CHAPTER 1

1. Fundamentals & Link Layer

Objectives

- To understand about Network requirements and building a network.
- To explain basics of networking.
- To know about internet architecture.
- To explain about layers and protocols.
- To explain about flow and error control.

1. Introduction

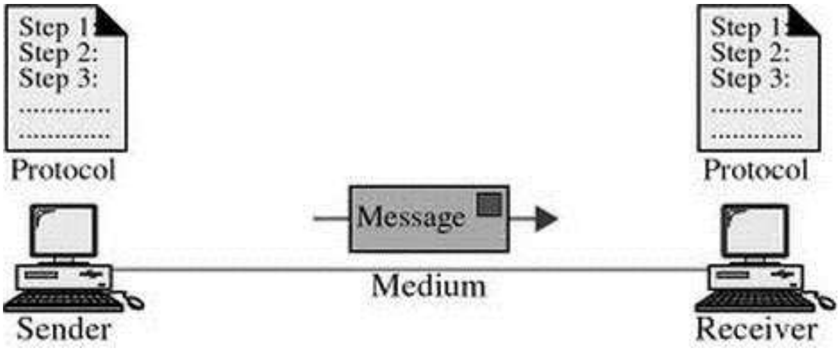
1.1. Building a Network

Data Communication

Data communication is defined as the exchange of data or information between different devices through any destined transmission medium, example, wire cable. Data communication occurs with the communicating devices or systems which are composed of a combination of hardware and software. Hardware is stated as any physical equipment and software is stated as programs using any programming language. The efficiency of this system relies on 4 important features such as

- Accuracy
- Timelines
- Delivery
- Jitter

Components of a Network



- Sender
- Receiver
- Message
- Protocol
- Transmission medium

Accuracy - The system is deemed to deliver the data exactly.

Timelines - Data should be delivered in a2 timely manner.

Delivery - The system has to deliver data to the destined location.

Jitter - The difference in the time of arrival of packets.

Sender - Device that sends the data to receiver.

Receiver - Device that receives the data from sender.

Message - The information to be communicated.

Protocol - Set of guidelines to administer data communication.

Transmission medium - Physical pattern where a message migrates from sender to receiver.

1.2. Requirements

Perspectives

Network design depends upon the following perspectives.

- **Application programme -** Specifies the list of services needed by application.
- **Network designer -** Lists attributes of low cost but efficient design.
- **Network provider -** Lists the features of a system which is easy to manage and provide security.

Scalable Connectivity

In network, only few nodes were selected for privacy and security. A system which is capable of supporting the growth of the system to an arbitrary large size is meant to be scalable.

Data Representation

- Text
- Numbers
- Audio
- Video
- Images

Data Flow

Two devices can be communicated through 3 different forms such as simplex, half duplex and full duplex.

- **Simplex**

The connectivity is unidirectional ie., one way in simplex mode. Any one of any two systems in a connection can send and only the next system can receive.

E.g: television used in our day to day life.

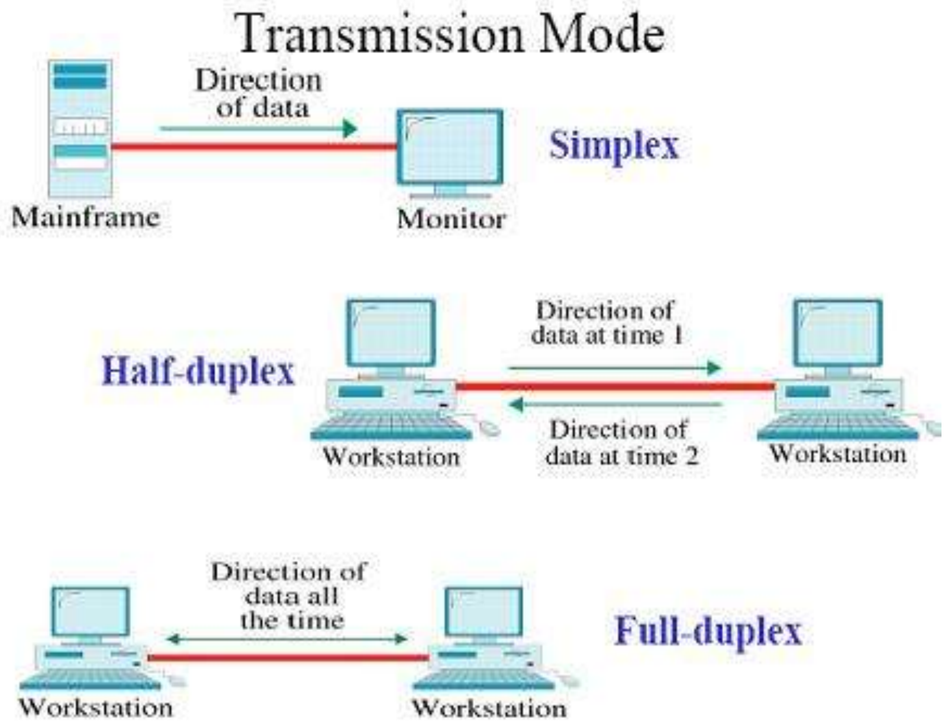
- **Half duplex**

All stations send and receive the messages in different timelines, which is not simultaneously passed at the same time in half duplex. This is given as when one device transmits data, the other receives data.

E.g: walky-talky, CB radios.

- **Full duplex**

Both stations send and receive simultaneously, where the data can be passed at the same time under full duplex mode. Communication can be performed in both directions at the same time. E.g: Telephone.



Network

A set of devices or nodes linked through communication links is called as network. Nodes->computer, printer, and scanner. All devices send and receive data, formulated by other nodes on network. Network uses distributed systems where there is sharing of any process by different systems.

Network Criteria

The metrics of network criteria are performance, reliability and security.

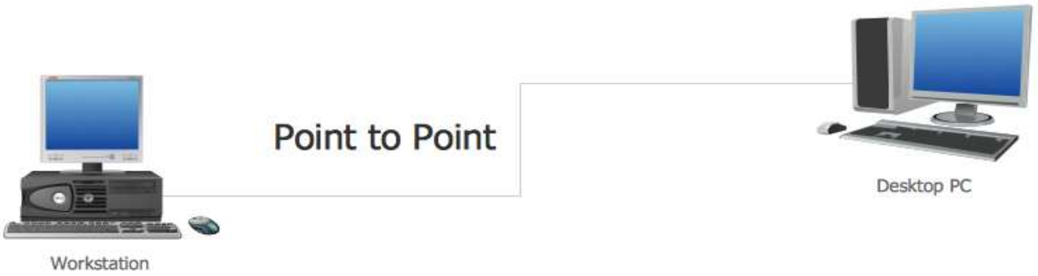
Physical Structure

Connection and its types – Connection establishment is the connectivity between devices in a network. A link is a pathway to communicate and send and receive data between devices. The types are given as follows.

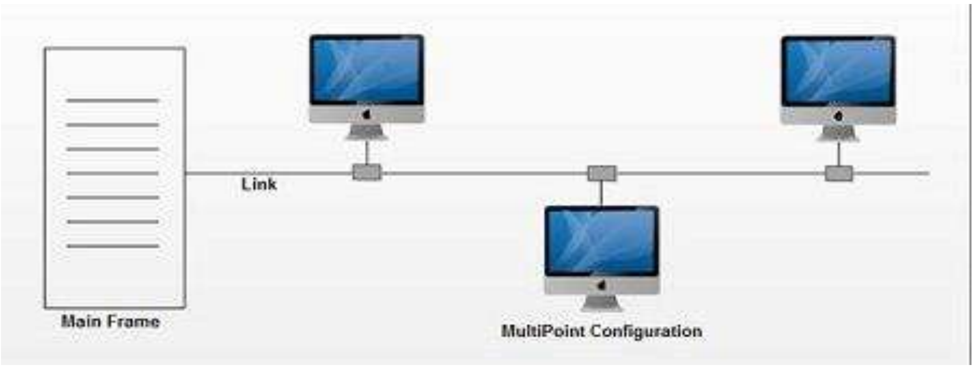
- Point to point
- Multipoint

Point to point – The establishment of connection between 2 individual devices.

E.g: Television satellite link.



Multipoint – when a single link is shared by more than two devices, it is called as multipoint (multidrop).



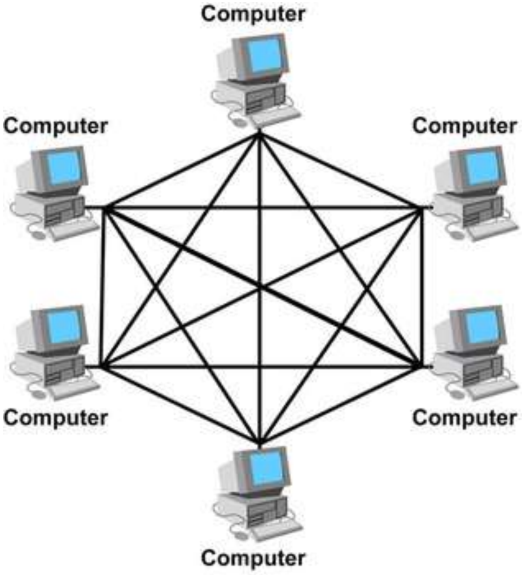
Categories of Topology

The physical establishment of network connectivity is called as topology. They are categorised as mesh, star, bus, ring and hybrid.

- **Mesh**

All devices establish a point to point connectivity to other devices in its scope of contact, in mesh topology. The connected 2 devices carry messages in this topology.

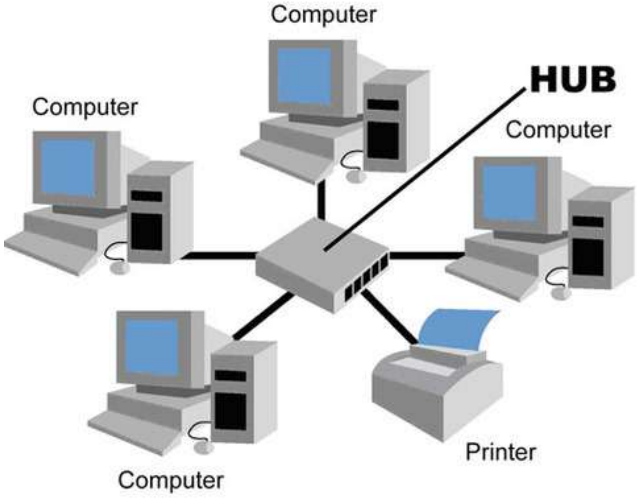
No of links = n (n-1)/2, where n stands for nodes



- **Star**

In star topology, a central controller holds the connectivity with the devices using devoted link and the central controller is hub.

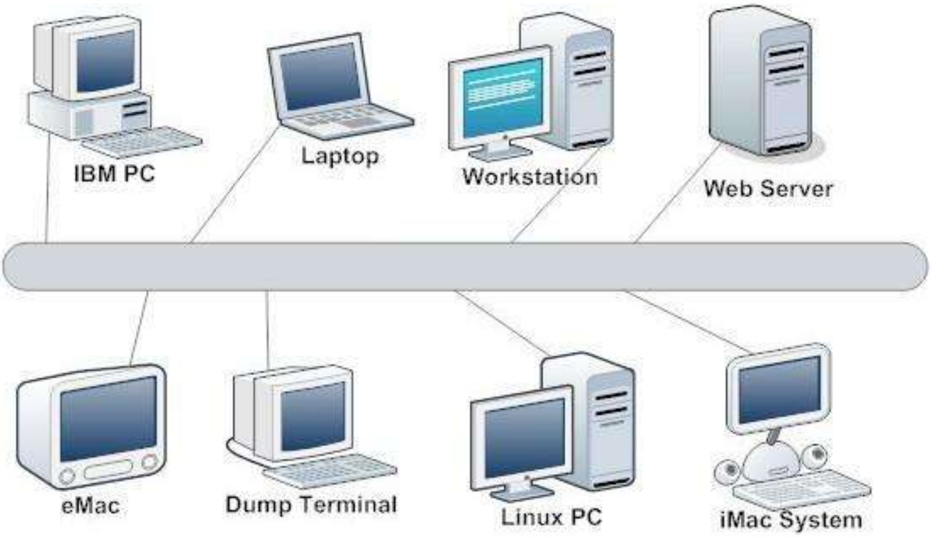
No of links = n, n stands for nodes.



- **Bus**

A bus is multipoint link. The connection between the device and the main cable is done by drop line. To establish connectivity with the metallic core a connector splices into the main cable or punctures the sheathing of a cable through tap.

