COMPUTER NETWORKS –Notes

MODULE 1

What is a Computer Network?

A computer network is a system in which multiple computers are connected to each other to share information and resources. Computer network is a telecommunication channel through which we can share our data. It is also called data network. The best example of computer network is Internet.

Properties of Good Network

1. Interpersonal Communication : We can communicate with each other efficiently and easily example emails, chat rooms, video conferencing etc.
2. Resources can be shared : We can use the resources provided by network such as printers etc.
3. Sharing files, data : Authorized users are allowed to share the files on the network.

Data Communications

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

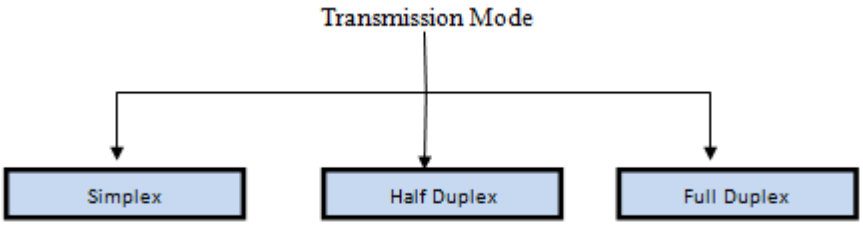
Components of Data Communication

1. Message : It is the information to be delivered.
2. Sender : Sender is the person who is sending the message.
3. Receiver : Receiver is the person to him the message is to be delivered.
4. Medium : It is the medium through which message is to be sent for example modem.
5. Protocol : These are some set of rules which govern data communication.

Data Flow /Transmission Modes in Computer Networks

Transmission mode means transferring of data between two devices. It is also called communication mode. These modes direct the direction of flow of information. There are three types of transmission mode. They are :

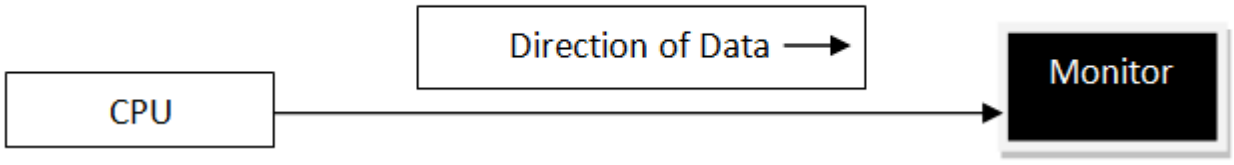
- Simplex Mode
- Half duplex Mode
- Full duplex Mode



SIMPLEX Mode

In this type of transmission mode data can be sent only through one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems.

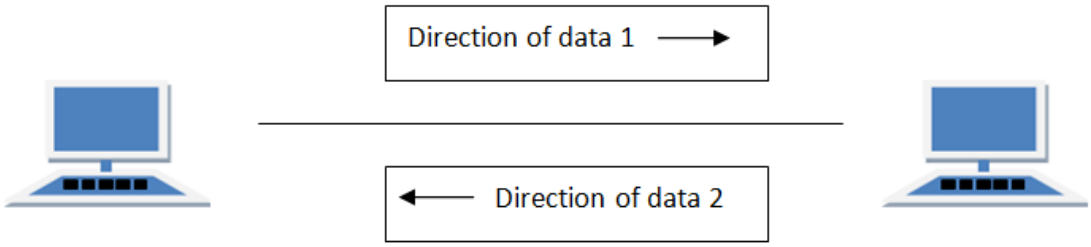
Examples of simplex Mode is loudspeaker, television broadcasting, television and remote, keyboard and monitor etc.



HALF DUPLEX Mode

In half duplex system we can send data in both directions but it is done one at a time that is when the sender is sending the data then at that time we can't send the sender our message. The data is sent in one direction.

