

UNIT 1

INTRODUCTION TO DATA COMMUNICATIONS:

It is the exchange of data between two devices through some transmission medium.

Types:

1. Local
2. Remote

1. Local:

If the devices are restricted in a geographical area.

2. Remote:

If the devices are farther away without any geographical restriction.

Fundamental Characteristics:

1. Delivery
2. Accuracy
3. Timeliness

Components:

Data communication systems are made up of five components.

1. Message
2. sender
3. Receiver
4. Medium
5. Protocol

1. Message:

This is the information to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

2. Sender:

It is the device that sends the data message. It may be a computer, workstation, telephone handset, video camera...

3. Receiver:

It is the device that receives the message. It may be a computer, workstation, telephone handset, television...

4. Medium:

It is the physical path which a message travels from sender to receiver. It may consist of twisted pair wire, coaxial cable, fiber optic cable, laser or radio waves.

5. Protocol:

It is a set of rules that governs data communication. It is an agreement between the communication devices.

NETWORKS:

A network is a set of devices connected by a media link. Devices often referred to as nodes can be a computer, printer, or any other devices capable of sending/ receiving data.

Distributed processing:

Here tasks are divided among multiple computers. Each separate computer handles a subset.

Advantages:

1. Security/ Encapsulation
2. Distributed database
3. Faster problem solving
4. Security through redundancy
5. collaborative processing

Network Criteria:

A network must meet a number of criteria to be considered as effective and efficient.

The criteria are,

1. Performance
2. Reliability
3. Security

1. Performance:

The performance can be measured by two times are,

- I. Transit time
- II. Response time

I. Transit time:

It is the amount of time required for a message to travel from one device to another device.

II. Response time:

It is the elapsed time between an inquiry and a response.

The performance can be measured by number factors are,

- i. Number of user
- ii. Type of transition medium
- iii. Hardware
- iv. Software

i. Number of user:

Large number of concurrent users produces slow response time and heavy traffic loads.

ii. Type of transition medium:

The medium defines the speed of data travel.

iii. Hardware:

The type of hardware can affect the speed and capacity of transmission.

iv. Software:

The software can affect speed and reliability of a network link.

2. Reliability:

The reliability is measured by frequency to failure, the time it takes a link to recover from a failure and the network's robustness in a catastrophe.

i. Frequency of Failure:

A network that fails often.

ii. Recovery time:

How much time it takes to recover service after a failure has occurred?

iii. Catastrophe:

Failures due to such reasons are fire, earthquake, theft...

3. Security:

It refers to protecting data from unauthorized access and viruses.

i. Unauthorized Access:

Sensitive data must be protected from unauthorized access. Protection can be done by user identification and passwords at the lowest level. At the highest level, encryption techniques may use.

ii. Viruses:

A virus is an illicitly introduced code that damages the system.

CATEGORIES OF NETWORKS:

There are three primary categories are,

1. Local area network.
2. Metropolitan area network.
3. Wide area network.

1. Local Area Network:

They are usually privately owned and link the devices in a single office, building and campus. Currently LAN size is limited to a few kilometers. It may be from two PC's to throughout a company.

The most common LAN topologies are bus, ring and star. They have data rates from 4 to 16 Mbps. Today the speed is on increasing and can reach 100 mbps.

2. Metropolitan Area Network:

They are designed to extend over an entire city. It may be a single network or connecting a number of LANs into a large network. So the resources are shared between LANs. Example of MAN is, telephone companies provide a popular MAN service called switched multi megabit data service (SMDS).

3. Wide Area Network:

It provides a long distance transmission of data, voice, image and video information over a large geographical area like country, continent or even the whole world.

TYPE OF CONNECTION:

There are two types are,

1. Point to point
2. Multi point

1. Point To Point:

It provides a dedicated link between two devices of the channel. The entire capacity of the channel is reserved for transmission between those two devices.

2. Multipoint:

More than two devices can share a link by using this type of connection. It also called as multidrop. The capacity channel is shared either temporary or spatially. If simultaneously use, it is spatially shared. If it takes turns, it is time shared line configuration.

TOPOLOGIES:

Topology refers to the way a network is laid out either physically or logically. Two or more devices connect to a link; two or more links form a topology. It is the geographical representation of the relationship of all the links and linking devices to each other.

1. Mesh
2. Star
3. Tree
4. Bus
5. Ring

1. Mesh Topology:

Here every device has a dedicated point to point link to every other device. A fully connected mesh can have $n(n-1)/2$ physical channels to link n devices. It must have $n-1$ IO ports.

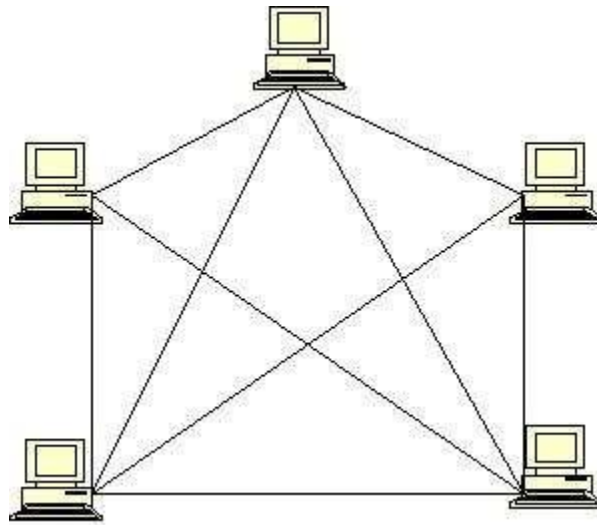


Figure: Mesh Topology

Advantages:

1. They use dedicated links so each link can only carry its own data load. So traffic problem can be avoided.
2. It is robust. If any one link get damaged it cannot affect others
3. It gives privacy and security
4. Fault identification and fault isolation are easy.

Disadvantages:

1. The amount of cabling and the number IO ports required are very large. Since every device is connected to each other devices through dedicated links.
2. The sheer bulk of wiring is larger than the available space
3. Hardware required to connect each device is highly expensive.

Example:

A mesh network has 8 devices. Calculate total number of cable links and IO ports needed.

Solution:

Number of devices = 8

Number of links = $n(n-1)/2$

$$= 8(8-1)/2$$

$$= 28$$

Number of port/device = $n-1$

$$= 8-1 = 7$$

2. STAR TOPOLOGY:

Here each device has a dedicated link to the central „hub“. There is no direct traffic between devices. The transmission are occurred only through the central controller namely hub.



Figure: Star Topology

Advantages:

1. Less expensive than mesh since each device is connected only to the hub.
2. Installation and configuration are easy.
3. Less cabling is needed than mesh.
4. Robustness.
5. Easy to fault identification & isolation.

Disadvantages:

1. Even it requires less cabling than mesh when compared with other topologies it still large.

TREE TOPOLOGY:

It is a variation of star. Instead of all devices connected to a central hub here most of the devices are connected to a secondary hub that in turn connected with central hub. The central hub is an active hub. An active hub contains a repeater, which regenerate the received bit pattern before sending.



Figure: Tree Topology

The secondary hub may be active or passive. A passive hub means it just precedes a physical connection only.

Advantages:

1. Can connect more than star.
2. The distance can be increased.
3. Can isolate and prioritize communication between different computers.

4. BUS TOPOLOGY:

A bus topology is multipoint. Here one long cable is act as a backbone to link all the devices are connected to the backbone by drop lines and taps. A drop line is the connection between the devices and the cable. A tap is the splice into the main cable or puncture the sheathing.

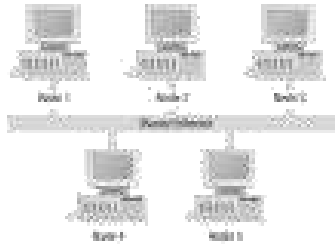


Figure: Bus Topology

Advantages:

1. Ease of installation.
2. Less cabling.

Disadvantages:

1. Difficult reconfiguration and fault isolation.
2. Difficult to add new devices.
3. Signal reflection at top can degradation in quality
4. If any fault in backbone can stops all transmission.

5. RING TOPOLOGY:

Here each device has a dedicated connection with two devices on either side of it. The signal is passed in one direction from device to device until it reaches the destination and each device have repeater.

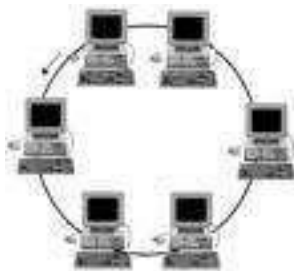


Figure: Ring Topology

Advantages:

1. Easy to install.
2. Easy to reconfigure.
3. Fault identification is easy.

Disadvantages:

1. Unidirectional traffic.
2. Break in a single ring can break entire network.

PROTOCOLS AND STANDARDS:**Protocols:**

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. But two entities cannot communicate each other as sending or receiving. For communication occurs the entities must agree on a protocol.

A protocol is a set of rules that govern data communication. A protocol defines what is communicated how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics and timing.

Syntax:

Syntax refers to the structure or format of the data, means to the order how it is presented.

Semantics:

Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and when action is to be taken based on the interpretation.

Timing:

Timing refers to two characteristics. They are,

1. When data should be sent
2. When data to be received.

Standards:

A standard provides a model for development of a product, which is going to develop. Standards are essential to create and maintain a product.

Data communication products are fall into two categories. They are,

1. De facto
2. De jure

1. De facto:

They are further classified into

1. Proprietary
2. Non proprietary

1. Proprietary:

They are originally invented by a commercial organization as a basis for the operation of its product. They are wholly owned by the company, which invented them. They are closed standards.

2. Nonproprietary:

Groups or committees that have passed them into public domain develop them. They are open standards.

2. De jure:

They have been legislated by an officially recognized body.

STANDARDS ORGANIZATION:

Standards are developed by,

1. Standards creation committee
2. Forums
3. Regularity agencies

1. Standards creation committees:

1. International Standards Organization (ISO)
2. International Telecommunications Union – Telecommunications Standards Section (ITU-T formally CCITT)
3. The American National Standards Institute (ANSI)
4. The Institute of Electrical and Electronics Engineers (IEEE)
5. The Electronic Industries Association (EIA)
6. Telcordia

2. Forums:

1. Frame Relay Forum
2. ATM Forum & ATM consortium
3. Internet Society (ISOC) & Internet Engineering Task Force (IETF)

3. Regularity Agencies:

1. Federal Communication commission

NETWORK ARCHITECTURE

A computer network must provide general, cost effective, fair and robust among a large number of computers. It must evolve to accommodate changes in both the underlying technologies. To help to deal this network designers have developed general blueprints called network architecture that guide the design and implementation of networks.

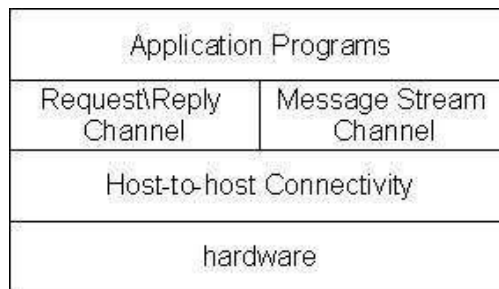
LAYERING AND PROTOCOL

To reduce the complexity of getting all the functions maintained by one a new technique called layering technology was introduced. In this, the architecture contains several layers and each layer is responsible for certain functions. The general idea is that the services offered by underlying hardware, and then add a sequence of layers, each providing a higher level of service. The services provided at the higher layers are implemented in terms of the services provided by the lower layers. A simple network has two layers of abstraction sandwiched between the application program and the underlying hardware.