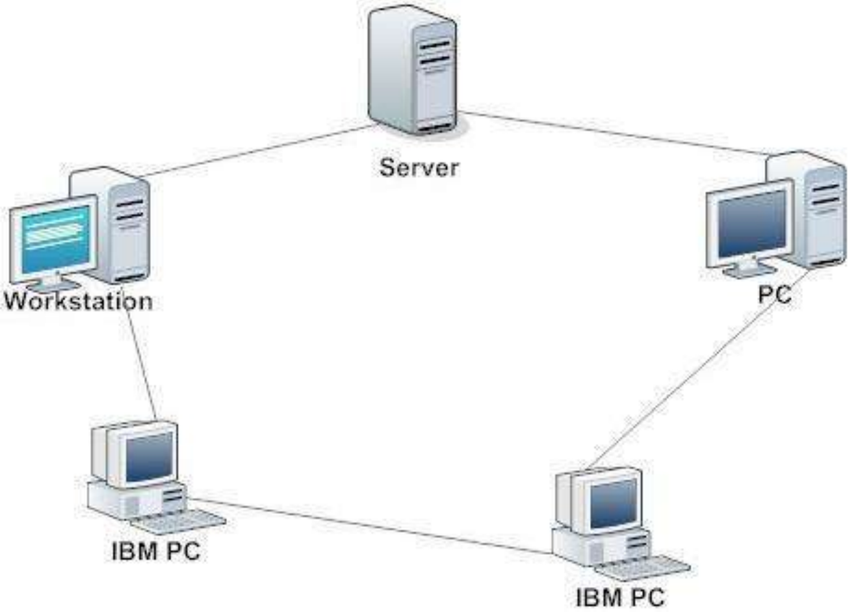
No. of links = 1 backbone, n droplines



- **Ring**

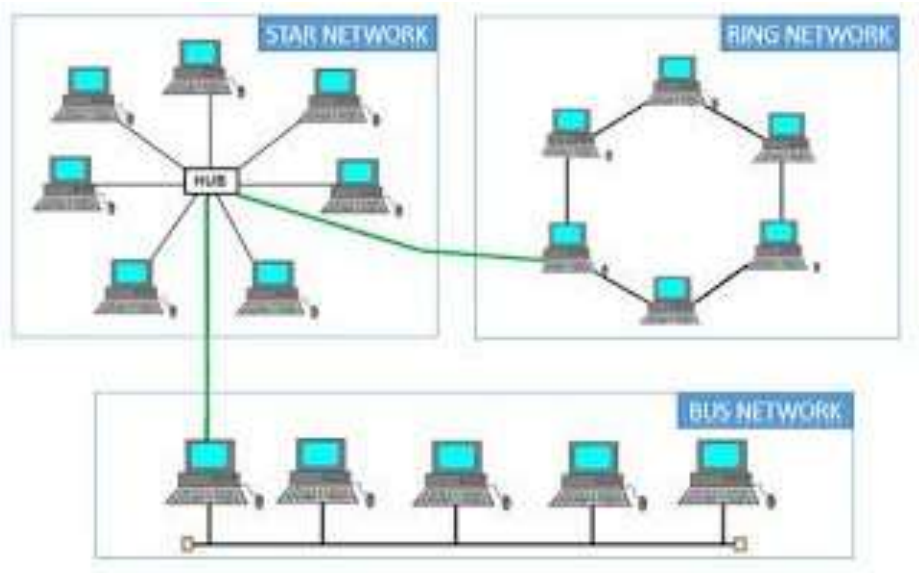
A connectivity is established between 2 devices in ring topology which are in close proximity on both sides. The transmission proceeds through the ring in a direction. Each system in ring connects with repeater. Repeater generates bits and passes them.

No of links= n-1, n is the number of nodes



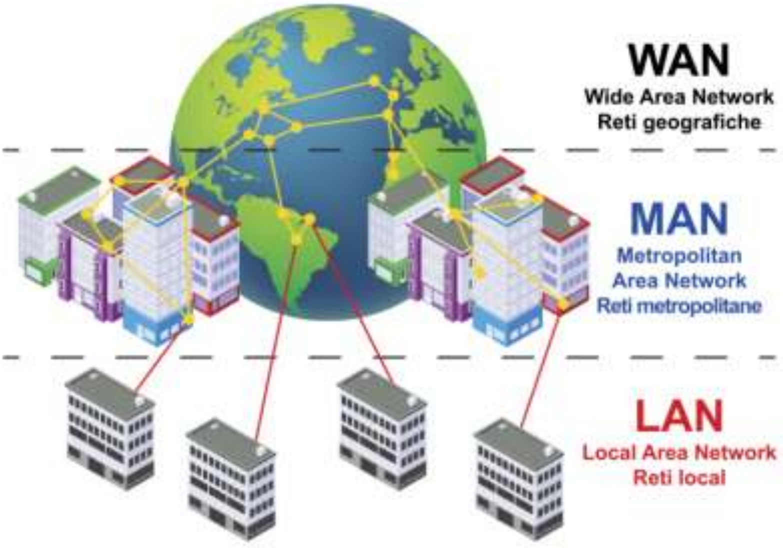
- **Hybrid**

The mixture of different topologies is Hybrid topology.



Network Models or Categories

- **LAN -** Local Area Network (less than 2m).
- **WAN -** Wide Area Network (world-wide connectivity).
- **MAN -** Metropolitan Area Network (span ten of miles).



1.3. Layering and Protocols

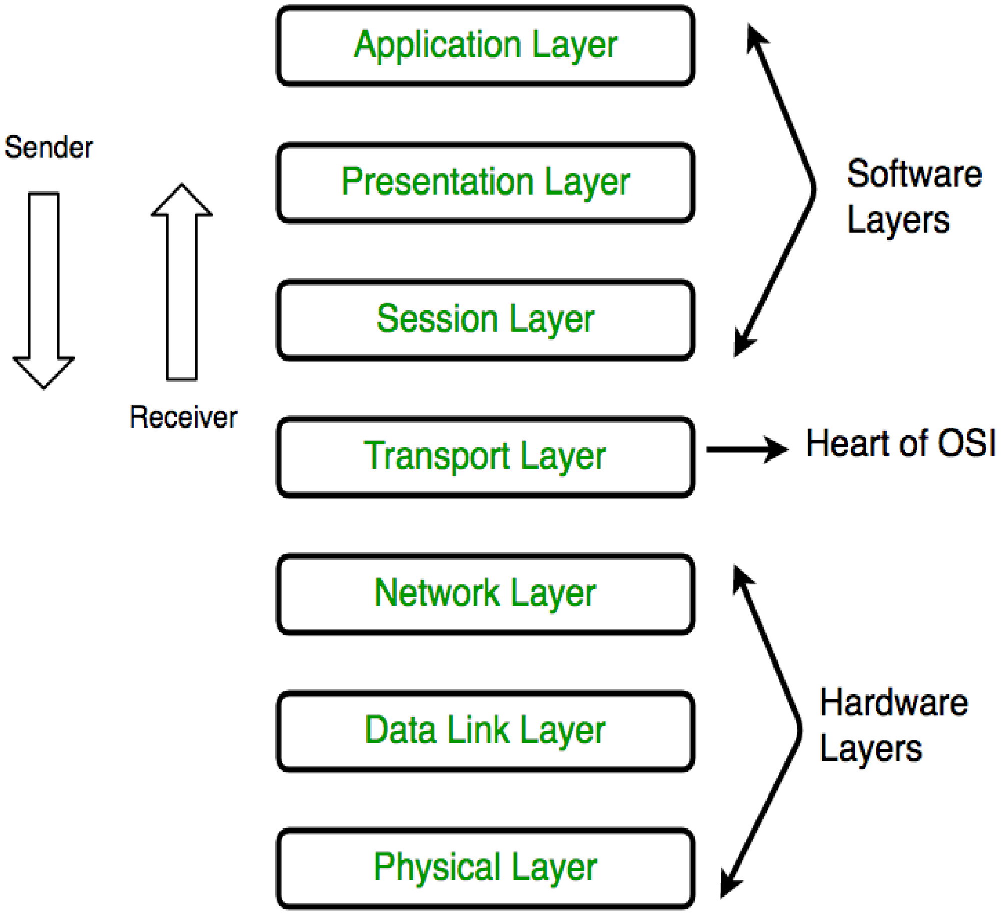
Protocols → syntax, semantics, timing

Standards → de facto, de jure

1.3.1. Networks Models

The International Standards Organization (ISO) devoted worldwide International Standards in 1947. In 1970, an ISO standard covers all aspects of network communications in Open System Interconnection (OSI) models. In order to formulate connectivity with various systems irrespective of logic of software in hardware, is the motive of OSI model. It is used to design network architecture, which is flexible, robust and interoperable. ISO holds OSI as model.

It consists of 7 layers which used to explore data communication. The communication is governed by instructions and resolutions as protocol. The event in a system that enables a communication is peer to peer process.



Over the adjacent layers of the sender and the receiver the data along with network information is traversed or passed by interfacing.

Network Support Layers

Physical

Datalink

Network

Transport → link these 2 layers

User Support Layers

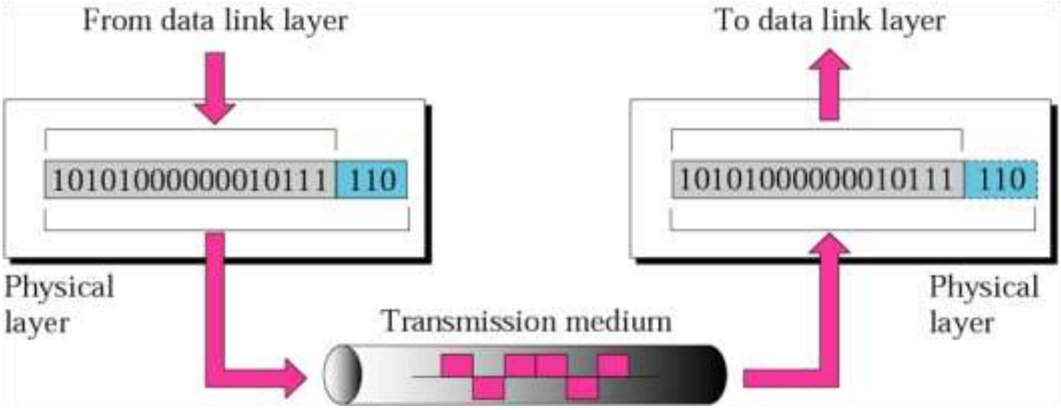
Session

Presentation

Application

Physical Layer

It performs the process to carry a bit stream through a physical medium. It instructs the physical systems and interfaces perform the data transfer, being properly transferring individual bits from one system to another. Physical layer positions process to data link layer, through the transmission medium.

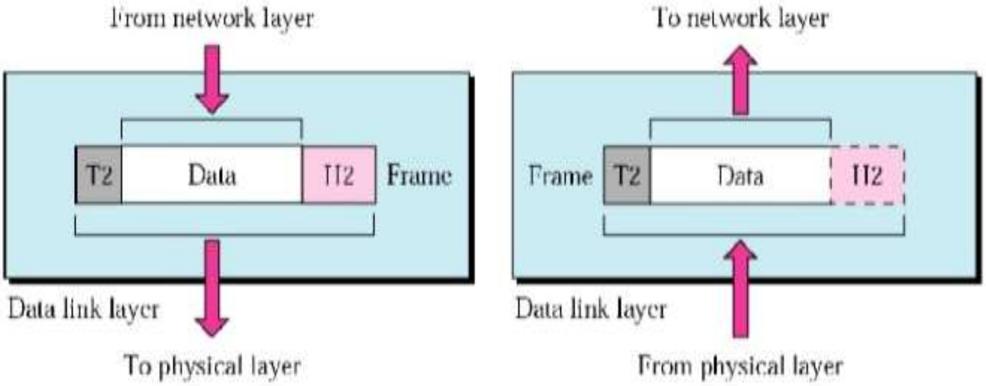


Characteristics

1. Physical characteristics of interfaces and medium
2. Representation of bits
3. Data rate (transmission rate)
4. Synchronization of bits
5. Line configuration
6. Physical topology
7. Transmission mode

1. *Data Link Layer*

It is the next layer to the physical layer makes it look error-free to network layer. The frame movement between devices is done by the data link layer. The data units being transferred to network layer as bit streams is frames. This illustrates node-to-node delivery.



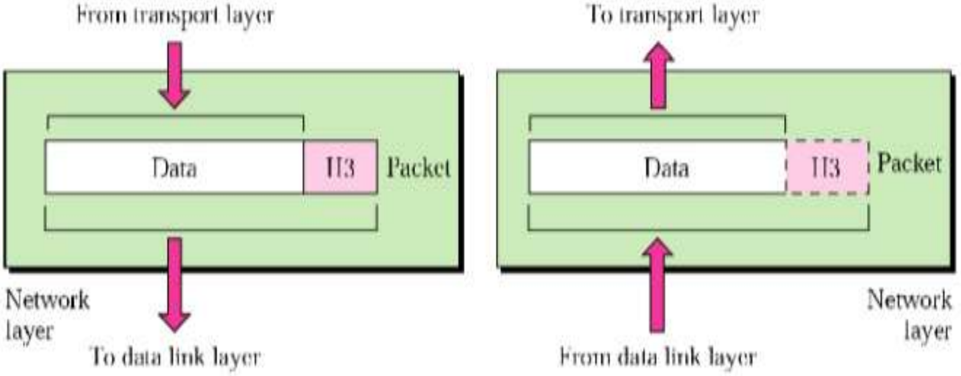
Characteristics

Different characteristics are listed as follows.

