CS19541 COMPUTER NETWORKS

UNIT-I FUNDAMENTALS AND DATA LINK LAYER

Building a network – Requirements – Layering and protocols – Internet Architecture – Network software – Application Programming Interface (sockets) - Performance – Link layer Services - Framing – Error Detection and Correction - Reliable transmission.

UNIT-II MEDIA ACCESS AND INTERNETWORKING

Media Access Protocols – ALOHA - CSMA/CA/CD –Ethernet – Wireless LANs - 802.11- Bluetooth - Switching and Forwarding - Bridges and LAN Switches – Basic Internetworking- IP Service Model – IP fragmentation - Global Addresses – ARP - DHCP – ICMP- Virtual Networks and Tunnels.

UNIT-III ROUTING

Routing – Network as Graph - Distance Vector – Link State – Global Internet – Subnetting - Classless Routing (CIDR) - BGP- IPv6 – Multicast routing - DVMRP- PIM.

UNIT-IV TRANSPORT LAYER

Overview of Transport layer – UDP – TCP - Segment Format – Connection Management – Adaptive Retransmission - TCP Congestion control - Congestion avoidance (DECbit, RED) – QoS – Application requirements.

UNIT-V APPLICATION LAYER

E-Mail (SMTP, MIME, POP3, IMAP), HTTP – DNS - FTP - Telnet – web services - SNMP – MIB – RMON.

Text Books

1. Larry L. Peterson, Bruce S. Davie, “Computer Networks: A Systems Approach”, Fifth Edition, Morgan Kaufmann Publishers Inc., 2011.
2. Behrouz A. Forouzan, “Data Communications and Networking”, Fifth Edition, McGrawHill, 2017

Reference Books

1. William Stallings, “SNMP, SNMPv2, SNMPv3 and RMON 1 and 2”, Third Edition, Pearson Edition, 2009.
2. James F. Kurose, Keith W. Ross,” Computer Networking - A Top-Down Approach Featuring the Internet”, Seventh Edition, Pearson Education, 2017.
3. Andrew S. Tanenbaum, David J. Wetherall, “Computer Networks”, 5th Edition, Prentice Hall publisher, 2010.
4. William Stallings, “Data and Computer Communications”, Eighth Edition, Pearson Education, 2011.s

CS19541 - COMPUTER NETWORKS

UNIT-I FUNDAMENTALS AND DATA LINK LAYER

Building a network – Requirements – Layering and protocols – Internet Architecture – Network software –Application Programming Interface (sockets) - Performance – Link layer Services - Framing– Error Detection and Correction - Reliable transmission

Computer network

Computer network is defined as the interconnection of nodes (computers and other devices) connected by a communication channel (wired or wireless) that facilitates communication among users and allows them to share resources (Information, hardware and software resources.)

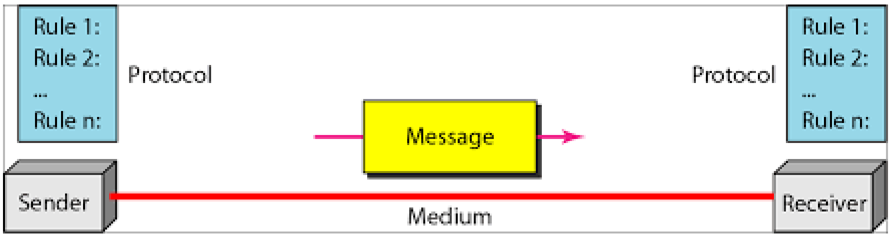
INTRODUCTION

Data Communications is the transfer of data or information between a sender and a receiver. The sender transmits the data and the receiver receives it.

The effectiveness of a data communication depends on three characteristics,

Delivery : The system must deliver data to correct destination.
Accuracy : The system must deliver data accurately.
Timeliness : The system must deliver data in a timely manner.

Components of data communication



- **Sender:** It is the transmitter of data. Some examples are Terminal, Computer, and Mainframe.
- **Medium:** The communication stream through which the data is being transmitted. Some examples are: Cabling, Microwave, Fiber optics, Radio Frequencies (RF), Infrared Wireless
- **Receiver:** The receiver of the data transmitted. Some examples are Printer, Terminal, Mainframe, and Computer.
- **Message:** It is the data that is being transmitted from the Source/Sender to the Destination/Receiver.

- **Protocol:** It is the set of rules and regulations (resides in the form of software and hardware) that are to be followed for communication. If protocol is not present it implies the nodes are connected but they can't communicate.

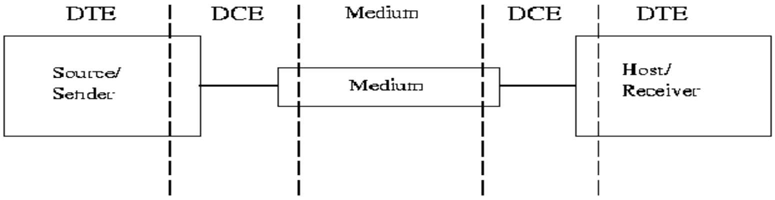


Figure 1.2: DTE and DCE

- **DCE:** The interface between the Sender and the Medium, and the Medium & the Receiver is called the DCE (Data Communication Equipment) and is a physical piece of equipment.
- **DTE:** Data Terminal Equipment is the Telecommunication name given to the Source and Receiver's equipment.

Direction of Data Flow

It defines how the data flows between two end points. Based on the direction and time of flow there are three kinds of data flow,

1. Simplex
2. Half-Duplex
3. Full-duplex.

Simplex:

In this type of data communication, the data flows in only one direction on the data communication line (medium).

Examples are Keyboard, Monitor, Radio and Television broadcasts

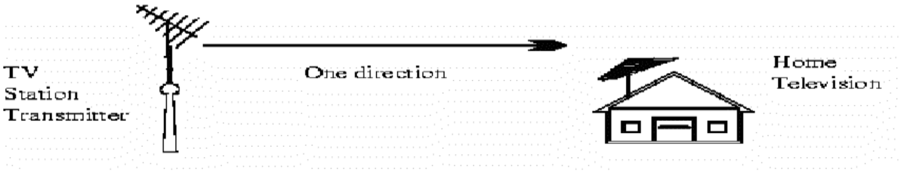


Figure 1.3: Simplex Data Flow

Half-Duplex:

In this type of data communication, the data flows in both directions but at a time in only one direction on the data communication line.

Example Conversation on walkie-talkies is a half-duplex data flow.

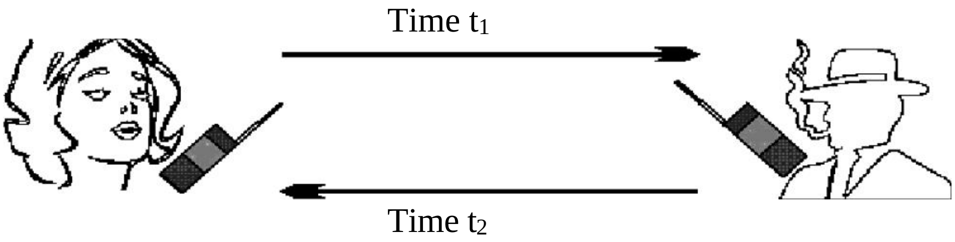


Figure: Half-Duplex Data Flow

Full-Duplex:

In this type of data communication, the data flows in both directions simultaneously. Example Telephones and Modems

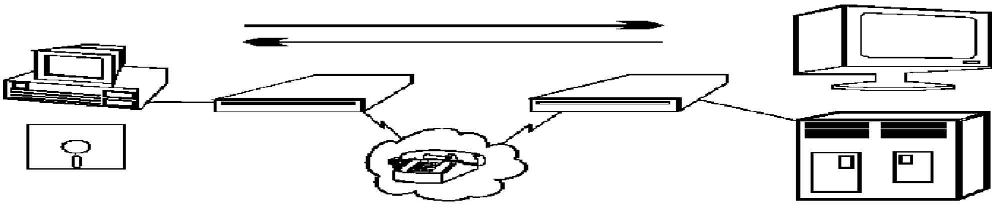


Figure: Full-Duplex Data Flow

Types of Connections / Line configuration / Direct links

There are two types of line configuration, they are

1. point to po4int
2. multipoint

Point to Point

- It provides a dedicated link between two devices.
- The entire capacity (bandwidth) of the link is reserved for transmission between these two devices.
  The two devices are connected by means of a pair of wires or using a microwave or satellite link.
- Eg : Computers connected by telephone line
  PPP connection between remote and TV

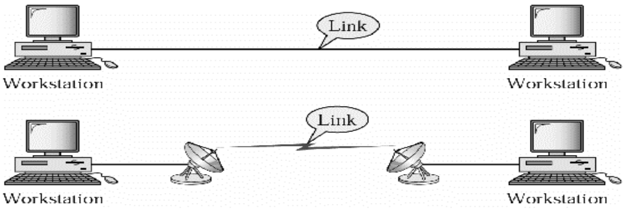


Figure: Point-to-point link

Multipoint (Multiple Access)

- It is a connection in which more than two devices share a single link.
- In this environment a single channel is shared, either spatially or temporally.
- If several devices can use the link at the same time it said to be spatially shared.
- If the devices take turn to use the link then it is referred to as timesharing.

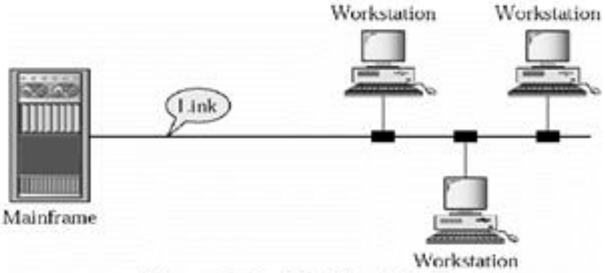


Figure : Multipoint link

Different Communication Modes

1) **Unicast - one to one**
   Unicast packets are sent from host to host. The communication is from a single host to another single host.
2) **Broadcast – one to all**
   Broadcast is when a single device is transmitting a packet to all other devices in a given address range.
3) **Multicast – one to many**
   Multicast enables a single device to communicate with a specific set of hosts.

Categories of networks

The three primary categories of network are Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN). The category into which a network fall is determined by its size, ownership, the distance it covers and its physical architecture.

LAN

- A LAN is usually privately owned and links the devices in a single office, building or campus.
- A LAN can be as simple as two PCs or it can extend throughout a company. LAN size is limited to a few kilometers.
- The most widely used LAN technology is the Ethernet technology developed by the Xerox Corporation.

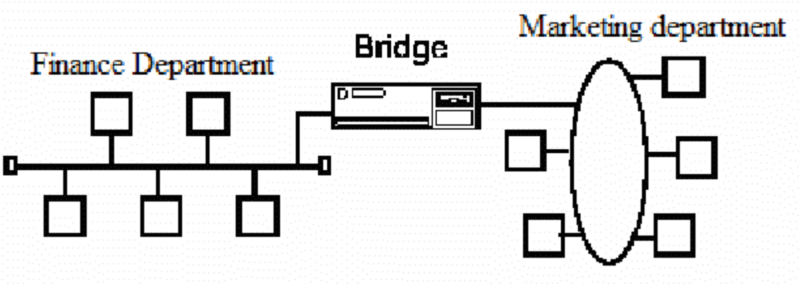


Figure 1.8: Local Area Network

MAN

- A MAN is designed to extend over an entire city.
- It could be a single network such as cable TV network or connect a number of LANs into a larger network.
- A MAN can be owned by a private company or it may be a service provided by a public company, such as local telephone company.
- Telephone companies provide a popular MAN service called (SMDS) Switched Multi-megabit Data Services.

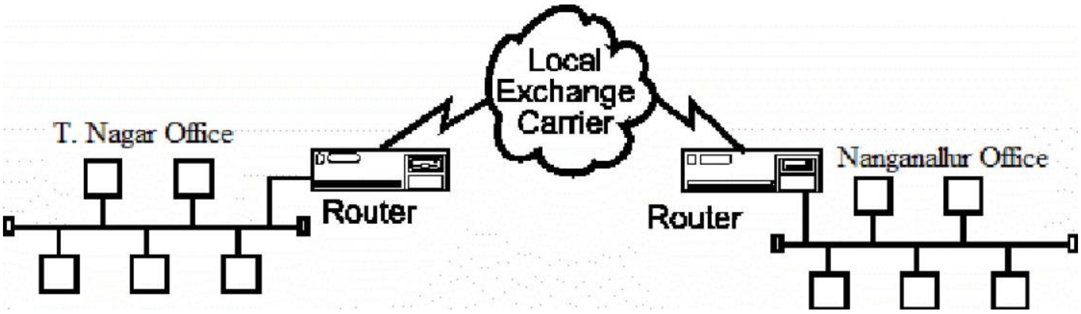
- 

Figure: Metropolitan Area Network

WAN

- A WAN provides long distance transmission of data, voice, image and video information over large geographic areas.
- Transmission rates are typically 2 Mbps, 34 Mbps, 45 Mbps, 155 Mbps and 625 Mbps. WAN utilize public, leased, or private communication equipment usually in combinations and therefore span an unlimited number of miles.
- A WAN that is wholly owned and used by a single company is referred to as an Enterprise Network.

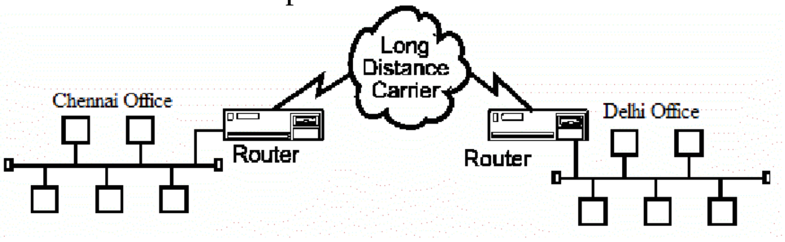


Figure 1.10: Wide Area Network

PAN

- A Personal Area Network (PAN) is the interconnection of devices within the range of an individual person, typically within a range of 10 meters.
- For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology.
- Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks.

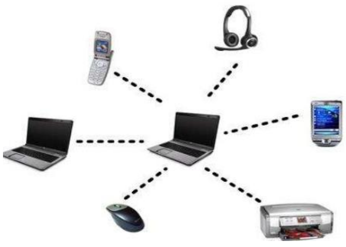


Figure: Personal Area Network

Topology

Physical Topology refers to the fashion in which nodes in the network is laid out physically. The topology of a network is the geometric representation of the relationship of all the links and the linking devices tone another. It defines the physical layout of the network.