Application Programs
Process-to-process Channels
Host-to-host Connectivity
hardware

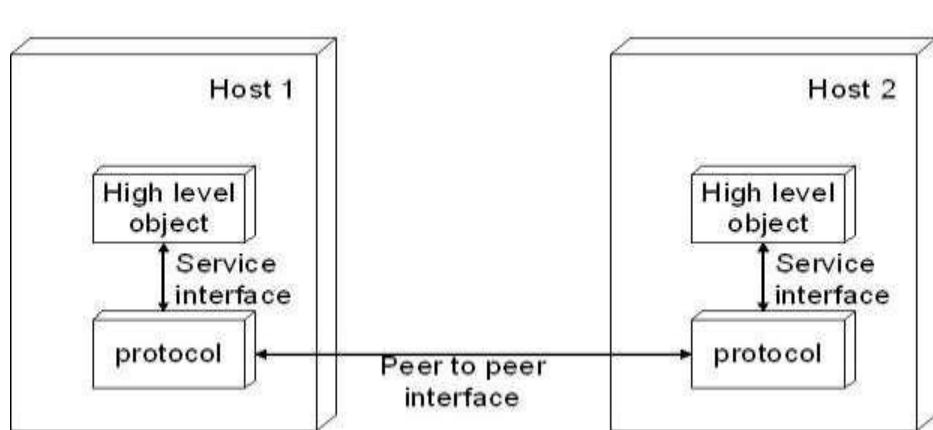
The layer immediately above the hardware in this case might provide host to host connectivity, and the layer above it builds on the available host to host communication service and provides support for process to process channels.

Features of layering are: 1. It decomposes the problem of building a network into more manageable components. 2. It provides a more modular design. Addition of new services and modifications are easy to implement.

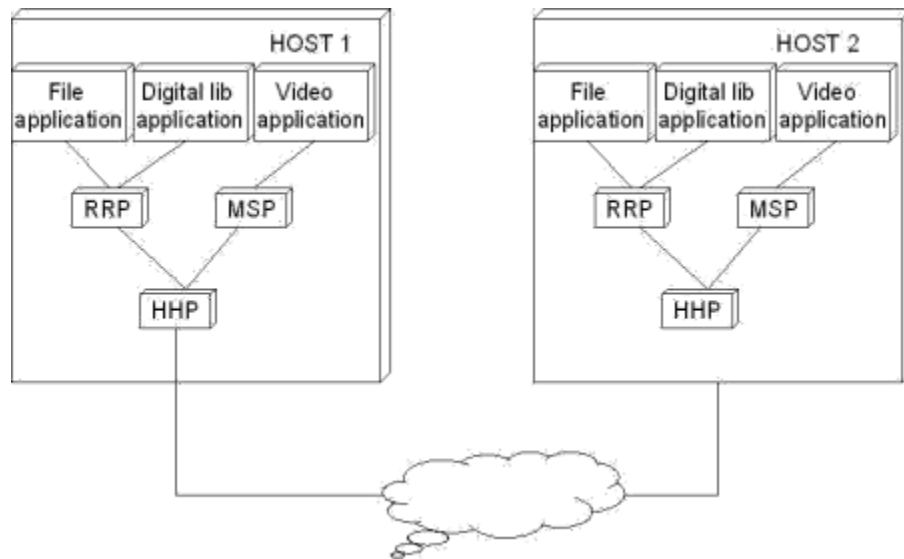


In process to process channels, they have two types of channels. One for request/reply service and the other for message stream service.

A protocol provides a communication service that higher level objects use to exchange message. Each protocol defines two different interfaces. First it defines a service interface to other objects on the same system that want to use its communication services. This interface defines the operations that local objects can perform on the protocol. Second a protocol defines a peer interface to its counterpart on another machine. It defines the form and meaning of message exchanged between protocol peers to implement the communication service.



There are potentially multiple protocols at any given level, each providing a different communication service. It is known as protocol graph that make up a system.



ISO / OSI MODEL:

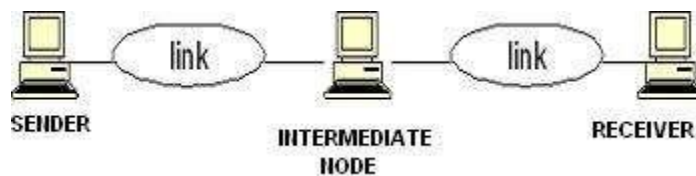
ISO refers International Standards Organization was established in 1947, it is a multinational body dedicated to worldwide agreement on international standards.

OSI refers to Open System Interconnection that covers all aspects of network communication. It is a standard of ISO.

Here **open system** is a model that allows any two different systems to communicate regardless of their underlying architecture. Mainly, it is not a protocol it is just a model.

OSI MODEL

The open system interconnection model is a layered framework. It has seven separate but interrelated layers. Each layer having unique responsibilities.



ARCHITECTURE

The architecture of OSI model is a layered architecture. The seven layers are,

1. Physical layer
2. Datalink layer
3. Network layer
4. Transport layer

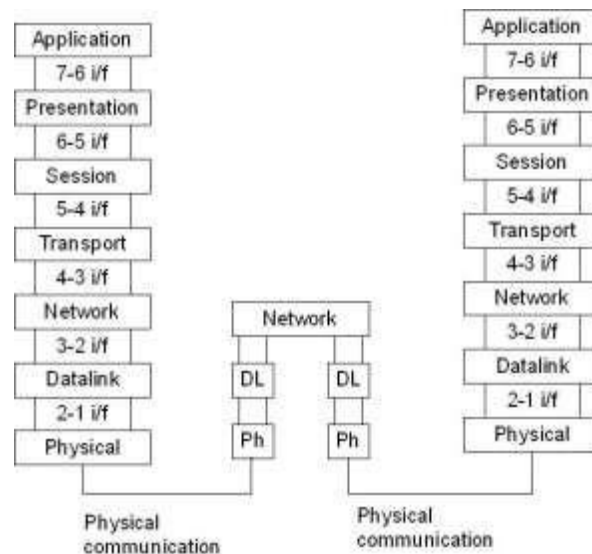
5. Session layer
6. Presentation layer
7. Application layer

The figure shown below shows the layers involved when a message sent from A to B pass through some intermediate devices.

Both the devices A and B are formed by the framed architecture. And the intermediate nodes only having the layers are physical, Datalink and network. In every device each layer gets the services from the layer just below to it. When the device is connected to some other device the layer of one device communicates with the corresponding layer of another device. This is known as **peer to peer process**.

Each layer in the sender adds its own information to the message. This information is known as **header** and **trailers**. When the information added at the beginning of the data is known as header. Whereas added at the end then it called as trailer. Headers added at layers 2, 3, 4, 5, 6. Trailer added at layer 2.

Each layer is connected with the next layer by using interfaces. Each interface defines what information and services a layer must provide for the layer above it.



ORGANIZATION OF LAYERS

The seven layers are arranged by three sub groups.

1. Network Support Layers
2. User Support Layers
3. Intermediate Layer

Network Support Layers:

Physical, Datalink and Network layers come under the group. They deal with the physical aspects of the data such as electrical specifications, physical connections, physical addressing, and transport timing and reliability.

User Support Layers:

Session, Presentation and Application layers comes under the group. They deal with the interoperability between the software systems.

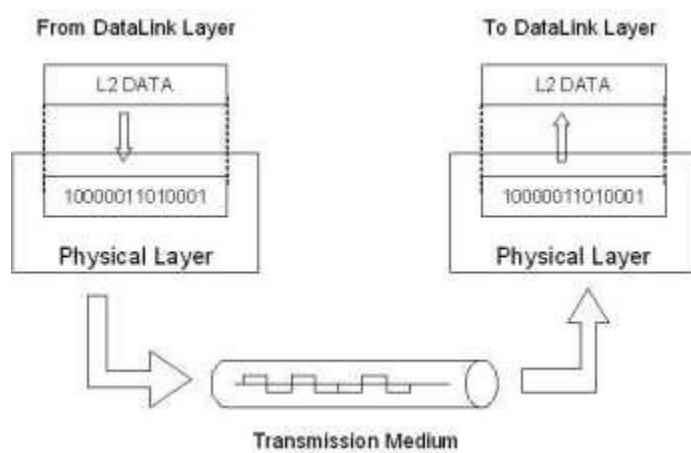
Intermediate Layer

The transport layer is the intermediate layer between the network support and the user support layers.

FUNCTIONS OF THE LAYERS

PHYSICAL LAYER

The physical layer coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and the transmission medium.



The functions are,

1. Physical Characteristics Of Interfaces and Media:

- * It defines the electrical and mechanical characteristics of the interface and the media.
- * It defines the types of transmission medium

2. Representation of Bits

- * To transmit the stream of bits they must be encoded into signal.
- * It defines the type of encoding whether **electrical or optical**.

3. Data Rate

- * It defines the transmission rate i.e. the number of bits sent per second.

4. Synchronization of Bits

- * The sender and receiver must be synchronized at bit level.

5. Line Configuration

- * It defines the type of connection between the devices.
- * Two types of connection are,
 1. point to point
 2. multipoint

6. Physical Topology

- * It defines how devices are connected to make a network.
- * Five topologies are,
 1. mesh
 2. star
 3. tree
 4. bus
 5. ring

7. Transmission Mode

It defines the direction of transmission between devices.

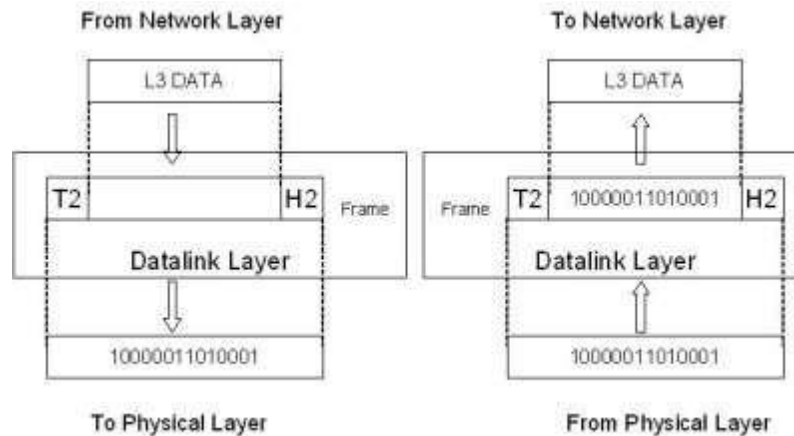
Three types of transmission are,

1. simplex
2. half duplex

3. full duplex

DATALINK LAYER

Datalink layer responsible for node-to-node delivery.



The responsibilities of Datalink layer are,

1. Framing

It divides the stream of bits received from network layer into manageable data units called **frames**.

2. Physical Addressing

- * It adds a header that defines the physical address of the sender and the receiver.
- * If the sender and the receiver are in different networks, then the receiver address is the address of the device which connects the two networks.

3. Flow Control

- * It imposes a flow control mechanism used to ensure the data rate at the sender and the receiver should be same.

