UNIT I
FUNDAMENTALS & LINK LAYER

Building a network

A **computer network** or **data network** is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along network links (data connections). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

To build a computer network is defining what a network is and understanding how it is used to help a business meet its objectives. A network is a connected collection of devices and end systems, such as computers and servers, which can communicate with each other.

These are the four major categories of physical components in a computer network:

- **Personal computers (PCs):** The PCs serve as endpoints in the network, sending and receiving data.
- **Interconnections:** The interconnections consist of components that provide a means for data to travel from one point to another point in the network. This category includes components such as the following:
    - Network interface cards (NICs) that translate the data produced by the computer into a format that can be transmitted over the local network
    - Network media, such as cables or wireless media, that provide the means by which the signals are transmitted from one networked device to another
    - Connectors that provide the connection points for the media
- **Switches:** Switches are devices that provide network attachment to the end systems and intelligent switching of the data within the local network.
- **Routers:** Routers interconnect networks and choose the best paths between networks.

Network User Applications:

The key to utilizing multiple resources on a data network is having applications that are aware of these communication mechanisms. Although many applications are available for users in a network environment, some applications are common to nearly all users.

The most common network user applications include the following:

- **E-mail:** E-mail is a valuable application for most network users. Users can communicate information (messages and files) electronically in a timely manner, to not only other users in the same network but also other users outside the network (suppliers, information resources, and customers, for example). Examples of e-mail programs include Microsoft Outlook and Eudora by Qualcomm.

- **Web browser:** A web browser enables access to the Internet through a common interface. The Internet provides a wealth of information and has become vital to the productivity of both home and business users. Communicating with suppliers and customers, handling orders and fulfillment, and locating information are now routinely done electronically over the Internet, which saves time and increases overall productivity. The most commonly used browsers are Microsoft Internet Explorer, Netscape Navigator, Mozilla, and Firefox.
- **Instant messaging:** Instant messaging started in the personal user-to-user space; however, it soon provided considerable benefit in the corporate world. Now many instant messaging applications, such as those provided by AOL and Yahoo!, provide data encryption and logging, features essential for corporate use.
- **Collaboration:** Working together as individuals or groups is greatly facilitated when the collaborators are on a network. Individuals creating separate parts of an annual report or a business plan, for example, can either transmit their data files to a central resource for compilation or use a workgroup software application to create and modify the entire document, without any exchange of paper. One of the best-known traditional collaboration software programs is Lotus Notes. A more modern web-based collaboration application is a wiki.
- **Database:** This type of application enables users on a network to store information in central locations (such as storage devices) so that others on the network can easily retrieve selected information in the formats that are most useful to them. Some of the most common databases used in enterprises today are Oracle and Microsoft SQL Server

Requirements

- ***An application programmer*** would list the services that his or her application needs—for example, a guarantee that each message the application sends will be delivered without error within a certain amount of time or the ability to switch gracefully among different connections to the network as the user moves around.

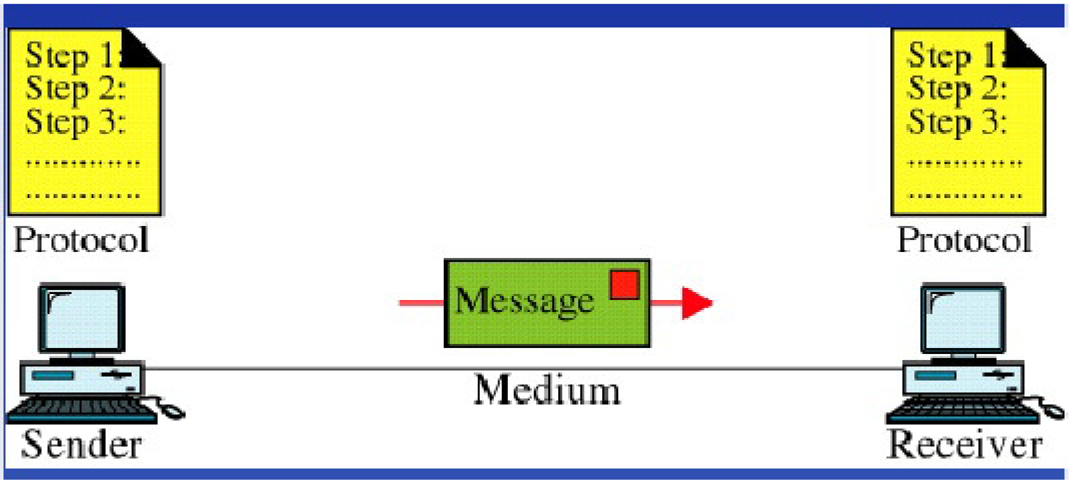
- ***A network operator*** would list the characteristics of a system that is easy to administer and manage—for example, in which faults can be easily isolated, new devices can be added to the network and configured correctly, and it is easy to account for usage.

- ***A network designer*** would list the properties of a cost-effective design—for example, that network resources are efficiently utilized and fairly allocated to different users. Issues of performance are also likely to be important. This section attempts to distill these different perspectives into a high-level.

Components:

The components of a data communication are

Message
Sender
Receiver
Medium
Protocol



Message : The message is the information to be communicated. It can consist of text ,pictures, numbers, sound, video or audio .

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

Receiver. The receiver is the device that receives the message. It can be a computer or workstation telephone handset, video camera and so on..

Medium. The transmission medium is the physical path by which a message travels from sender to receiver. It could be a twisted pair wire , coaxial cable, fiber optic cable, or radio waves.

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

DATA FLOW

When two devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

1. Simplex
2. Half Duplex
3. Full Duplex

1. Simplex

In Simplex, communication is unidirectional

Only one of the devices sends the data and the other one only receives the data.

Example: in the above diagram: a cpu send data while a monitor only receives data.

2. Half Duplex

In half duplex both the stations can transmit as well as receive but not at the same time.

When one device is sending other can only receive and vice-versa (as shown in figure above.)

Example: A walkie-talkie.

3. Full Duplex

In Full duplex mode, both stations can transmit and receive at the same time.

Example: mobile phones

Topology

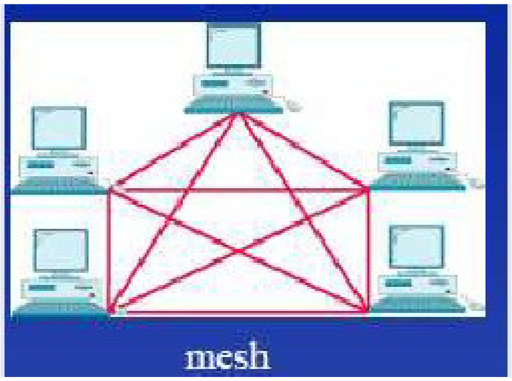
Physical Topology refers to the way in which network is laid out physically. Two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and the linking devices tone another.

The basic topologies are
Mesh
Star

tree
Bus
Ring

Mesh

In a mesh topology each device has a dedicated point to point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.



