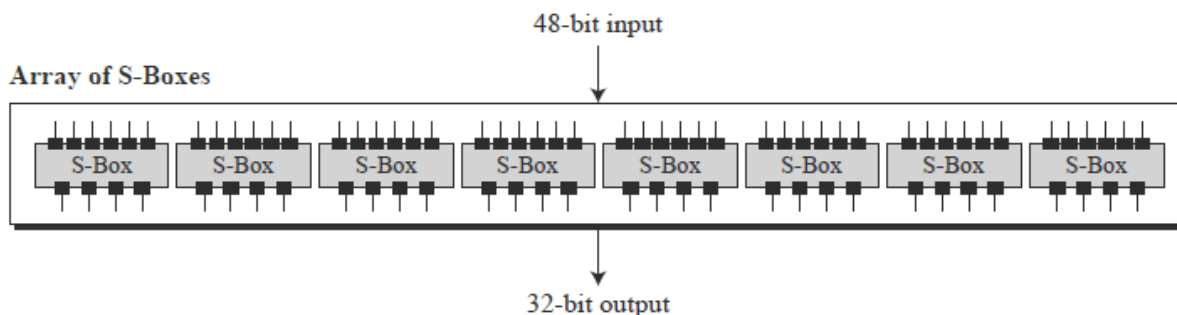


Figure-6: S-Boxes

The 48-bit data from the second operation is divided into eight 6-bit chunks, and each chunk is fed into a box. The result of each box is a 4-bit chunk; when these are combined the result is a 32-bit text. The substitution in each box follows a pre-determined rule based on a 4-row by 16-column table. The combination of bits 1 and 6 of the input defines one of four rows; the combination of bits 2 through 5 defines one of the sixteen columns. This will become clear in the examples. Because each S-box has its own table, we need eight tables, as shown in Tables 3 to 10, to define the output of these boxes. The values of the inputs (row number and column number) and the values of the outputs are given as decimal numbers to save space. These need to be changed to binary.

Table-3: S-Box1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Table-4: S-Box2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

Table-5: S-Box 3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

Table-6: S-Box 4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	6	09	10	1	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

Table-7: S-Box 5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
1	14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
2	04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
3	11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

Table-8: S-Box 6

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
1	10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
2	09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
3	04	03	02	12	09	05	15	10	11	14	01	07	10	00	08	13

Table-9: S-Box 7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	00	08	13	03	12	09	07	05	10	06	01
1	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
2	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
3	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

Table-10: S-Box 8

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
1	01	15	13	08	10	03	07	04	12	05	06	11	10	14	09	02
2	07	11	04	01	09	12	14	02	00	06	10	10	15	03	05	08
3	02	01	14	07	04	10	8	13	15	12	09	09	03	05	06	11

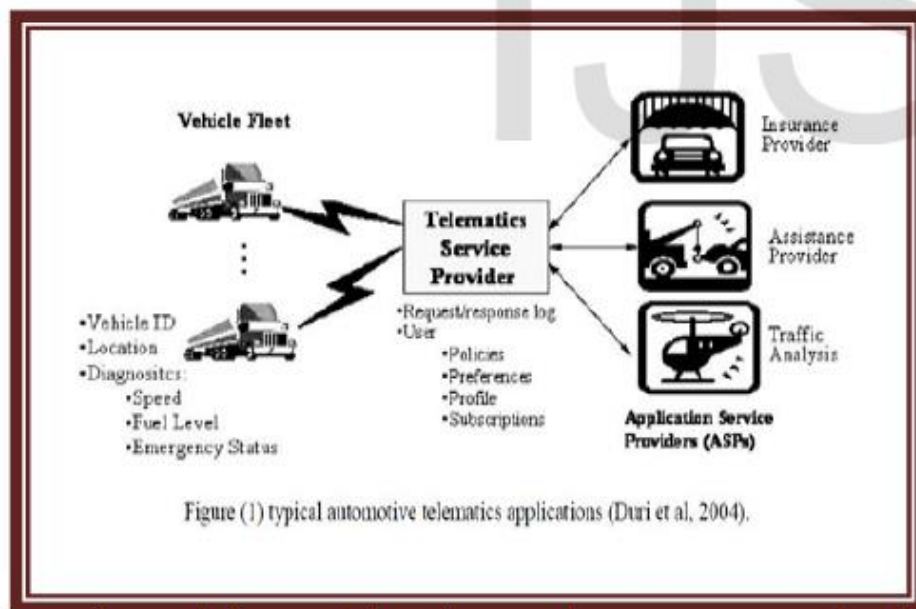
Telematics

Telematics is a term that combines the words telecommunications and informatics to broadly describe the integrated use of communications and information technology to transmit, store and receive information from telecommunications devices to remote objects over a network.

Telematics is a delivery service which is used to exchange information. This information relates to the services. Telematics is a service provider which has connection with user devices and ASP (Application Service Provider). These services need user information that is essential. As a result, the system service has to protect it. Therefore, integrity and protection of data are two important features in secure system in any organization which wants to use information. Both of hardware devices and software are used in telematics system. These devices support the system to improve operational efficiency which includes maintenance, back-offline administration and repair some other devices which are out of service.

Telematics system installs on vehicle or any other machines which is needed to monitor or transferring information. Telematics monitoring systems is a factor to decrease or eliminate fraudulences and theft because of the ability of a telematics system to find places of vehicle.

Advantages



Telematics system has safety features because of reducing the number of accidents in vehicles. Telematics system saves time because it provides information on user in near real-time. Web service sends back answer to request in short time, when user sends the request. Using the web application in telematics is a reason for reducing cost because the user does not need to purchase software.