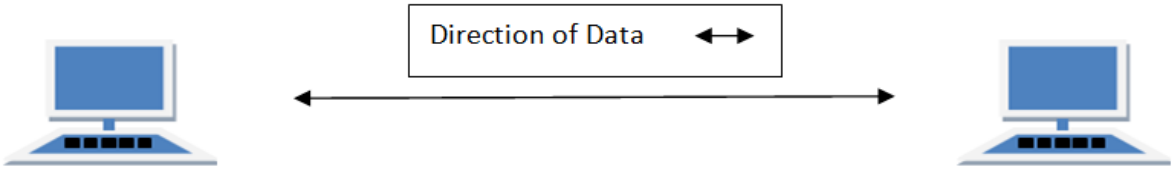
Example of half duplex is a walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



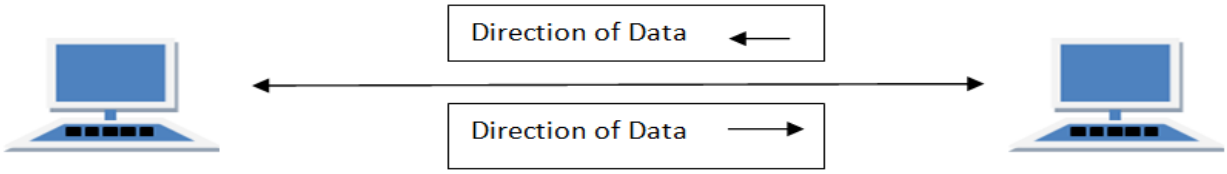
FULL DUPLEX Mode

In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.

Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



In full duplex system there can be two lines one for sending the data and the other for receiving data.



Bandwidth - Bit Rate and Baud Rate

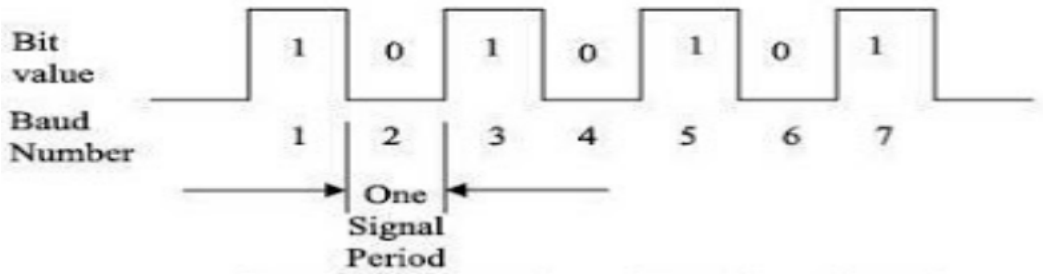
Bit Rate

- The bit rate is the speed of communication.
- Number of bits transmitted per second or bps rate.
- The amount of data that a computer network can transmit is called bandwidth of network and is usually measured in kilo bits per second (Kbps) or mega bits per second (Mbps).
- A bit the smallest unit of information what computer can process can have one of two values, either 0 or 1.

- A kilo bit in one thousand bit while a mega bit is one million bit the speed at which information can be transmitted across the internet depends on the lowest information transporting capacity along the route and the number of people using that route at any given time.

Baud Rate

- The signaling rate of a line is measured in bauds.
- It is the switching speed or number of the transition (Voltage or frequency changes) that are made per second. The speed at which data is transmitted referred to as baud.
- Baud is commonly identified as the number of bits per second that can be transmitted over a communication line.



Discuss Transmission Media in detail.

Transmission Media connects the message source with the message receiver by means of Guided or Unguided Media.

I Guided Media/Bound Media: Guided Transmission Media uses a "cabling" system that guides the data signals along a specific path. Some of the common examples of guided media are Twisted Pair, Coaxial cable and Fiber optics.

♦ **Twisted-Pair Wire:**

- Twisted-pair is ordinary telephone wire,
- consisting of copper wire twisted into pairs.
- It is the most widely used media for telecommunications
- It is used for both voice and data transmissions.

- It is used extensively in home and office telephone systems and many LANs and WANs.

♦ **Coaxial Cable:**

- This telecommunication media consists of copper or aluminum wire wrapped with spacers to insulate and protect it.
- Coaxial cables can carry a large volume of data and allows high-speed data transmission
- It is used in high-service metropolitan areas for cable TV systems, and for short-distance connection of computers and peripheral devices.
- It is used extensively in office buildings and other work sites for local area networks.