A fully connected mash network therefore has n(n-1)/2 physical channels to link n devices. To accommodate that many links every device on the network has (n-1) I/O ports.

<u>Merits.</u>

- Dedicated link guarantees that each connection can carry its own data load. This eliminates the traffic problems that occur when links shared by multiple devices.
- If one link becomes unusable ,it does not incapacitate the entire system.
- Privacy or security: When every message travels along a dedicated line only the intended recipient

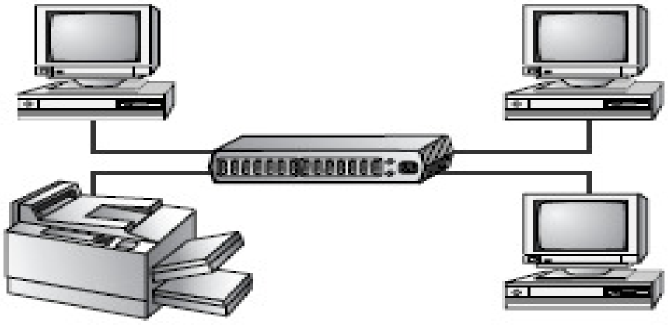
<u>Demerits</u>

- The amount of cabling and the I/O ports required
- Installation and reconnection are difficult
- The sheer bulk of the wire accommodate more space than available.

The hardware required to connect each link can be prohibitively expensive.

Star topology

Each device has a dedicated point to point link only to a central controller usually called a hub. If one device has to send data to another it sends the data to the controller, which then relays the data to the other connected device.



Merits

- Less expensive than a mesh topology. Each device needs only one link and I/O port to connect it to any number of others.
- Installation and reconfigure is easy.
- Robustness. If one link fails only that link is affected.
- Requires less cable than a mesh.

Demerits

- Require more cable compared to bus and ring topologies

Tree Topology:

The top level of the hierarchy, the central root node is connected to some nodes that are a level low in the hierarchy by a point-to-point link where the second level nodes that are already connected to central root would be connected to the nodes in the third level by a point-to-point link. The central root would be the only node having no higher node in the hierarchy. The tree hierarchy is symmetrical. The BRANCHING FACTOR is the fixed number of nodes connected to the next level in the hierarchy. Such network must have at least three levels. Physical Linear Tree Topology would be of a network whose Branching Factor is one.

Advantages of a Tree Topology

Point-to-point wiring for individual segments.
Supported by several hardware and software venders.

Disadvantages of a Tree Topology

Overall length of each segment is limited by the type of cabling used.
If the backbone line breaks, the entire segment goes down.
More difficult to configure and wire than other topologies.

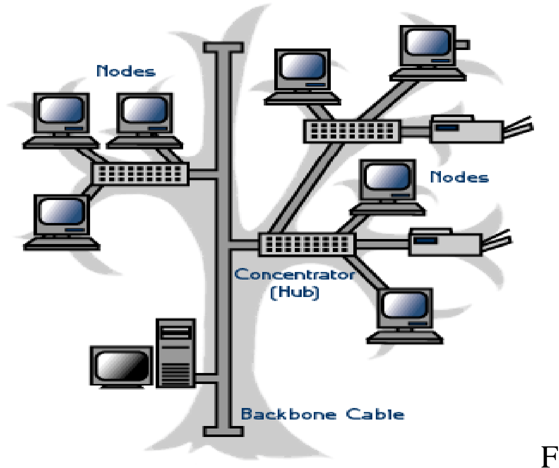
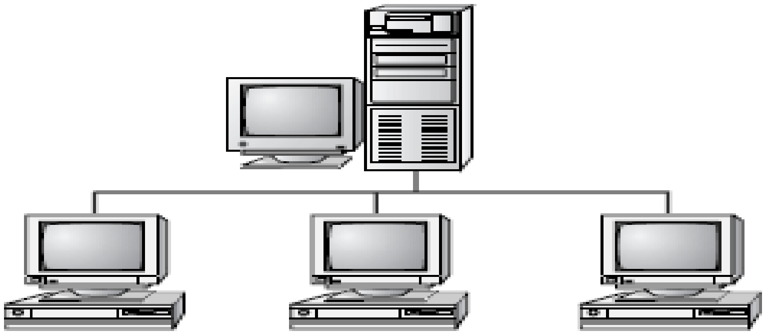


FIG:TREE TOPOLOGY

Bus topology

One long cable acts as a backbone to link all the devices in a network Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with a metallic core.



BUS TOPOLOGY

As the signal travels farther and farther ,it becomes weaker .So there is limitation in the number of taps a bus can support and on the distance between those taps.(In this diagram taps and connectors are

Merits

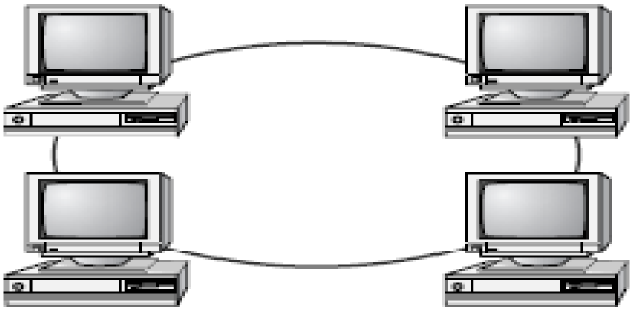
- Ease of installation.
- Bus use less cabling than mesh or star topologies.

Demerits

- Difficult reconnection and isolation.
- Signal reflection at the taps can cause degradation in quality.
- A fault or break in the bus cable stops all transmission. It also reflects signals back in the direction of origin creating noise in both directions.

Ring topology

Each device has a dedicated point to point connection only with the two devices on either side of it.
A signal is passed along the ring in one direction from device to device until it reaches the destination
Each device in the ring incorporates a repeater. It regenerates the bits and passes them along ,when it receives the signal intended for another device.



Merits:

- Easy to install and reconfigure.
- To add or delete a device requires changing only two connections.
- The constraints are maximum ring length and the number of devices.
- If one device does not receive the signal within a specified period, it issue an alarm that alerts the network operator to the problem and its location

Demerits

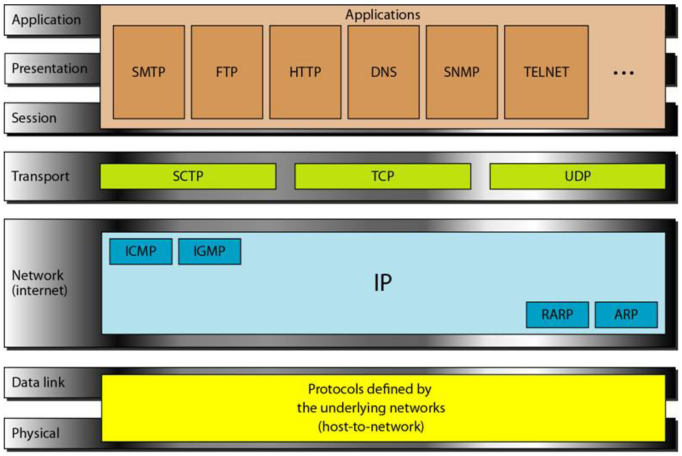
- A break in the ring disables the entire network. It can be solved by using a dual ring or a switch capable of closing off the break.