1. Framing
2. Physical addressing
3. Flow control
4. Error control
5. Access control

2. *Network Layer*

It facilitates the delivery of packets across networks, through links from source to destination. It delivers packets between two devices in same network. Both networks and links are connected to create networks of networks or mass networks called as routers or switches.



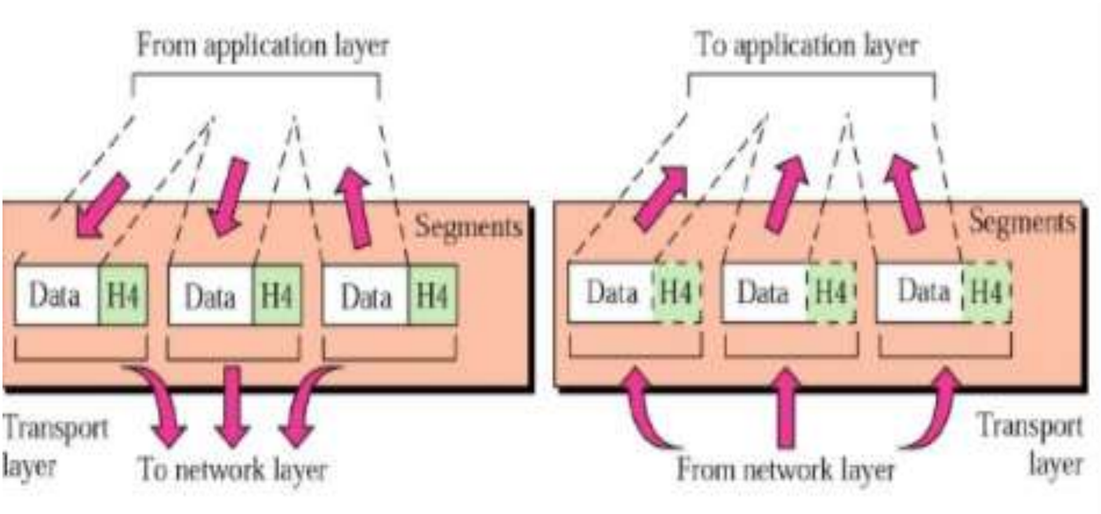
Characteristics

The various characteristics are listed as follows.

- Logical addressing
- Routing

3. Transport Layer

The delivery of the complete messages without damage is the purpose of this layer. An application program executed on a host machine performs the said process.



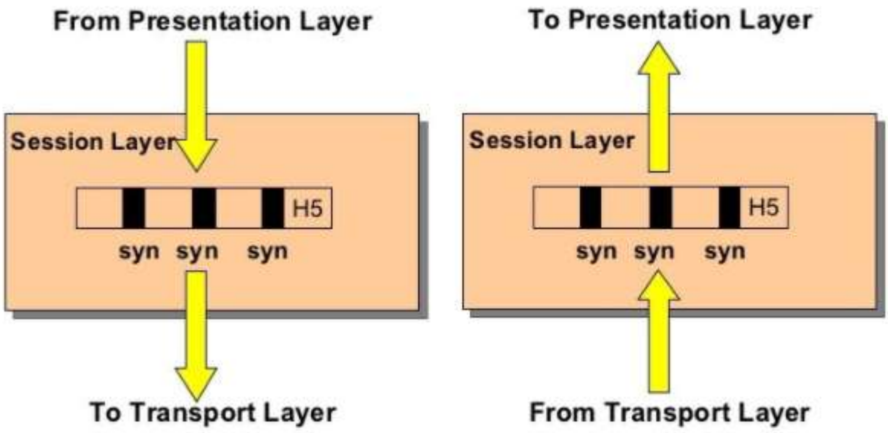
Characteristics

The various characteristics are listed as follows.

1. Service-point addressing
2. Segmentation and reassembly
3. Connection control
4. Flow control
5. Error control

4. Session Layer

The facilitation, maintenance and synchronization are the activities of session layer. It is the network dialog controller.



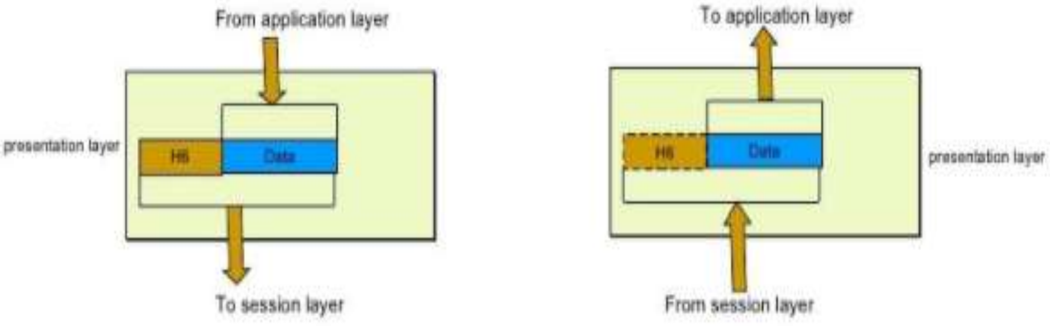
Characteristics

The various characteristics are listed as follows.

- Dialog control
- Synchronization

5. Presentation Layer

The syntax and semantics of messages are preserved in this layer. It holds the responsibilities of performing translation, compression and encryption.



Characteristics

The various characteristics are listed as follows.

- Translation
- Encryption
- Compression

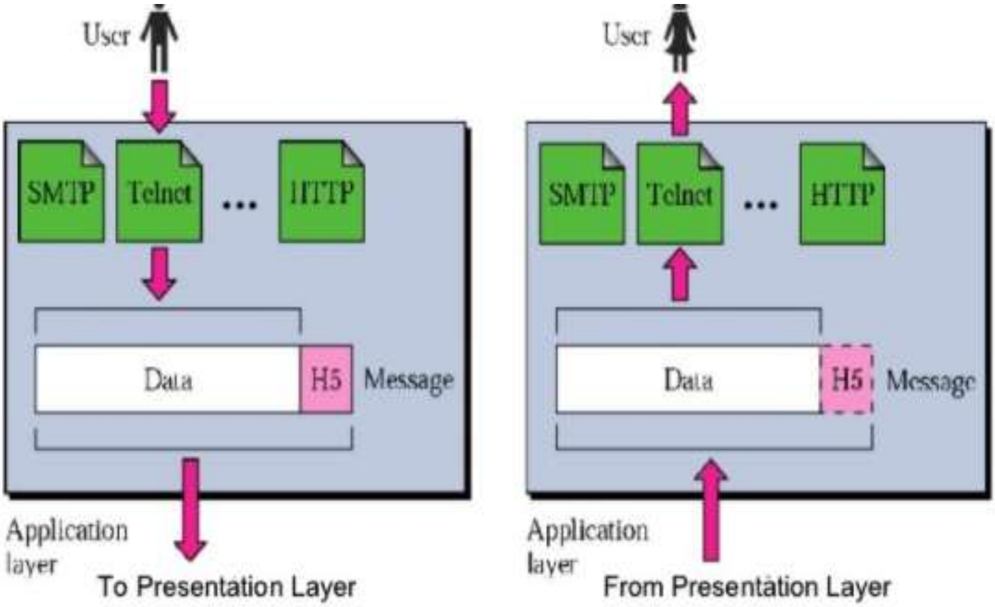
6. Application Layer

User interfacing is enunciated in this layer which supports various services like e-mail, remote file control, shared database management and distributed information services.

Characteristics

The various characteristics are listed as follows.

- Network virtual terminal
- File management
- Mailing services
- Directory services



Types of Connections

Link means two or more devices connected to each other through physical connection in a network. Computers connected in link is also referred as nodes, hosts, work stations.

1. Point to point connection
2. Multipoint connection

1. Point – to – point

A dedicated direct connectivity is established between systems.

Example - Remote control, TV control system.

2. Multipoint

Multipoint connection supports sharing of channel capacity among stations in the network.

- Spatially shared communication.
- Time shared connection.

Spatially shared - more than one device sharing the link simultaneously.

Time shared - devices share the link on turn by turn basis.

Switched Network

Switching is a methodology which interconnects multiple connectivity to establish a large network to have an effective communication. A switched network contains a sequence of nodes that are interlinked with each other known as switches. The circuit switching, packet switching and message switching are the categories of switching.

Circuit switching - It is established by physical connectivity to form networks of 'n' number of channels.

Packet switching - The message is divided into packets of fixed or variable size and transmitted.

Message switching - Messages are received, stored and transmitted.

Internetwork

When two or more devices are connected by an established communication link for sharing data or resources or exchanging messages is called as network or networking. When two or more networks need to be connected for the same purpose is called an internetworking or network of computer network. The connecting devices, routers, gateways are used to connect independent networks to form internetwork.

Addressing

The address of a node given by LAN or WAN or MAN is the physical address. Logical address is essential for universal communications to identify each host uniquely which are not basically dependent on underlying physical networks. Physical address changes hop-to-hop. Logical address remains same. Process of forwarding the messages to the destined node as per its addressing is called as routing.

Types of Address

1. **Unicast -** Once source & one specific destination.
2. **Broadcast -** One source & all nodes on the network.
3. **Multicast -** One source & some subsets of nodes on the network.

Cost Effective Resource Sharing

1. Modem (Modulator+ Demodulator)

It is used to perform both modulation and demodulation according to the requirement.

2. Multiplexer & Demultiplexer

The process of transmitting more signals simultaneously on one path is termed as multiplexer. The process used to perform demultiplexing, which separates the signal and send it to the appropriate destination device.

Reliability

1. Error Control

The data must be delivered to their destination accurately as it was sent from the source. Reliability is achieved by check summing each packet in source and verifying the checksum at the destination. Internet protocol (IP) is the mechanism which is used by TCP/IP protocols for transmission of data.

Types of Error

1. single bit
2. multiple bit(or) burst error

Single bit – If only one bit in a given data string is permissible to change during the transmission.

Burst bit - if two or more consecutive bits in a data string are permissible to change.

- Single bits affect only one character.
- Burst bits affect one or more characters.

1. Congestion

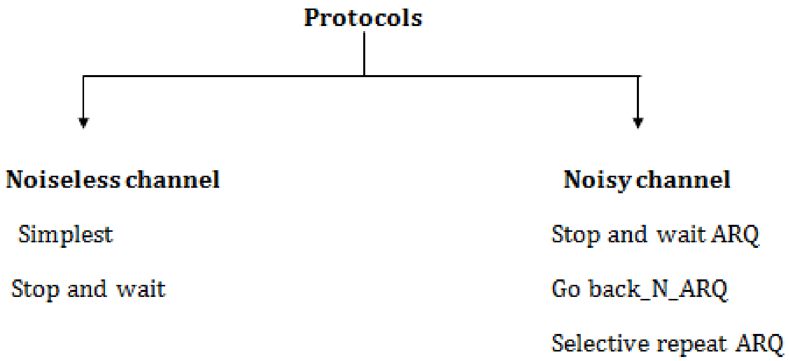
Packets are lost due to congestion in the link to overcome in the network uses congestion control mechanisms. Congestion occurs if the users of the network send data at a rate that is greater than the network can handle (number of packets). When enormous packets are present in the subnet, the performance of the network will be degraded. To handle congestion as prevention or control, this is used.

2. Retransmission

If a packet is damaged, lost, delayed during transit (or) if the acknowledgment has not yet been received, then it will be retransmitted.

1.3.2. Protocols

The process of framing and achieving appropriate control over flow and error handling in delivery of data is implemented in datalink layer using protocols.