GPS wireless passive tracking saves money for the driver because after installing the system the driver does not need to purchase software and hardware. Telematics has advantages in health care. It is used to record patient information and communication between patients and doctors. It is used to monitor patients at home. Home hemodialysis (HD) is used for patients who have renal failure. This system transfers information about the patient such as plus rate, arterial pressure and plus oxymetry (Po₂). These data are displayed on HD machine and monitored by nursing staff in Central Control Station (CCS). Telematics system increases patient's independence, while it does not reduce patient service.

Telematics system has provided service in education area such as email, computer conferencing and telematics- based distance which is "face to face teaching and learning at distance".

Disadvantages

Cost: Installing a telematics system is expensive even, if user has ability to install the telematics system because it needs to purchase hardware and software. GPS types have different prices. Cellular based tracking has lowest price which is about \$700. However, the user has to pay about \$35 monthly for information which is displayed over the internet. Hardware price needs \$700, and \$800 for the database and network in wireless passive tracking. Furthermore, average cost for the Satellite based real-time tracking is between five and hundred dollars.

Tracking: User of the system gives a lot of privacy information to the system. It is easy to track the user because of sending his privacy information into the system. Sometimes users do not want to control by systems because the system can find the user easily.

Distraction: Automotive telematics have a disadvantage which is distracting the driver by looking at the navigation. Drivers may have an accident because of looking at the road and navigation at the same time.

Management issue in education area: this technology may have a management issue because of having an insufficient plan and isolating students from their colleagues and their teachers. As a result, it has a side effect on the education system.

Electronic mail

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

E-Mail Address

Each user of email is assigned a unique name for his email account. This name is known as E-mail address.

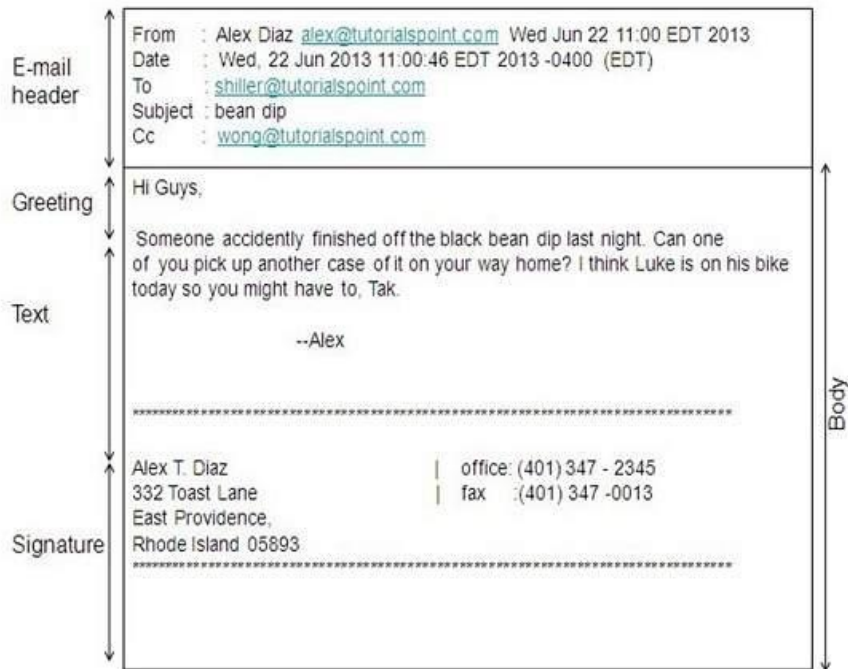
E-mail is generally of the form username@domainname.

- The username and the domain name are separated by @ (**at**) symbol.
- E-mail addresses are not case sensitive.
- Spaces are not allowed in e-mail address.

E-Mail Message Components

E-mail message comprises of different components: E-mail Header, Greeting, Text, and Signature. These components are described in the following diagram:

Greeting: It is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.



E-Mail Header

The first five lines of an E-mail message is called E-mail header. The header part comprises of following fields:

- From
- Date
- To
- Subject
- CC
- BCC

From: The From field indicates the sender's address i.e. who sent the e-mail.

Date: The Date field indicates the date when the e-mail was sent.

To: The To field indicates the recipient's address i.e. to whom the e-mail is sent.

Subject: The Subject field indicates the purpose of e-mail. It should be precise and to the point.

CC: CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

BCC: BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

Greeting: Greeting is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.

Text: It represents the actual content of the message.

Signature: This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

Advantages

- **Reliable:** Many of the mail systems notify the sender if e-mail message was undeliverable.
- **Convenience:** There is no requirement of stationary and stamps. One does not have to go to post office. But all these things are not required for sending or receiving an mail.
- **Speed:** E-mail is very fast. However, the speed also depends upon the underlying network.
- **Inexpensive:** The cost of sending e-mail is very low.
- **Printable:** It is easy to obtain a hardcopy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.
- **Global:** E-mail can be sent and received by a person sitting across the globe.
- **Generality:** It is also possible to send graphics, programs and sounds with an e-mail.

Disadvantages

- **Forgery:** E-mail doesn't prevent from forgery, that is, someone impersonating the sender, since sender is usually not authenticated in any way.
- **Overload:** Convenience of E-mail may result in a flood of mail.

- **Misdirection:** It is possible that you may send e-mail to an unintended recipient.
- **Junk:** Junk emails are undesirable and inappropriate emails. Junk emails are sometimes referred to as spam.
- **No Response:** It may be frustrating when the recipient does not read the e-mail and respond on a regular basis