Hybrid Topology

Hybrid topologies are a combination of two or more different topologies.

TCP/IP

Figure 2.16 *TCP/IP and OSI model*



2.2

SMTP (Simple Mail Transfer Protocol) - Protocol used to send email messages between servers.

FTP (File Transfer Protocol) - Used to transfer files over the internet using TCP/IP.

HTTP (Hypertext Transfer Protocol) - Underlining protocol used by the World Wide Web. Allows Web servers and browsers to communicate with each other.

DNS (Domain Name Service) - An internet service that translates domain names, such as www.yahoo.com, into IP addresses

Simple Network Management Protocol, a set of protocols for managing complex networks.

Telnet - terminal emulation program that allows you to connect to a server and enter information and commands similar to if you were actually on the server terminal.

SCTP -(Stream Control Transmission Protocol) is a protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network.

TCP (Transmission Control Protocol) - enables two to establish a connection and exchange streams of data.

UDP (User Datagram Protocol) - offering a direct way to send and receive datagrams over an IP network with very few error recovery

ICMP (Internet Control Message Protocol) - an extension of IP which supports packets containing error, control, and informational messages.

Internet Group Management Protocol.
It's used to establish host memberships in particular multicast groups on a single network.

Reverse Address Resolution Protocol, a TCP/IP protocolthat permits a physical addresss uch as an Ethernet address, to be translated into an IP address

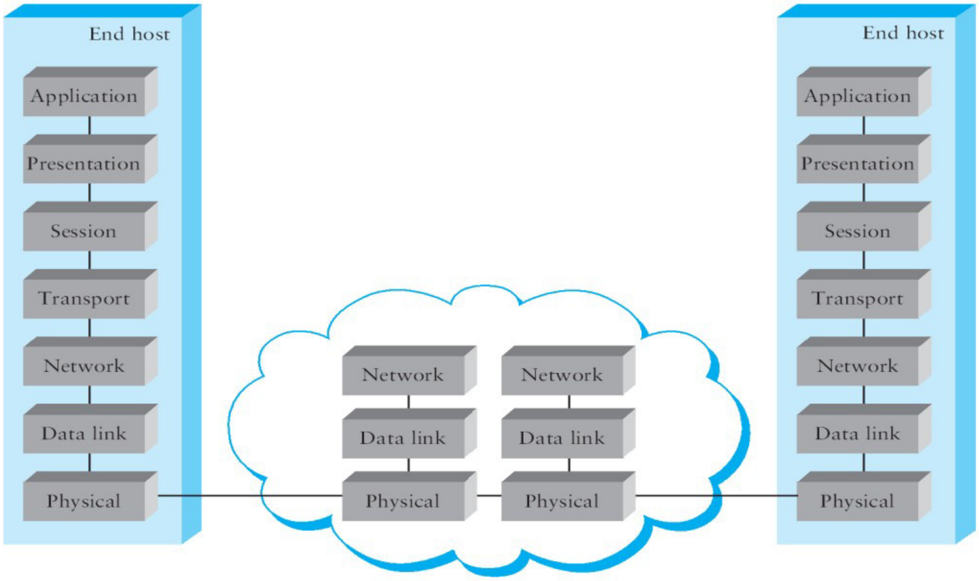
ARP (Address Resolution Protocol) - used to convert an IP address to a physical address.

IP (Internet Protocol) - specifies the format of packets and the addressing schemes

Layering and protocols:
OSI Architecture:

- ISO defines a common way to connect computer by the architecture called Open System Interconnection(OSI) architecture.

- Network functionality is divided into seven layers.



One or more nodes within the network

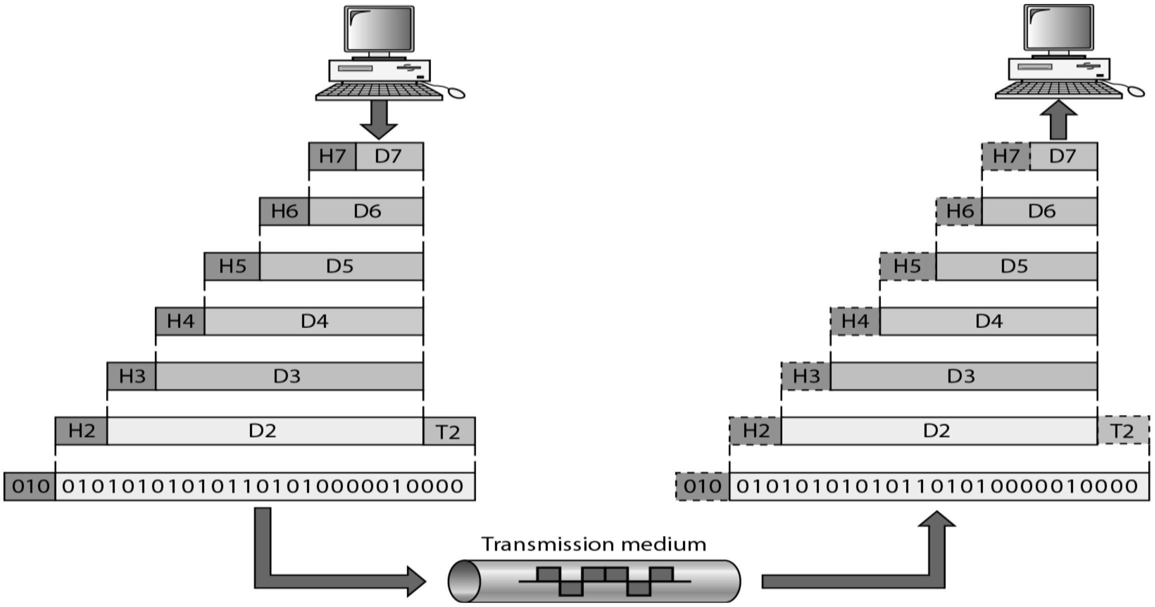
Organization of the layers

The 7 layers can be grouped into 3 subgroups

1. **Network Support Layers**
   Layers 1,2,3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.
2. **Transport Layer**
   Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.

3. **User Support Layers**
   Layers 5,6,7 – Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems

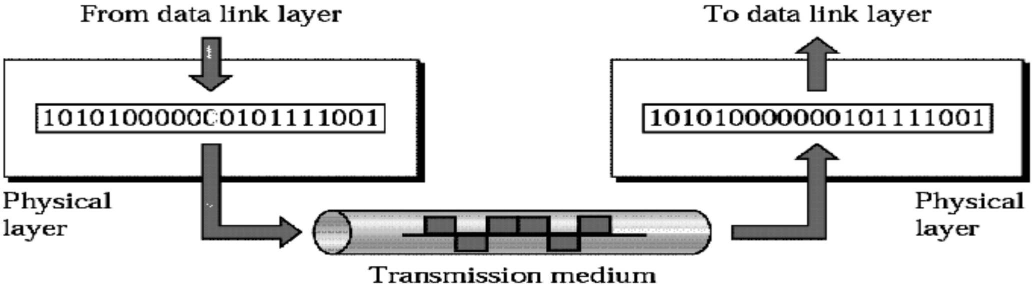
An Data exchange using the OSI model



Functions of the Layers

1. Physical Layer

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.