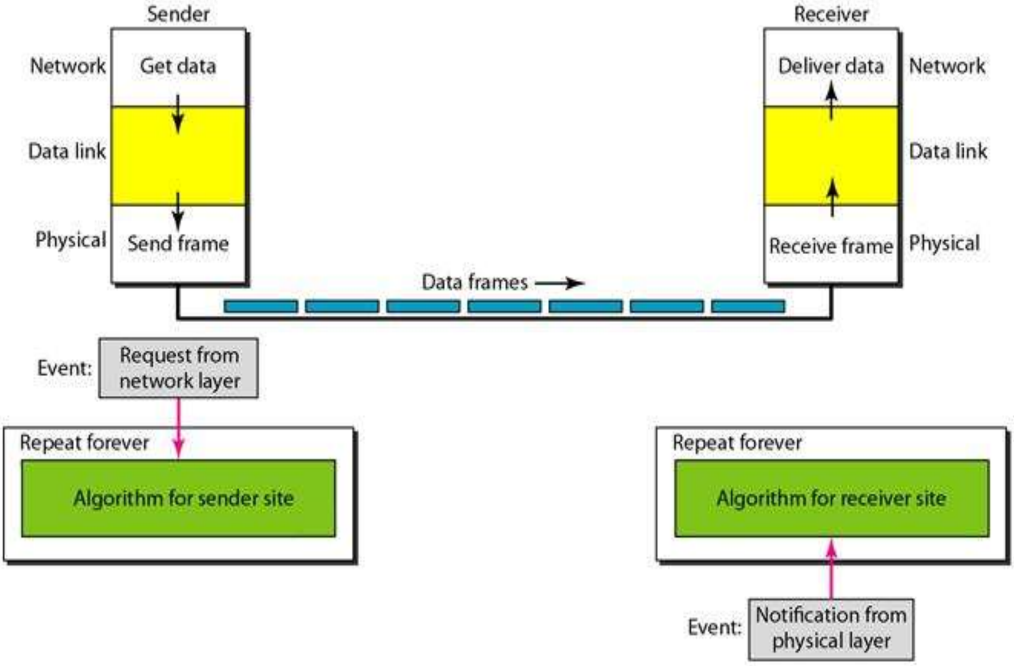
In general, the data frames travel from sender to receiver because of unidirectional property. The acknowledgement (ACK) and negative acknowledgement (NAK) which are identified as special frames flow in direction which contradict one another with the data flow direction. Piggybacking is the process of including ACK and NAK in the data frames, to hold the flow and error control information.

Noiseless Channel

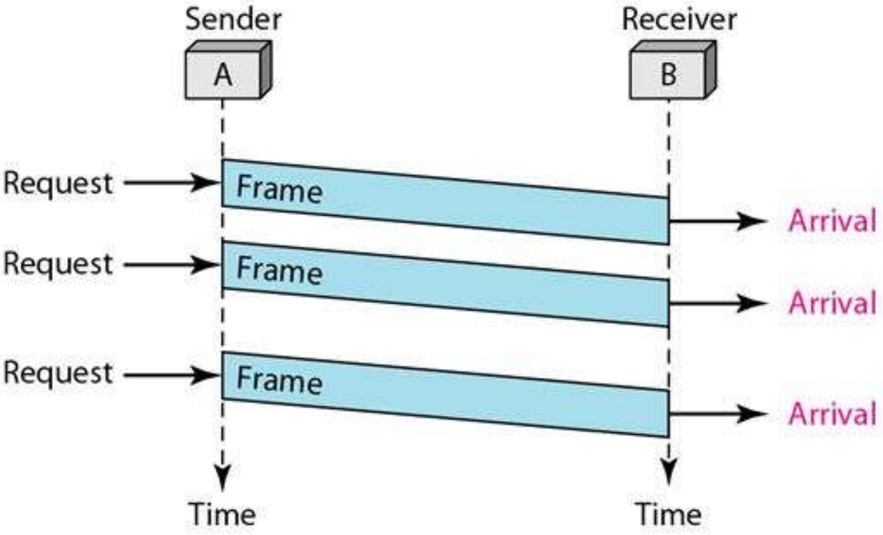
The protocol of noiseless channel devoid usage of flow control.

1. Simplest Protocol

This protocol lacks flow control. At the transmitter's site, data in the data link layer is obtained from network layer by preparing a frame and transmitting it. On the other end, at the receiver end, the frame is received via the physical layer and the data is extracted from the received frame and delivered to the network layer. It is noted that the datalink layers offer transmission to the sender and receiver and vice versa, to its network layers. Also, in order to transmit bits physically, these data link layers use the services provided by their physical layers. A frame is transmitted from the sender's site only when a data packet is held by the network layer and this data packet is delivered only when the frame arrives the receiver site. When the event at the sender site or receiver site is running constantly, and no action will be encountered until the network layer requests at the sender site or any notification is received at the receiver's site.



Flow Diagram

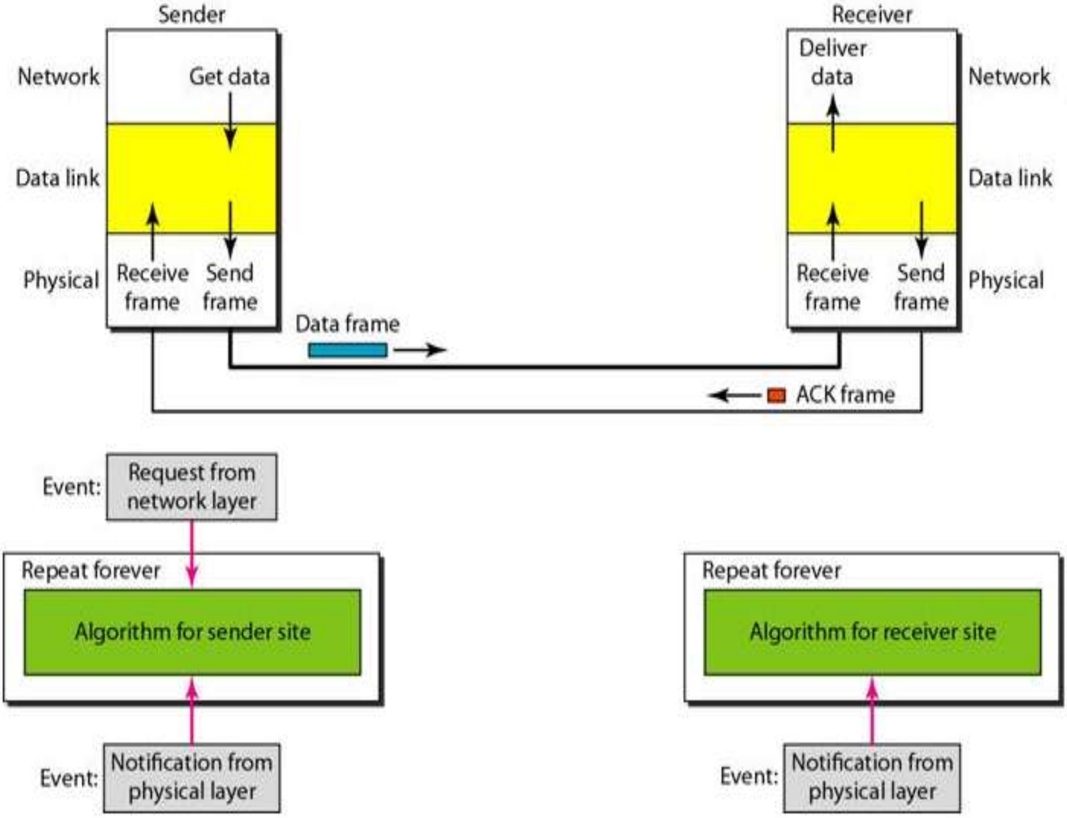


2. Stop and Wait Protocol

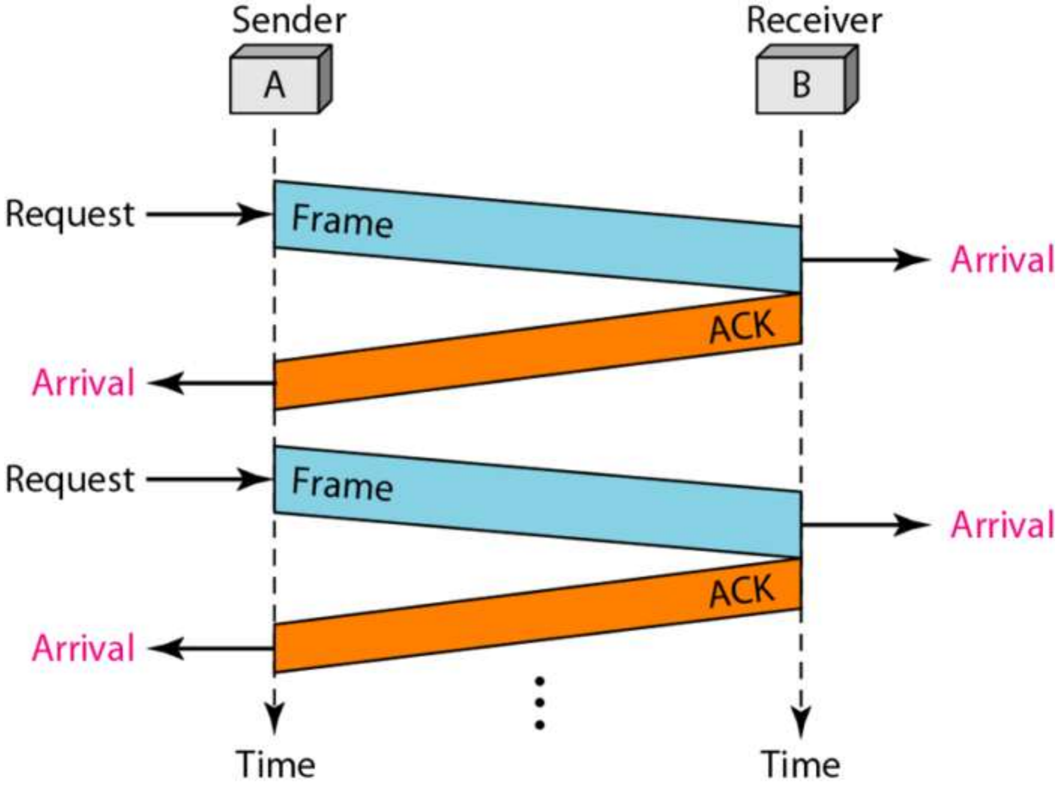
The arrival of data being earlier at receiver location, the data frames have to be retained before its deployment. Particularly when receiving data from several sources, the receiver just doesn't have enough storage capacity.

This either results in the abandoning of frames or denial - of - service. To stop the receiver being overloaded with frames, instruct the sender to slow down. Feedback from the recipient to the sender must be present. The sender sends a frame in stop-and-wait protocol, stops until the recipient receives the approval and then continues to transfer. For data frames it is unidirectional communication but ACK auxiliary frames move from the other direction. The traffic is visible on the channels enunciating the forward for data and backward trail for ACK. Here they employ half-duplex connection. Either a request from network layer or an arrival note from physical layer or both are done.

Until the recognition of the frame, the reply has to be deferred or ignored. The channel does not repeat the frames and is error free. However, the network layer can post a request continuously ignoring in-between arrival. It stops the data frame from being sent straight away. When a frame is sent and when the receiver receives the data frame, the variable is set to send ACK. When an ACK is received it sets it as true to allow the next frame to be sent. If it's a false it can't allow the sender to send the next frame. Note the protocol sending two frames includes the sender in four events, and the recipient performs two events.



Flow Diagram



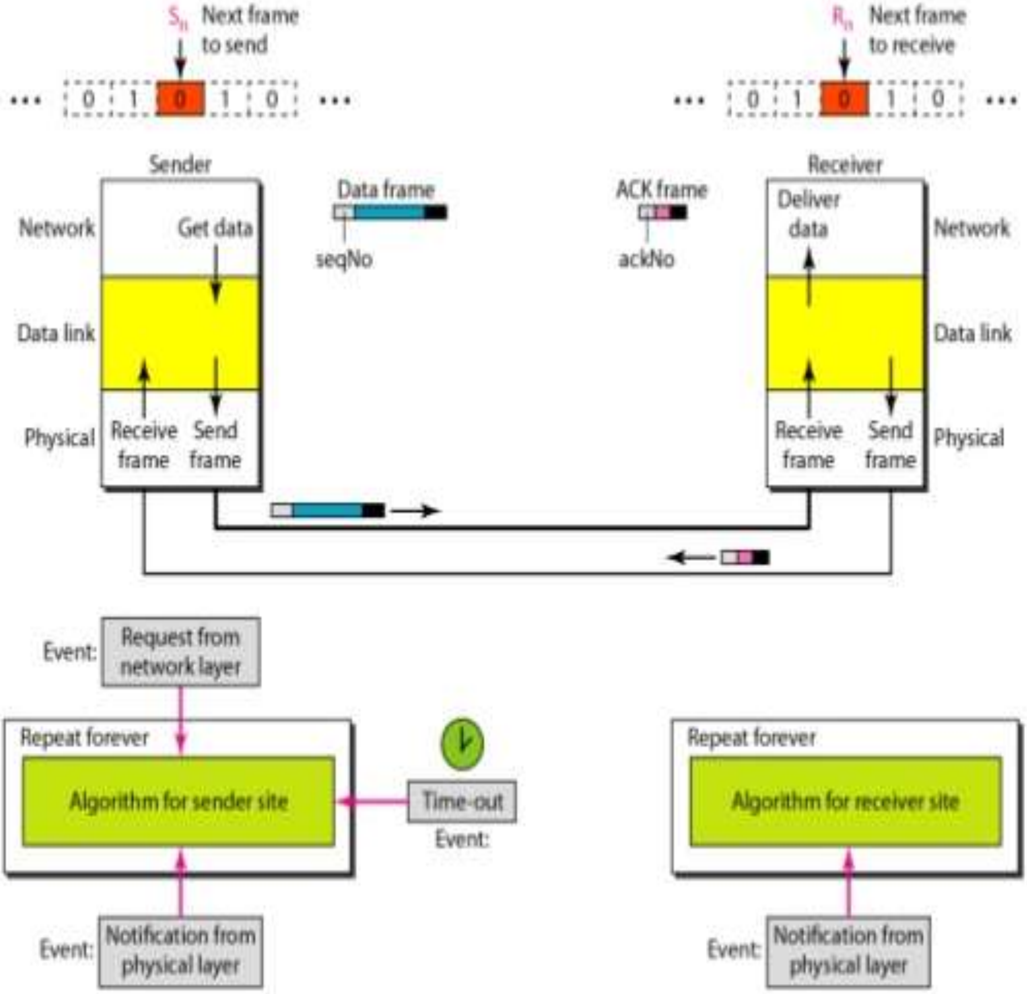
Noisy Channels (It Adds Idea to Flow Control)