♦ **Fiber Optics:**

- This media consists of one or more hair-thin filaments of glass fiber wrapped in a protective jacket.
- Signals are converted to light form and fired by laser in bursts.
- Optical fibers can carry digital as well as analog signals and provides increased speed and greater carrying capacity than coaxial cable and twisted-pair lines.

II Unguided Media/Unbound Media:

- Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path.
- The data signals are not bound to a cabling media.
- Some of the common examples of unguided media are Terrestrial Microwave, Radio Waves, Micro Waves, Infrared Waves and Communication Satellites.

Terrestrial Microwave: Terrestrial microwave media uses the atmosphere as the medium through which to transmit signals and is used extensively for high-volume as well as long-distance communication of both data and voice in the form of electromagnetic waves.

Radio Waves: Radio waves are an invisible form of electromagnetic radiation that varies in wavelength from around a millimeter to 100,000 km, making it one of the widest ranges in the electromagnetic spectrum. Radio waves are most commonly used transmission media in the wireless Local Area

Networks.

Micro Waves: Microwaves are radio waves with wavelengths ranging from as long as one meter to as short as one millimeter, or equivalently, with frequencies between 300 MHz (0.3 GHz) and 300 GHz. These are used for communication, radar systems, radio astronomy, navigation and spectroscopy.

Infrared Waves: Infrared light is used in industrial, scientific, and medical applications. Night-vision devices using infrared illumination allow people or animals to be observed without the observer being detected.

Communication Satellites:

- Communication satellites use the atmosphere (microwave radio waves) as the medium through which to transmit signals.
- A satellite is some solar-powered electronic device that receives, amplifies, and retransmits signals; the satellite acts as a relay station between satellite transmissions stations on the ground (earth stations).
- They are used extensively for high-volume as well as long-distance communication of both data and voice.
-

Switching techniques

Packet Switching and Message Switching.

♦ **Circuit Switching:**

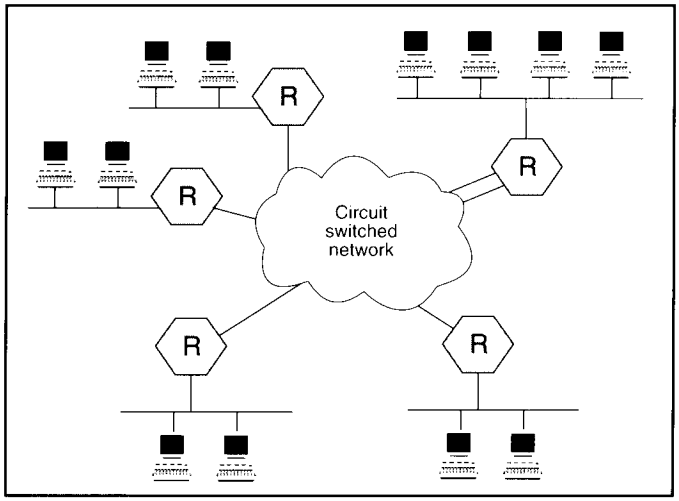
- When two nodes communicate with each other over a dedicated communication path, it is called Circuit Switching.
- An important property of circuit switching is the need to set up an end-to-end path before any data can be sent which can either be permanent or temporary.
- Applications which use circuit switching may have to go through three phases:

  Establish a circuit,

Transfer of data and

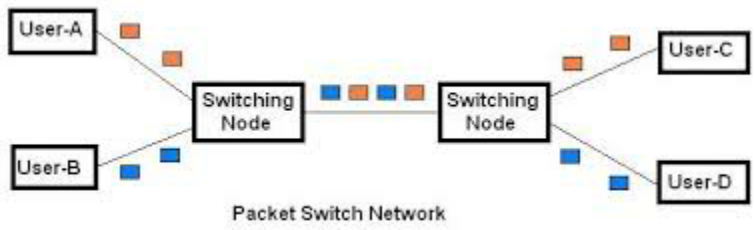
Disconnect the circuit.

- The bandwidth is reserved all the way from sender to receiver and all the data packets follow the same path, thus, ensuring the sequence of data packets are in order.