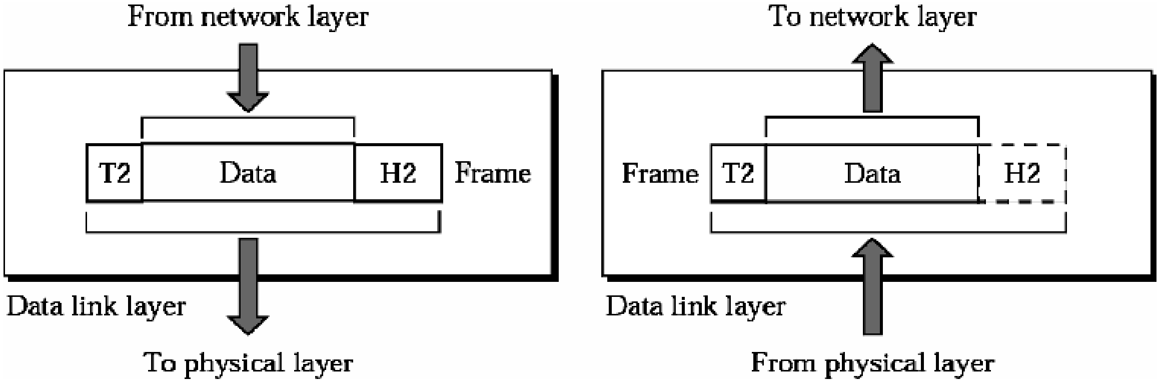
The physical layer is concerned with the following:

- **Physical characteristics of interfaces and media -** The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- **Representation of bits -** To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
- **Data Rate or Transmission rate -** The number of bits sent each second – is also defined by the physical layer.
- **Synchronization of bits -** The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.

- **Line Configuration -** In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
- **Physical Topology -** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.
- **Transmission Mode -** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

2. Data Link Layer

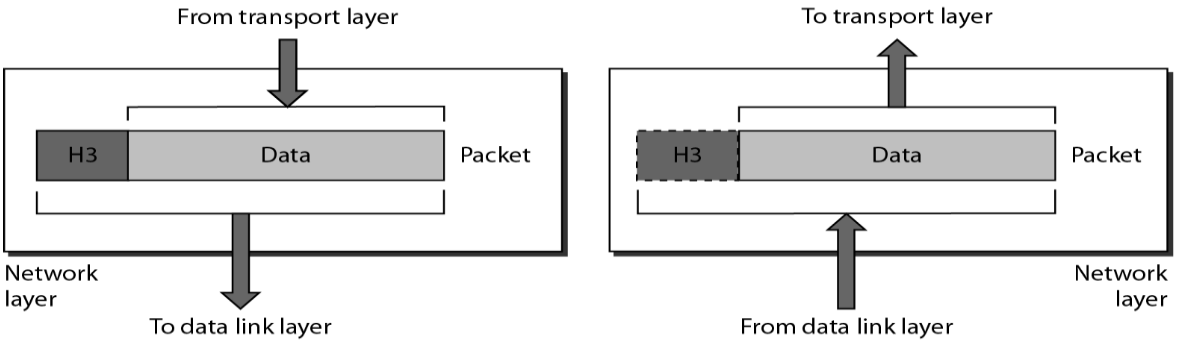
It is responsible for transmitting frames from one node to next node.



The other responsibilities of this layer are

- **Framing -** Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the n/w , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

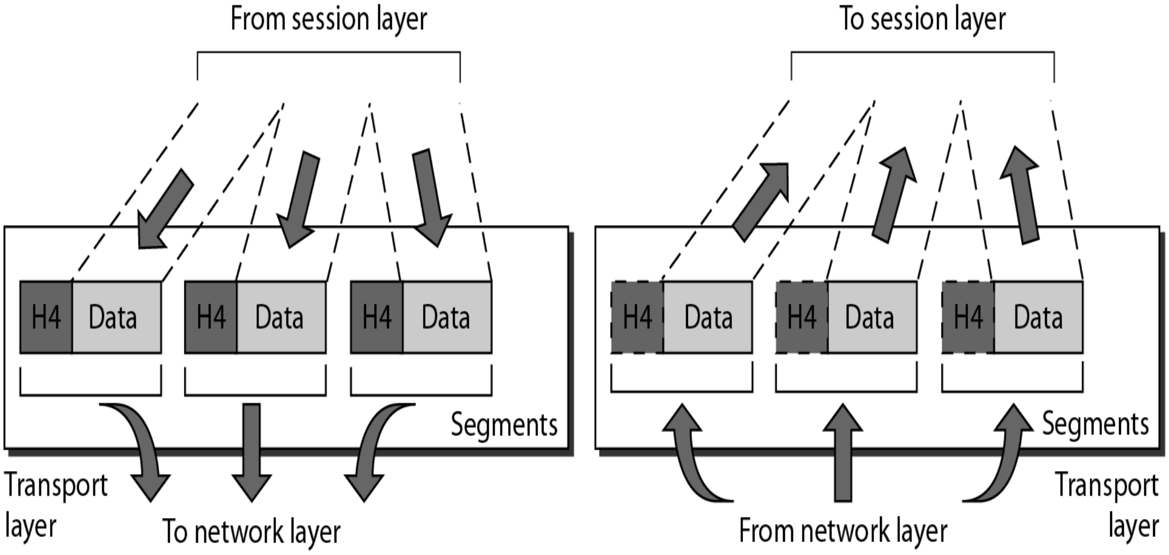


t is mainly required, when it is necessary to send information from one network to another.
The other responsibilities of this layer are

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

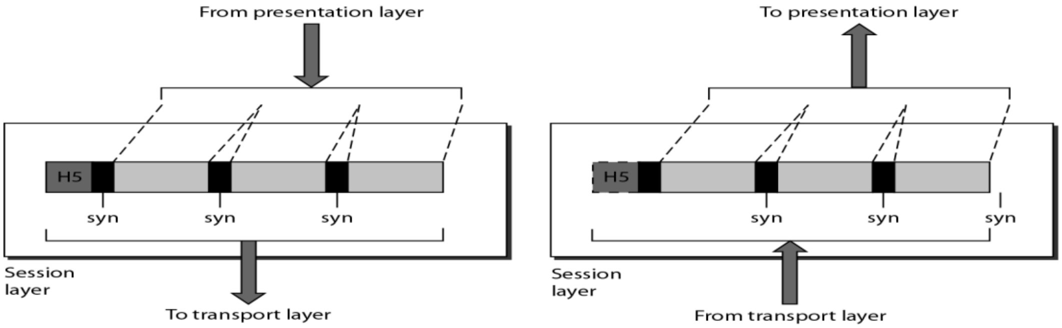
4. TRANSPORT LAYER

- It is responsible for **Process to Process** delivery.
- It also ensures whether the message arrives in order or not.