The basic topologies are:

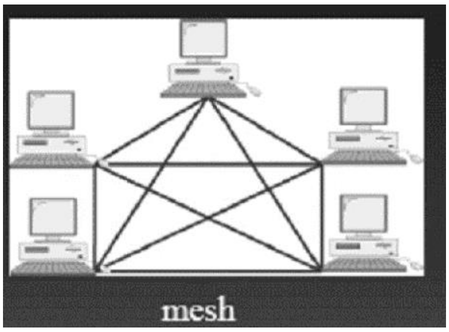
- Mesh
- Star
- Bus
- Ring
- Hybrid (combination of other types)

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

Merits

- Eliminates the traffic problems that occur when the links are shared by multiple devices.
- If one link becomes unusable, it does not incapacitate the entire system.
- Since every message travels along a dedicated line only the intended recipient will receive the message and hence the data is secure.

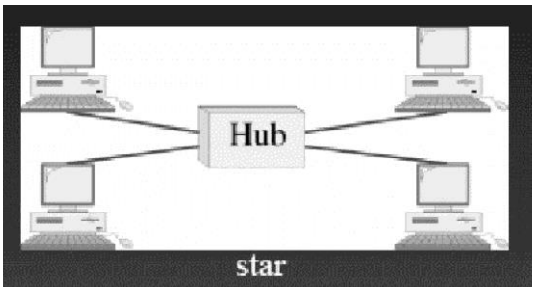


Demerits

- The amount of cabling and the I/O ports required increases with the number of devices connected in the network
- Installation and reconnection are difficult
- The sheer bulk of the wire accommodates more space than available.
- The hardware required to connect each link can be prohibitively expensive.

Star

- 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.
- 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.
- Failure of the central controller incapacitates the entire network.

Bus

- 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 to create a contact with a metallic core.
- 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.

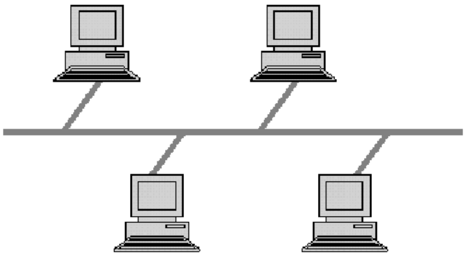


Figure 1.15: Bus Topology

Merits

- Ease of installation.
- Bus uses 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

- 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

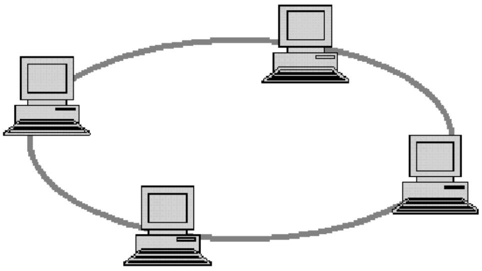


Figure 1.16: Ring Topology

Merits:

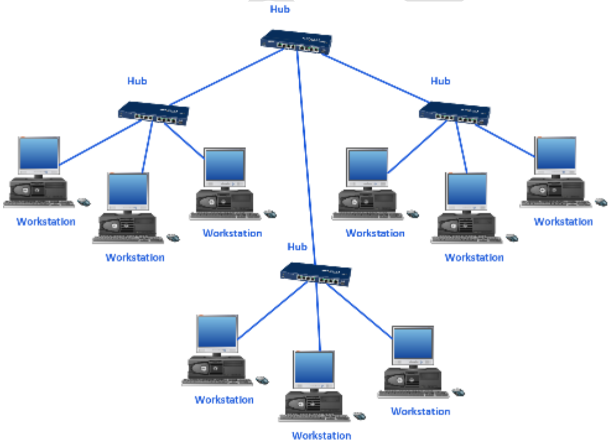
- Easy to install and reconfigure.
- To add or delete a device requires changing only two connections.

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

- A hybrid topology is a type of network topology that uses two or more other network topologies, including bus topology, mesh topology, ring topology, star topology, and tree topology.



Requirements

The following are the requirements to be followed to build any network,

- ✓ Identification of constraints and requirements
- ✓ Connectivity need to be decided
- ✓ Cost-effective resource sharing
- ✓ Support for common services

Identification of constraints and requirements of a network

Three groups of people might list their requirements for a network,

1. Application Programmer
   - List the services that his application needs: delay bounded delivery of data
2. Network Designer
   - Designs a cost-effective network with sharable resources
3. Network Provider
   - List the characteristics of a system that is easy to manage

Connectivity in a network:

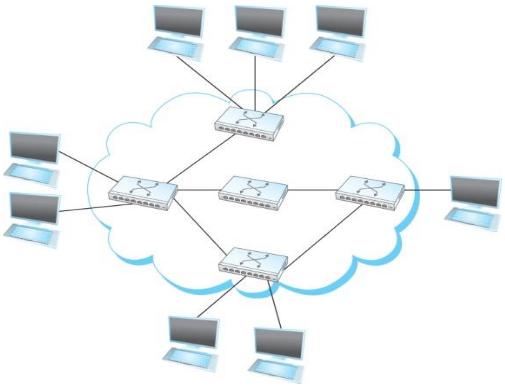
Links, Nodes, and Clouds

Network connectivity occurs at many different levels. At the lowest level, a network can consist of two or more computers directly connected by some physical medium, such as a coaxial cable or an optical fiber. We call such a physical medium a *link*, and we often refer to the computers it connects as *nodes.*

A set of computers can be indirectly connected. A set of independent networks (clouds) are interconnected to form an internetwork. A node that is connected to two or more networks is commonly called a router or gateway. A router/gateway forwards messages from one network to another.

Switched Network

Those nodes that are attached to at least two links run software that forwards data received on one link out on another. If organized in a systematic way, these forwarding nodes form a switched network. There are numerous types of switched networks, of which the two most common are circuit switched and packet switched.



Types of switched networks

1. **Circuit Switched**

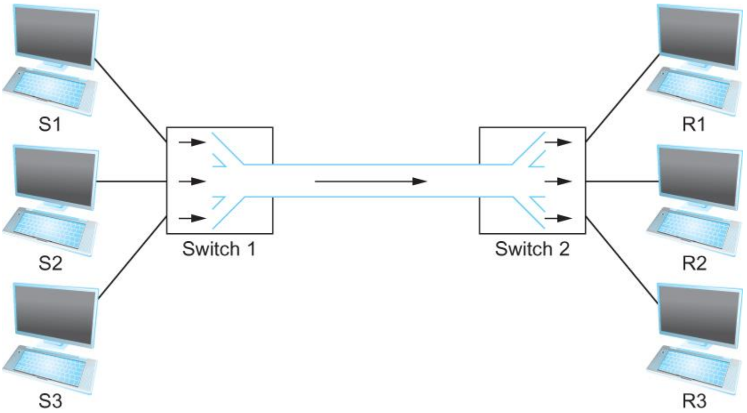
   First establishes a dedicated circuit across a sequence of links and then allows the source node to send a stream of bits across this circuit to a destination node.

2. **Packet Switched networks**

   It uses a strategy called store-and-forward. Each node in a store-and-forward network first receives a complete packet over some link, stores the packet in its internal memory, and then forwards the complete packet to the next node.

Cost-Effective Resource Sharing

- Resource: links and nodes
- How to share a link?
  - **Multiplexing**
    Analogy to a timesharing computer system.
  - **De-multiplexing**



Multiplexing multiple logical flows over a single physical link

Synchronous Time-division Multiplexing (STDM)

- Equal-sized quanta
- Round-robin fashion
- Time slots/data transmitted in predetermined slots

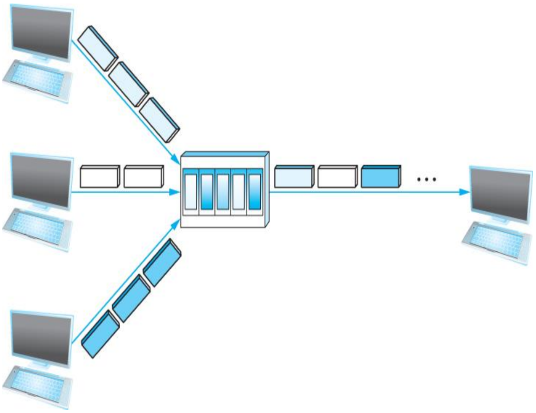
Frequency Division Multiplexing(FDM)

Eg:Diff. TV stations with diff. frequencies.

- Both STDM and FDM waste resources and hard to accommodate changes (fixed time slots and frequencies)

Statistical Multiplexing

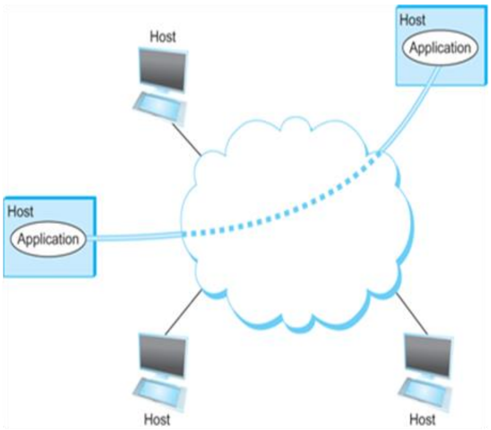
Like STDM: sharing over time but data is transmitted based on demand rather than during a predetermined time slot.



A switch multiplexing packets from multiple sources onto one shared link

Support for Common Services

- Logical Channels
  - Application-to-Application communication path or a pipe
- Client/Server
- Two types of communication channel
  - Request/Reply Channels
  - Message Stream Channels



Process communicating over an abstract channel

NETWORK ARCHITECTURES

Network designers have developed general blueprints—usually called network architectures—that guide the design and implementation of networks.

1. Layering & protocols
2. OSI layers
3. Internet Architecture

Layering and Protocols

Layering provides two nice features.

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.

First, it decomposes the problem of building a network into more manageable components. Rather than implementing a monolithic piece of software that does everything you will ever want, you can implement several layers, each of which solves one part of the problem.

Second, it provides a more modular design. If you decide that you want to add some new service, you may only need to modify the functionality at one layer, reusing the functions provided at all the other layers.

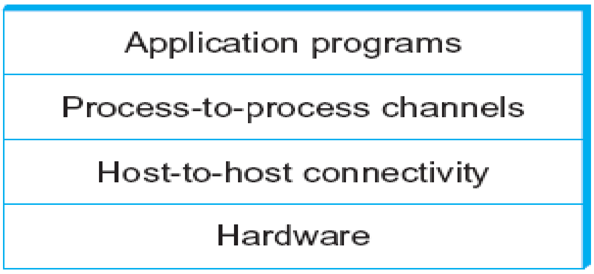
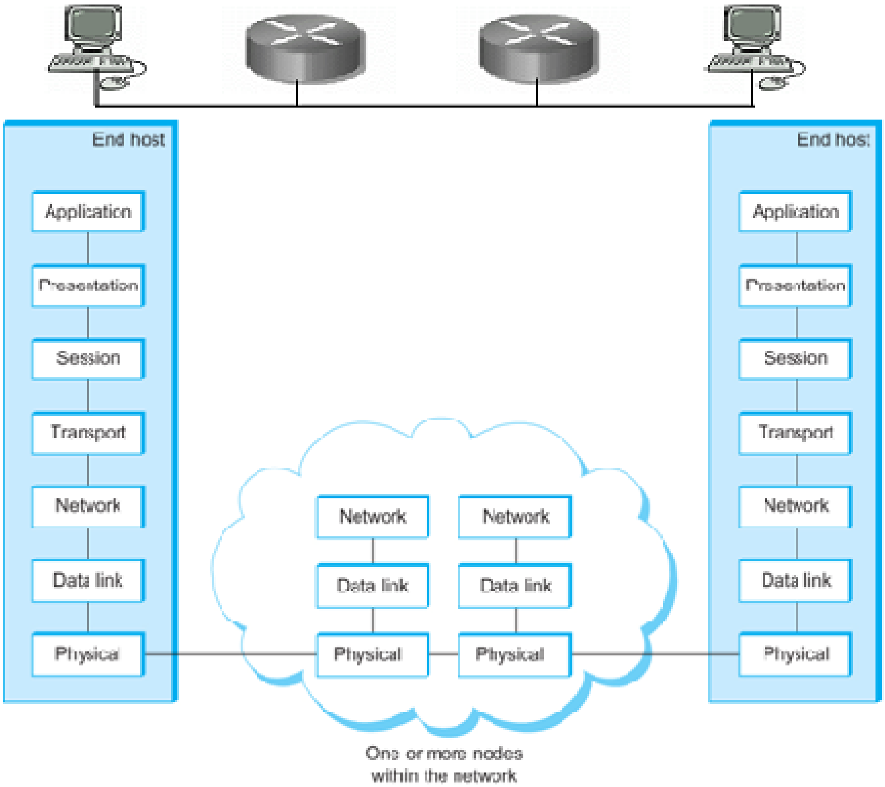


Fig: Example of a layered network system

ISO - OSI reference Model

- The International Standards Organization (ISO) - Open Systems Interconnect (OSI) is a standard which defines a set of rules to govern the data communication between two devices without worrying about the underlying architecture of the devices. It describes the functionalities for transfer of data between each layer. Each layer has a specific function.
  - *ISO is the organization; OSI is the model.*
  - There are 7 Layers in the OSI model

1. Physical Layer
2. Datalink Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



Two interfaces

- Service interface
- Peer interface

Service interface- defines the operations that local objects can perform on the protocol.

Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

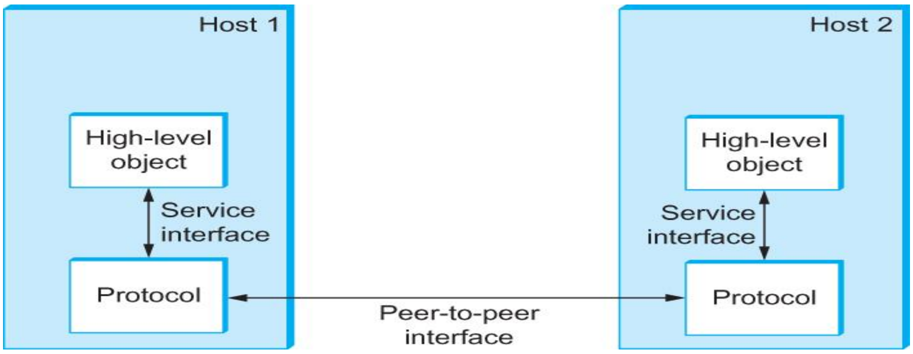
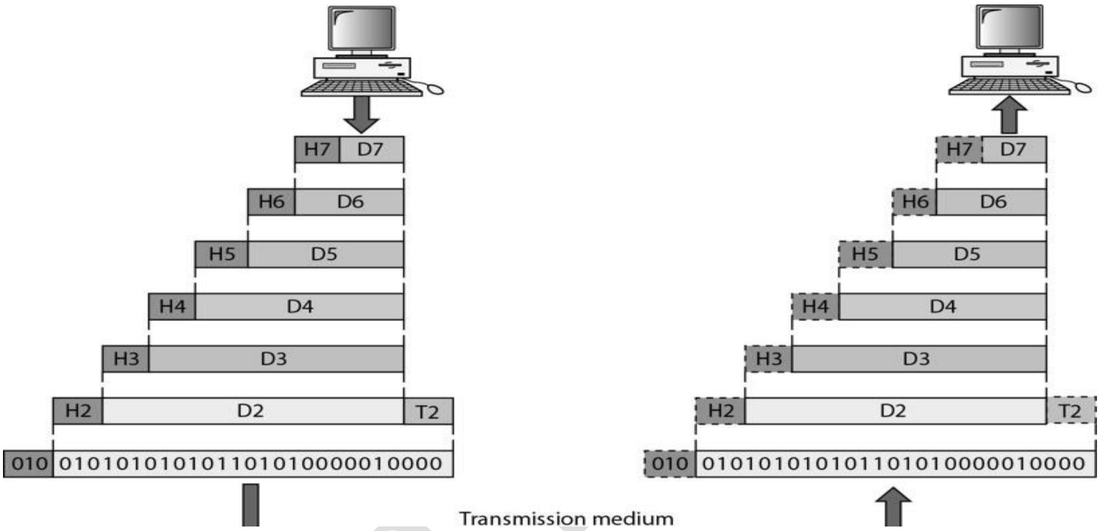


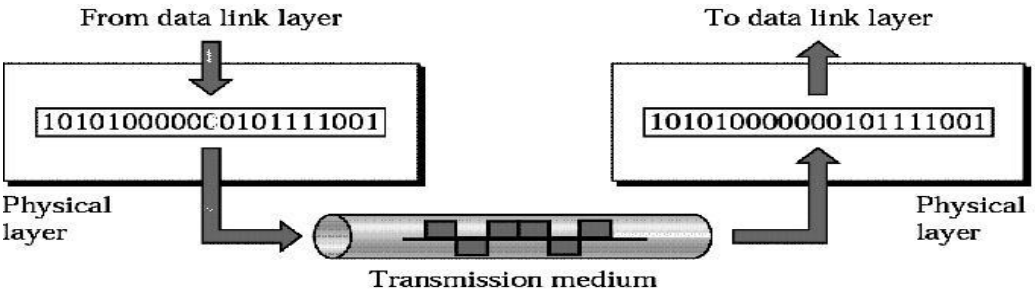
Fig : Service and Peer Interfaces

A Data exchange using the OSI model



1. <u>PHYSICAL LAYER</u> (bit level transmission)

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It is responsible for moving bits from one node to the next.



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.

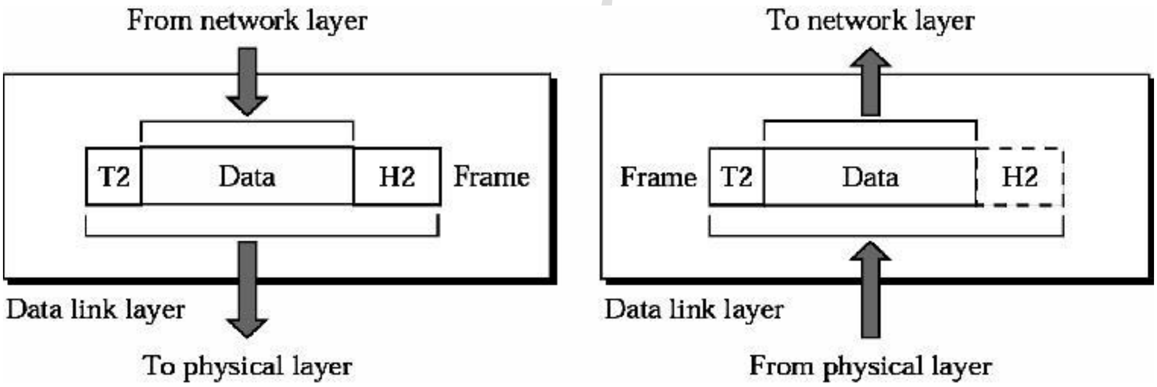
- ✓ **Line Configuration -** In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.

- ✓ **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
(Node to node delivery or hop to hop delivery of frames)

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 control mechanism.

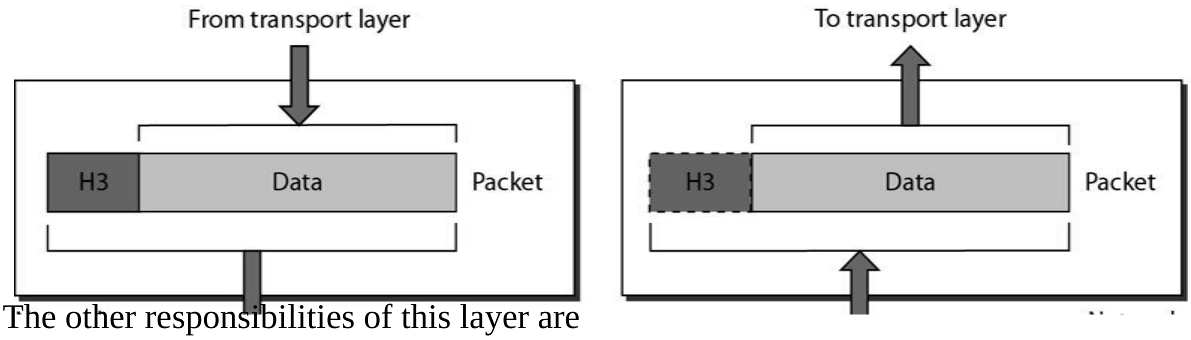
- ✓ **Error control-** Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

- ✓ **Access control -**Used to determine which device has control over the link at any given time.

3. NETWORK LAYER
(Source to destination delivery of individual packets)

This layer is responsible for the delivery of packets from source to destination. It is mainly required, when it is necessary to send information from one network to another.

It ensures that each packet gets from its point of origin to its final destination.

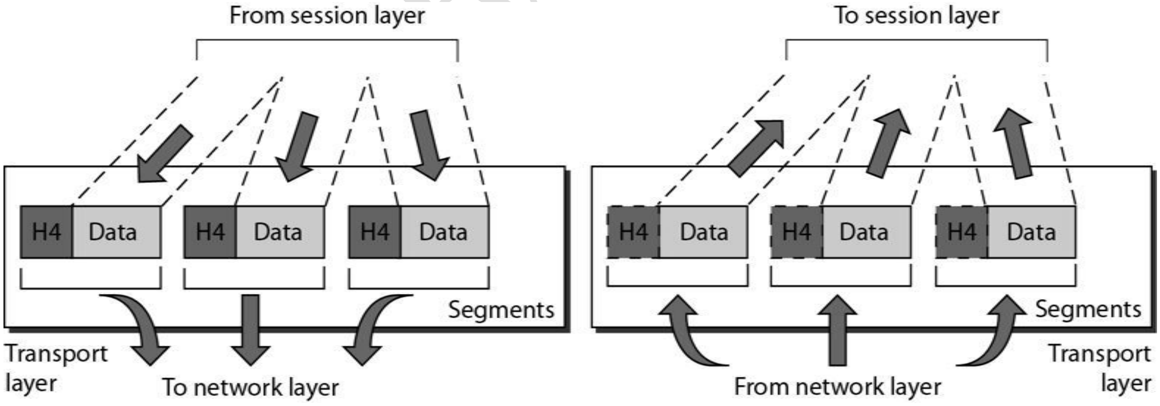


The other responsibilities of this layer are

- ✓ **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
(Source to destination delivery of entire message)

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



The other responsibilities of this layer are

- ✓ **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.

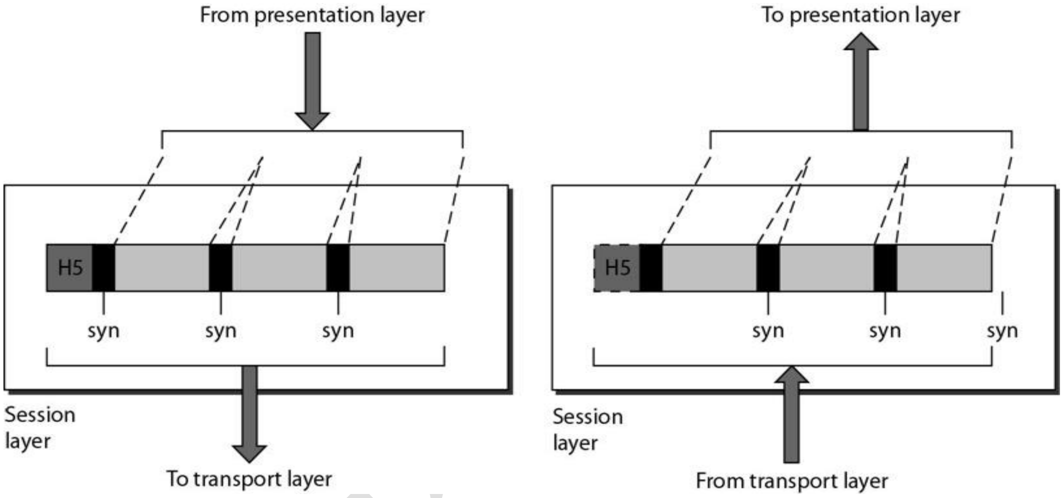
- ✓ **Connection control -** This can either be **connectionless or connection-oriented.** The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.

- **Flow and error control -** Similar to data link layer, but process to process take place. ie end to end error & flow control

5. SESSION LAYER

(Responsible for dialog control and synchronization)

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. Example: If a system is sending a file of 2000 pages, check points may be inserted after every 100 pages to ensure that each 100 page unit is advised and acknowledged independently. So if a crash happens during the transmission of page 523, retransmission begins at page 501, pages 1 to 500 need not be retransmitted.

6. PRESENTATION LAYER

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

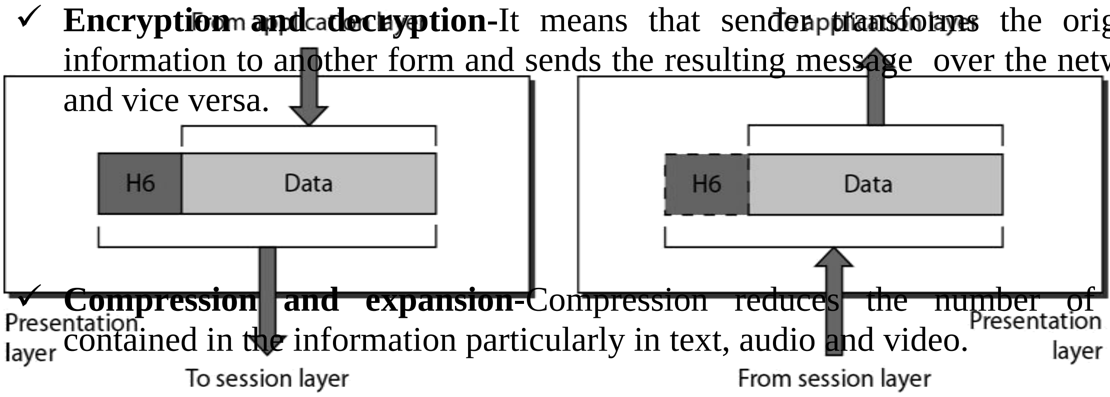
The presentation layer is responsible for translation, compression, and encryption. It is concerned with the syntax and semantics of information exchanged between two systems.

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.

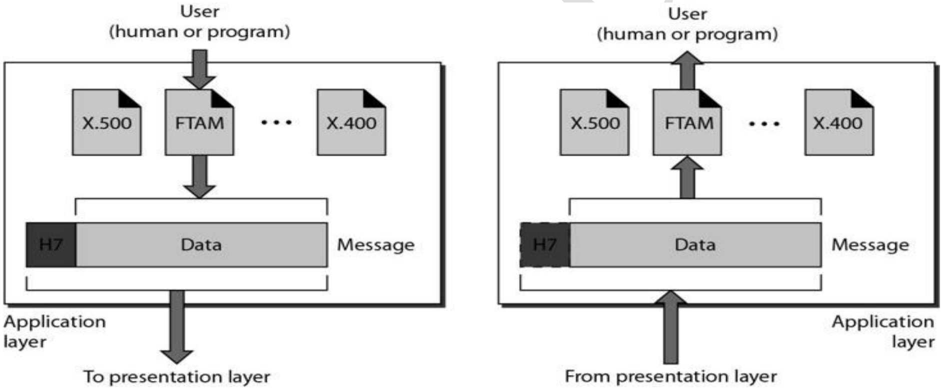
- ✓ **Encryption and decryption-**It means that sender transforms the original information to another form and sends the resulting message over the network and vice versa.

- ✓ **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 network resources**. 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.
- ✓ **Network Virtual terminal:** A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host.
- ✓ **Mail services -** Provides email forwarding and storage.
- ✓ **Directory services -** Provides database sources to access information about various sources and objects.

Internet(TCP/IP) Architecture

The Internet architecture, which is sometimes called the TCP/IP architecture after its two main protocols. 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 model, and the experience gained from building them was a major influence on the OSI reference model.

Layers of TCP / IP model

Application layer
Transport layer
Internet layer
Network interface layer

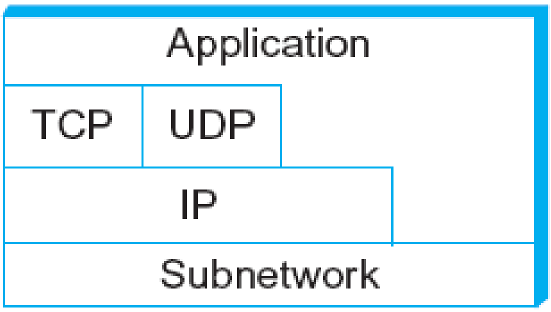
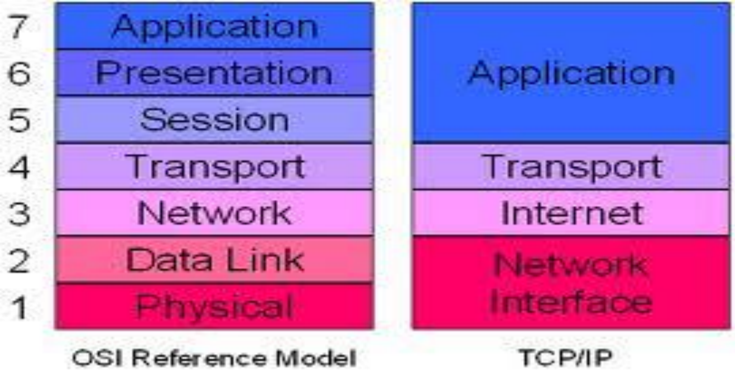


Fig: Alternative view of the Internet architecture. The “Network Interface” layer shown here is sometimes referred to as the “sub-network” or “link” layer.