1. Stop and Wait Automatic Repeat Channels

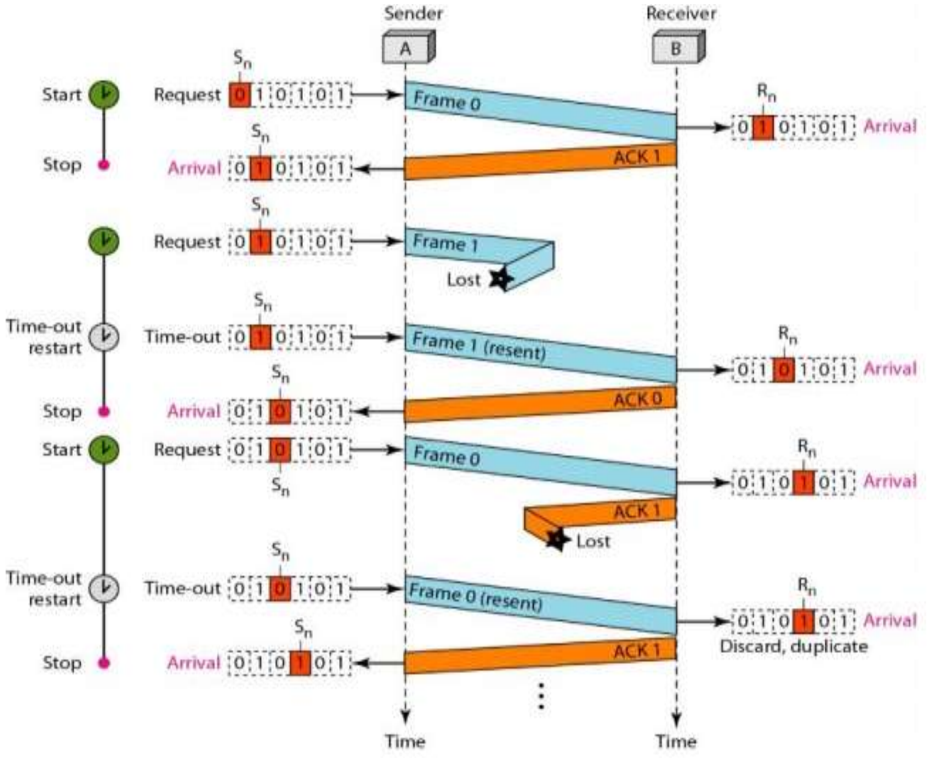
Stop and Wait-ARQ is a basic protocol which aids in error control mechanism. It is important to add redundancy bits to the data frame to identify and correct corrupted frames. The broken message is tested and discarded at the receiver. In this protocol, the detection of errors is manifested by the receiver's silence. Lost frames are toughest to manage than corrupted ones. There is no way for a frame to be marked. The right one or a duplicate frame or a frame out of order might be the receiver frame. When the receiver receives an out-of-order data frame, that means frames have either been missed or recreated.

Timer is used in this protocol, as and when the timer expires and if the sent frame is not acknowledged, the frame is resent, the copy is preserved and the timer is restarted. The protocols use the stop and wait system, as redundant data prevails in the network, there is only one unique frame that requires an ACK. By holding a copy of the sent frame and retransmitting the frame when the timer expires, error correction is done in stop and wait ARQ.

Whereas an ACK frame can sometimes be distorted or destroyed, redundancy bits and a sequence number are required as well. The ACK frame for that portal has a number field sequence. The sender actually discards a damaged ACK frame or avoids an out-of-order in this protocol.

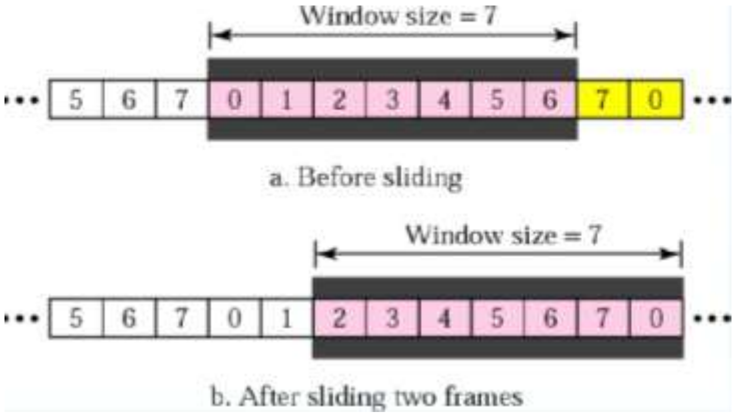


It states that sequence numbers must be designated to each frame. A field is added to the data frame by storing the sequence number of that frame. We provide sequence number frames in Stop and Wait ARQ. The sequence numbers are based on the arithmetic of mod-2. The data frames and the ACK frames have to possess same sequence number. The number of the acknowledgment often alerts the recipient with next frame by sharing its sequence number.



2. *Go Back 'N' ARQ*

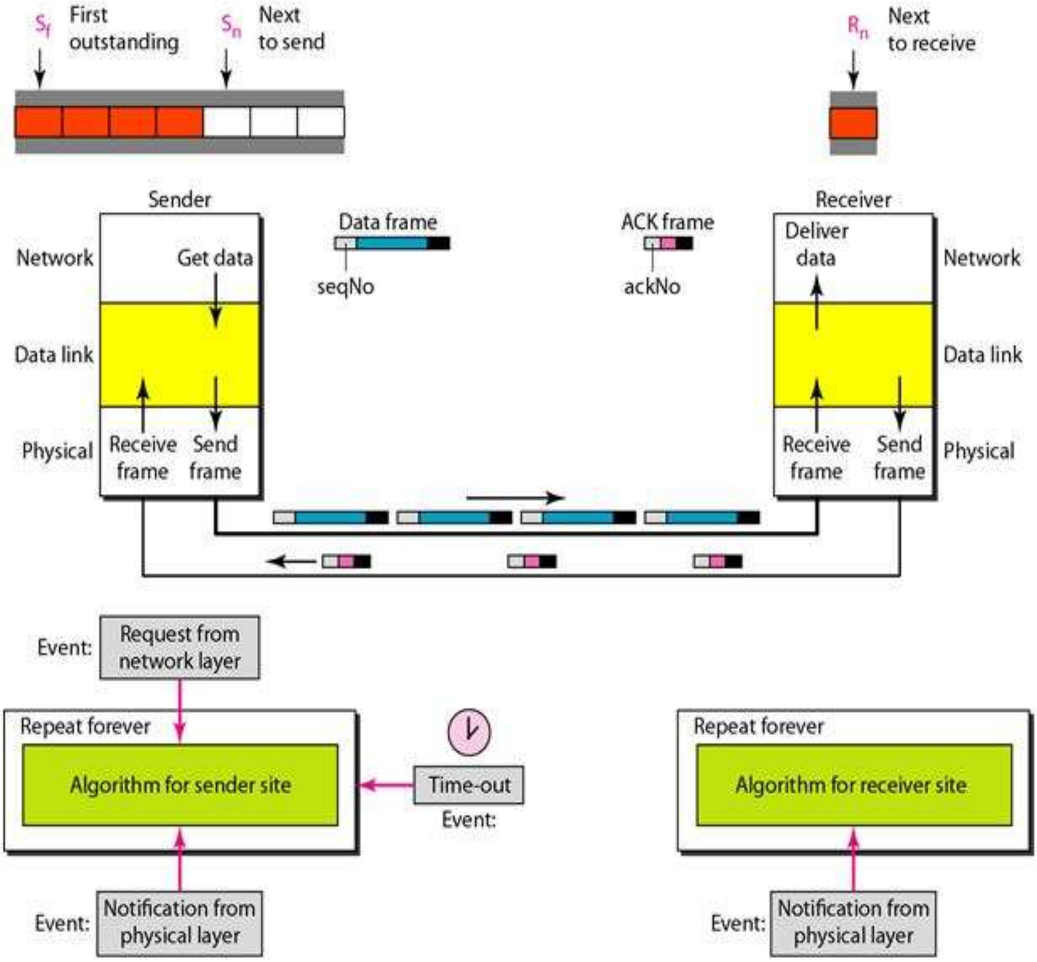
In the stop-and-wait procedure, the transmission time needed for a frame to enter the receiver plus the transmission time for the recognition to return is negligible. In system like satellite system, the round-trip time can be as long as 500 ms (propagation delay) this protocol is also known as back N ARQ. This technique is used to resolve the stop and wait ARQ inefficiency by enabling the transmitter to continue to send adequate frames so that the channel is kept occupied while the transmitter is waiting for recognition. If one frame is damaged or lost, all frames are sent after retransmission of last frame.



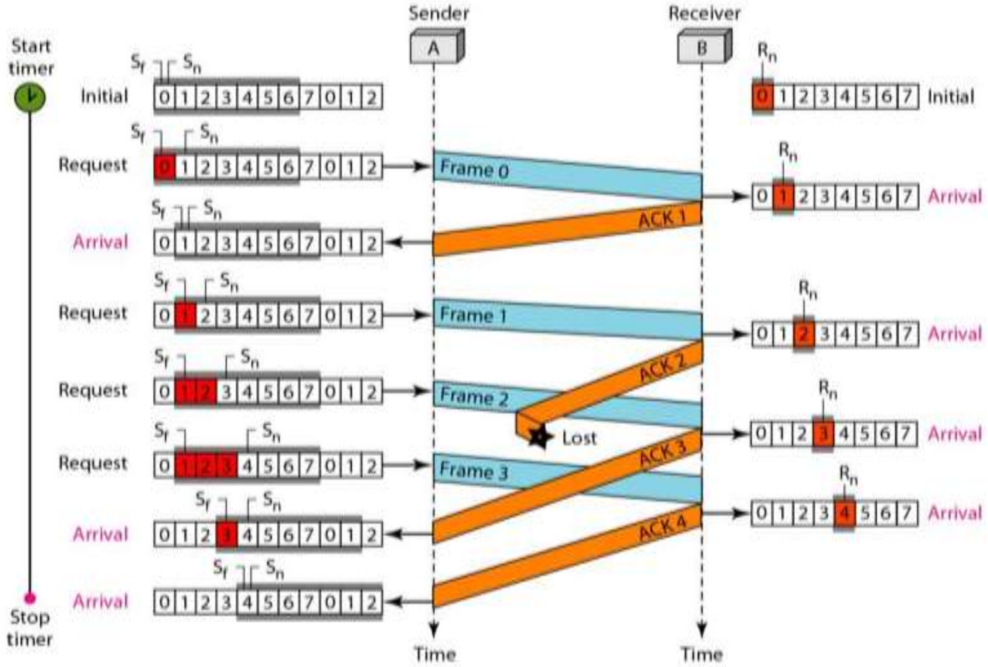
a. Before sliding

b. After sliding two frames

The sender does not wait for an ACK signal for the next frame to be transmitted. It continuously transmits the frames as long as the NAK signal is not received by it. NAK is sent to sender by the recipient. If the transmitted frames are damaged or destroyed, or if the acknowledgment is destroyed, the error can be implemented. If the second frame is impaired, error is detected and NAK – 2 signal is sent to the receiver back. The transmitter begins retransmission from frame 2 upon receiving this signal. The receiver discards all of the frames obtained after frame 2.



If the receiver does not receive a specific data frame, it sends a NAK to the transmitter and the transmitter retransmits all the frames received from the last recognised frame. After each data frame the transmitter does not anticipate an acknowledgment in return N. The transmitter can send as many frames as the window allows until an acknowledgment is awaited. It must wait until the timer goes off and retransmit all frames again until limit has been reached or the transmitter has no more frames to transmit. The selective repeat ARQ is most powerful but complex of all ARQ protocols. In this process, the sender retransmits only the frame that is damaged or lost. Like go-back N process, the lost ACK or NAK frames are handled in the same way. This method employs pipelining. The previous task is completed as pipelining in the networking of a task is always initiated. It increases transmission quality.