- **Port addressing** - The header in this must therefore include a address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be **connectionless or connection-oriented.** The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control** - Similar to data link layer, but process to process take place.

5. SESSION LAYER



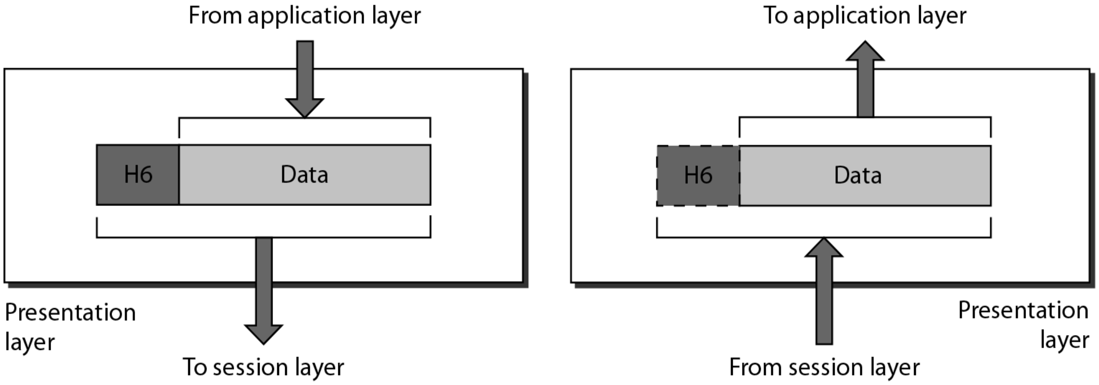
This layer establishes, manages and terminates connections between applications.

The other responsibilities of this layer are

- **Dialog control -** This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization**-This allows to add checkpoints into a stream of data.

6. PRESENTATION LAYER

It is concerned with the syntax and semantics of information exchanged between two systems.

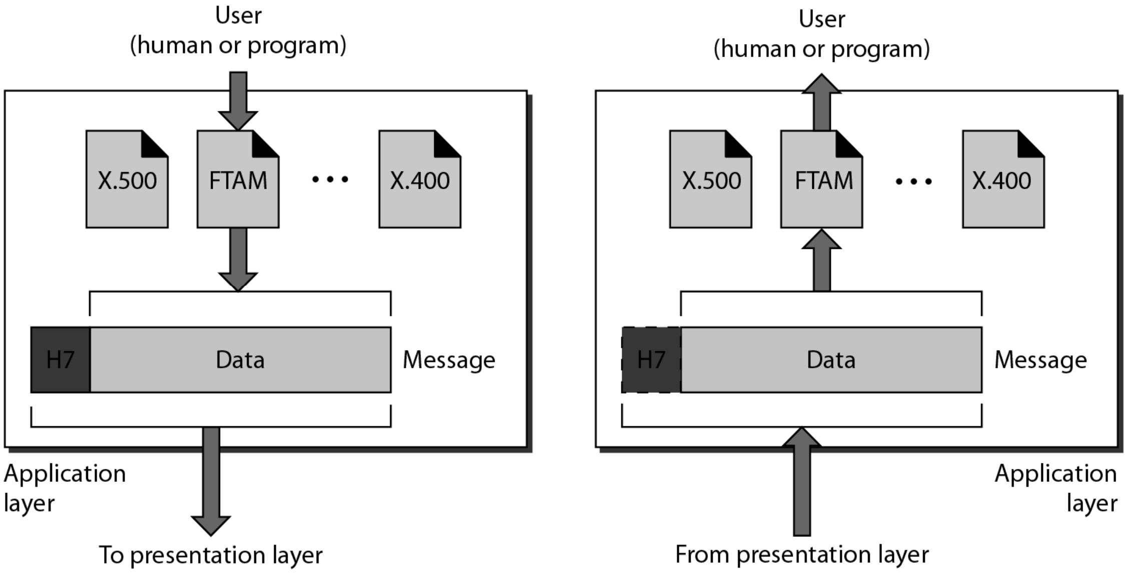


The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

7. APPLICATION LAYER

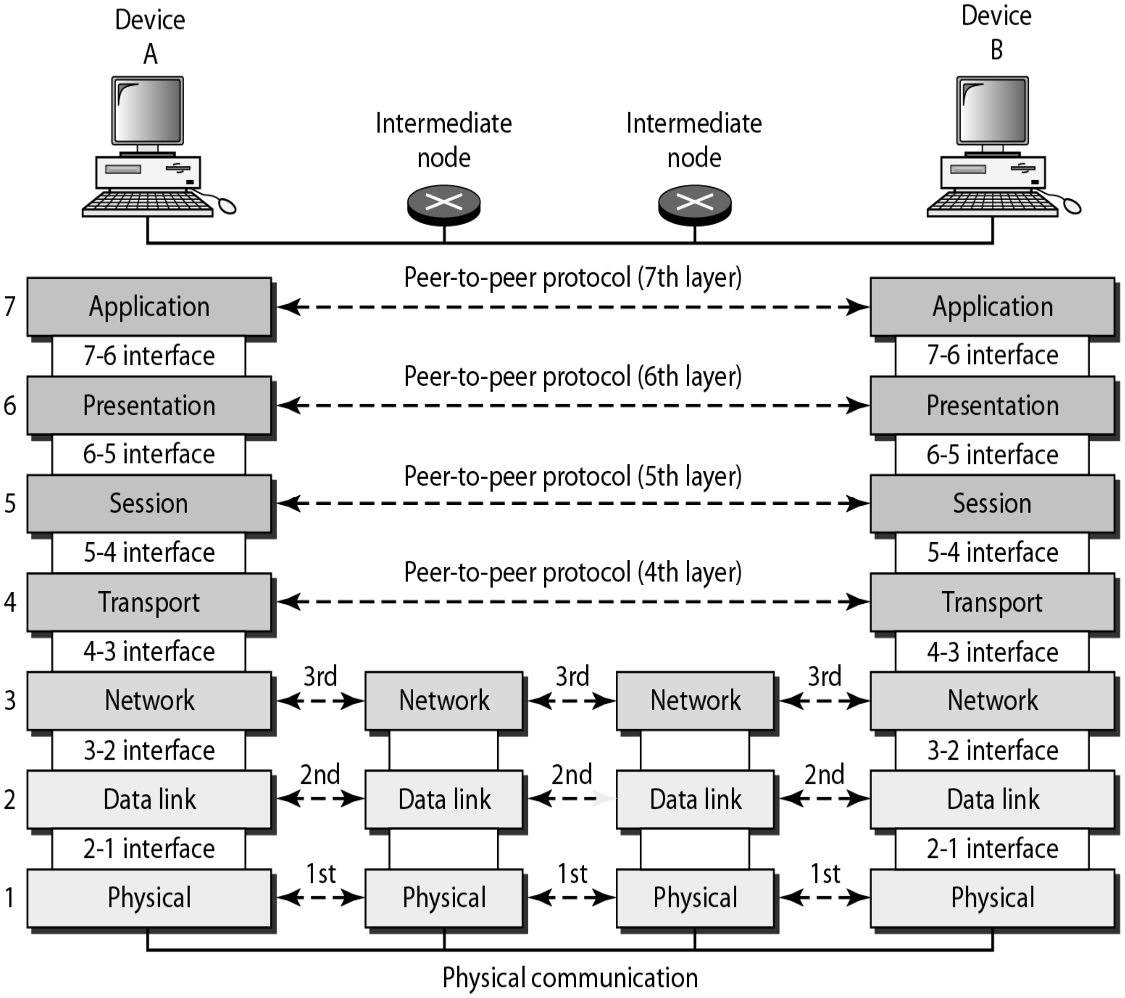
This layer enables the user to access the n/w. This allows the user to log on to remote user.