4. Error Control

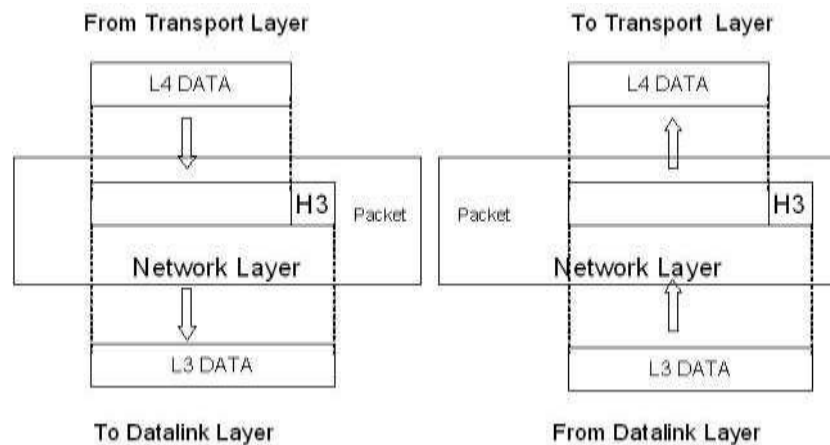
- * To improve the reliability the Datalink layer adds a trailer which contains the error control mechanism like CRC, Checksum etc.

5. Access Control

- * When two or more devices connected at the same link, then the Datalink layer used to determine which device has control over the link at any given time.

NETWORK LAYER

When the sender is in one network and the receiver is in some other network then the network layer has the responsibility for the source to destination delivery.



The responsibilities are,

1. Logical Addressing

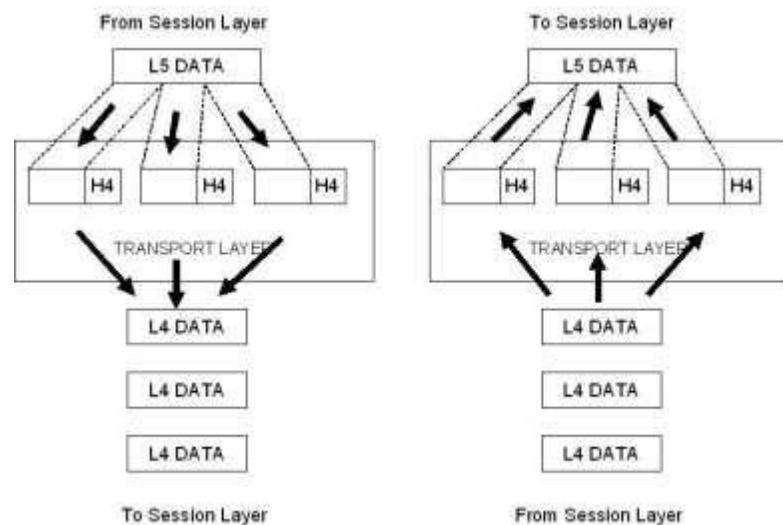
- * If a packet passes the network boundary that is when the sender and receiver are places in different network then the network layer adds a header that defines the logical address of the devices.

2. Routing

- * When more than one networks connected and to form an internetwork, the connecting devices route the packet to its final destination.
- * Network layer provides this mechanism.

TRANSPORT LAYER

The network layer is responsible for the end to end delivery of the entire message. It ensures that the whole message arrives in order and intact. It ensures the error control and flow control at source to destination level.



The responsibilities are,

1. Service point Addressing

- * A single computer can often run several programs at the same time.
- * The transport layer gets the entire message to the correct process on that computer.
- * It adds a header that defines the port address which used to identify the exact process on the receiver.

2. Segmentation and Reassembly

- * A message is divided into manageable units called as segments.
- * Each segment is reassembled after received that information at the receiver end.
- * To make this efficient each segment contains a sequence number.

3. Connection Control

- * The transport layer creates a connection between the two end ports.
- * It involves three steps. They are,

1. connection establishment
2. data transmission
3. connection discard

4. Flow Control

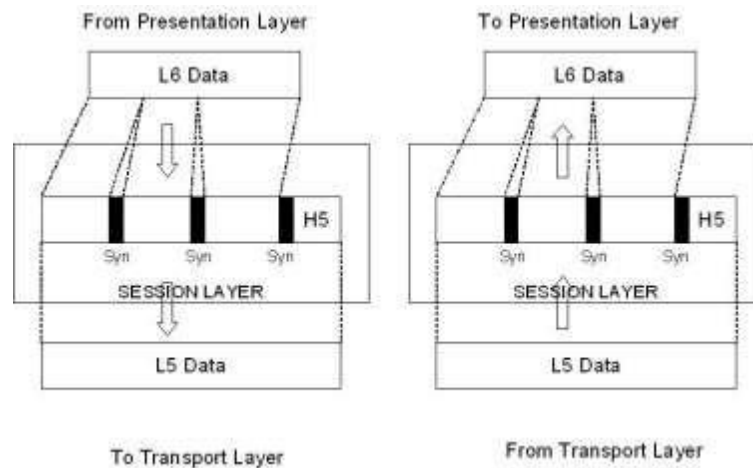
- * Flow control is performed at end to end level

5. Error Control

- * Error control is performed at end to end level.

SESSION LAYER

It acts as a dialog controller. It establishes, maintains and synchronizes the interaction between the communication devices.



The responsibilities are,

1. Dialog Control

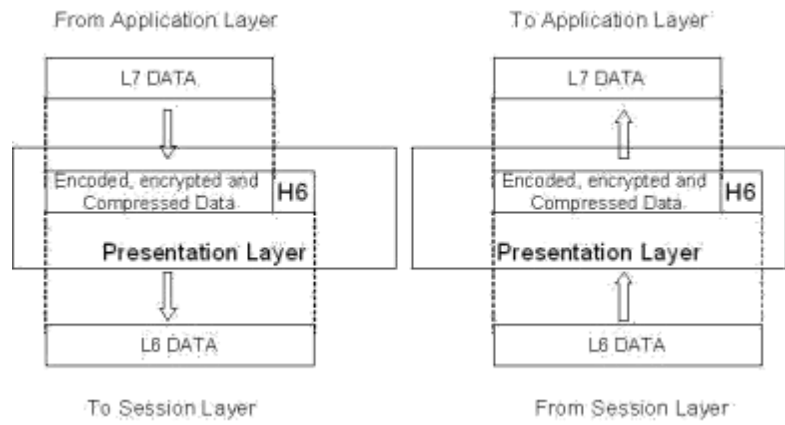
- * The session layer allows two systems to enter into a dialog.
- * It allows the communication between the devices.

2. Synchronization

It adds a synchronization points into a stream of bits.

PRESENTATION LAYER

The presentation layer is responsible for the semantics and the syntax of the information exchanged.



The responsibilities are,

1. Translation

- * Different systems use different encoding systems.
- * The presentation layer is responsible for interoperability between different systems.
- * The presentation layer at the sender side translates the information from the sender dependent format to a common format. Likewise, at the receiver side presentation layer translates the information from common format to receiver dependent format.

2. Encryption

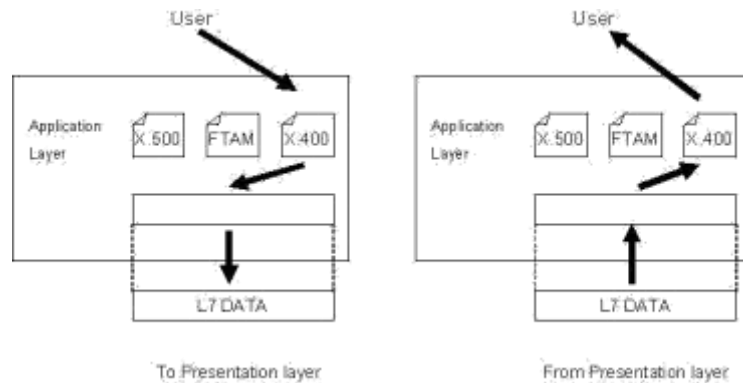
- * To ensure security encryption/decryption is used
- * Encryption means transforms the original information to another form
- * Decryption means retrieve the original information from the encrypted data

3. Compression

- * It is used to reduce the number of bits to be transmitted.

APPLICATION LAYER

The application layer enables the user to access the network. It provides interfaces between the users to the network.



The responsibilities are,

1. Network Virtual Terminal

- * It is a software version of a physical terminal and allows a user to log on to a remote host.

2. File Transfer, Access, and Management

- * It allows a user to access files in a remote computer, retrieve files, and manage or control files in a remote computer.

3. Mail Services

- * It provides the basis for e-mail forwarding and storage.

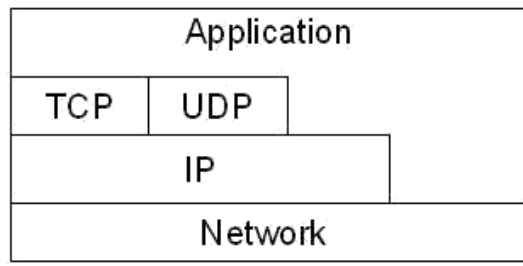
4. Directory Services

- * It provides distributed database sources and access for global information about various objects and services.

INTERNET ARCHITECTURE

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).

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. Instead of having seven layers, a four layer model is often used in Internet.



At the lowest level are a wide variety of network protocols, denoted NET1, NET2 and so on. The second layer consists of a single protocol the Internet Protocol IP. It 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 User Datagram Protocol (UDP). TCP provides a reliable byte stream channel, and UDP provides unreliable datagram delivery channel. They are called as end to end protocol they can also be referred as transport protocols.

Running above the transport layer, a range of application protocols such as FTP, TFTP, Telnet, and SMTP that enable the interoperation of popular applications.

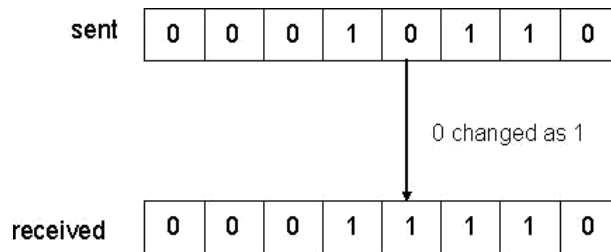
ERROR

Networks must be able to transfer data from one device to another with complete accuracy. Some part of a message will be altered in transit than that the entire content will arrive intact. Many factors like line noise can alter or wipe out one or more bits of a given data unit. This is known as errors.

TYPES OF ERRORS

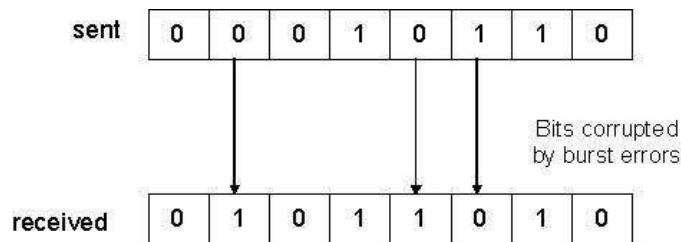
There are two types. They
are, 1. Single Bit Error

It means that only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



2. Burst Bit Error

It means that two or more bits in the data unit have changed.



- A burst bit does not necessarily means that the errors occur in consecutive bits
- The length of the bust error is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not be corrupted.