While the 7-layer OSI model can, with some imagination, be applied to the Internet, a 4-layer model is often used instead.

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.

Comparison of OSI and TCP / IP layers



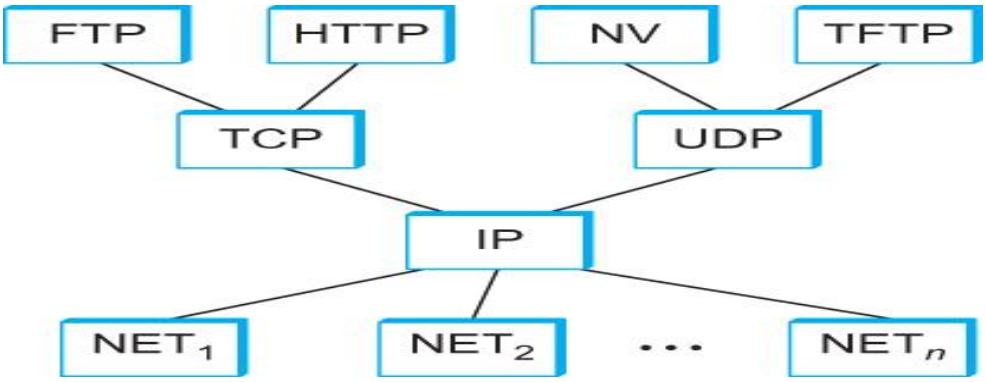


fig: Internet Protocol Graph

At the lowest level is a wide variety of network protocols, denoted NET1, NET2, and so on. In practice, these protocols are implemented by a combination of hardware (e.g., a network adaptor) and software (e.g., a network device driver). For example, you might find Ethernet or wireless protocols (such as the 802.11 Wi-Fi standards) at this layer. (These protocols in turn may actually involve several sublayers, but the Internet architecture does not presume anything about them.)

The second layer consists of a single protocol—the Internet Protocol (IP). This is the protocol that supports the interconnection of multiple networking technologies into a single, logical internetwork.

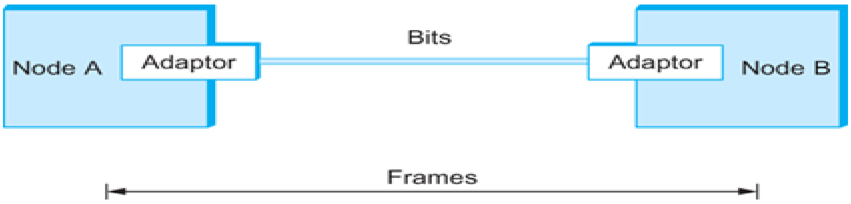
The third layer contains two main protocols—the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).TCP and UDP provide alternative logical channels to application programs: TCP provides a reliable byte-stream channel, and UDP provides an unreliable datagram delivery channel (datagram may be thought of as a synonym for message). In the language of the Internet, TCP and UDP are sometimes called end-to-end protocols, although it is equally correct to refer to them as transport protocols.

Running above the transport layer is a range of application protocols, such as HTTP, FTP, Telnet (remote login), and the Simple Mail Transfer Protocol (SMTP), that enable the interoperation of popular applications.

Framing-Datalink Layer

Data link layer divides the stream of bits received from the upper layer (network layer) into manageable data units called frames. It adds a header to the frame to define the physical address (source address & destination address).

- Blocks of data (called frames at this level) are exchanged between nodes.
- It is the network adaptor that enables the nodes to exchange frames.
- When node A wishes to transmit a frame to node B, it tells its adaptor to transmit a frame from the node's memory.
- This results in a sequence of bits being sent over the link.
- The adaptor on node B then collects together the sequence of bits arriving on the link and deposits the corresponding frame in B's memory.
- Recognizing exactly what set of bits constitutes a frame—that is, determining where the frame begins and ends—is the central challenge faced by the adaptor.



Bits flow between adaptors, frames between hosts

Fixed-Size Framing: Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.

Variable-Size Framing: In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Three approaches were used for this purpose:

Framing Protocols:

(i) Byte-oriented protocols
(ii) Bit-oriented protocols
(iii) Clock-based protocols

Byte-oriented protocols:

- sentinel approach
  1. BISYNC – Binary Synchronous Communication
  2. PPP – Point-to-point Protocol
- Byte-counting approach
  3. DDCMP- Digital Data Communication Message Protocol

Bit-oriented protocols:

(i) HDLC – High Level Data Link Control

Clock-based protocols:

(i) SONET - Synchronous Optical Network

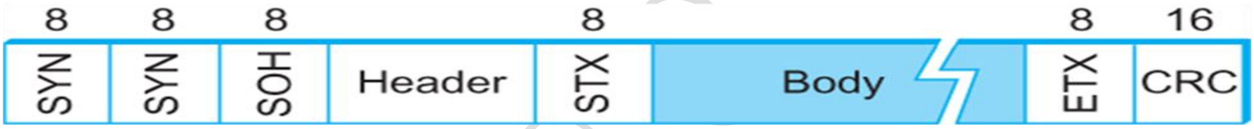
Byte oriented Protocols

Sentinel Approach

- It uses special characters known as sentinel characters to indicate where the frame starts and ends.

Binary Synchronous Communication (BISYNC)

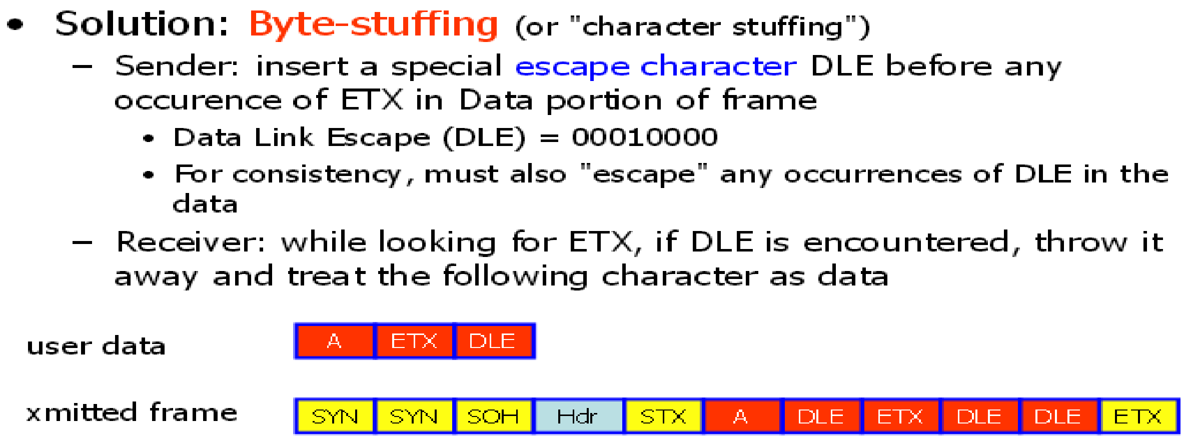
- The beginning of a frame is denoted by sending a special SYN (synchronization) character.
- The data portion of the frame is then contained between special *sentinel characters:* STX (start of text) and ETX (end of text).
- The SOH (start of header) field serves much the same purpose as the STX field.



BISYNC Frame Format

- The problem with the sentinel approach, of course, 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 often called **byte stuffing** or **character stuffing** because extra characters are inserted in the data portion of the frame.

Example



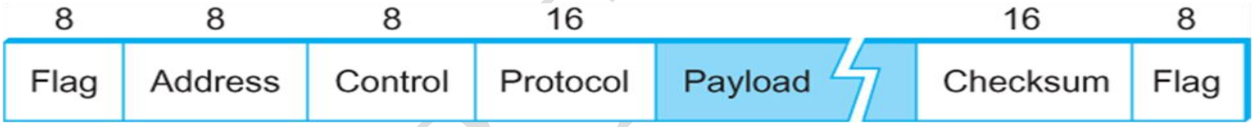
- Solution: Byte-stuffing (or "character stuffing")
  - Sender: insert a special escape character DLE before any occurence of ETX in Data portion of frame
    - Data Link Escape (DLE) = 00010000
    - For consistency, must also "escape" any occurrences of DLE in the data
  - Receiver: while looking for ETX, if DLE is encountered, throw it away and treat the following character as data

user data: A | ETX | DLE

xmitted frame: SYN | SYN | SOH | Hdr | STX | A | DLE | ETX | DLE | DLE | ETX

***PPP* - Point-to-Point Protocol (PPP):**

- It is similar to BISYNC in that it uses character stuffing. The format for a PPP frame is given below.
- The special start-of-text character, denoted as the Flag field is 01111110, which is byte stuffed if it occurs within the payload field.
- The Address and Control fields usually contain default values.
- The Address field which is always set to the binary value 11111111, indicates that all stations are to accept the frame. This value avoids the issue of using data link addresses.
- The default value of the Control field is 00000011. This value indicates an unnumbered frame. In other words, PPP does not provide reliable transmission using sequence numbers and acknowledgements.
- The Protocol field is used for demultiplexing. It identifies the high-level protocol such as IP or IPX (an IP-like protocol developed by Novell).
- The frame payload size can be negotiated, but it is 1500 bytes by default.
- The Checksum field is either 2 (by default) or 4 bytes long.
- The PPP frame format is unusual in that several of the field sizes are negotiated rather than fixed.
- This negotiation is conducted by a protocol called LCP (Link Control Protocol). PPP and LCP work in tandem: LCP is also involved in establishing a link between two peers when both sides detect the **carrier signal.**

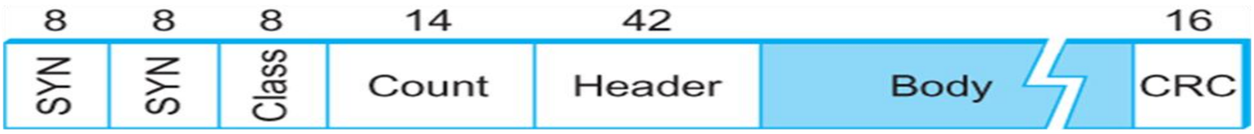


PPP Frame Format

Byte-counting approach

DDCMP protocol – Digital Data Communication Message Protocol:

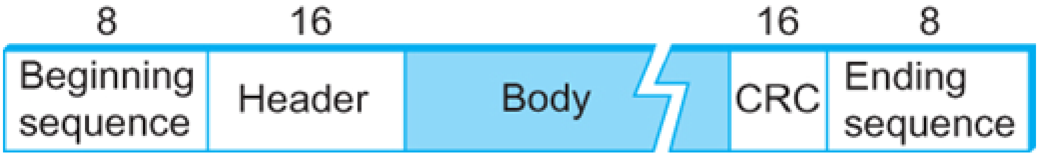
- The COUNT field specifies how many bytes are contained in the frame's body.
- One danger with this approach is that a transmission error could corrupt the COUNT field, in which case the end of the frame would not be correctly detected.This is sometimes called a **framing error.**
- The receiver will then wait until it sees the next SYN character to start collecting the bytes that make up the next frame.



DDCMP Frame Format

Bit-Oriented Protocols (HDLC)

- A bit oriented protocol is not concerned with byte boundaries—it simply views the frame as a collection of bits.
- The Synchronous Data Link Control (SDLC) protocol developed by IBM is an example of a bit-oriented protocol; SDLC was later standardized by the ISO as the High-Level Data Link Control (HDLC) protocol.

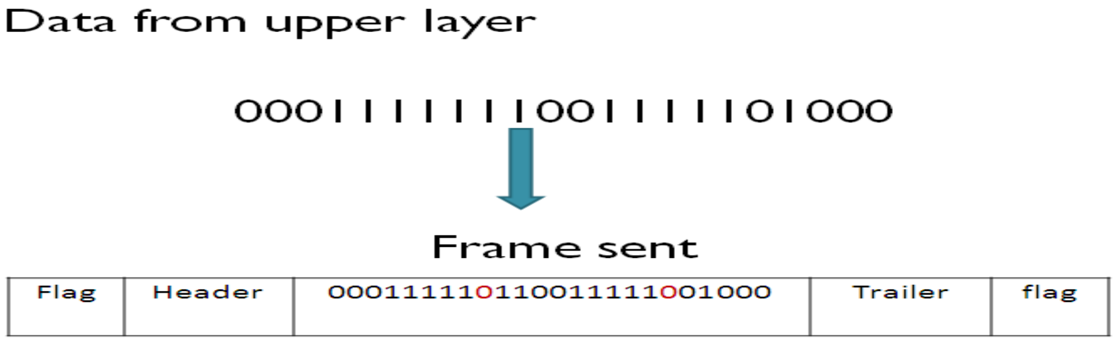


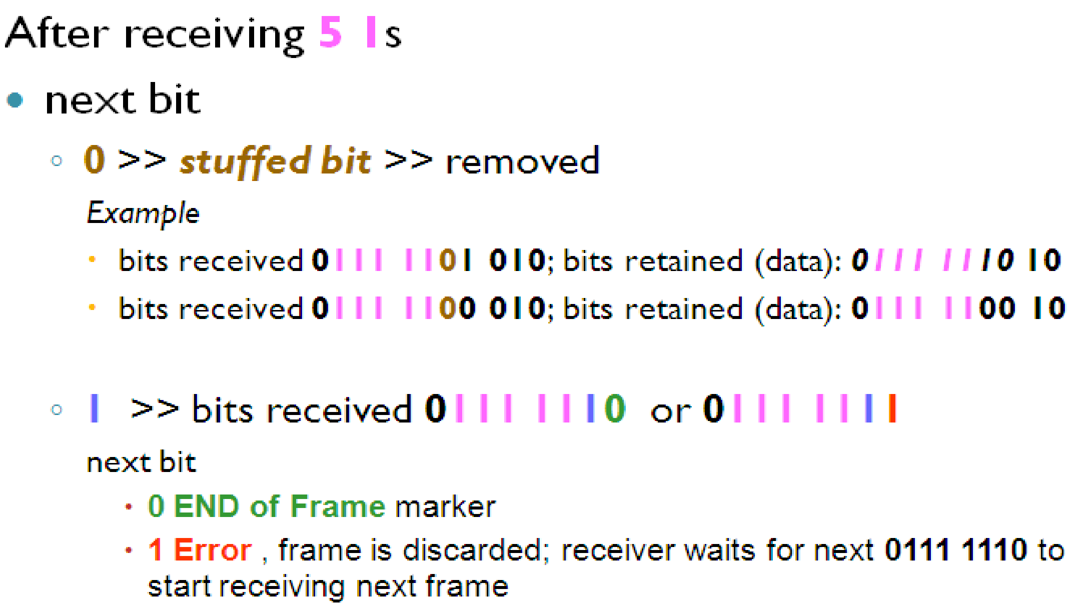
- HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110.
- This sequence is also transmitted during any times that the link is idle so that the sender and receiver can keep their clocks synchronized.
- Because this sequence might appear anywhere in the body of the frame—in fact, the bits 01111110 might cross byte boundaries—bit-oriented protocols use a technique known as ***bit stuffing***.