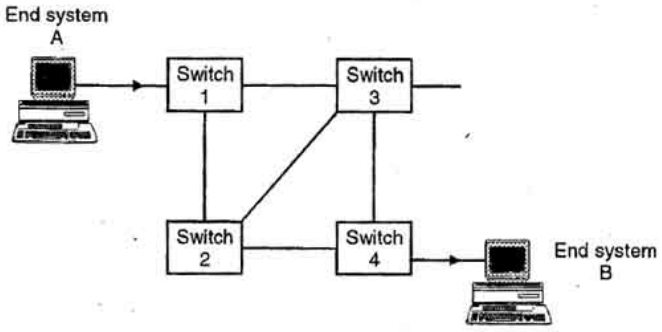
♦ **Packet Switching:**

- The entire message is broken down into smaller transmission units called packets.
- The switching information is added in the header of each packet and transmitted independently.
- It is easier for intermediate networking devices to store smaller size packets and they do not take much resources either on carrier path or in the switches' internal memory.
- In packet switched network, first packet of a multi-packet message may be forwarded before the second one has fully arrived, thus reducing delay and improving throughput.
- Since, there is no fixed path, different packets can follow different path and thus they may reach to destination out of order.



♦ **Message Switching/ Store-and-Forward:**

- In message switching, no physical path is established between sender and receiver in advance.
- The whole message is treated as a data unit and is transferred in its entirety which contains the entire data being delivered from the source to destination node.
- . A switch working on message switching first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.
- E-mail and voice mail are examples of message switching systems.



Message switched data network

MODULE 2

MODULE 2

Protocols

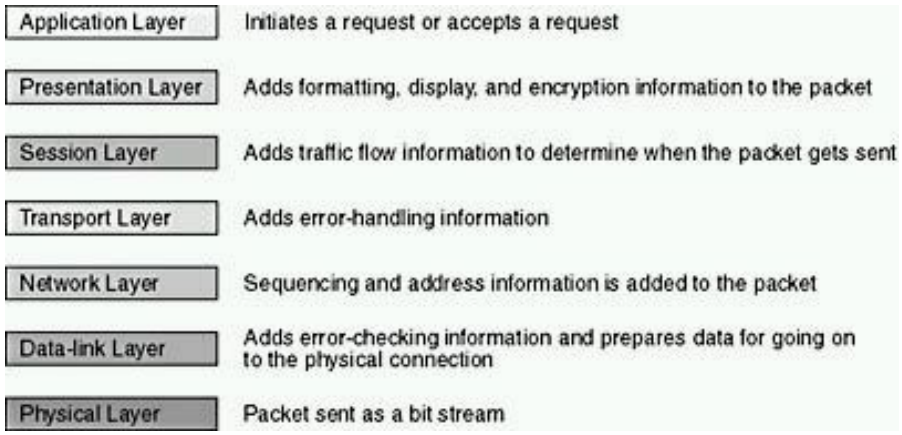
- Protocols are rules and procedures for communicating.
- When several computers are networked, the rules and technical procedures governing their communication and interaction are called protocols.
- There are many protocols. While each protocol facilitates basic communications, each has different purposes and accomplishes different tasks.
- Protocols can also work together in a protocol stack, or suite.:different protocols also work together at different levels in a single protocol stack.

Layering.

- In a network, several protocols have to work together. By working together, they ensure that the data is properly prepared, transferred to the right destination, received, and acted upon.
- The work of the various protocols must be coordinated so that no conflicts or incomplete operations take place. The results of this coordination effort are known as layering.

Protocol Stacks

- A protocol stack is a combination of protocols.
- Each layer of the stack specifies a different protocol for handling a function or subsystem of the communication process.
- Each layer has its own set of rules.
- Figure shows the OSI reference model and the rules associated with each layer.
- The protocols define the rules for each layer in the OSI reference model.