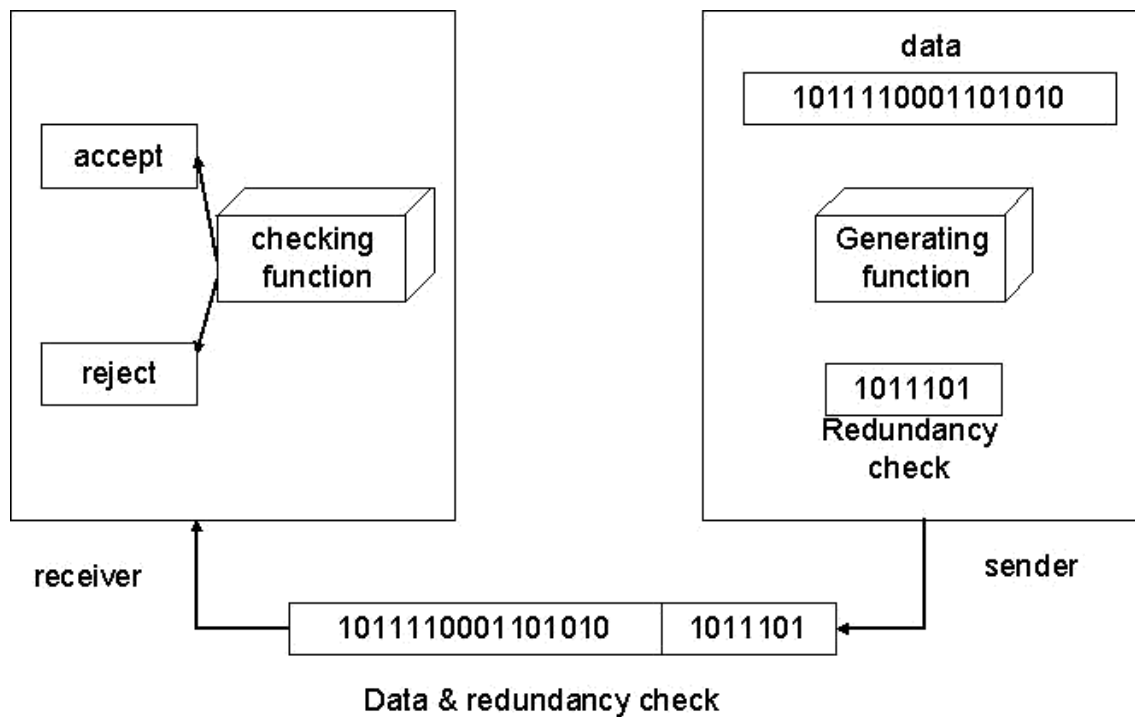
ERROR DETECTION

For reliable communication errors must be detected and corrected. For error detection we are using many mechanisms.

REDUNDANCY

One error detection mechanism is sending every data unit twice. The receiving device then would be able to do a bit for bit comparison between the two versions of the data. Any discrepancy would indicate an error, and an appropriate correction mechanism could be used.

But instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit. This technique is called redundancy because extra bits are redundant to the information. They are discarded as soon as the accuracy of the transmission has been determined.



TYPES

Four types of redundancy checks are used in data communications. They are,

1. vertical redundancy check (VRC)
2. longitudinal redundancy check (LRC)
3. cyclic redundancy check (CRC)
4. checksum

VERTICAL REDUNDANCY CHECK:

It is also known as parity check. In this technique a redundant bit called a parity bit is appended to every data unit so that the total number of 1s in the unit including the parity bit becomes even for even parity or odd for odd parity.

In even parity, the data unit is passed through the even parity generator. It counts the number of 1s in the data unit. If odd number of 1s, then it sets 1 in the parity bit to make the number of 1s as even. If the data unit having even number of 1s then it sets in the parity bit to maintain the number of 1s as even. When it reaches its destination, the receiver puts all bits through an even parity checking function. If it counts even number of 1s than there is no error. Otherwise there is some error.

EXAMPLE:

The data is : 01010110

The VRC check : 010101100

In odd parity, the data unit is passed through the odd parity generator. It counts the number of 1s in the data unit. If even number of 1s, then it sets 1 in the parity bit to make the number of 1s as odd. If the data unit having odd number of 1s then it sets in the parity bit to maintain the number of 1s as odd. When it reaches its destination, the receiver puts all bits through an odd parity checking function. If it counts odd number of 1s than there is no error. Otherwise there is some error.

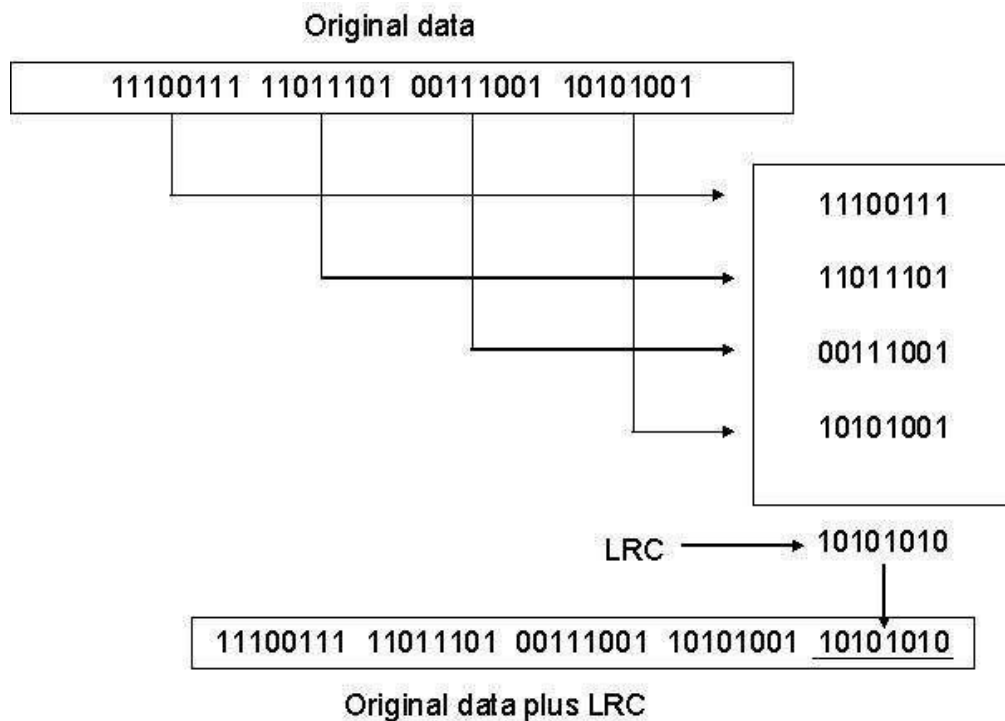
EXAMPLE

The data is: 01010110

The VRC check: 01010111

LONGITUDINAL REDUNDANCY CHECK

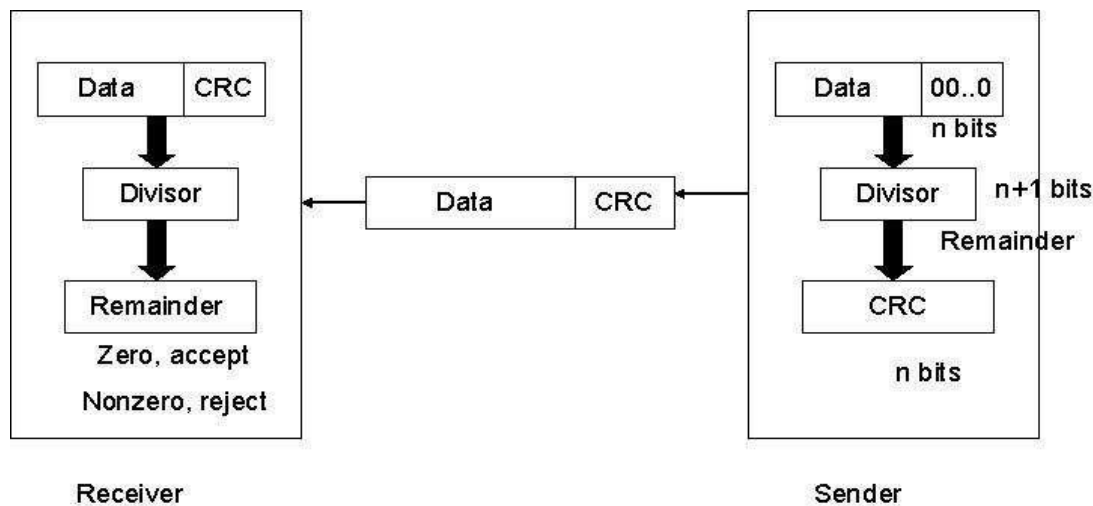
In this, a block of bits is organized in a table (rows and columns). For example, instead of sending a block of 32 bits, we organize them in a table made of four rows and eight columns. We then calculate the parity bit for each column and create a new row of eight bits which are the parity bits for the whole block



CYCLIC REDUNDANCY CHECK

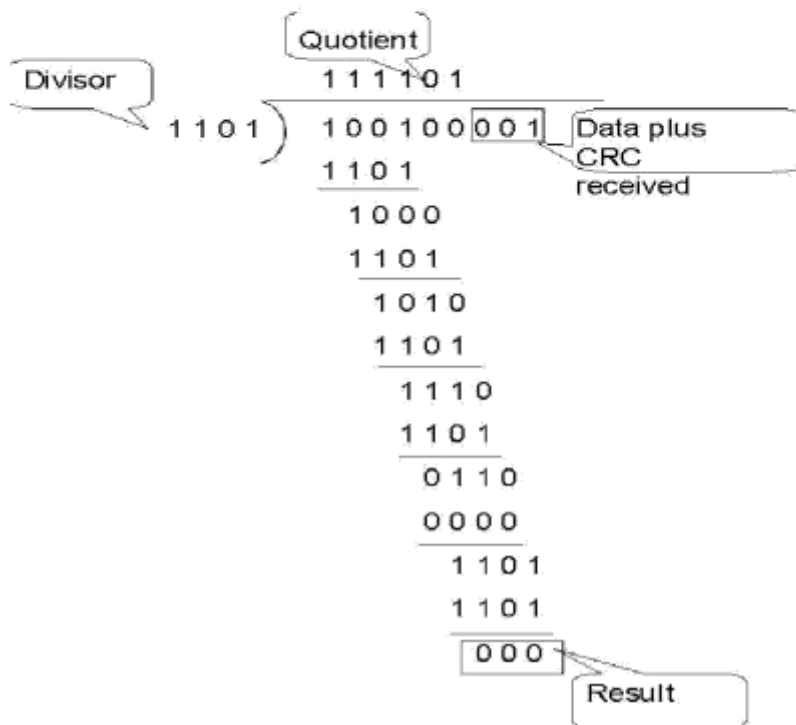
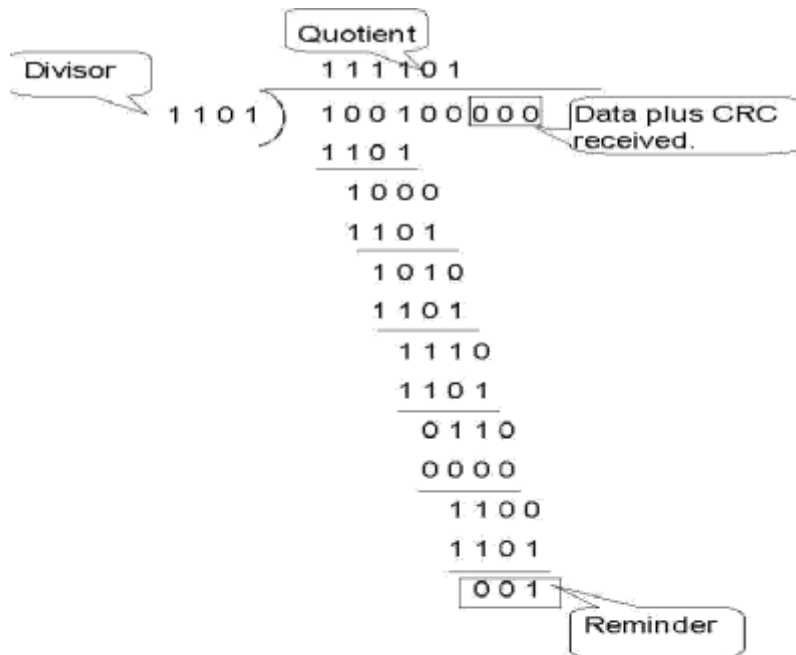
CRC is based on binary division. In this a sequence of redundant bits, called CRC remainder is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by a second predetermined binary number. At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be intact and therefore accepted. A remainder indicates that the data unit has been changed in transit and therefore must be rejected.