Bit stuffing in the HDLC protocol works as follows.

- On the sending side, whenever 0 followed by five consecutive 1's has been seen in the body of the message the sender inserts a 0.
- On the receiving side, when 0 followed by five consecutive l's arrive, the receiver makes its decision based on the next bit it sees (i.e., the bit following the five 1' s).
- If the next bit is 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.





After receiving 5 1s

- next bit
  - 0 >> ***stuffed bit*** >> removed

    Example

    - bits received **0111 1101 010**; bits retained (data): ***0111 1110 10***
    - bits received **0111 1100 010**; bits retained (data): **0111 1100 10**
  - 1 >> bits received **0111 1110** or **0111 1111**

    next bit

    - **0 END of Frame** marker
    - **1 Error** , frame is discarded; receiver waits for next **0111 1110** to start receiving next frame

Clock based Protocols

Clock-Based Framing (SONET):

- A third approach to framing is exemplified by the Synchronous Optical Network (SONET) standard.
- SONET addresses both the framing problem and the encoding problem.
- It also addresses a problem that is very important for phone companies—the multiplexing of several low-speed links onto one high-speed link.
- No bit stuffing is used, so that a frame's length does not depend on the data being sent.
- A STS-1 (lowest-speed SONET link runs at 51.84 Mbps.) frame is shown in Figure 2.13.
- It is arranged as nine rows of 90 bytes each.
- The first 3 bytes of each row are overhead, with the rest being available for data that is being transmitted over the link.
- The first 2 bytes of the frame contain a special bit pattern, and it is these bytes that enable the receiver to
  the receiver looks for the special bit pattern consistently, hoping to see it appearing once every 810 bytes, since each frame is 9 × 90 = 810 bytes long.
- When the special pattern turns up in the right place enough times, the receiver concludes that it is in sync and can then interpret the frame correctly.

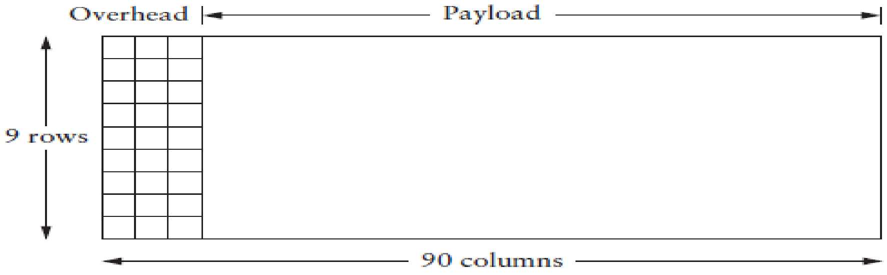


Fig : A SONET STS-1 Frame

For example, 64 Kbps of a SONET link's capacity is set aside for a voice channel that is used for maintenance.

The overhead bytes of a SONET frame are encoded using Non Return to Zero (NRZ), the simple encoding described in the previous section where 1s are high and 0s are low.

However, to ensure that there are plenty of transitions to allow the receiver to recover the sender's clock, the payload bytes are *scrambled*.

This is done by calculating the exclusive-OR (XOR) of the data to be transmitted and by the use of a well-known bit pattern. The bit pattern, which is 127 bits long, has plenty of transitions from 1 to 0, so that XORing it with the transmitted data is likely to yield a signal with enough transitions to enable clock recovery.

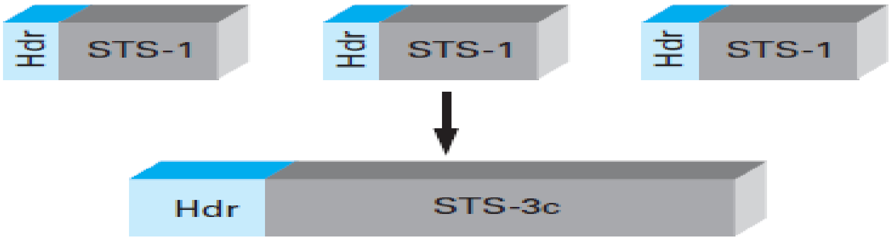


Fig : Three STS-1 Frames multiplexed onto one STS-3c frame.

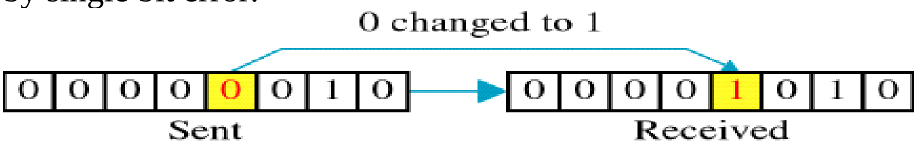
ERROR DETECTION AND CORRECTION

ERROR

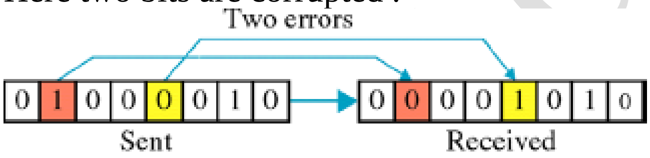
Data can be corrupted during transmission. Signals flows from one point to another. They are subjected to unpredictable interferences from heat, magnetism and other forms of electricity. For reliable communication, errors must be detected and corrected.

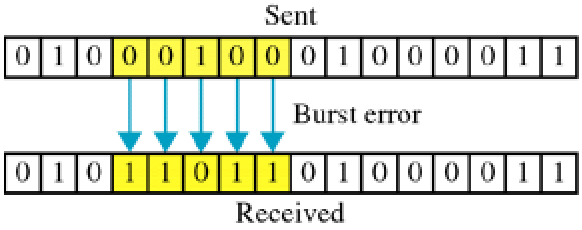
TYPES OF ERRORS

- **Single bit Error:**
  The term single bit error means that only one bit of a given data unit is changed from 1 to 0 or 0 to 1. 010101 is changed to 110101 here only one bit is changed by single bit error.



- **Burst Error:**
  A burst error means that 2 or more bits in the data unit have changed.
  Example:
  Here two bits are corrupted .





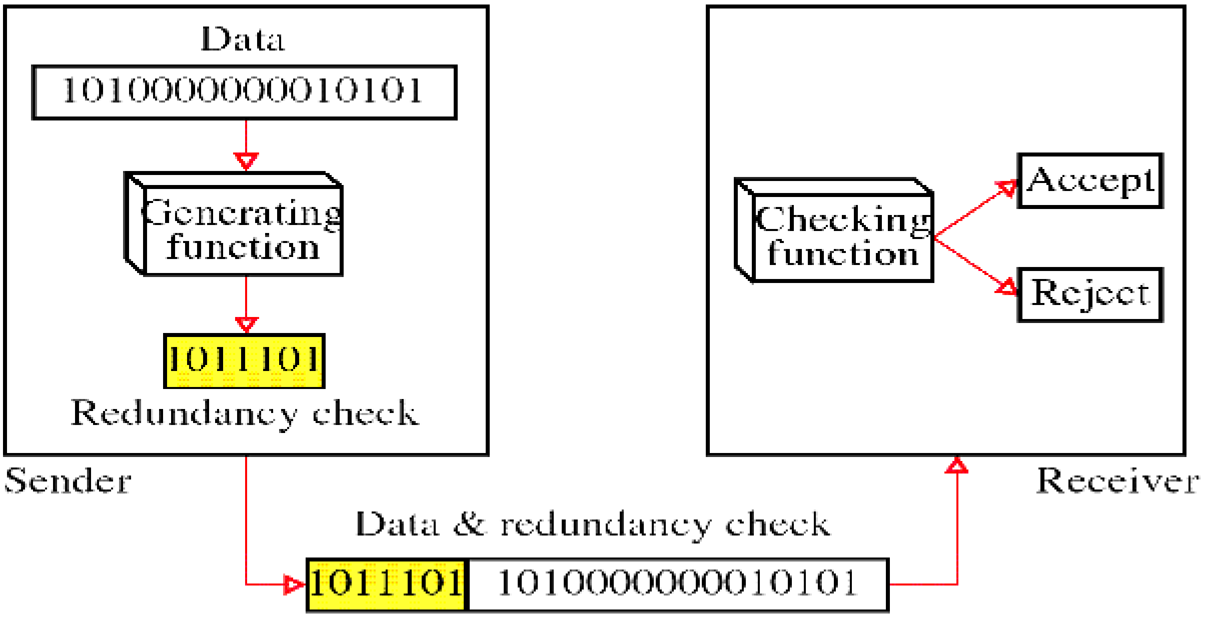
Errors can happen in the following ways,

- The bits in the frame can be inverted, anywhere within the frame including the data bits or the frame's control bits.
- Additional bits can be inserted into the frame, before the frame or after the frame and
- Bits can be deleted from the frame.

ERROR DETECTION

Redundancy

Error detection use the concept of redundancy, which means adding extra bits for detecting errors .i.e., instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit.



Error Detection methods

1. **Parity check**
   - *Simple parity check (Vertical Redundancy Check)*
   - Two dimensional Parity Check (*Longitudinal Redundancy Check)*
2. **Cyclic redundancy check**
3. **Checksum**

Parity check

A redundant bit called parity bit, is added to every data unit so that the total number of 1's in the unit becomes even (or odd).

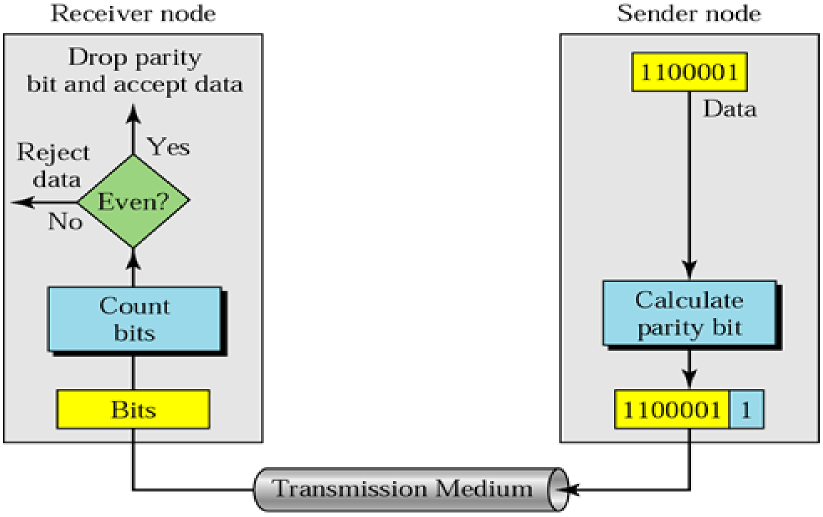
Simple parity check (Vertical Redundancy Check)

Sender Side:

In a simple parity check a redundant bit is added to a stream of data so that total number of 1's in the data become even or odd.

Receiver Side:

The total data bit+ Redundant bit is then passed through parity checking function. For even parity, it checks for even number of 1's and for odd parity it checks even number of 1's. If the check fails, it implies error is detected the data is rejected otherwise accepted.

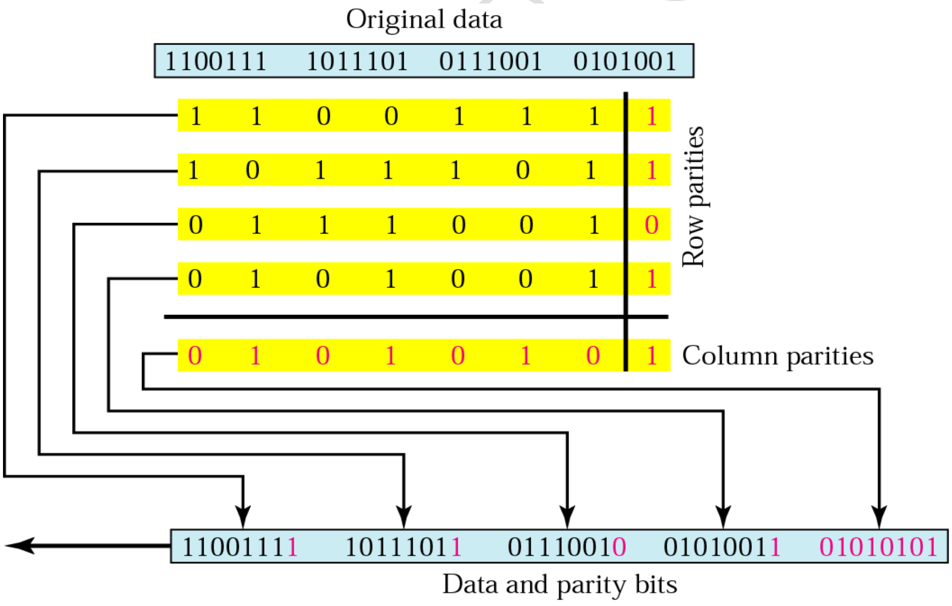


Note :

- *Simple parity check can detect all single-bit errors. It can detect burst errors only if the* total number *of bits changed in each data unit is odd.*

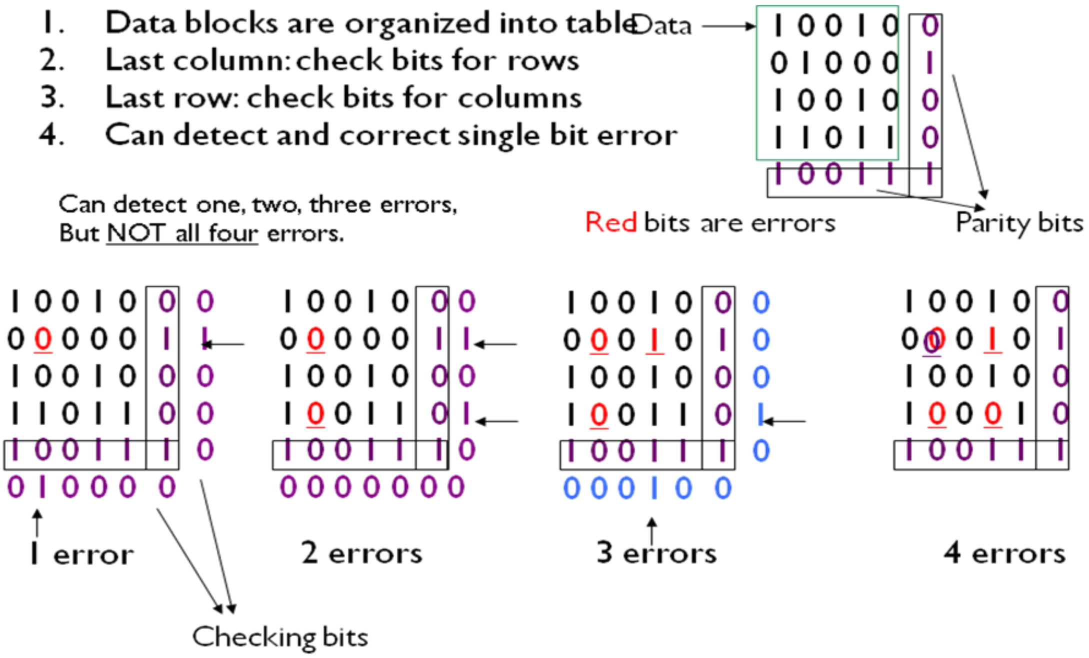
<u>Two dimensional Parity Check (*Longitudinal Redundancy Check*)</u>

In two-dimensional parity check, a block of bits is divided into rows to form a 2-dimensional array; add single parity check bits to each row and each column; transmit row-by-row.