The other responsibilities of this layer are

- **FTAM(file transfer,access,mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

The interaction between layers in the OSI model



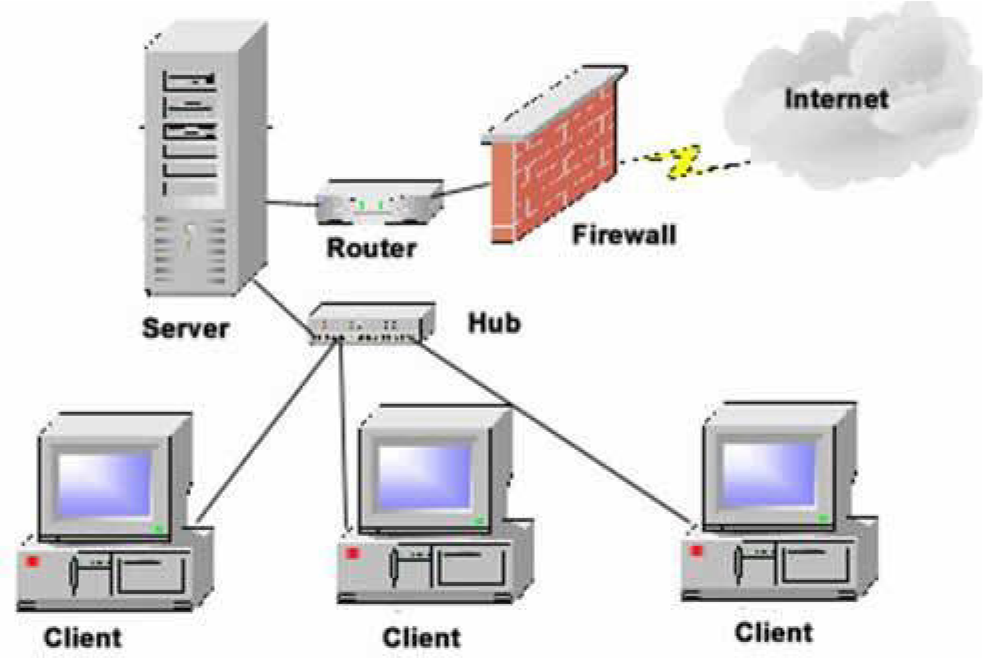
Internet Architecture

The Internet architecture, which is also sometimes called the TCP/IP architecture after its two main protocols, is depicted in Figure. An alternative representation is given in Figure. The Internet architecture evolved out of experiences with an earlier packet-switched network called the ARPANET. Both the Internet and the ARPANET were funded by the Advanced Research Projects Agency (ARPA), one of the research and development funding agencies of the U.S. Department of Defense. The Internet and ARPANET were around before the OSI architecture, and the experience gained from building them was a major influence on the OSI reference model.

Internet architecture is by definition a meta-network, a constantly changing collection of thousands of individual networks intercommunicating with a common protocol.

The Internet's architecture is described in its name, a short from of the compound word "inter-networking". This architecture is based in the very specification of the standard *TCP/IP* protocol, designed to connect any two networks which may be very different in internal hardware, software, and technical design. Once two networks are interconnected, communication with TCP/IP is enabled end-to-end, so that any node on the Internet has the near magical ability to communicate with any other no matter where they are. This openness of design has enabled the Internet architecture to grow to a global scale.

Network software



Networking software, in the most basic sense, is software that facilitates, enhances or interacts with a computer network. One type of networking software allows computers to communicate with one another, while another type of networking software provides users access to shared programs. Networking software is a key component of today's computer networks, including the Internet. Understanding the types of networking software is the first step in understanding how your computer network really works.

Performance

Bandwidth and Latency

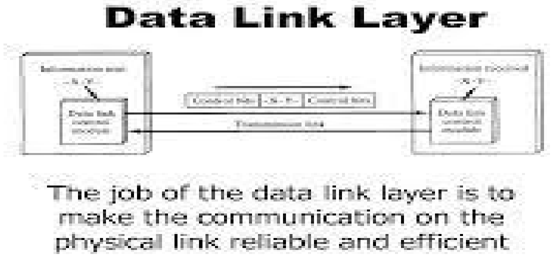
Network performance is measured in two fundamental ways: *bandwidth* (also called *throughput*) and *latency* (also called *delay*). The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.

Bandwidth and throughput are two of the most confusing terms used in networking. While we could try to give you a precise definition of each term, it is important that you know how other people might use them and for you to be aware that they are often used interchangeably.

Latency = Propagation+Transmit+Queue
Propagation = Distance/SpeedOfLight
Transmit = Size/Bandwidth

Category	Metric	Units
Productivity	Throughput Effective capacity	Mbps
Responsiveness	Delay Round trip time Queue size	Milliseconds Packets
Utilization	Channel utilization	Percentage of time busy
Losses	Packet loss rate Frame retries	Loss percentage
Buffer problems	AP queue overflow Playout buffer underflow	Packet drops Rebuffed events

Link layer Services


Data Link Layer
The job of the data link layer is to
make the communication on the
physical link reliable and efficient

Link layer Services:

The main task of the data link layer is that it transfers data from the network layer of one machine to the network layer of another machine. This is a part of the services it gives to the upper layer. If you remember, above the data link layer, we have the network layer. The data link layer gives a service to the network layer, and this service is the transfer of data from one network layer to the other, and this in turn uses the physical layer. It converts the raw bit stream of the physical layer into groups of bits or frames.

DLL offers unacknowledged connectionless and acknowledged connectionless services. In unacknowledged connectionless, there is no attempt to recover lost frame and there is no acknowledgement from the other side. I t is suited for low error rate networks or for fault tolerant applications such as voice. By voice tolerant application, we mean that even if some of the bits in a digitized voice stream drop, there will be some degradation on the other side. But to the human ear, it is imperceptible. That is why it is fault-tolerant. In acknowledged connectionless service, each frame is acknowledged by the receiver and it is suited for unreliable channels, where acknowledgement is required for special reliability.
.