Here, the remainder is the CRC. It must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor.



First, a string of $n-1$ 0s is appended to the data unit. The number of 0s is one less than the number of bits in the divisor which is n bits. Then the newly elongated data unit is divided by the divisor using a process called binary division. The remainder is CRC. The CRC is replaces the appended 0s at the end of the data unit.

The data unit arrives at the receiver first, followed by the CRC. The receiver treats whole string as the data unit and divides it by the same divisor that was used to find the CRC remainder. If the remainder is 0 then the data unit is error free. Otherwise it having some error and it must be discarded.



CHECKSUM

The error detection method used by the higher layer protocols is called checksum. It consists of two parts. They are,

1. checksum generator
2. checksum checker

Checksum Generator:

In the sender, the checksum generator subdivides the data unit into equal segments of n bits. These segments are added with each other by using one's complement arithmetic in such a way that the total is also n bits long. That total is then complemented and appended to the end of the data unit.

Checksum Checker:

The receiver subdivides the data unit as above and adds all segments together and complements the result. If the extended data unit is intact, the total value found by adding the data segments and the checksum field should be zero. Otherwise the packet contains an error and the receiver rejects it.

EXAMPLE

At the sender

Data unit: 10101001 00111001

10101001

00111001

Sum 1100010

Checksum 00011101

At the receiver

1)

Received data: 10101001 00111001

00011101 10101001 00111001

00011101

Sum 11111111

Complement 00000000

It means that the pattern is ok.

2)

Received data: 1010111 111001 00011101

	10101111
	11111001
	00011101
Result	11000101
Carry	1
Sum	11000110
Complement	00111001

It means that the pattern is corrupted.

ERROR CORRECTION

Error correction is handled in two ways. In one, when an error is discovered, the receiver can have the sender retransmit the entire data unit. In the other, a receiver can use an error correcting code, which automatically corrects certain errors.

Types of error correction:

1. Single bit error correction
2. Burst bit error correction

Single Bit Error Correction

To correct a single bit error in an ASCII character, the error correction code must determine which of the seven bits has changed. In this case we have to determine eight different states: no error, error in position 1, error in position 2, error in position 3, error in position 4, error in position 5, error in position 6, error in position 7. It looks like a three bit redundancy code should be adequate because three bits can show eight different states. But what if an error occurs in the redundancy bits? Seven bits of data and three bits of redundancy bits equal 10 bits. So three bits are not adequate.

To calculate the number of redundancy bits (r) required to correct a given number of data bits (m) we must find a relationship between m and r .

If the total number of bits in a transmittable unit is $m+r$ then r must be able to indicate at least $m+r+1$ different states. Of these, one state means no error and $m+r$ states indicate the location of an error in each of the $m+r$ positions.

So $m+r+1$ states must be discoverable by r bits. And r bits can indicate 2^r different states. Therefore, 2^r must be equal to or greater than $m+r+1$;

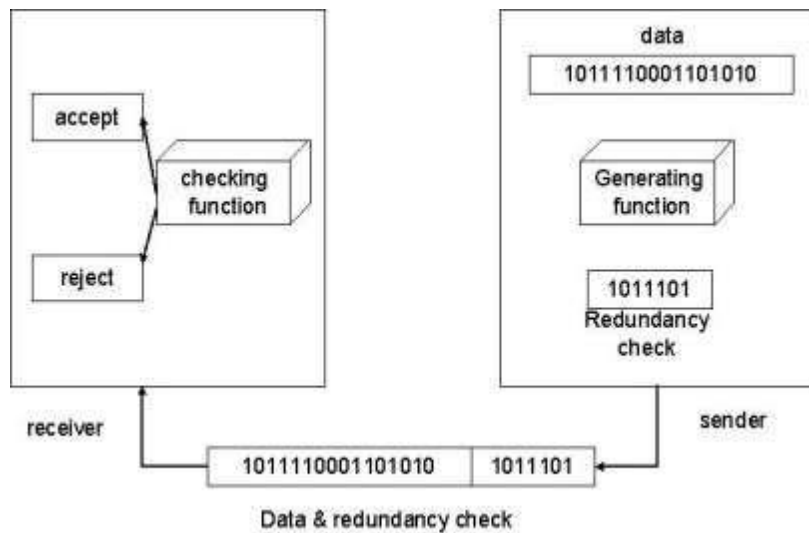
$$2^r \geq m+r+1$$

NUMBER OF DATA BITS (M)	NUMBER OF REDUNDANCY BITS (R)	TOTAL BITS (M+R)
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Hamming Code:

The hamming code can be applied to data units of any length and uses the relationship between data and redundancy bits.

Positions of redundancy bits in hamming code



The combinations used to calculate each of the four r values for a seven bit data sequence are as follows:

r1 : 1,3,5,7,9,11

r2 : 2,3,6,7,10,11

r3 : 4,5,6,7

r4 : 8,9,10,11

Here, r1 bit is calculated using all bit positions whose binary representation includes a 1 in the rightmost position (0001, 0011, 0101, 0111, 1001, and 1011). The r2 bit is calculated using all bit positions with a 1 in the second position (0010, 0011, 0110, 0111, 1010 and 1011), and for r3 1 at third bit position (0100, 0101, 0110 and 0111) for r4 1 at fourth bit position (1000, 1001, 1010 and 1011).

Calculating the r Values:

In the first step, we place each bit of the original character in its appropriate positions in the 11 bit unit. Then, we calculate the even parities for the various bit combinations. The parity value of each combination is the value of the corresponding r bit. For example r1 is calculated to provide even parity for a combination of bits 3, 5, 7, 9, 11.

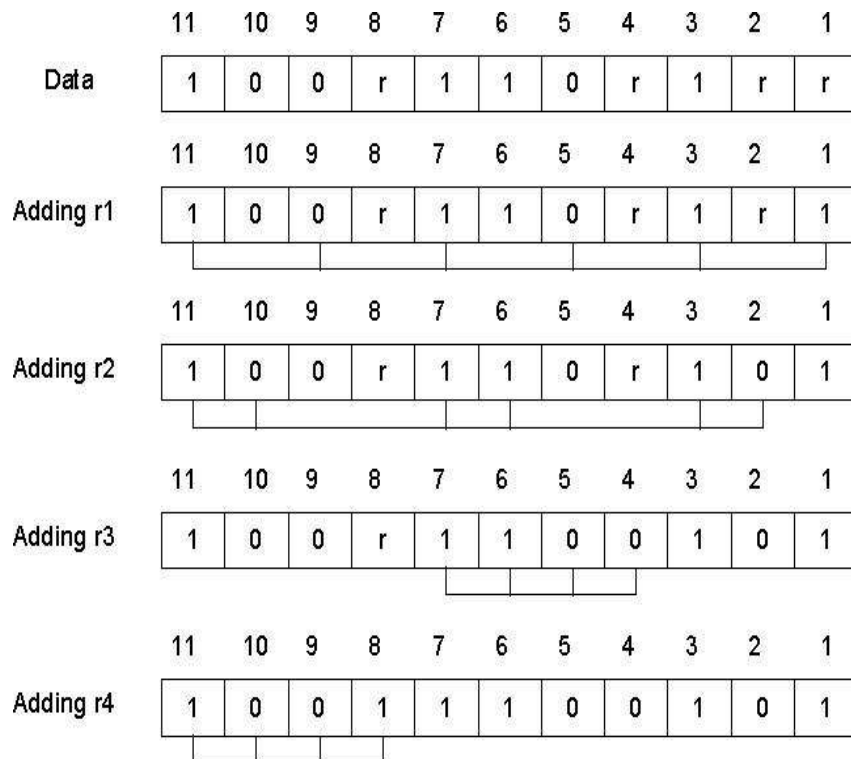
Error Detection and Correction:

Example:

At the sender:

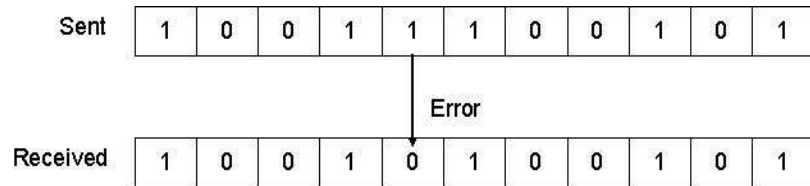
Data to be sent: 1001101

Redundancy bit calculation:



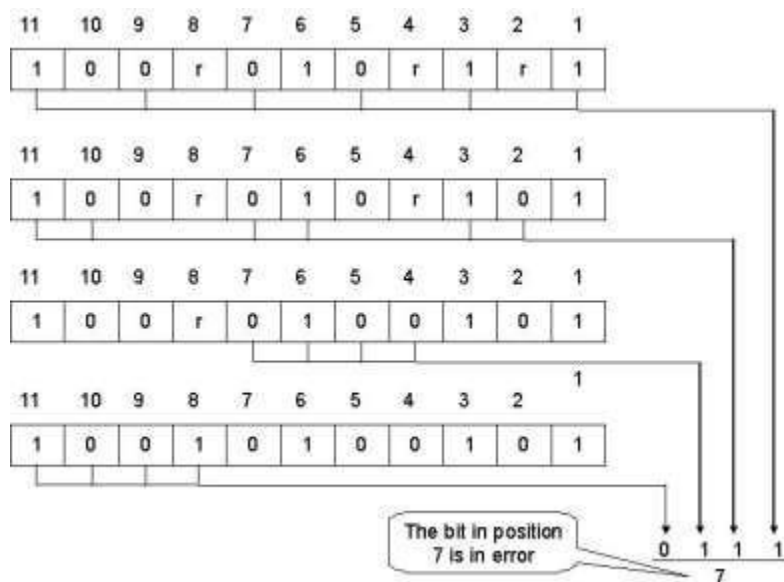
Data sent with redundancy bits: 10011100101

During transmission:



At the receiver:

The receiver takes the transmission and recalculates four new r values using the same set of bits used by the sender plus the relevant parity (r) bit for each set. Then it assembles the new parity values into a binary number in order of r position (r_8, r_4, r_2, r_1).



Once the bit is identified, the receiver can reverse its value and correct the error.

Burst Bit Error Correction:

A hamming code can be designed to correct burst errors of certain length. The number of redundancy bits required to make these corrections, however, is dramatically higher than that required for single bit errors. To correct double bit errors, for example, we must take into consideration that the two bits can be a combination of any two bits in the entire sequence. Three bit correction means any three bits in the entire sequence and so on.