1.4. Internet Architecture

Internet Architecture or Internetworking Architecture → Transmission Control Protocol / Interconnecting Architecture → TCP/IP

TCP / IP is a compilation of rules and procedures setting out how all transmissions are transmitted over the Internet In 1969, TCP/IP was originally developed as protocol for networks that was connected to advanced research project agency network (ARPANET) ponded by defence advanced research projects agency (DARPA) in us. This protocol is composed of a broad set protocol, released as standards.

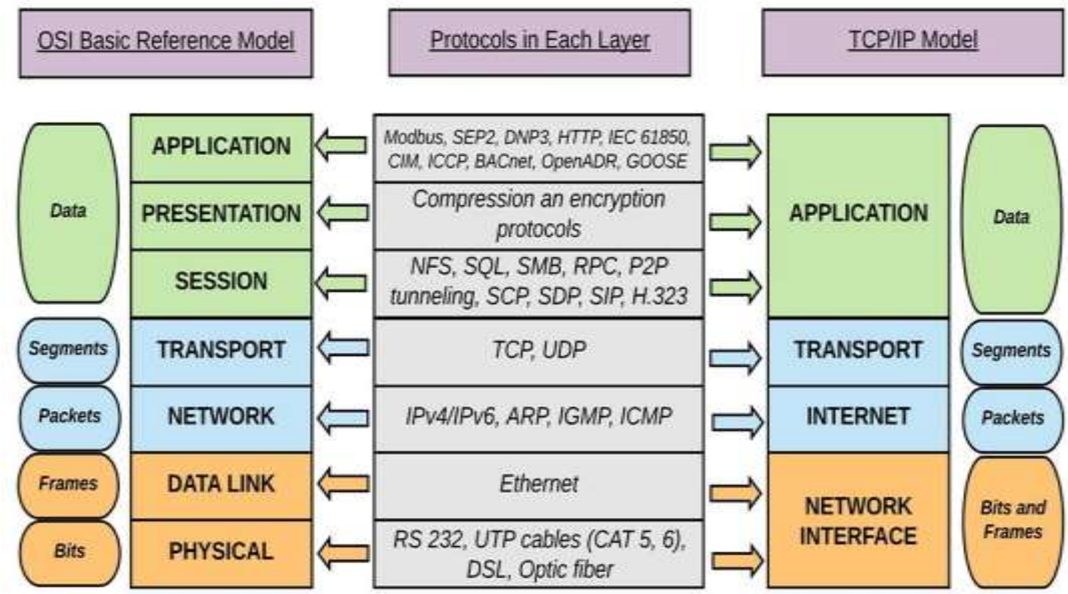
Internet Standards by the Internet Activities Board (IAB)

There are 4 layers in TCP/IP:

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Host to Network

TCP/IP layers was developed prior to OSI model. Host to network is a mix of physical as well as datalink layer. The Internet layer is comparable to the network layer of the network. The application layer consists of a mixture of session, presentation, and application layer with transport layer support. The basic functionalities of these 4 layers are given so.

At transport layer, TCP/IP supports 3 protocols namely, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and SCTP (Stream Control Transmission Protocol).


OSI Basic Reference Model
Protocols in Each Layer
TCP/IP Model
Data
APPLICATION
Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE
PRESENTATION
Compression an encryption protocols
SESSION
NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323
APPLICATION
Data
Segments
TRANSPORT
TCP, UDP
TRANSPORT
Segments
Packets
NETWORK
IPv4/IPv6, ARP, IGMP, ICMP
INTERNET
Packets
Frames
DATA LINK
Ethernet
Bits
PHYSICAL
RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber
NETWORK INTERFACE
Bits and Frames

TCP/IP is hierarchical consisting of networking devices, each with a particular feature.

1. Host to Network (Physical and Datalink Layer)

- At physical and datalink layers, no specific protocol is given in TCP/IP.
- It adheres to work with standards and propriety procedures.
- TCP/IP can be a LAN or WAN.

2. Network Layer (Internet Layer)

- The IP in the network layer is supported by TCP/IP.

Internetworking Protocol (IP)

- This protocol is unstable and connectivity-free as the strongest service delivery effort.
- Best effort means IP doesn't check or monitor errors.
- IP transports data in packets called datagrams.

Address Resolution Protocol (ARP)

- ARP is used to connect a physical or station address with a logical address.
- A station address is defined by each device on a connexion.
- ARP is used specifically to locate a node's physical address when its internet address is identified.

Reverse Address Resolution Protocol (RARP)

- RARP helps a host to explore when its physical address is identified at international addresses.
- This is invoked when a computer initially establishes connectivity with network or during the booting of a diskless computer.

Internet Control Message Protocol (ICMP)

- ICMP is enabled during data issues and intimates to the host through gateway to notify sender.
- ICMP sends messages about query and costs from accidental loss.

Internet Group Message Protocol (ICMP)

- IGMP facilitates the simultaneous transmission of messages to a set of receivers.

3. Transport Layer

- Two protocols addressed the transport layer in TCP / IP: TCP, UDP.
- IP is a device communication -to-host which can send a packet from one physical device to the next.
- UDP and TCP are transport-level protocols which carry a process-to - process communication.

User Datagram Protocol (UDP)

- The simplest of TCP / IP protocol is the UDP.
- It is a process - to - process protocol that adds data from the data to the upper layer with only port address, checksum, error control and length information.

Transmission Control Protocol (TCP)

- TCP facilitates applications with complete transport facilities.
- A stable stream transport protocol is TCP.

- A link between both ends of the transmission must be formed before the data can be transmitted either.
- TCP breaks a data stream into smaller units at the transmitting end, called segments.
- TCP collects each datagram at the receiving end, as it reorders the transmission based on sequence numbers at the receiving end.

Stream Control Transmission Protocol (SCTP)

The SCTP supports new applications such as voice over internet.

The best features of UDP and TCP are combined in the transport layer protocol.

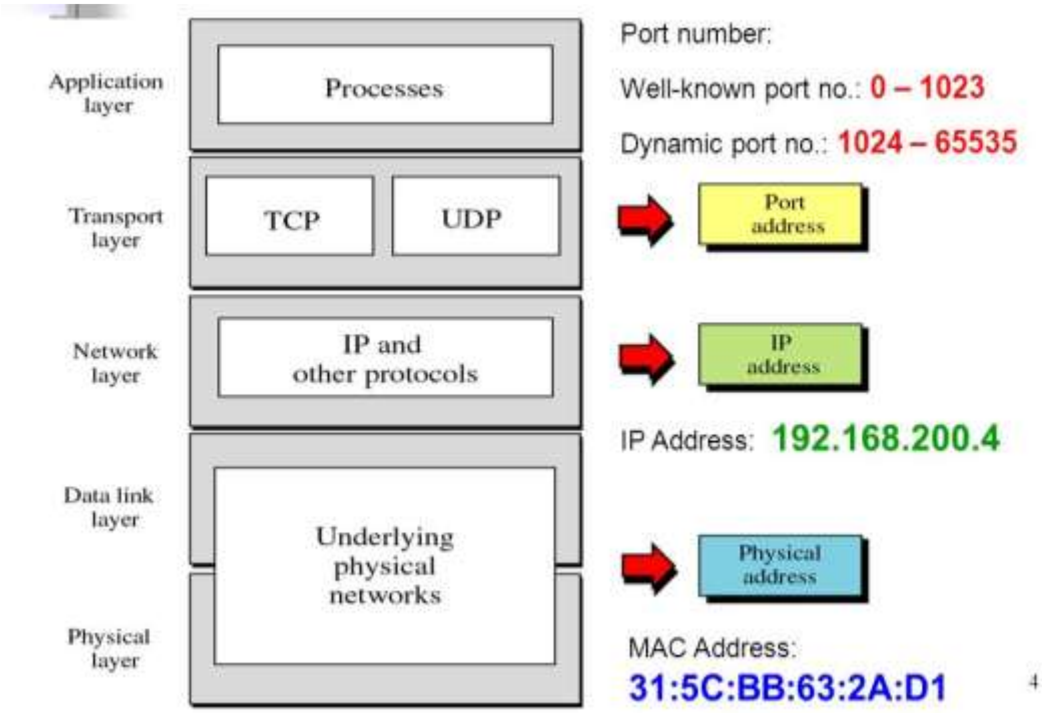
4. Application Layer

The TCP / IP application layer equals OSI session, presentation and application layers.

Addressing in TCP/IP

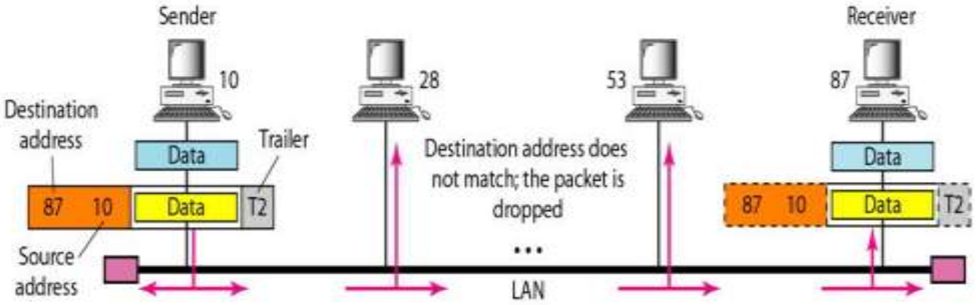
Various levels of addresses used in TCP/IP protocols are:

1. Physical (link) Address
2. Logical (IP) Address
3. Port Address
4. Specific Address



1. Physical Address

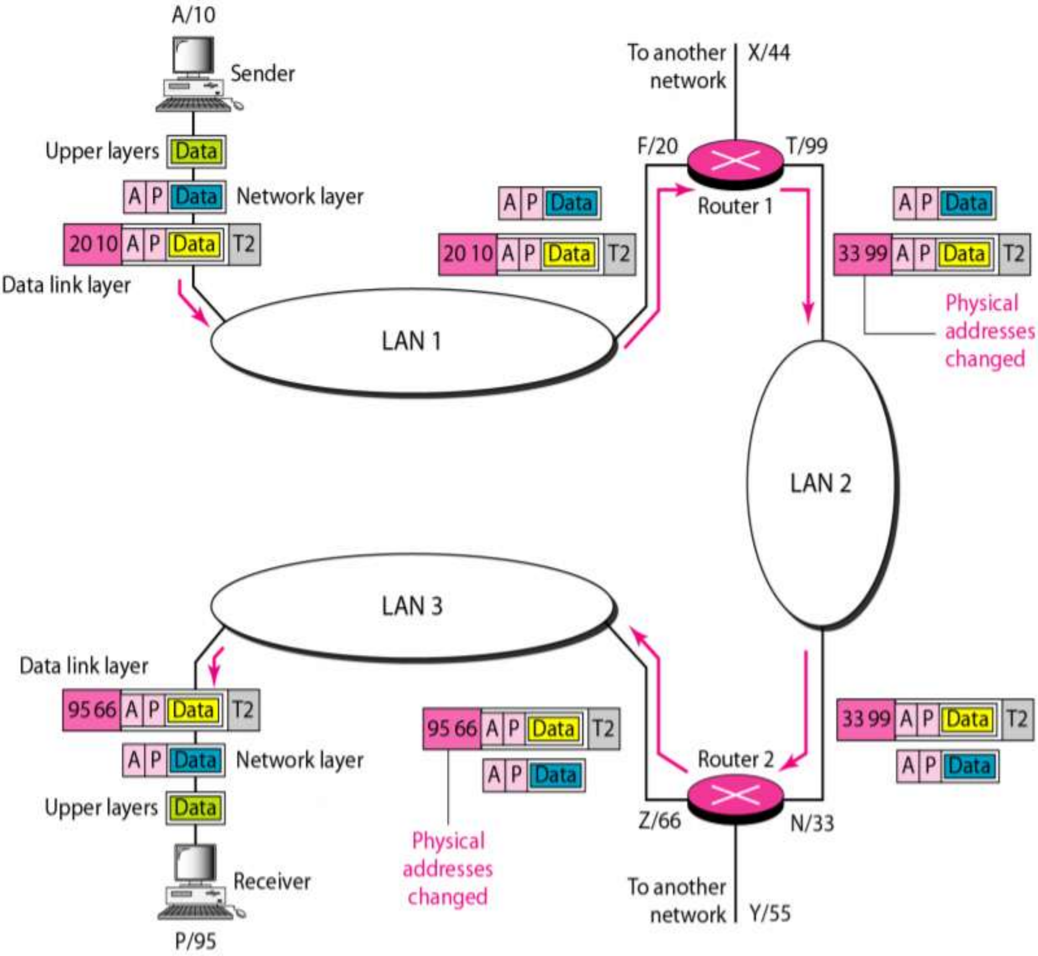
- The physical address is known as the link address.
- It is a node's address as specified by its LAN or WAN.
- It is included in the frame that the data link layer uses.
- Physical Address holds the authority over Networks (LAN or WAN).
- These address size and format differ depending on the network.