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

Example 2



1. Data blocks are organized into table
2. Last column: check bits for rows
3. Last row: check bits for columns
4. Can detect and correct single bit error

Can detect one, two, three errors,
But NOT all four errors.

CYCLIC REDUNDANCY CHECK (CRC)

CRC is based on binary division. In CRC, a sequence of redundant bits, called the CRC or the CRC remainder is generated by performing binary division (using a predetermined divisor) and it is appended to the end of the data unit at the sender side.

At the receiver side, if the resulting unit (data + CRC) becomes exactly divisible by the same predetermined binary number (divisor) , the data is accepted. If a remainder results it indicates that the data unit has been damaged in transit and therefore must be rejected.

STEP BY STEP PROCEDURE

- First a starting of n 0's is appended to the data unit. The number n is one less than the number of bits in the predetermined divisor, which is n+ 1 bit.
- The newly elongated data unit is divided by the divisor, using a process called binary division. The remainder resulting from this division is the CRC.
- The CRC of n bits derived in step 2 replaces the appended 0s at the end of the data unit and the data is transmitted.(Note: CRC can also be all 0's)
- The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole stream as unit and divides it by the same divisor that was used to find the CRC remainder.
- If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes. If the stream has been changed in transit, the division yields a non zero remainder and the data does not pass.

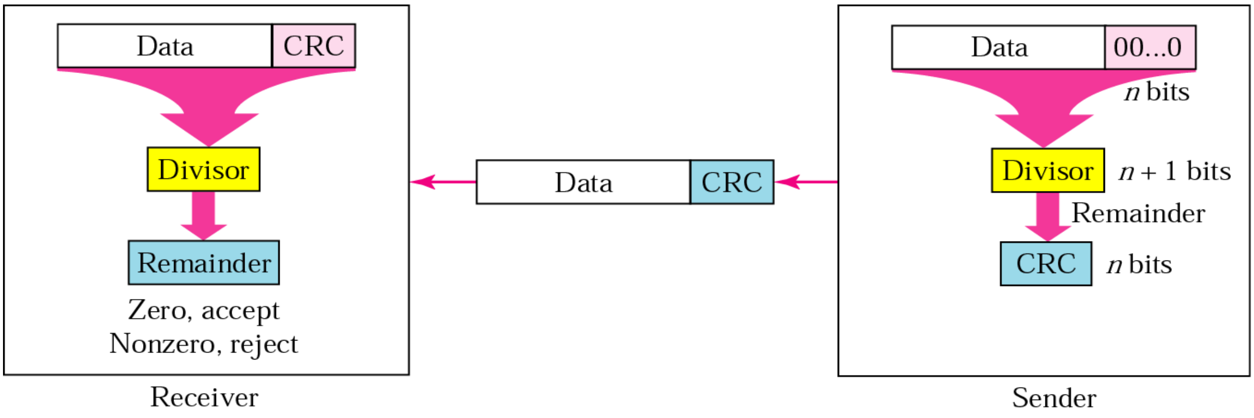


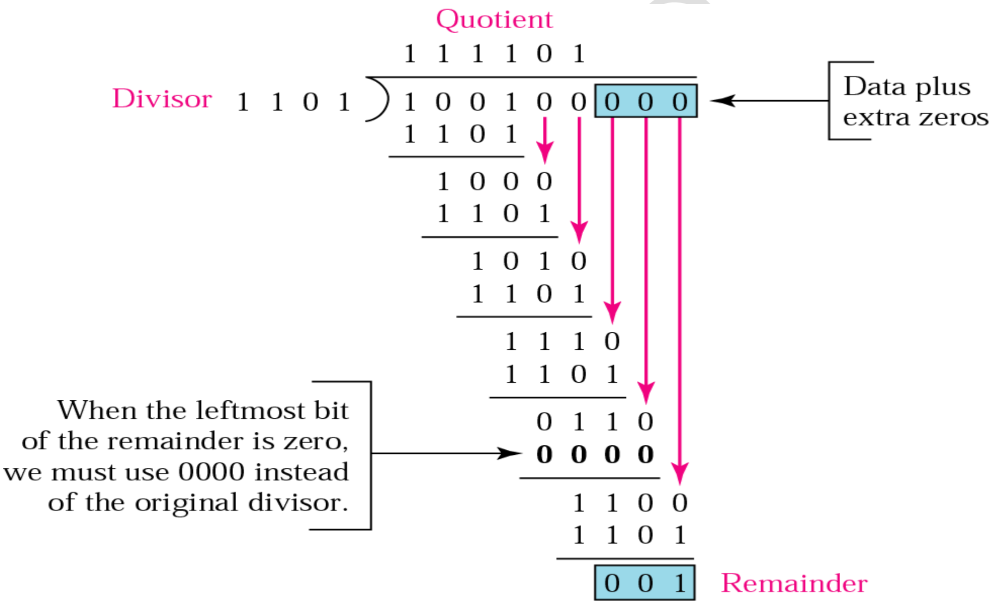
Figure : *CRC generator and checker*

CRC GENERATOR AND CHECKER

Example: Data is 100100 and Divisor is 1101

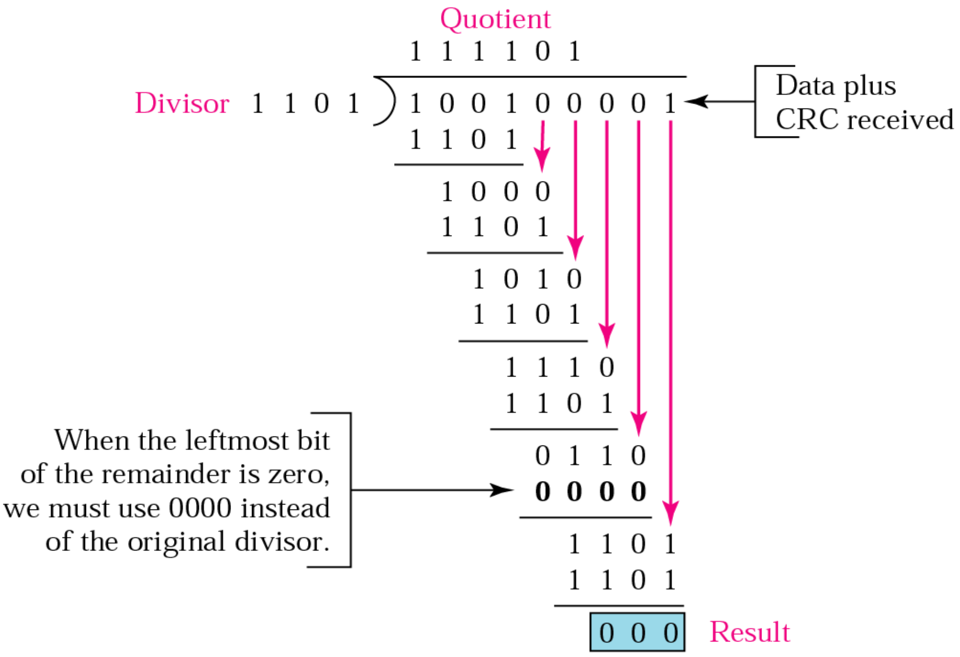
CRC GENERATOR

It uses modulo-2 division. The following figure shows this process.



CRC CHECKER

- A CRC checker function is exactly as the generator does. After receiving the data appended with the CRC, it does the same modulo-2 division.
- If the remainder is all 0s, the CRC is dropped and the data are accepted; otherwise, the received stream of bits is discarded and data are resent.
- The following figure shows the process of division in the receiver.

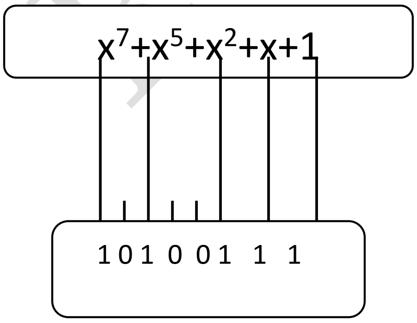


POLYNOMIALS

The divisor in the CRC most often represented not as a string of 1s and 0s, but as an algebraic polynomial. The polynomial format is useful to solve the concept mathematically.

$$\boxed{x^7+x^5+x^2+x+1}$$

A polynomial



The polynomial generator should have following properties:

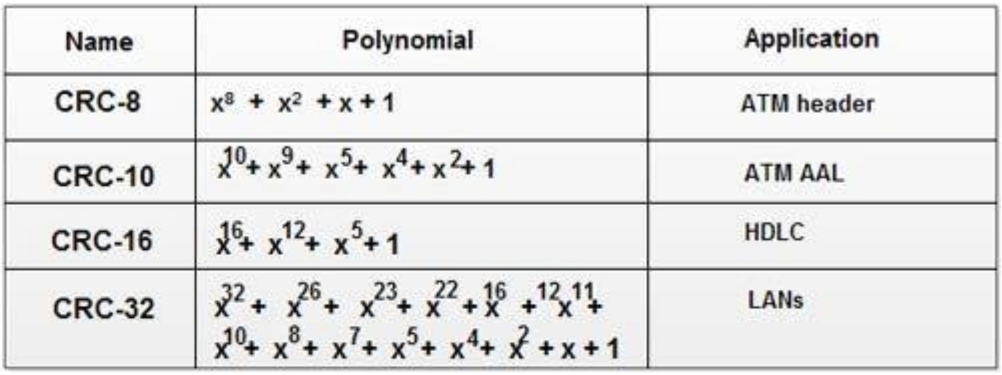
1. It should have at least two terms.

2. The coefficient of the term x^0 should be 1.

3. It should not be divisible by x.

4. It should be divisible by x+ 1.

There are several different standard polynomials used by popular protocols for CRC generation.



Name	Polynomial	Application
CRC-8	$x^8 + x^2 + x + 1$	ATM header
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$	ATM AAL
CRC-16	$x^{16} + x^{12} + x^5 + 1$	HDLC
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	LANs

CRC Performance

- *All* burst errors with length **less than** or **equal** to the degree of the polynomial (r)
- CRC can detect ***all*** burst errors that affect an **odd number** of bits
- CRC can detect ***all*** burst errors of length **equal** to the degree of the polynomial+1 **(r+1)** with probability $1 – (1/2)^{r–1}$.
- CRC can detect burst errors of length **greater** than the degree of the polynomial+1 **(r+1)** with probability $1 – (1/2)^r$

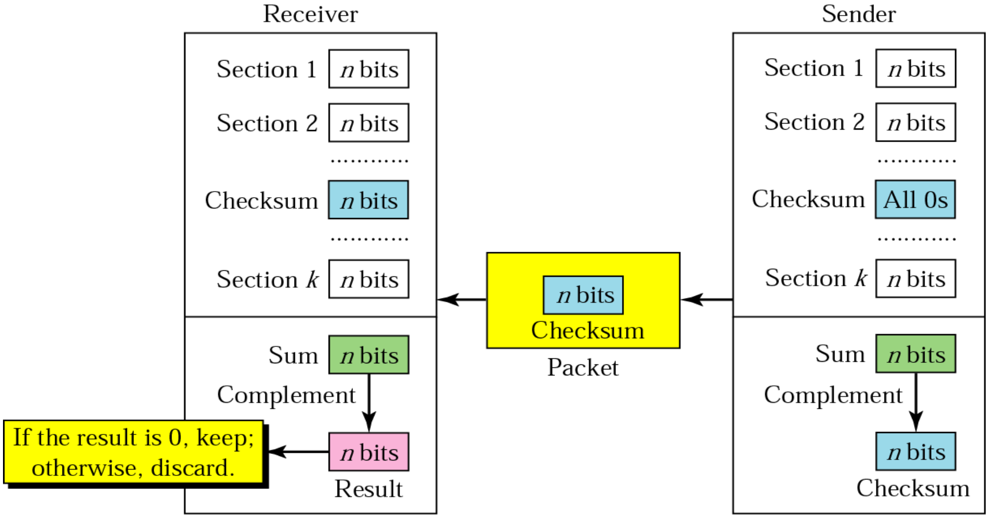
  (where r is the degree of the CRC polynomial)

CHECKSUM

The checksum is based on the redundancy.

CHECKSUM GENERATOR (sender side)

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one’s complement addition.
4. The sum is complemented and becomes the checksum (redundancy bits).
5. The checksum is sent with the data across the network



CHECKSUM CHECKER (receiver side)

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

EXAMPLE

Suppose the block of 16 bits is to be sent using a checksum of 8 bits.

10101001   00111001

the numbers are added using one's complement arithmetic

```
 1 0 1 0 1 0 0 1     block 1
   0 0 1 1 1 0 0 1     block 2
 _______________

   1 1 1 0 0 0 1 0
   0 0 0 0 0 0 0 0      initial checksum
  _________________
   1 1 1 0 0 0 1 0      sum

   0 0 0 1 1 1 0 1      Checksum ( 1's complement value of sum )
```

The data sent it is 10101001   00111001   00011101

Now the receiver receives the pattern with no error

10101001   00111001   00011101

the receiver adds these three sections, it will get all ones, which, after complementing, is all 0s and shows that there is no error.

```
 1 0 1 0 1 0 0 1
   0 0 1 1 1 0 0 1
   0 0 0 1 1 1 0 1
 _______________
1 1 1 1 1 1 1 1     sum

0 0 0 0 0 0 0 0     complement (DATA is correct )
```

suppose there is a burst error of length 5 that affects four bits.