FUNCTIONS OF DATA LINK LAYER:

The data link layer is responsible for the following functions. They are,

1. Line discipline or Access control
2. Flow control
3. Error control
4. Framing

LINE DISCIPLINE

Communications requires at least two devices, one to send and one to receive. If both devices are ready to send some information and put their signals on the link then the two signals collide each other and become nothing. To avoid such a situation the data link layer uses a mechanism called line discipline.

Line discipline coordinates the link system. It determines which device can send and when it can send. It answers the question, who should send now?

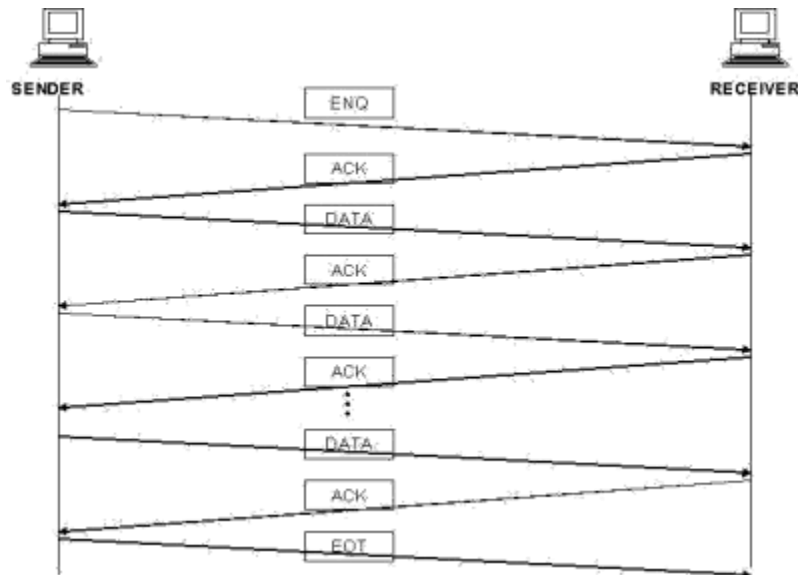
Line discipline can serve in two ways:

1. enquiry / acknowledgement (ENQ / ACK)
2. poll / select (POLL / SELECT)

ENQ / ACK:

This method is used in peer to peer communications. That is where there is a dedicated link between two devices.

The initiator first transmits a frame called an enquiry (ENQ) asking if the receiver is available to receive data. The receiver must answer either with an acknowledgement (ACK) frame if it is ready to accept or with a negative acknowledgement (NAK) frame if it is not ready. If the response is positive, the initiator is free to send its data. Otherwise it waits, and tries again. Once all its data have been transmitted, the sending system finishes with an end of transmission (EOT) frame.



POLL / SELECT

This method of line discipline works with topologies where one device is designated as primary and the other devices are secondary.

Whenever a multi point link consists of a primary device and multiple secondary devices using a single transmission line, all exchanges must be made through the primary device even when the ultimate destination is a secondary. The primary device controls the link. The secondary devices follow its instructions. The primary device only determines which device is allowed to use the channel at a given time.

The primary asks the secondary if they have anything to send; this function is called polling. And the primary tells the target secondary to get ready to receive; this function is called selecting.

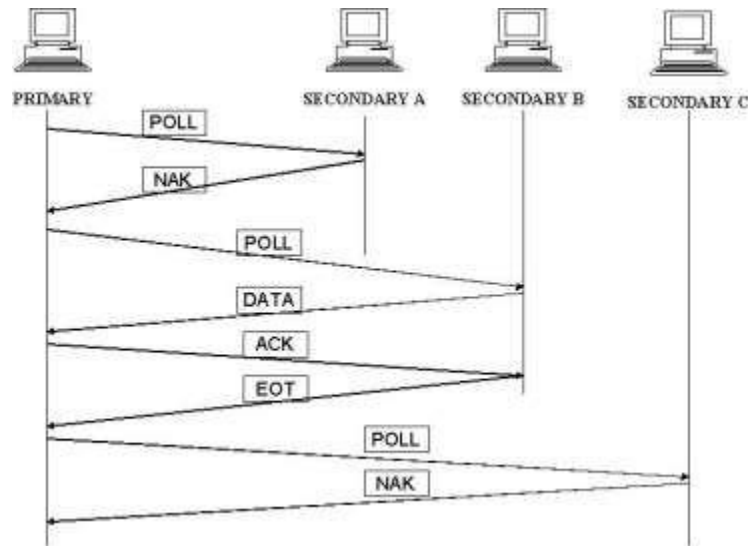
POLL:

This function is used by the primary device to solicit transmission from the secondary devices. The secondary are not allowed to transmit data unless asked by the primary device.

When the primary ready to receive data, it must ask (poll) each device in turn if it has anything to send. If the secondary have data to transmit it sends the data frame otherwise sends a negative acknowledgment (NAK).

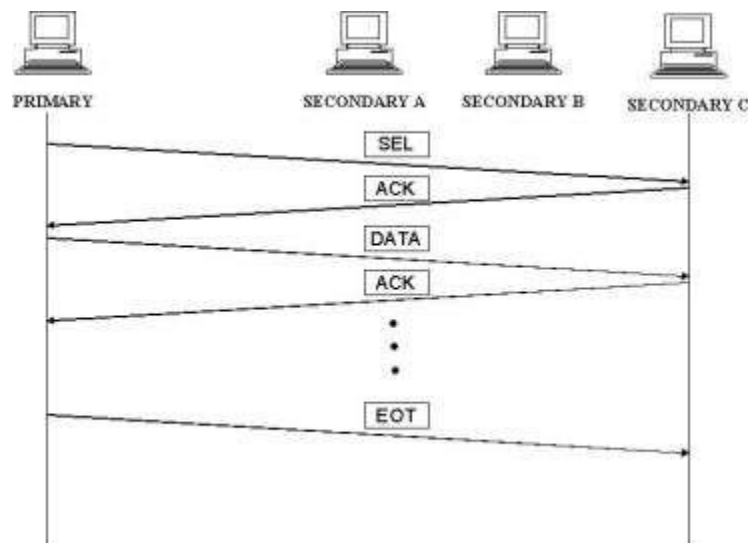
The primary then polls the next secondary. When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK).

There are two possibilities to terminate the transmission: either the secondary sends all data, finishing with an EOT frame, or the primary says “timer’s up”. Then the primary can poll the remaining devices.



SELECT:

This mode of function is used whenever the primary device has something to send. It alerts the intended secondary device get ready to receive data. Before sending data it sends the select (SEL) frame. The receiver returns an ACK frame. Then the primary sends data.



FLOW CONTROL AND ERROR CONTROL

FLOW CONTROL

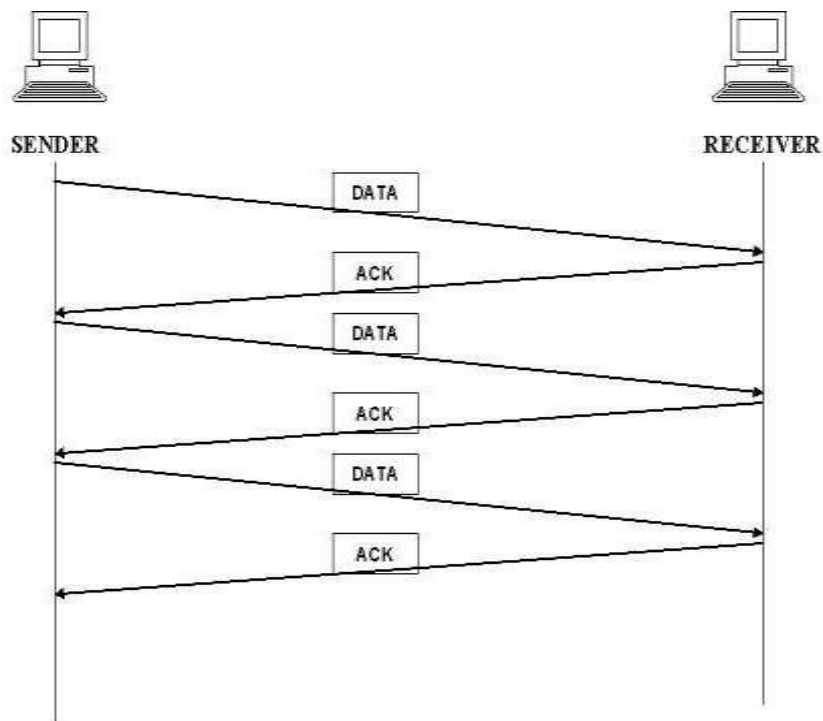
It refers to a set of procedures used to restrict the amount of data flow between sending and receiving stations. It tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

There are two methods are used. They are,

1. stop and wait
2. sliding window

STOP AND WAIT:

In this method the sender waits for acknowledgment after every frame it sends. Only after an acknowledgment has been received, then the sender sends the next frame.

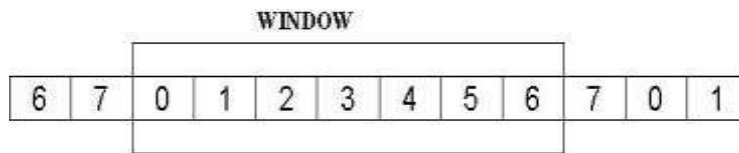


The advantage is simplicity. The disadvantage is inefficiency.

SLIDING WINDOW:

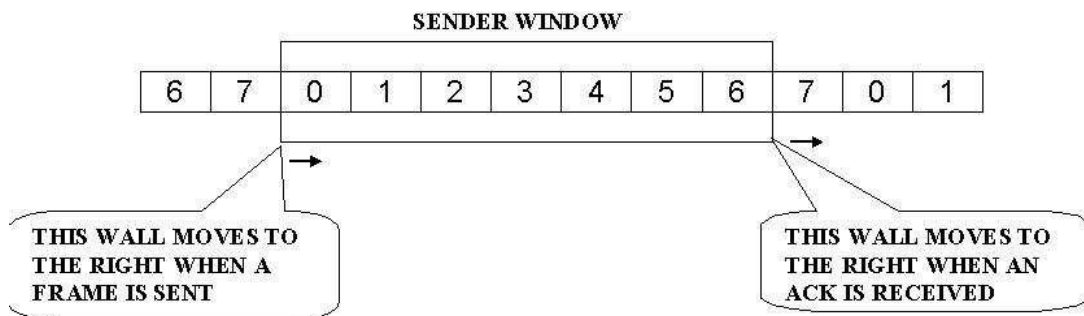
In this method, the sender can transmit several frames before needing an acknowledgment. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

The sliding window refers to imaginary boxes at both the sender and receiver. This window provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement. To identify each frame the sliding window scheme introduces the sequence number. The frames are numbered as 0 to n-1. And the size of the window is n-1. Here the size of the window is 7 and the frames are numbered as 0,1,2,3,4,5,6,7.