Transmission Control Protocol (TCP)

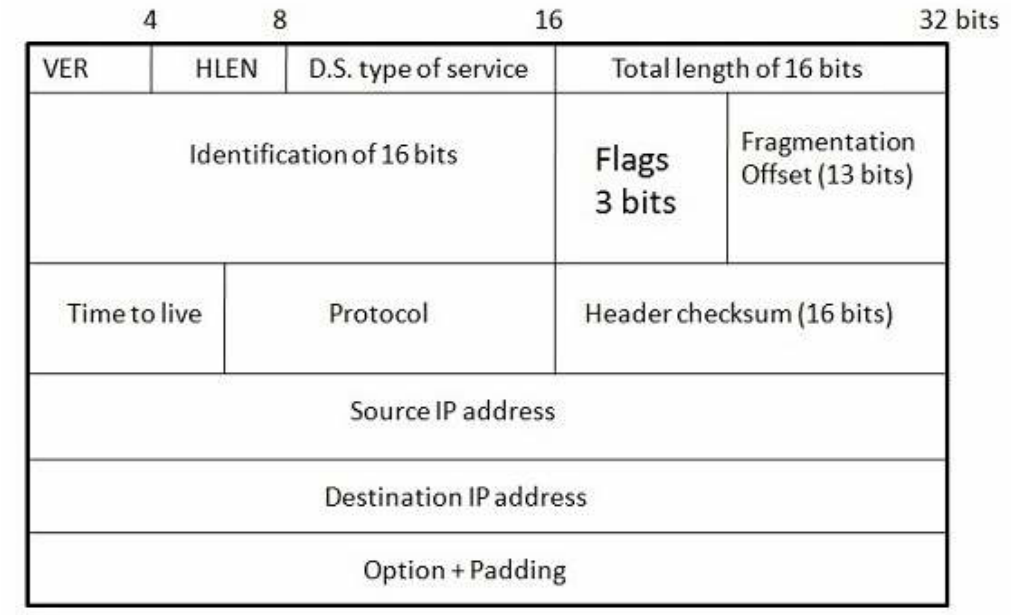
TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection. It exhibits the following key features:

- Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.
- TCP is a reliable and connection oriented protocol.
- TCP offers:
  - Stream Data Transfer.
  - Reliability.
  - Efficient Flow Control
  - Full-duplex operation.
  - Multiplexing.

- TCP offers connection oriented end-to-end packet delivery.
- TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect to receive.
- It retransmits the bytes not acknowledged with in specified time period.

Internet Protocol (IP)

- Internet Protocol is **connectionless** and **unreliable** protocol. It ensures no guarantee of successfully transmission of data.
- In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.
- Internet protocol transmits the data in form of a datagram as shown in the following diagram:



Points to remember:

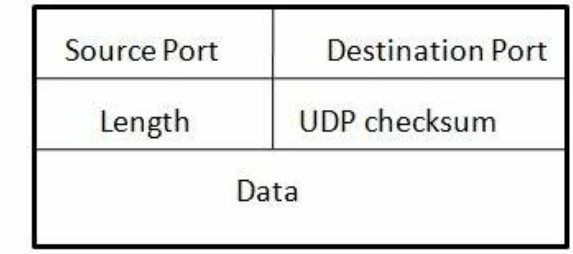
- The length of datagram is variable.
- The Datagram is divided into two parts: **header** and **data.**
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.

User Datagram Protocol (UDP)

- Like IP, UDP is connectionless and unreliable protocol. It doesn't require making a connection with the host to exchange data. Since UDP is unreliable protocol, there is no mechanism for

ensuring that data sent is received.

- UDP transmits the data in form of a datagram. The UDP datagram consists of five parts as shown in the following diagram:



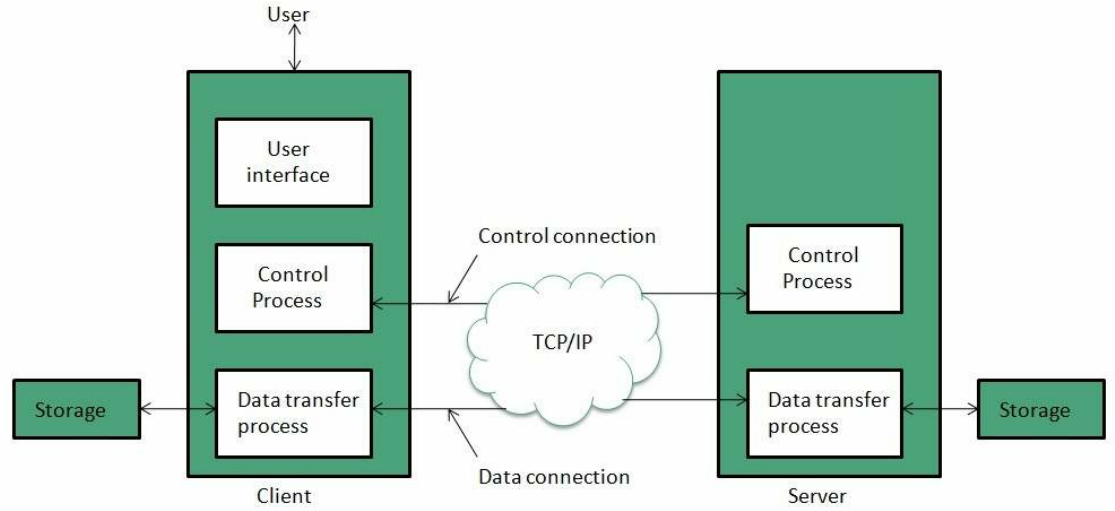
Points to remember:

- UDP is used by the application that typically transmit small amount of data at one time.
- UDP provides protocol port used i.e. UDP message contains both source and destination port number, that makes it possible for UDP software at the destination to deliver the message to correct application program.

File Transfer Protocol (FTP)

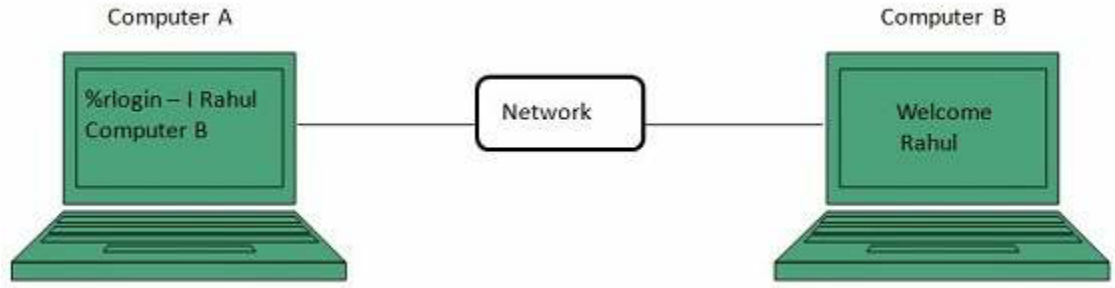
FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:

- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- **Control connection** is made between **control processes** while**Data Connection** is made between<="" b="" style="box-sizing: border-box;">
- FTP uses **port 21** for the control connection and **Port 20** for the data connection.



Telnet

Telnet is a protocol used to log in to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.



Hyper Text Transfer Protocol (HTTP)

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

HTTP Request

HTTP request comprises of lines which contains:

- Request line
- Header Fields
- Message body

Key Points

- The first line i.e. the **Request line** specifies the request method i.e.**Get** or **Post.**
- The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

HTTP Response

Like HTTP request, HTTP response also has certain structure. HTTP response contains:

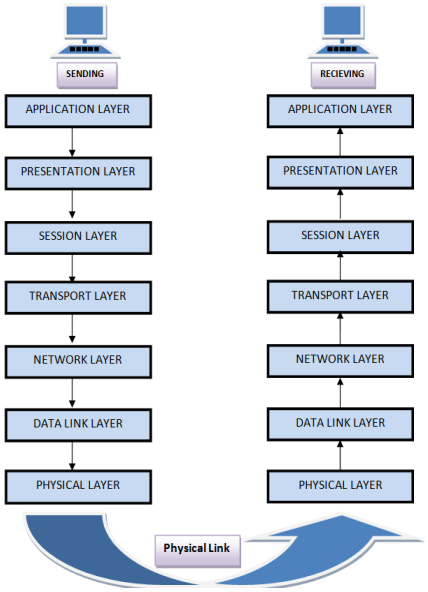
- Status line
- Headers
- Message body

ISO/OSI Model in Communication Networks

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other.