10101***11***1   ***11***111001   00011101

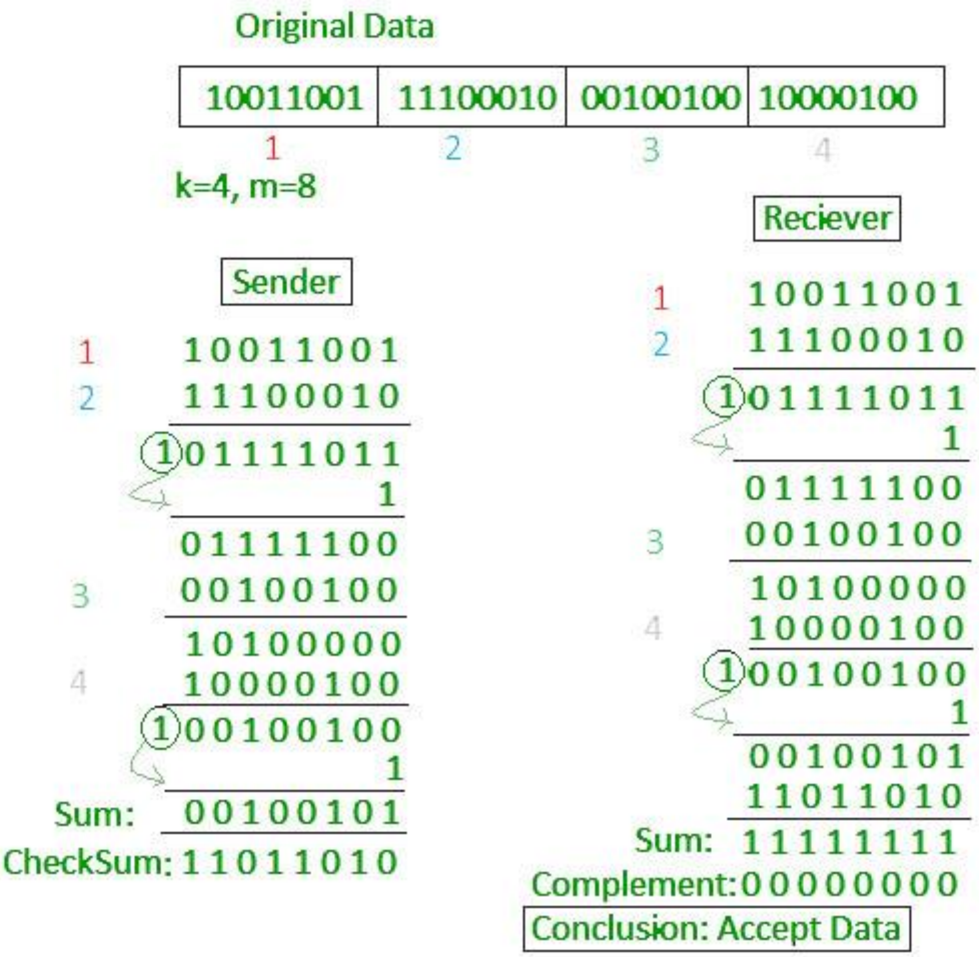
when the receiver adds these sections, it gets

```
 1 0 1 0 1 1 1 1
   1 1 1 1 1 0 0 1
 _______________
(1)1 0 1 0 1 0 0 0
                1 (carry 1)
 _______________
 1 0 1 0 1 0 0  1
   0 0 0 1 1 1 0 1
 _______________
   1 1 0 0 0 1 1 1  (carry 1)
```

1 1 0 0 0 1 0 1 sum
0 0 1 1 1 0 0 0 complement

As the complement is non zero we assume that (the data is errored)

Example 2:



PERFORMANCE

- It detects all errors involving an odd number of bits as well as most errors involving an even number of bits.
- If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in the second segment are also damaged, the sum of those columns will not change and the receiver will not detect the problem.

Error correction

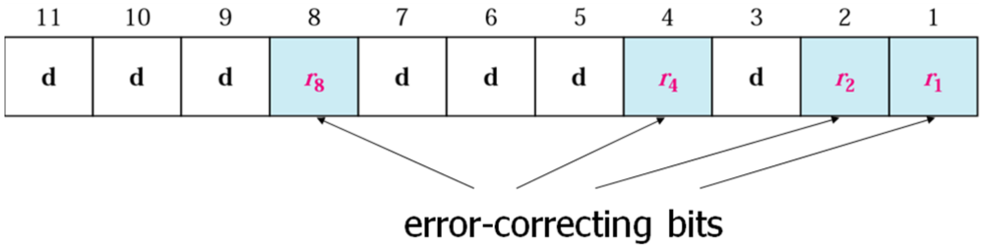
- Two methods
  1. Retransmission after detecting error
     -retransmit the data if error is detected
  2. Forward error correction (FEC)
     -hamming code is used to correct the error

HAMMING CODE

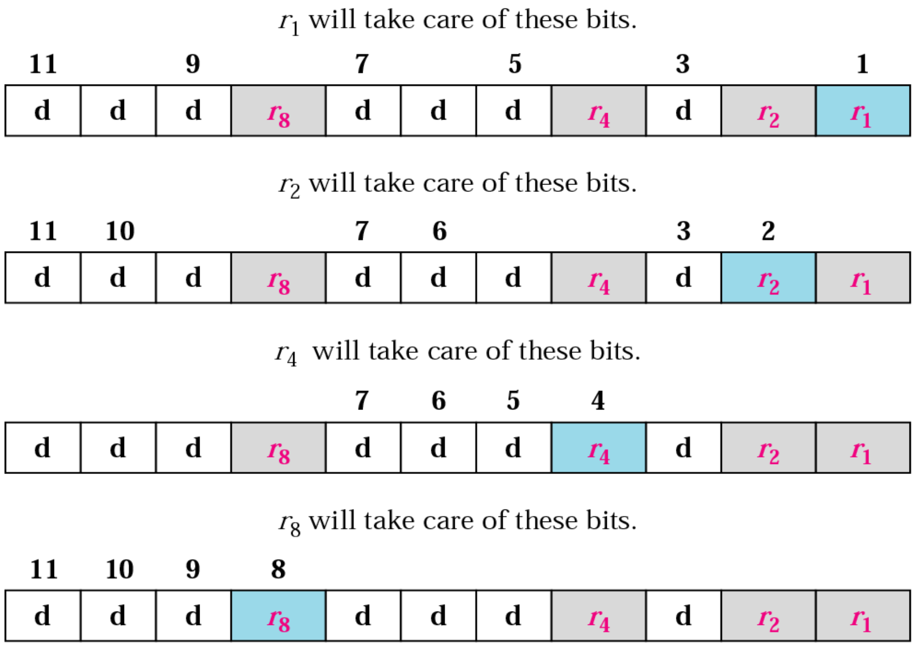
- ✓ A ***minimum number of redundancy bits*** needed to correct any single bit error in the data
- ✓ A minimum of 4 redundancy bits is needed if the number of data bits is 4.
- ✓ Redundancy bits in the Hamming code are placed in the codeword bit positions that are a power of 2
- ✓ Each redundancy bit is the parity bit for a different combination of data bits
- ✓ Each data bit may be included in more than one parity check.
- ✓ But the r bits are also transmitted along with data; hence
- ✓ $2^r \geq k+r+1$

Number of Redundant Bits

Number of data bits *k*	**Number of redundancy bits *r***	**Total bits *k + r***
1	**2**	**3**
2	**3**	**5**
3	**3**	**6**
4	**3**	**7**
5	**4**	**9**
6	**4**	**10**
7	**4**	**11**



Redundant Bit Calculation


r_1 will take care of these bits.
11 9 7 5 3 1
d d d r_8 d d d r_4 d r_2 r_1
r_2 will take care of these bits.
11 10 7 6 3 2
d d d r_8 d d d r_4 d r_2 r_1
r_4 will take care of these bits.
7 6 5 4
d d d r_8 d d d r_4 d r_2 r_1
r_8 will take care of these bits.
11 10 9 8
d d d r_8 d d d r_4 d r_2 r_1

For r_1,

The bits considered are -1,3,5,7,9,11(to decide on these bits, follow this trick, since r_1 bit, start from 1st bit, take one and leave one and so on)

For r_2,

The bits considered are -2,3,6,7,10,11(to decide on these bits, follow this trick, since r_2 bit, start from 2nd bit, take two and leave two and so on)

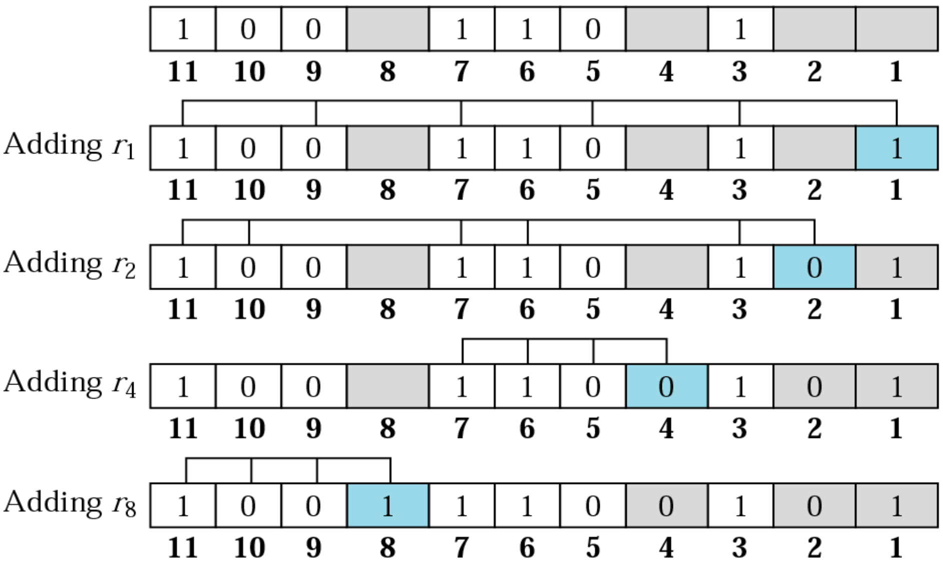
For r_4,

The bits considered are -4,5,6,7(to decide on these bits, follow this trick, since r_4 bit, start from 4th bit, take four and leave four and so on)

For r_8,

The bits considered are -8,9,10,11(to decide on these bits, follow this trick, since r_8 bit, start from 8th bit, take eight and leave eight and so on)

Example: *Hamming Code*

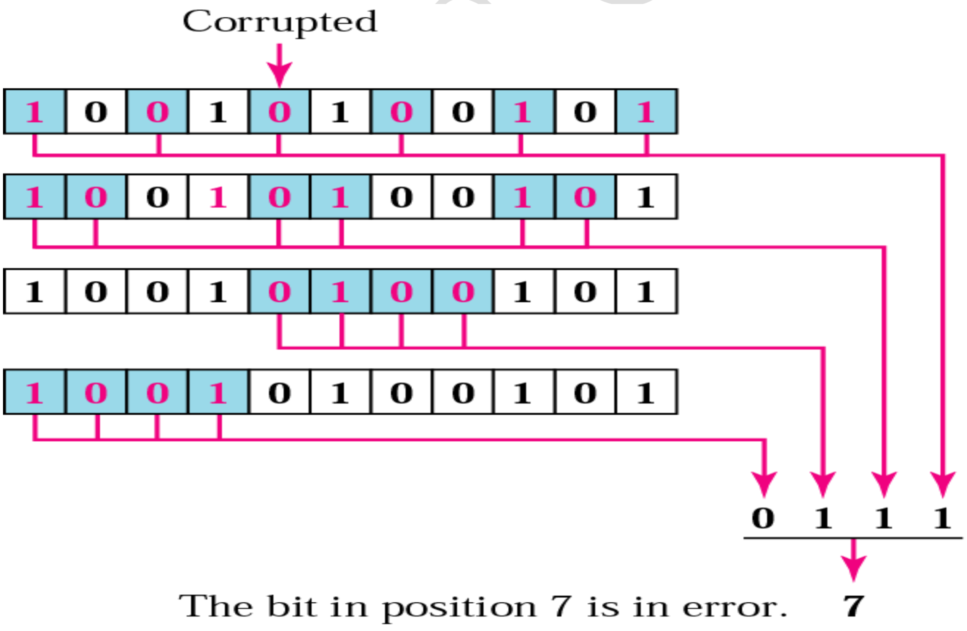


Data:
1 0 0 1 1 0 1

Code:
1 0 0 1 1 1 0 0 1 0 1

Example: *Correcting Error*

- **Receiver receives 10010100101**



FLOW CONTROL (RELIABLE TRANSMISSION)

Flow control is a technique used for the following reasons,

- ◦ If sender sends frames faster than recipient processes, then buffer overflow occurs at the receiver side.
- ◦ Receiver needs some time to process incoming frames.

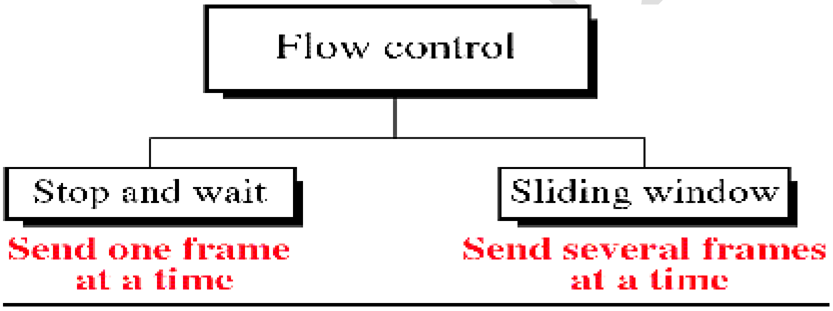
Flow control coordinates the amount of data that can be sent before receiving acknowledgement from the receiver. It is one of the most important duties of the data link layer.