Acknowledged connection-oriented service ensures that all frames are received and each is received exactly once and these services are accomplished using simplex not the usual, but half-duplex or full-duplex channels.

These are some examples. It is a reliable message stream. It may be connection-oriented service or connectionless service. It may be a reliable message stream (sequence of pages) or reliable byte stream (reliable login): in the latter it is coming byte by byte and in the former, it is page by page. An example of unreliable connection is digitized voice; unreliable datagram (electronic junk mail) is connectionless `service.

Framing

To transmit frames over the node it is necessary to mention start and end of each frame. There are three techniques to solve this frame

- Byte-Oriented Protocols (BISYNC, PPP, DDCMP)
- Bit-Oriented Protocols (HDLC)
- Clock-Based Framing (SONET)

Byte Oriented protocols

In this, view each frame as a collection of bytes (characters) rather than a collection of bits. Such a byte-oriented approach is exemplified by the **BISYNC** (Binary Synchronous Communication) protocol and the **DDCMP** (Digital Data Communication Message Protocol)

Sentinel Approach

The BISYNC protocol illustrates the sentinel approach to framing; its frame format is

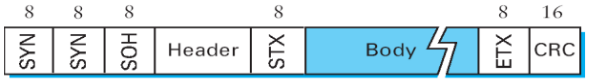


Fig: BISYNC Frame format

- The beginning of a frame is denoted by sending a special SYN (synchronization) character.
- The data portion of the frame is then contained between special sentinel characters: STX (start of text) and ETX (end of text).
- The SOH (start of header) field serves much the same purpose as the STX field.
- The frame format also includes a field labeled CRC (cyclic redundancy check) that is used to detect transmission errors.

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by ―escaping‖ the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called **character stuffing**.

Point-to-Point Protocol (PPP)

The more recent Point-to-Point Protocol (PPP). The format of PPP frame is

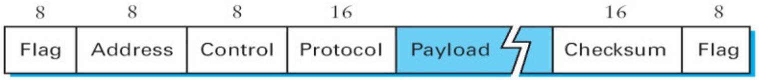


Fig: PPP Frame Format

- The Flag field has 01111110 as starting sequence.
- The Address and Control fields usually contain default values
- The Protocol field is used for demultiplexing.
- The frame payload size can he negotiated, but it is 1500 bytes by default.
- The PPP frame format is unusual in that several of the field sizes are negotiated rather than fixed.
- Negotiation is conducted by a protocol called LCP (Link Control Protocol).
- LCP sends control messages encapsulated in PPP frames—such messages are denoted by an LCP identifier in the PPP Protocol.

Byte-Counting Approach

The number of bytes contained in a frame can he included as a field in the frame header. DDCMP protocol is used for this approach. The frame format is

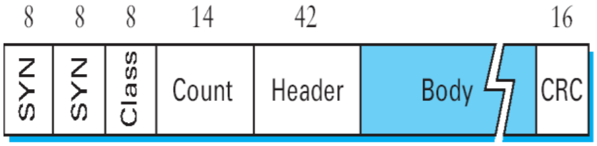


Fig: DDCMP frame format

- COUNT Field specifies how many bytes are contained in the frame’s body.
- Sometime count field will be corrupted during transmission, so the receiver will accumulate as many bytes as the COUNT field indicates. This is sometimes called a **framing error**.
- The receiver will then wait until it sees the next SYN character.

Bit-Oriented Protocols (HDLC)

In this, frames are viewed as collection of bits. High level data link protocol is used. The format is

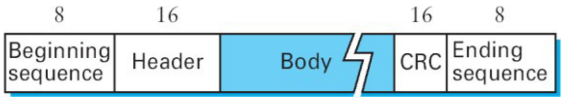


Fig: HDLC Frame Format

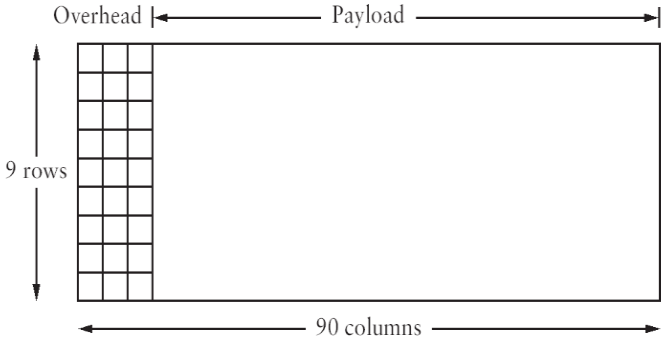
- HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110.
- This sequence might appear anywhere in the body of the frame, it can be avoided by bit stuffing.
- On the sending side, any time five consecutive 1's have been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 sequence), the sender inserts a 0 before transmitting the next bit.
- On the receiving side, five consecutive 1's arrived, the receiver makes its decision based on the next bit it sees (i.e., the bit following the five is).
- If the next bit is a 0, it must have been stuffed, and so the receiver removes it. If the next bit is a 1, then one of two things is true, either this is the end-of-frame marker or an error has been introduced into the bit stream.
- By looking at the next bit, the receiver can distinguish between these two cases:

  If it sees a 0 (i.e., the last eight bits it has looked at are 01111110), then it is the end-of-frame marker.

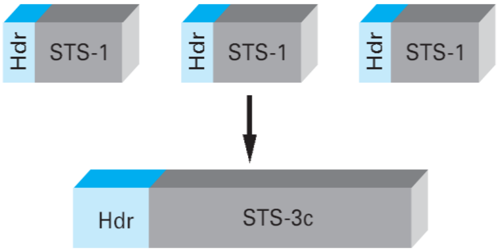
  If it sees a 1 (i.e., the last eight bits it has looked at are 01111111), then there must have been an error and the whole frame is discarded.

Clock-Based Framing (SONET)

- Synchronous Optical Network Standard is used for long distance transmission of data over optical network.
- It supports multiplexing of several low speed links into one high speed links.
- An STS-1 frame is used in this method.



- It is arranged as nine rows of 90 bytes each, and the first 3 bytes of each row are overhead, with the rest being available for data.
- The first 2 bytes of the frame contain a special bit pattern, and it is these bytes that enable the receiver to determine where the frame starts.
- The receiver looks for the special bit pattern consistently, once in every 810 bytes, since each frame is 9 x 90 = 810 bytes long.



- The STS-N frame can he thought of as consisting of N STS-1 frames, where the bytes from these frames are interleaved; that is, a byte from the first frame is transmitted, then a byte from the second frame is transmitted, and so on.
- Payload from these STS-1 frames can he linked together to form a larger STS-N payload, such a link is denoted STS-Nc. One of the bit in overhead is used for this purpose.