Physical Address is given by 6 Bytes (12 Hexadecimal Digits)

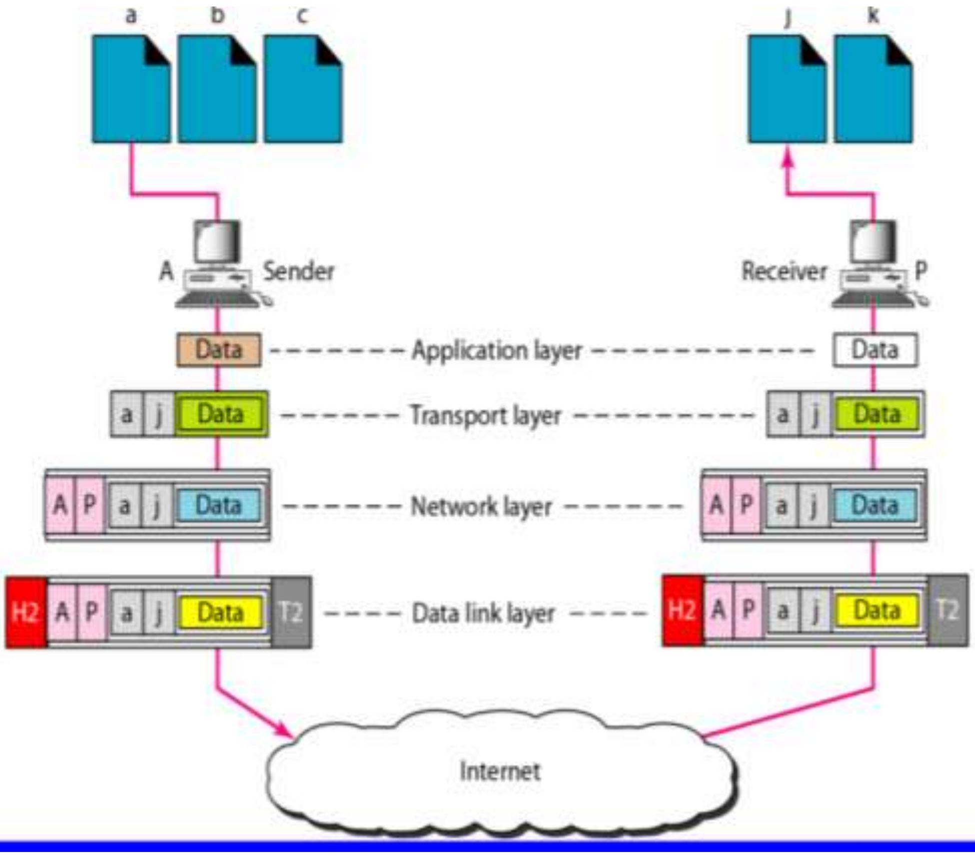
2. Logical Address

- It establishes global connectivity irrespective of the physical grids underlying them.
- A logical internet address is usually a 32-bit address that can be uniquely connected to the interconnect host
- The physical addresses will vary between hop to hop, but typically the logical addresses stay the same.
- Publicly addressed and visible hosts on the internet must have different IP addresses.



3. Port Address

- The IP and Physical address are required for information to be transported from source to destination host.
- Computer devices can concurrently run several processes.
- Internet networking is an interacting mechanism with other processes.
- In ICP / IP, a port address is called the label assigned to a method.
- The TCP / IP port address is 16 bits long.
- The Port address typically remains unchanged.
- A 16-bit port address is represented by a single number.



4. Specific Address

- User friendly addresses also exist for certain applications.
  E.g: E-Mail id, URL, WWW
- Sender can change the addresses with the corresponding port and logical address by the sender.

1.5. Network Software

Network design and protocol requirements are significant; however, the design is inadequate in justifying the internet's remarkable performance. The number of internet-connected computers has exponentially increased because of the functionality provided by the internet. Computer networks are capable in principle of transporting any kind of information such as digitized images, digital voice and so on. It was very slow to send and receive data to do something useful with the information. Today's networks are increasingly being used to carry multimedia, and their support for it can only increase as hardware becomes faster. Software applications are designed to communicate with users and a communication protocol set to communicate across the globe.

Application Programming Interface (API)

(sockets)

- The network-export interface is the place to start when implementing a network application.
- Most of the network protocols are software and network protocols along with operating system are utilized by neighbouring computers. nearby all computer systems implement their network protocols as part of the operating system (exported by the network).
- When the "exported via the network" interface normally refers to that given to its networking subsystem by the OS.
- This interface is also called the programming interface for network applications (APIs)
- Each operating system is allowed to define its own network API using socket interface.
- The benefits of any single API supported by industry are, the applications can be easily transferrable from one OS to another and the applications are simple to be developed.
- To describe socket interface, a set of services along with the syntax that can be provided on a particular computer system.
- Generalization is positively a goal of the socket interface.
- A good way to think of the socket is, at the point where a local application process gets connected to the network.
- The interface defines operations for
  1. Creating the socket
  2. Attaching the socket to the network
  3. Sending/receiving messages though the socket
  4. Closing the socket

1. Creating a Socket

int socket_fd (int domain, int type, int protocol)

The protocol family in the domain specifies 3 arguments namely, PF_INET - Internet family, PF_UNIX - Unix pipe facility and PF-PACKET - Direct access to the network interface.

The type argument indicates the semantic of the communication,

SOCK_STREAM_byte stream

SOCK_DGRAM_message-oriented service

The protocol argument identifies the specific protocol has been used,

UNSPEC combination of PP_INET&SOCK_SYSTEM

2. Attaching Socket to the Network

The attachment depends on the client and the server. A passive open is performed by the application process, on the server machine.

The server invokes 3 operations namely,

int bind (int socket_fd, struct sockaddr*address, int addr_ len)

int listen (int socket_fd, int backlog)

int accept (int socket_fd, struct sockaddr*address, int*addr_len)

To link the newly formed socket to the designated location, the link operation is used. Here, the local participant server addresses the network. The IP address of the server and the number of ports of the TCP is available at the address. The listening operation determines how many communications on the socket listed are pending. The accept procedure performs accessible passive. The blocking process will not return until the combination has been established by a remote participant. A new socket that is already in relation is returned once it is full and the address statement includes the address of the remote participants. An active open on the customer computer is performed by the application process, and a single operation given below is invoked by stating who seeks to make a connection,

int connect (int socket_fd, struct sockaddr *address, int addr_len)

The address includes the address of the remote participant. Typically, the client specifies only the address of the remote participant and the device fills in the local information. On a well-known port, the server listens to message.

3. Sending\Receiving Messages through Socket

In general, two operations are invoked by the application process once a connection is established, in order to send and receive the data messages,

int trx (int socket_fd, char*message, int mes_len, int flags)

int rcx (int socket_fd, char*buffer, intbuf-len, int flags)

Certain details of operations are controlled by both the operations taken as the set of flags.

1.6. Performance

Performance

- In network design, performance is an important factor for any computers.
- Two approaches measures network performance.
  - Bandwidth
  - latency
- Both are put in together, to define the performance of the given link.

Bandwidth

- "The number of bits that can be transmitted over the network in a certain period of time" is defined as the bandwidth of the network.

Bits Per Second (**BPS**)

Latency

- The time occupied by the transmit of messages from one end of the network to another end.

Round Trip Time (RTT)

- The consumption of time for message to travel between different ends.
- It has 3 components.

Latency=propagation + transmit + queue

Propagation = distance / speed of light

Transmit = size / bandwidth

Where distance = length of wire in which data travels

Speed of light = speed of light over that particular wire

Size = size of packet

Bandwidth = bandwidth at which is packet to be transmitted

Jitter

- Jitter is a parameter related to delay.
- Jitter time is the interval between the maximum effect (or minimal effect) of a signal in two periods.
- It is produced by electromagnetic interference and cross talking with other signal carriers.
- Different data packets encounter various delays.
- The data packets that hit the recipient at various times, triggering jitter.

Throughput = packet transfer size / packet transfer time

Transfer time = RTT + 1 / bandwidth + packet transfer size

Problems

1. If bandwidth is 10mbps, what is the bit duration time?

If bandwidth is 10mbps

The bit duration is

Bit duration=1/bandwidth

1/10*1000000

=10 microseconds

2. For I mb over a 1Gbps network with RTT 100 milliseconds, bind out the transfer time and throughput of the link

Transfer time =RTT+1/bandwidth*transfer size

=100ms+1/1Gbps*1MB

100+1/1*1000000000*1*1000000*8

=100ms+8ms =108ms

Throughput=transfer size/transfer time

=I MB/108ms

=1*8*1000000/108*1000

=74.1Mbps

3. Consider a p-p link 50 km in length. At what bandwidth would propagation delay (speed 2*100000000m/s) equal transmit delay for 100 bytes packet? What will be the 5/2 bytes packets?

Propagation delay = distance/speed of light

=50*1000/2*100000000 m/s =250 micro seconds

Propagation delay is equal to transmit delay

Transmit delay=size/bandwidth

=packet size/transmit delay

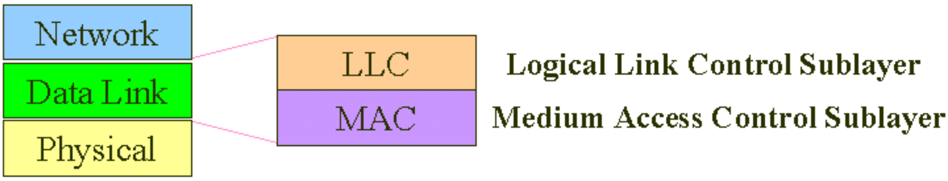
=800 bits/250 micro seconds

=3.2 micro bps

1000 bytes = 100*8 = 800 bits

1.7. Datalink Layer

The data link layer is responsible for converting a new transmission capacity into a link that is accountable for node-to-node (hop-to-hop) communication. The most important tasks of the data link layer are given below.



1. Logical Link Layer Access

Framing

Addressing

Flow control

Error control

2. Media Access Control

The layer of data links divides the stream of bits obtained from the network layer onto 1 manageable data unit called frames. A header is added to each frame at the data link layer in order to specify the frame addresses of the sender and receiver. By incorporating mechanisms for detecting and retransmitting defective, redundant or final frames, the datalink layer also adds stability to the physical layer.

1.8. Framing

Data transfer in the physical layer involves transferring bits from the source to the destination in the form of a single.

- The physical layer provides bit synchronisation to ensure the same bit and durations and timing are used by the sender and recipient.
- It packets bits into frames in the data link layer, which can be easily separated from each other.
- Framing the data link layer distinguishes the message from one source to the destination or from other messages to other destinations by adding the address of the sender and destination.
- The destination address specifies where the packet should go and the sender address determines which allows the receiver to recognise the receipt.

- If the frame is very wide, the flow and error management is very hard to perform efficiently.
- A 1 – bit error can cause retransmission of messages even though it is a big datagram.
- When a message is broken into smaller frames, only the small frame is influenced by a single bit.

There are two types of framing.

1. Fixed size framing
2. Variable size framing

1. Fixed Size Framing

Here the boundaries of the frames need not be defined**.** The size acts as the delimiter.

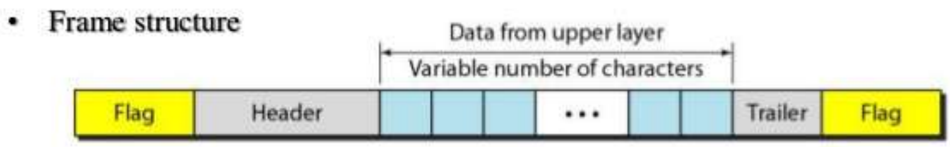
E.g: ATM wide area network, Frames of fixed size called cells.

2. Variable Size Framing

Here the end of the frame and also the beginning of the next frame are defined. There are two types **-** Character oriented approach and Bit oriented approach.