ISO has developed this. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.



Feature of OSI Model :

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Functions of Different Layers :

Layer 1: The Physical Layer :

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

Layer 2: Data Link Layer :

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer :

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Layer 4: Transport Layer :

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer :

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The Presentation Layer :

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It perfroms Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer :

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model:

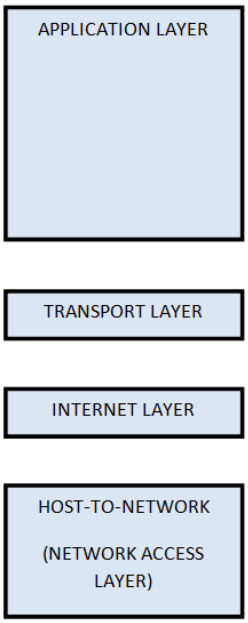
1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model:

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Description of different TCP/IP layers

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a

network.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

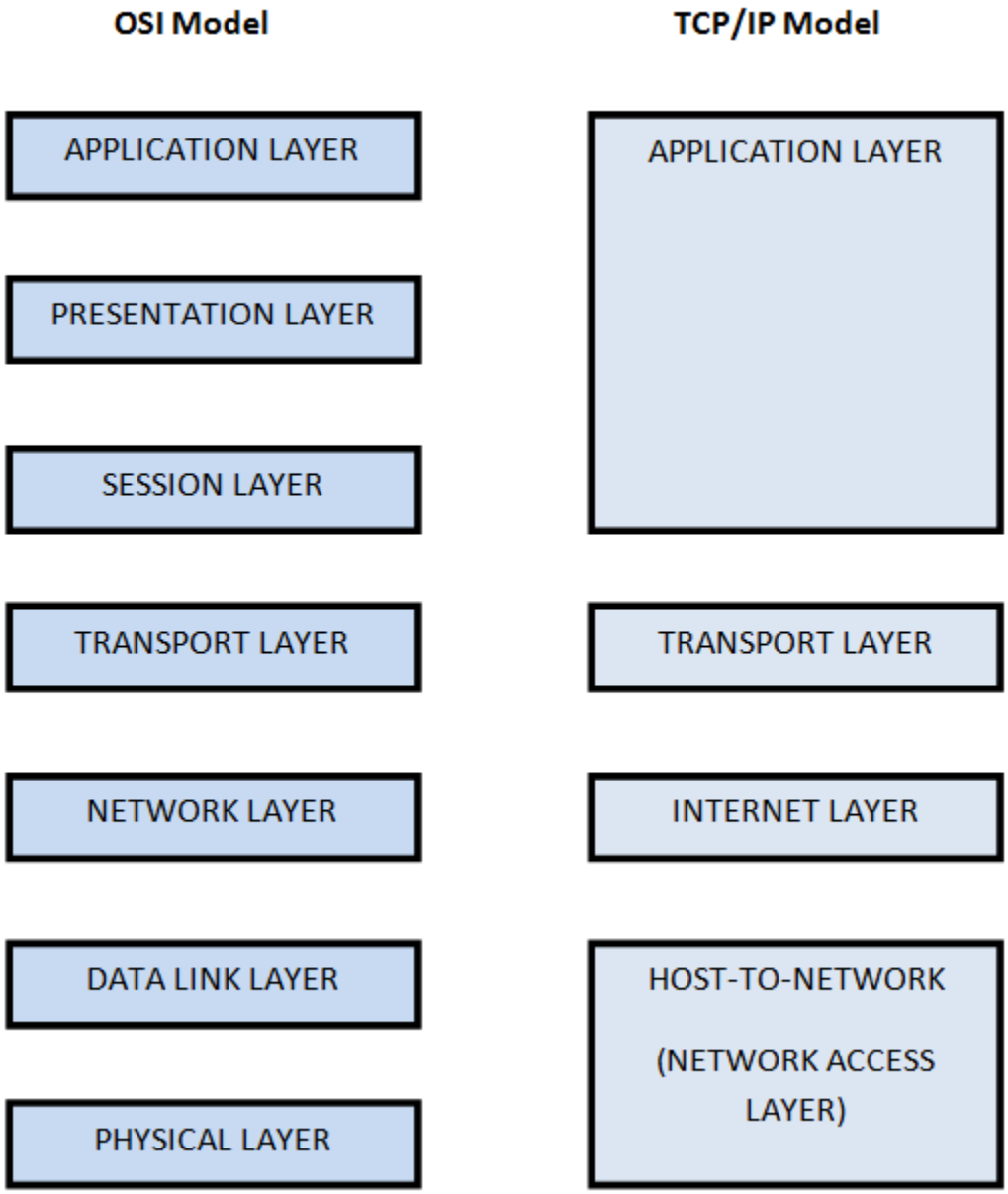
Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer	4. TCP/IP does not have a separate Presentation layer or