- ■ ***Flow control Refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment from the receiver.***

ACK

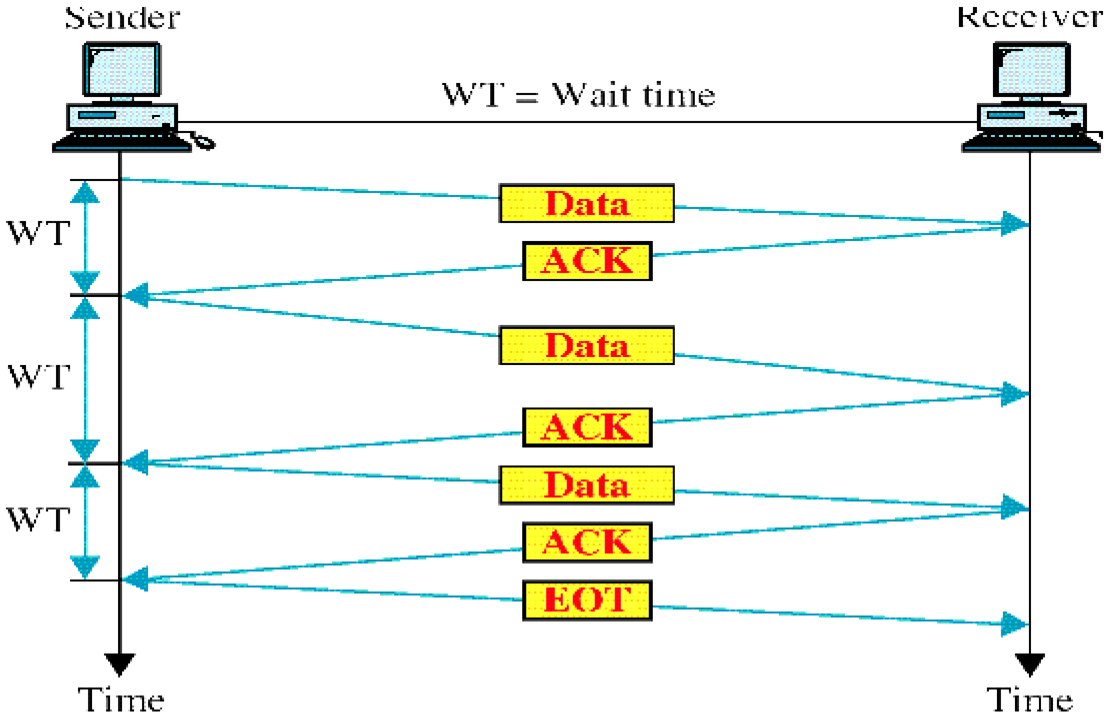
- An *acknowledgement* (ACK for short) is a small control frame that a protocol sends back to its peer saying that it has received the earlier frame.
    - ◦ A control frame is a frame with header only (no data).
    - ◦ The receipt of an *acknowledgement* indicates to the sender of the original frame that its frame was successfully delivered.

MECHANISMS



1. Stop and Wait Protocol

- Idea of stop-and-wait protocol is straightforward.
- After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.
- If the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame.



Timeline showing 4 different scenarios for the stop-and-wait algorithm

a) ***The ACK is received before the timer expires;***
b) ***the original frame is lost;***
c) ***the ACK is lost;***
d) ***the timeout fires too soon***

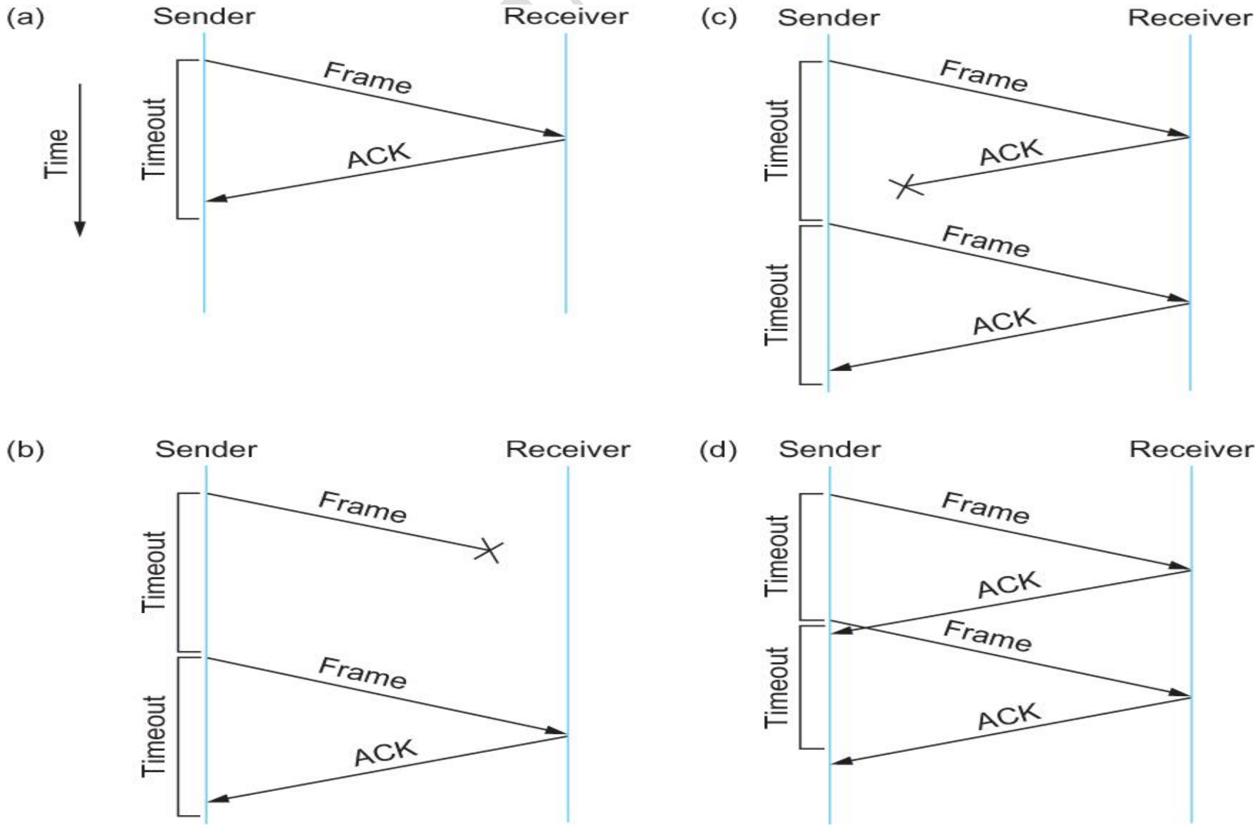
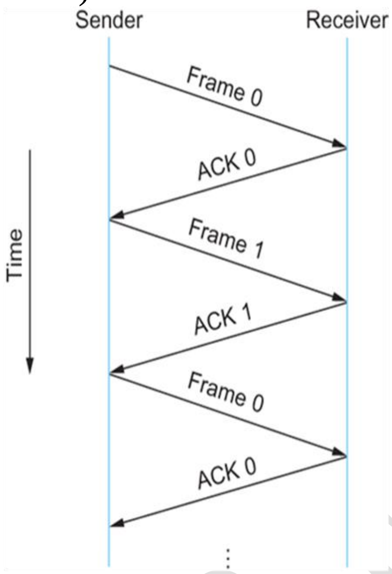


Fig: illustrates four different scenarios that result from the basic algorithm. The sending side is represented on the left, the receiving side is depicted on the right, and time flows from top to bottom.

- ✓ In Fig (a) ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon..

- ✓ Suppose the sender sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving. This situation is in (c) and (d). In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame.

- ✓ This makes the receiver to receive the duplicate copies. To avoid this two sequence numbers (0 and 1) must be used alternatively.



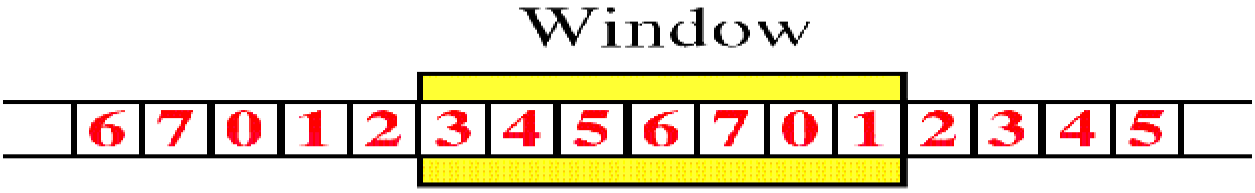
Timeline for stop-and-wait with 1-bit sequence number

The main drawback of the stop-and-wait algorithm is that it allows the sender have only one outstanding frame on the link at a time.

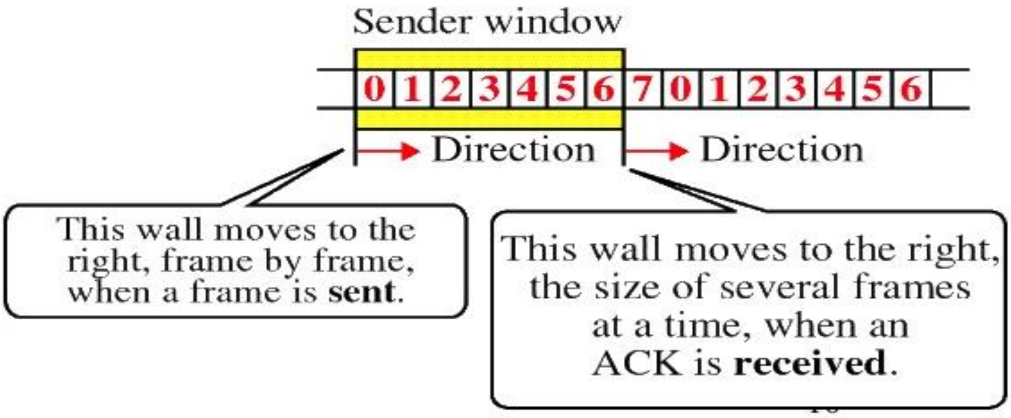
2. Sliding Window

- ✓ The sender can transmit several frames before needing an acknowledgement.
- ✓ Frames can be sent one right after another meaning that the link can carry several frames at once and it s capacity can be used efficiently.
- ✓ The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames
- ✓ Sliding Window refers to imaginary boxes at both the sender and the receiver.
- ✓ Window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.
- ✓ Frames are numbered modulo-n which means they are numbered from 0 to n-1
- ✓ For eg. If n=8 the frames are numbered 0,1,2,3,4,5,6,7. i.e the size of the window is n -1.
- ✓ When the receiver sends ACK it includes the number of the next frame it expects to receive.
  - ✓ When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

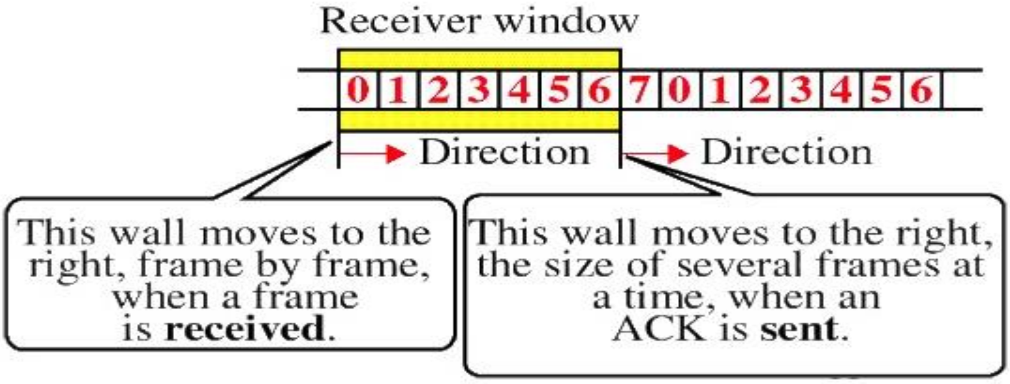
Sliding Window

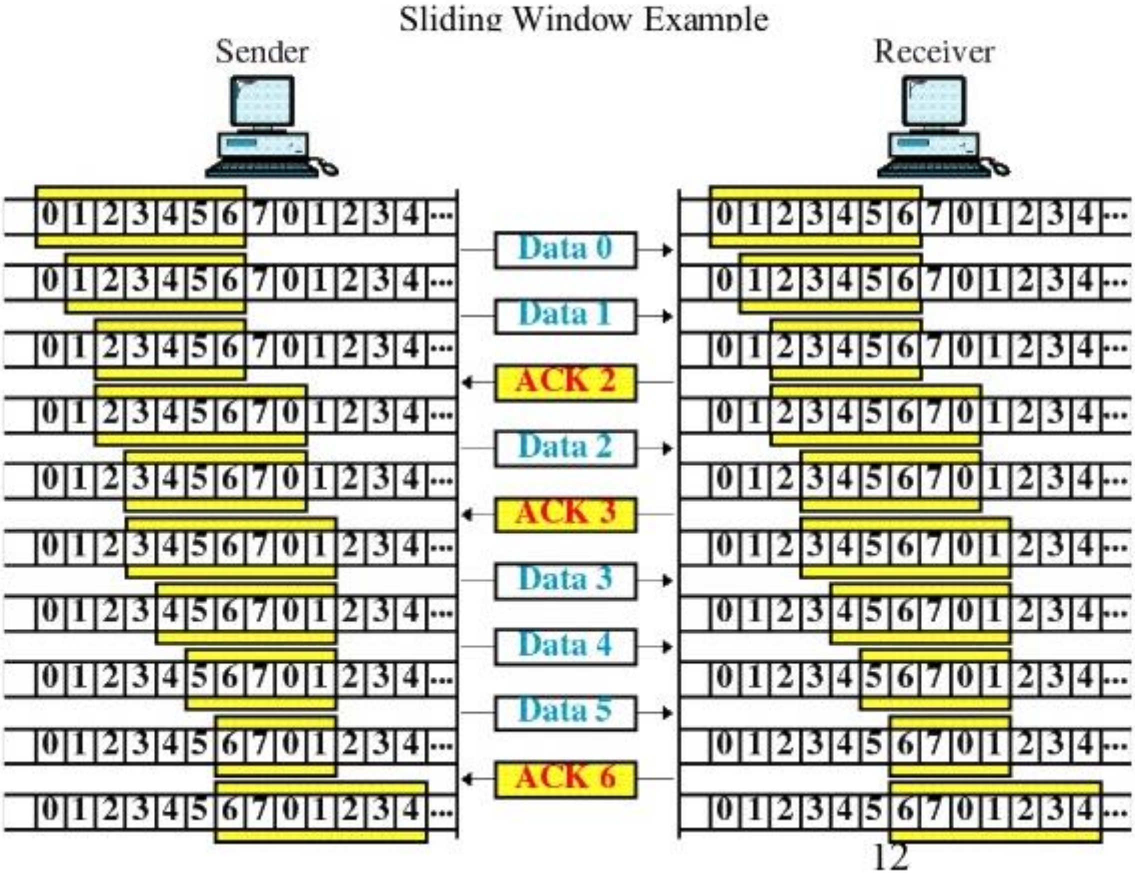


Sender Sliding Window


Sender window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right, frame by frame, when a frame is sent.
This wall moves to the right, the size of several frames at a time, when an ACK is received.

Receiver Sliding Window


Receiver window
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Direction
Direction
This wall moves to the right, frame by frame, when a frame is received.
This wall moves to the right, the size of several frames at a time, when an ACK is sent.


Sliding Window Example
Sender
Receiver
0 1 2 3 4 5 6 7 0 1 2 3 4 ···
Data 0
Data 1
ACK 2
Data 2
ACK 3
Data 3
Data 4
Data 5
ACK 6
12