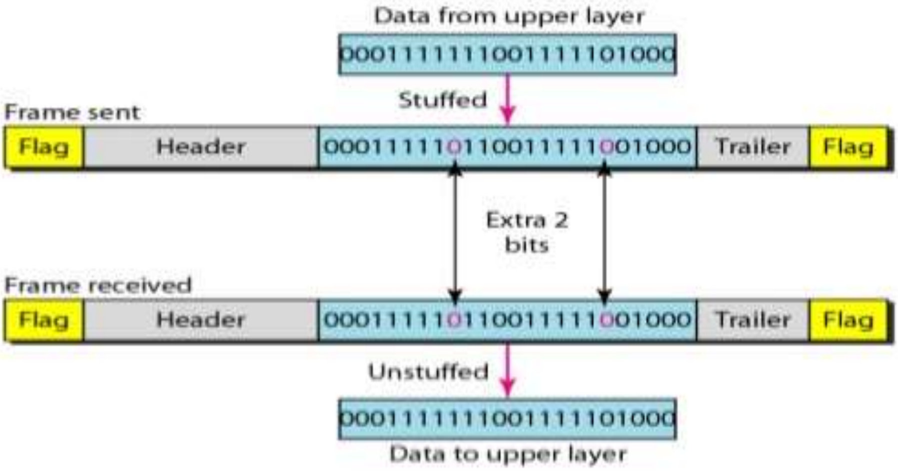
a. Character Oriented Approach

- Data carried from a coding scheme, such as ASCII, with 8-bit characters.
- The header carries the addresses of the source and destination and other control information, and the trailer carrying error detection or error correction redundant bits also has a number of 8 bits.
- To distinguish one frame and the end of the frame from the next frame.
- A flag composed of special characters based on the protocol, signals the start or end of the frame.
- Only text was exchanged in character-oriented framing via the data link layers.
- Byte stuffing (stuffing of characters) is a special byte applied to the frame's data segment as there is a character of the same pattern as the flag.
- There is an extra byte in the data segment called escape character (ESC)**.** Insertion of 1 additional byte to the frame, as a flag or escape character is byte stuffing.



b. Bit Oriented Approach

- A series of bits to be interpreted by the upper layer is the data portion of a frame.
- Delimiter is used separate frames from one another.
- Most protocols use a special flag 01111110 of 8-bit pattern which defines the beginning and the end of frame, as the delimiter.
- Here flag creates with byte_ oriented protocols.
- Bit stuffing is the process of inserting an extra 0 for every five consecutive times following a 0 in the data, so that the receiver does not mistake the 01111110 pattern for a flag.



1.9. Error Detection

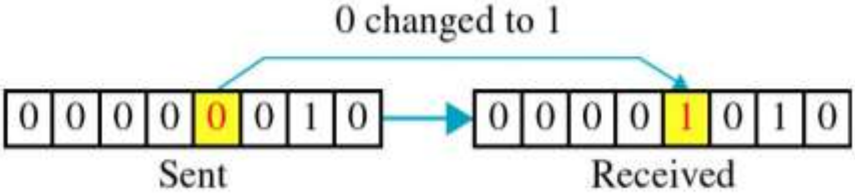
Errors

- As bits are transferred, certain unforeseeable changes occur due to interference.
- This can change the signal shape that some applications need to find and resolve errors.
- There are 2 types of errors.

1. single bit error
2. burst bit error

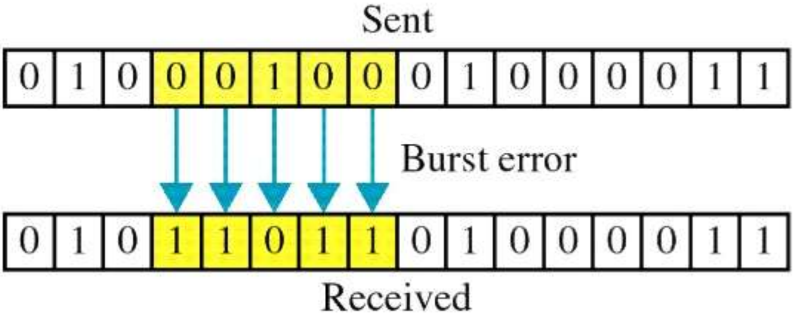
1. Single Bit Error

- Single-bit error means that only 1 bit of the data unit (byte, character, packet) has been inverted as 1 to 0 or 0 to 1.
- Only one Bit Data Unit has been modified in single bit error.



2. Burst Error

- A Term error means that the data unit has inverted 2 or more bits.
- When more bits are changed in the data device, it is called as Burst error.



Redundancy

- The principle is redundancy in identifying or fixing errors.
- Extra bits of original data (redundant) are needed to detect or correct errors.
- The sender attaches some unnecessary bits and the recipient eliminates them.
- This helps the receiver to spot corrupted bits or their degradation.

Error Detection

In frames, bit errors are inserted. Detecting mistakes is just one aspect of the issue, and error correction is another issue. There are two simple approaches taken. Where a message receiver discovers an error. When the sender sends the damaged message, a copy of the message can be retransmitted. If bits are uncommon, then the retransmitted copy would most likely be error-free. In certain forms of error detection, the algorithm requires the receiver to rely on Error Correcting codes to recreate the correct algorithm. In almost all connect level protocols, 2-dimensional parity and check sums are used. Cyclic redundancy check (CRC) is employed. The basic concept of error detection scheme is to appends details about redundancies, to determine if errors have been introduced.

Example

- If the receiver finds two copies, then both are accurate.
- If they vary, an error has been put into one or both of them and discarded.
- Two factors for weak identification of errors.
    1. It sends n redundant bits for an 1-bit message.
    2. Any mistake that appears to corrupt the same bit positions in the first and second copies of the message is undetected by several errors.
- The main aim of error detection codes holds high likelihood detection of errors.

Error Detecting Codes

- No new information will be added if the bits are redundant.
- Extracted by some well-defined algorithm directly from the original post.
- The algorithm is well-known to both the sender and recipient.
- The redundant bits produced may use the message algorithm.
- Both the message and a few additional bits are evoked.
- The same outcome of the sender is expected at the recipient when the same algorithm is applied.
- It compares the outcome with the one that the sender sends to it.
- If they match, it can be inferred that during transmission, no errors were inserted in the message.
- They are referred to as codes that detect errors.

Checksum

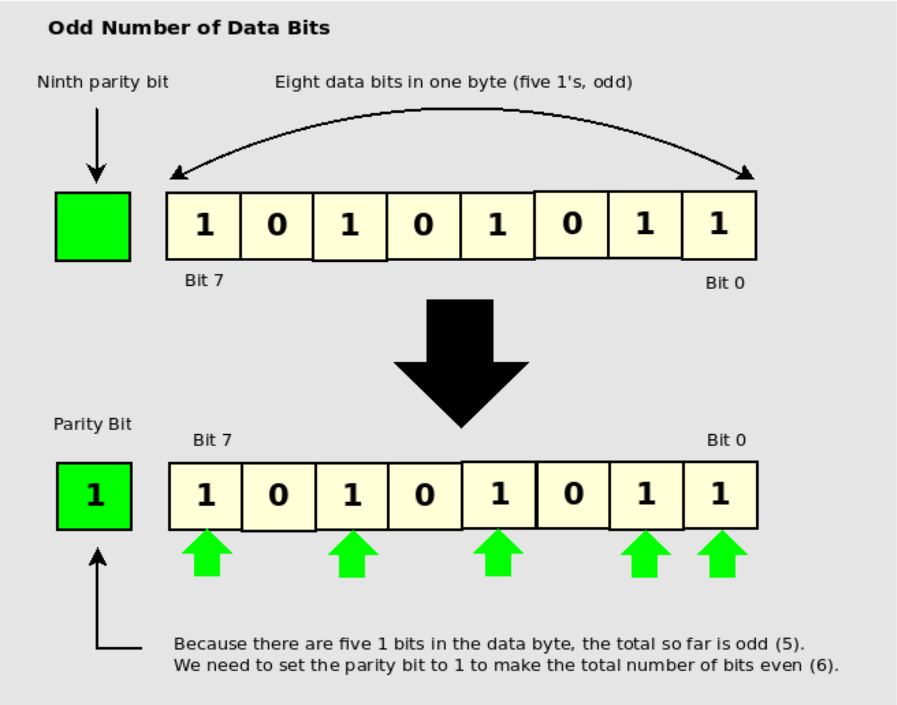
- A checksum can be named after the algorithm used for generating code gets applied.
- It is an error check which utilizes an algorithm for summing.
- The term checksum is sometimes used imprecisely to denote any type of code that detects errors like CRCs.

Two-Dimensional Parity

It is based on a "simple" (one-dimensional) parity typically involving adding an extra bit to a 7-bit code to match the number of 1s in the byte. In each location of bits, the two-dimensional parity manipulates in a similar way and holds a bit every byte as parity.

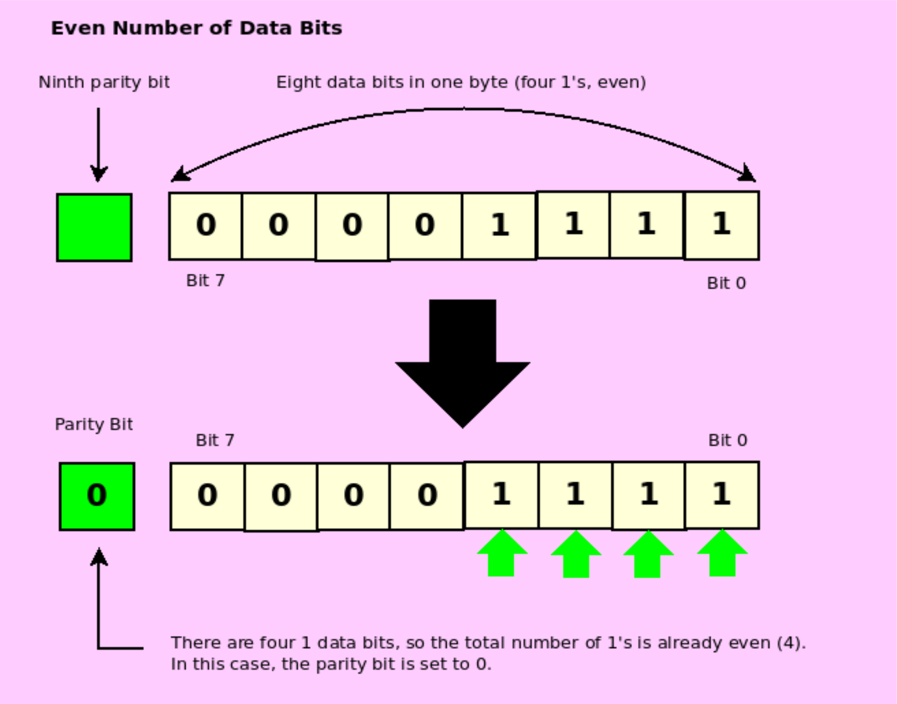
Even Parity

Even parity ensures that the number of 1 bits (8 data bits + 1 parity bit) is even.



Odd Number of Data Bits

Because there are five 1 bits in the data byte, the total so far is odd (5).
We need to set the parity bit to 1 to make the total number of bits even (6).



Even Number of Data Bits

There are four 1 data bits, so the total number of 1's is already even (4).
In this case, the parity bit is set to 0.

Internet Checksum Algorithm

- It offers the same kind of accessibility and parity as the CRCs.
- It adds up all the words that are transmitted in the internet checksum, and then transmits the results of that number. This is called checksum.
- On the received data, the receiver performs the same calculation and the results are compared with the checksum received.
- The results end up in a mismatch when any of the data transmitted is corrupted that includes the checksum too, which intimates discrepancy to the receiver.

Cyclic Redundancy Check (CRC)

- The key objective in developing algorithms for error detection is to increase the possibility of detecting errors using only a limited number of redundant bits.
- The conceptual underpinning of the CRC is embedded in a mathematical branch termed as the finite fields.

Error **correction** appears to be most beneficial when:

1. Errors are relatively reliable.
   E.g: wireless environment.
2. The rate value of retransmission is too high.
   E.g: satellite link.
   - Although error detection involves sending more bits when mistakes occur, error correction requires sending more bits all the time.
   - The use of networking error correction codes is referred to as forward error correction (FEC) as error correction is done in advance by transmitting additional details, rather than watching for problems to occur and grappling with it later through retransmission.

Eg:- 802.11 (wireless network)

- It involves vital methodologies like.

  1. Acknowledgements
  2. Timeouts
- An acknowledgment (ACK) is a tiny control frame sent back to its peer by a protocol indicating that it has received an earlier frame.
- Retransmission of the originating frame happens when the sender fails to acquire a receipt for a rational amount of time. This is often referred as a timeout.

- Identification of a data frame sending back in the opposite direction and receipt of acknowledgement is known as a piggy bank.

Error Control

- Error management is the detection of errors as well as error correction.
- It enables the recipient to notify the transmitter of any frames missing or disrupted in the propagation and schedules the sender's retransmission of those frames.
- Error management prefers error detection and retransmission approaches.
- Automatic Repeat Request (ARQ) is termed as the occurrence of errors obtained during a specific frame is transferred.
- Data link layer error management is based on the Automatic Repeat Request (ARQ), which is data retransmission.

1.10. Flow Control

- Flow control can be explained as the amount of information that can be controlled at the submission even before an acknowledgment is received.
- It is a collection of processes that involves in instructing the sender how much data can be transmitted before awaiting a receiver's acknowledgement.
- Data flow is restricted to overpower the receive.
- The recipient system is offered a limited speed to process the incoming data.
- It is also responsible for warning the transmitting system and request sending a lower number of frames or temporarily stop them, when the limit is observed.
- Reviewing and analysing the arriving information is to be taken place before it can be used.
- The rate of such processing is habitually leisurelier than the rate of transmission.
- Each receiving system has a memory block called a reversed buffer to store the incoming data before it is being processed.
- If the buffer starts filling up, the receiver must be able to tell the transmitter to interrupt transmission before it can be received again.
- Set of trials to limit the quantity of message sent by the sender unless awaiting the receipts.