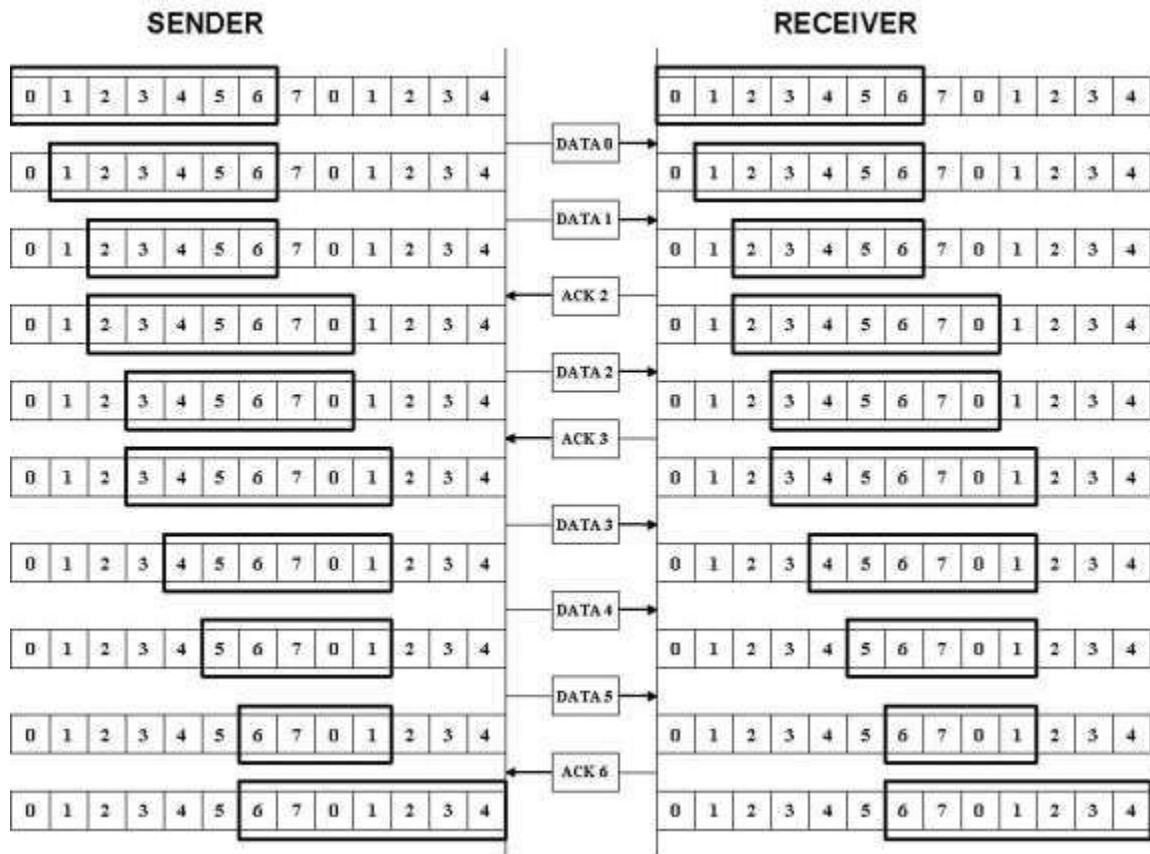


SENDER WINDOW:

At the beginning the sender's window contains n-1 frames. As frames are sent out the left boundary of the window moves inward, shrinking the size of the window. Once an ACK receives the window expands at the right side boundary to allow in a number of new frames equal to number of frames acknowledged by that ACK.



EXAMPLE:



ERROR CONTROL

Error control is implemented in such a way that every time an error is detected, a negative acknowledgement is returned and the specified frame is retransmitted. This process is called **automatic repeat request (ARQ)**.

The error control is implemented with the flow control mechanism. So there are two types in error control. They are,

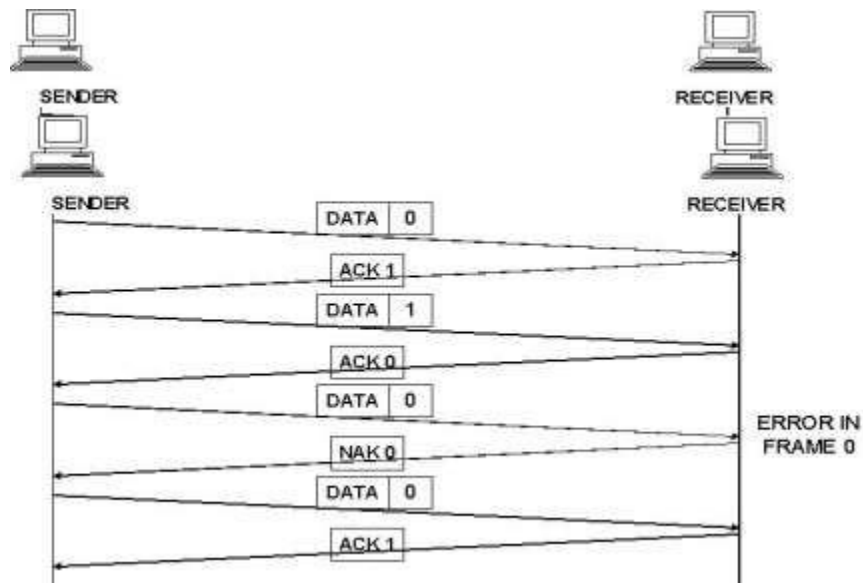
1. stop and wait ARQ
2. sliding window ARQ

STOP AND WAIT ARQ:

It is a form of stop and wait flow control, extended to include retransmission of data in case of lost or damaged frames.

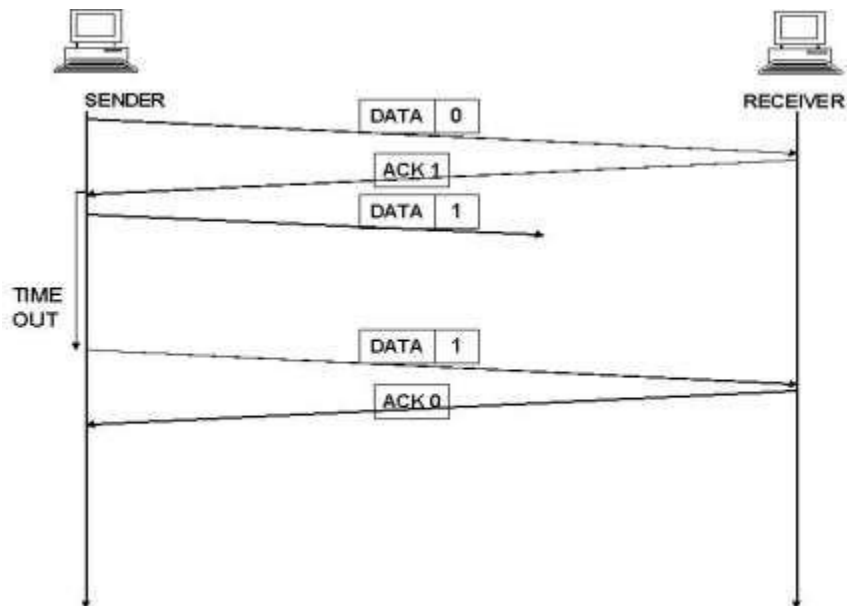
DAMAGED FRAME:

When a frame is discovered by the receiver to contain an error, it returns a NAK frame and the sender retransmits the last frame.



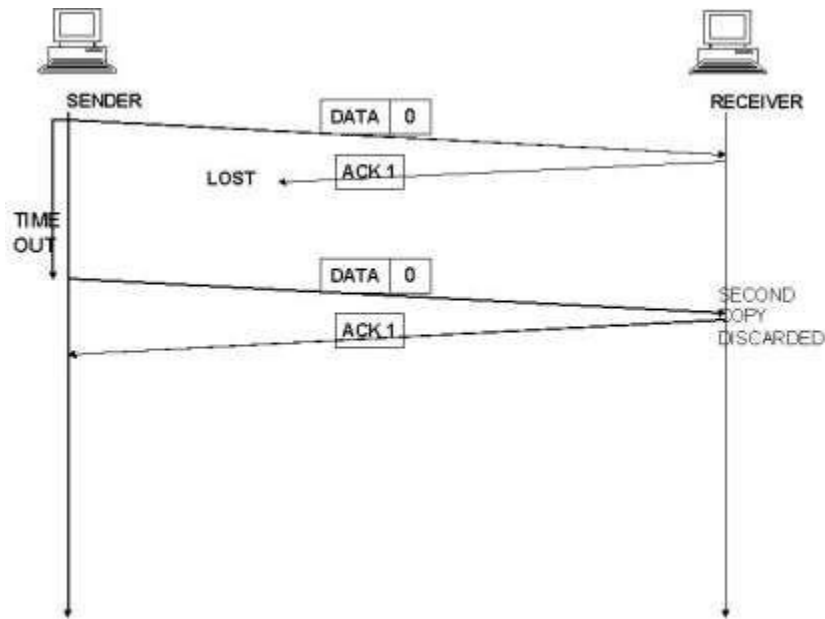
LOST DATA FRAME:

The sender is equipped with a timer that starts every time a data frame is transmitted. If the frame lost in transmission the receiver can never acknowledge it. The sending device waits for an ACK or NAK frame until its timer goes off, then it tries again. It retransmits the last data frame.



LOST ACKNOWLEDGEMENT:

The data frame was received by the receiver but the acknowledgement was lost in transmission. The sender waits until the timer goes off, then it retransmits the data frame. The receiver gets a duplicated copy of the data frame. So it knows the acknowledgement was lost so it discards the second copy.



SLIDING WINDOW ARQ

It is used to send multiple frames per time. The number of frame is according to the window size. The sliding window is an imaginary box which is reside on both sender and receiver side.

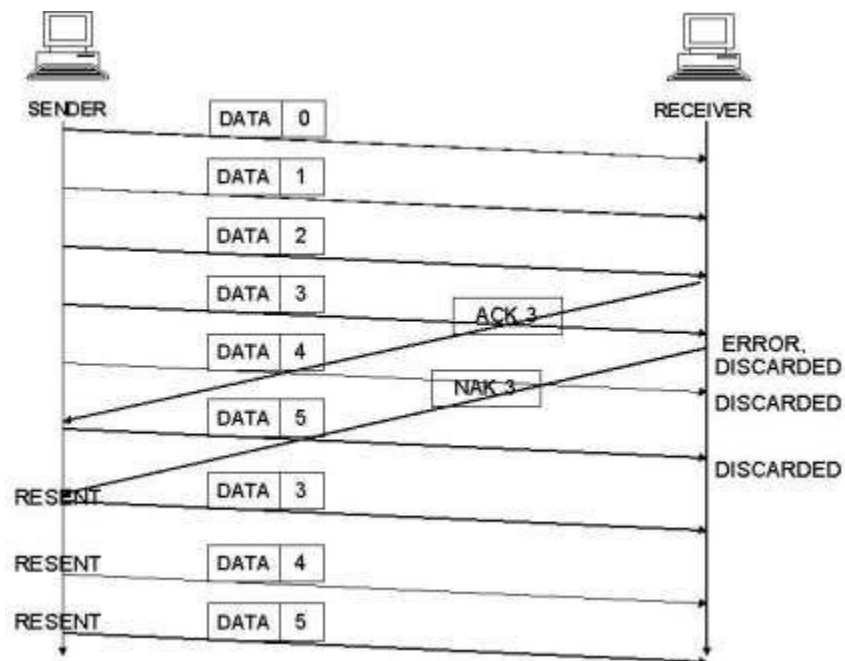
It has two types. They are,

1. go-back-n ARQ
2. selective reject ARQ

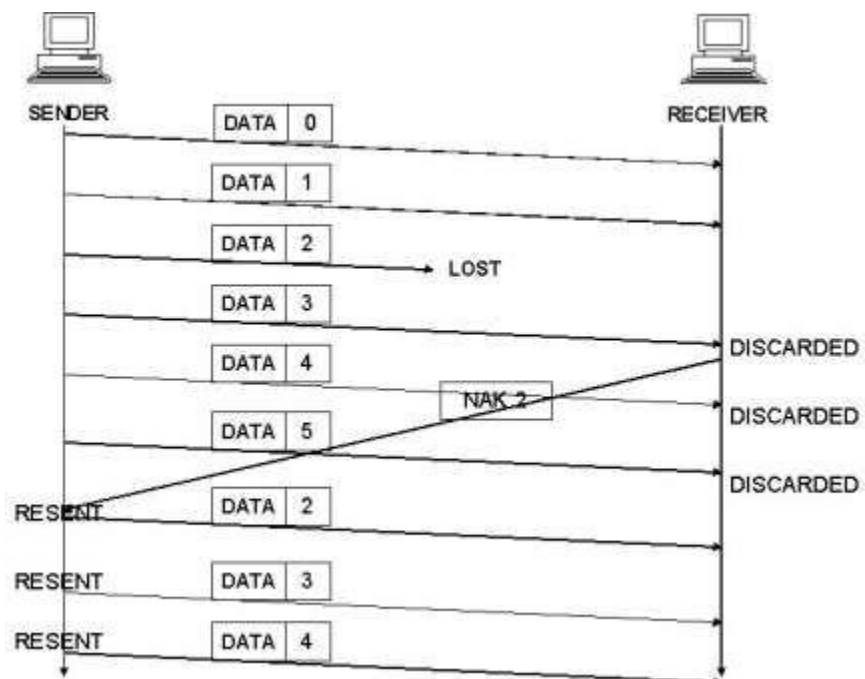
GO-BACK-N ARQ:

In this method, if one frame is lost or damaged, all frames sent since the last frame acknowledged or retransmitted.

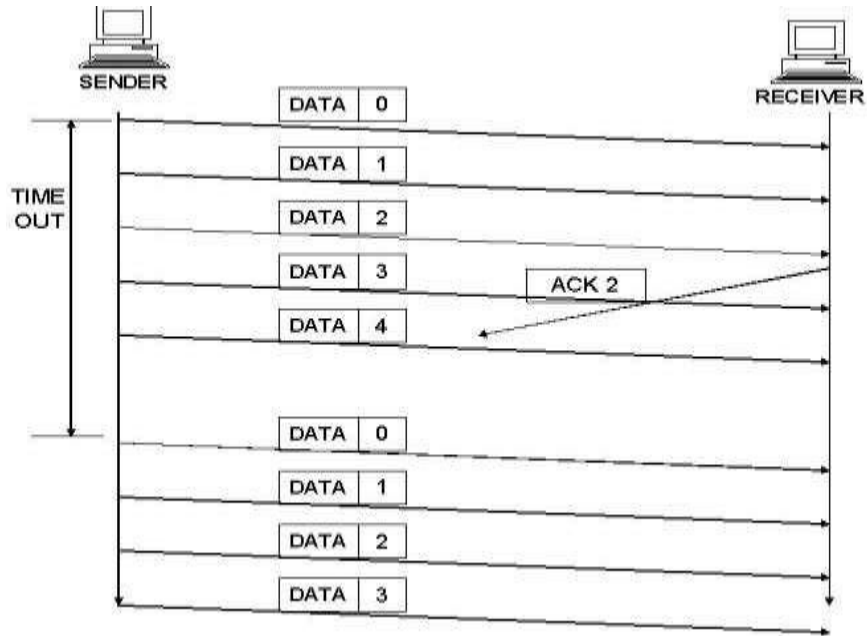
DAMAGED FRAME:



LOST FRAME:



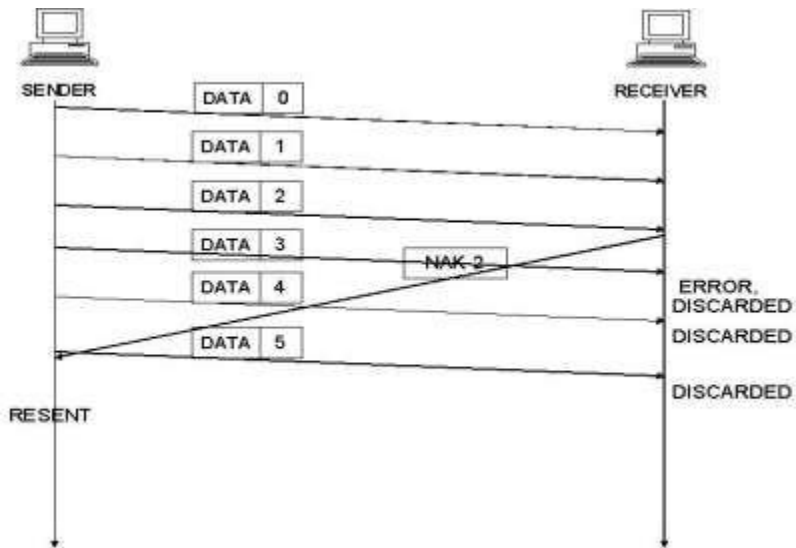
LOST ACK:



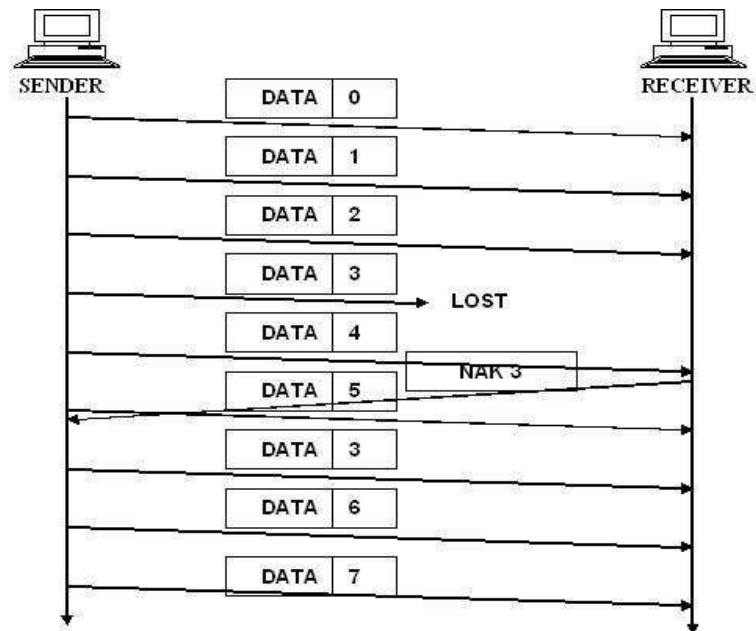
SELECTIVE REPEAT ARQ

Selective repeat ARQ re transmits only the damaged or lost frames instead of sending multiple frames. The selective transmission increases the efficiency of transmission and is more suitable for noisy link. The receiver should have sorting mechanism.

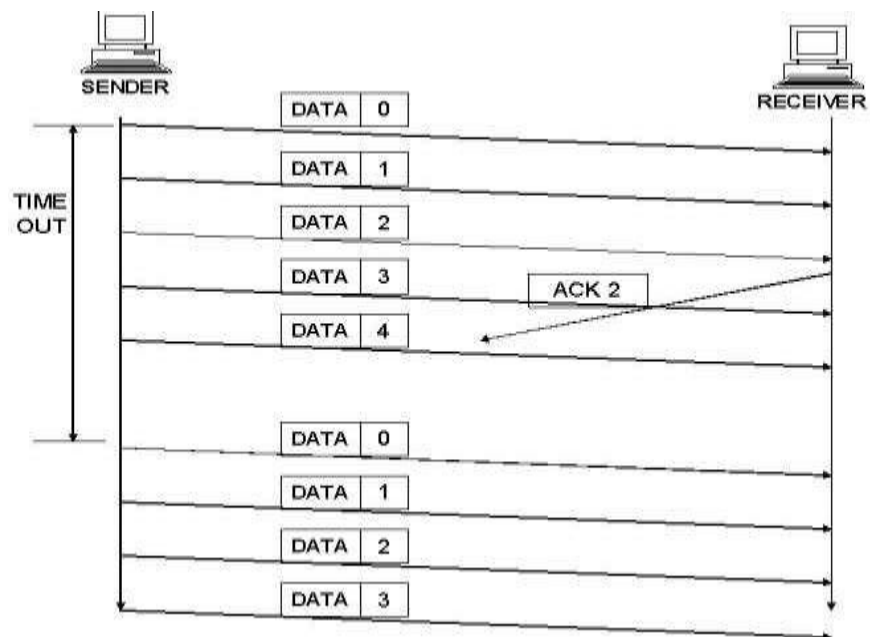
DAMAGED FRAME:



LOST FRAME



LOST ACK



FRAMING

The stream of bits are not advisable to maintain in networks. When an error occurs, then the entire stream have to retransmitted. To avoid this, the framing concept is used. In this, the stream of bits are divided into manageable bit units called frames. To achieve, we are using several ways. They are,

1. Byte Oriented Protocols
2. Bit Oriented Protocols
3. Clock Based Protocols

1. BYTE ORIENTED PROTOCOLS:

Each frame is considered as a collection of bytes rather than a collection of bits. There are two approaches. They are,

1. Sentinel approach

In this approach it uses special characters called sentinel characters to indicate where frames start and end. This approach is called character stuffing because extra characters are inserted in the data portion of the frame.

- Ex: 1. Binary Synchronous Communication (BISYNC)
 2. Point to Point Protocol

2. Byte Count Approach

In this approach no of bytes in frame are counted and entered in the header. The COUNT Field specifies how many bytes are contained in the frame's body.

- Ex: 1. Digital Data Communication Message Protocol

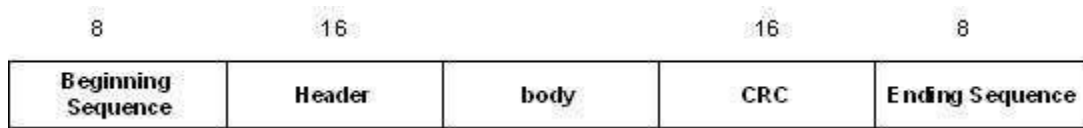
2. BIT ORIENTED PROTOCOLS:

It views the frames as a collection of bits. The Synchronous Data Link Control (SDLC) protocol developed by IBM is an example of a bit oriented protocol. It was later standardized by the ISO as the High Level Data Link Control (HDLC)

HDLC – HIGH LEVEL DATA LINK CONTROL

It is a bit oriented data link protocol designed to support both half duplex and full duplex communication over point to point and multi point links.

FRAME FORMAT



HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110. To guarantee that a special sequence does not appear in advertently anywhere else in the frame, HDLC uses a process called bit stuffing.

On the sending side, any time five consecutive 1s have been transmitted from the body of the message, the sender inserts a 0 before transmitting the next bit. On the receiver side, should five consecutive 1s arrive, the receiver makes its decision based on the next bit it sees. If the next bit is a 1, then one of the two things is true. Either this is the end of the frame or an error has been introduced. By looking at the next bit, it can conclude. If it sees a 0, then it is the end of frame. If else, then there must have an error and the whole frame has been discarded.

3. CLOCK BASED PROTOCOLS:

The Synchronous Optical Network (SONET) is one of the protocols using the clock based framing approach.

SONET:

It was developed by the ANSI for digital transmission over optical network. It addresses both the framing and encoding problems. A SONET frame has some special information to distinguish where the frame starts and ends.