ERRORS DETECTION

OBJECTIVE

INTRODUCTION:

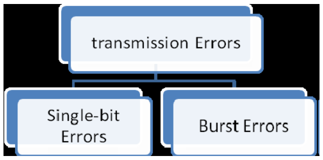
Errors in the data are basically caused due to the various impairments that occur during the process of transmission. When there is an imperfect medium or environment exists in the transmission it prone to errors in the original data.

Error correction:

The process of correcting bits that have been changed during transmission.

TYPES OF ERRORS:

If the signal comprises of binary data there can be two types of errors which are possible during the transmission:

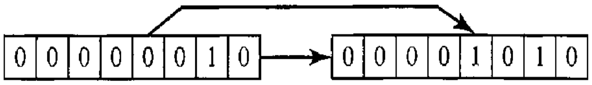


1. Single bit errors
2. Burst Errors

1. **Single-bit errors:**

   In single-bit error, a bit value of 0 changes to bit value 1 or vice versa. **Single bit errors are more likely to occur** in parallel transmission.

ochanged to I

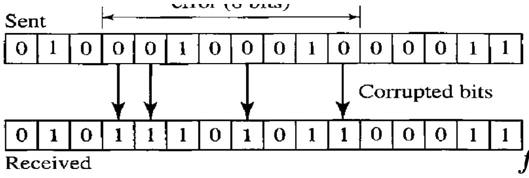


0 0 0 0 0 0 1 0 → 0 0 0 0 1 0 1 0

Sent **Received**

2. **Burst errors:**

   In Burst error, **multiple bits of the binary value changes**. Burst error can change any two or more bits in a transmission. These bits need not be adjacent bits. Burst errors are more likely to occur in serial transmission.



Sent

0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1

Corrupted bits

0 1 0 1 1 1 0 1 0 1 1 0 0 0 1 1

Received

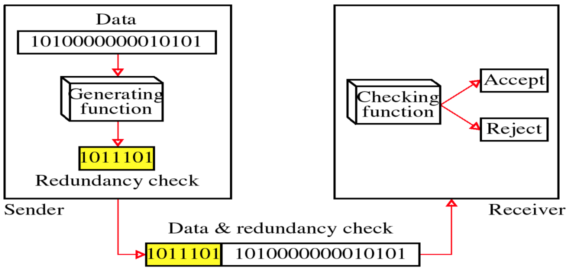
fig:Burst error

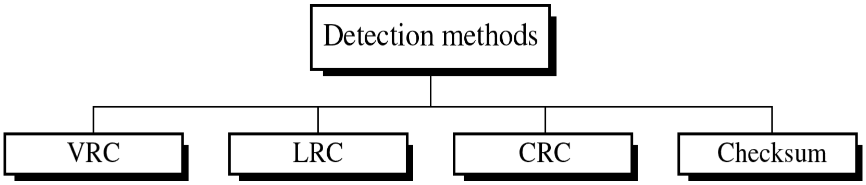
ERROR DETECTION

The process of determining whether or not some bits have been changed during transmission.

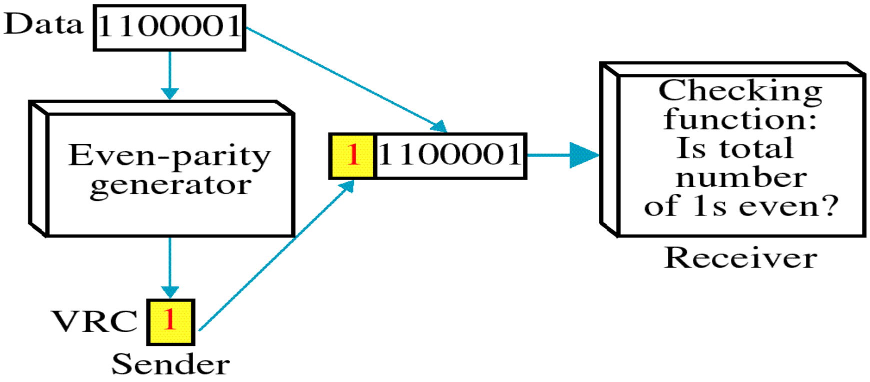
Redundancy[Addition of bits to a message for error control]

To detect or correct errors, we need to send extra (redundant) bits with data.



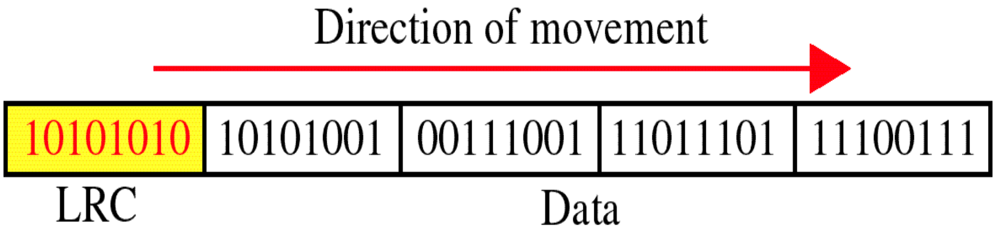


VRC



In VRc a parity bit is added to every data unit so that the total number of 1s become even.

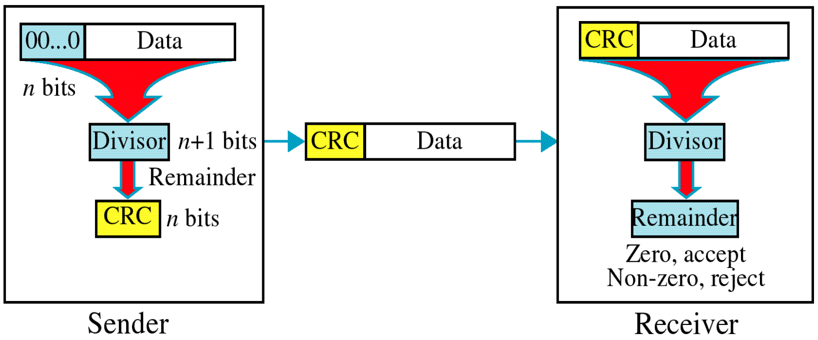
LRC

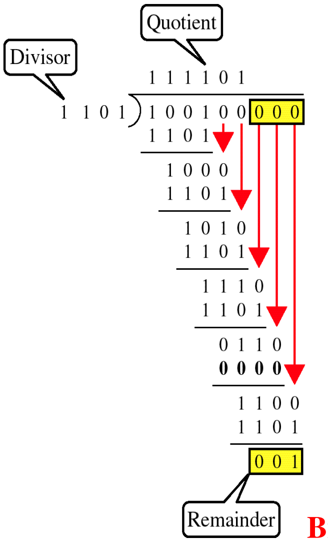


In LRC ,a block of bits is divided into rows and a redundant row of bits is added to the whole block.

CRC

Most powerful of the redundancy checkingtechniques is the cyclic redundancy check (CRC). This method is based on the binary division. In CRC, the desired sequence of redundant bits are generated and is appended to the end of data unit. It is also called as CRC reminder. So that the resulting data unit becomes exactly divisible by a predetermined binary number





Binary Division