and Session layer.	Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

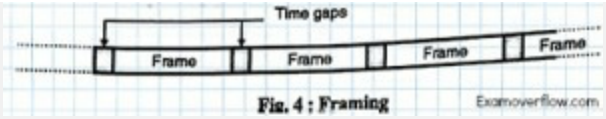
Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



Framing :

The bits to be is first broken into discrete frames at the data link layer. In order to guarantee that the bit stream is error free, the checksum of each frame is computed. When a frame is received, the data link there,

recomputes the checksum. If it is different from the checksum present in the frame, then the data link layer knows that an error has occurred. It then discards the bad frame and sends back a request for-retransmission. Breaking the bit stream into frames is called as framing. One way of doing it is by inserting time gaps between frames as shown in Fig. 4.

5. 

6. Framing

Byte-oriented framing Computer data is normally stored as alphanumeric characters that are encoded with a combination of 8 bits (1 byte). This type of framing differentiates one byte from another. It is an older style of framing that was used in the terminal/mainframe environment. Examples of byte-oriented framing include IBM's BISYNC protocol.

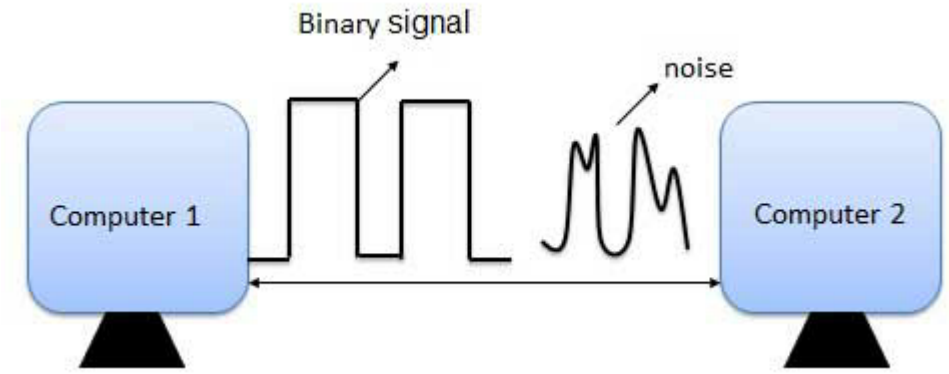
Bit-oriented framing This type of framing allows the sender to transmit a long string of bits at one time. IBM's SDLC (Synchronous Data Link Control) and HDLC (High-level Data Link Control) are examples of bit-oriented protocols. Most LANs use bit-oriented framing. There is usually a maximum frame size. For example, Ethernet has a maximum frame size of 1,526 bytes. The beginning and end of a frame is signaled with a special bit sequence (01111110 for HDLC). If no data is being transmitted, this same sequence is continuously transmitted so the end systems remain synchronized.

Error Detection & Correction

What is Error?

Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from

one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.



Types of Errors

There may be three types of errors:

- **Single bit error**

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

- **Multiple bits error**

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

- **Burst error**

Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

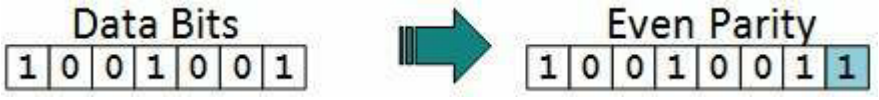
Error Detection

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

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

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

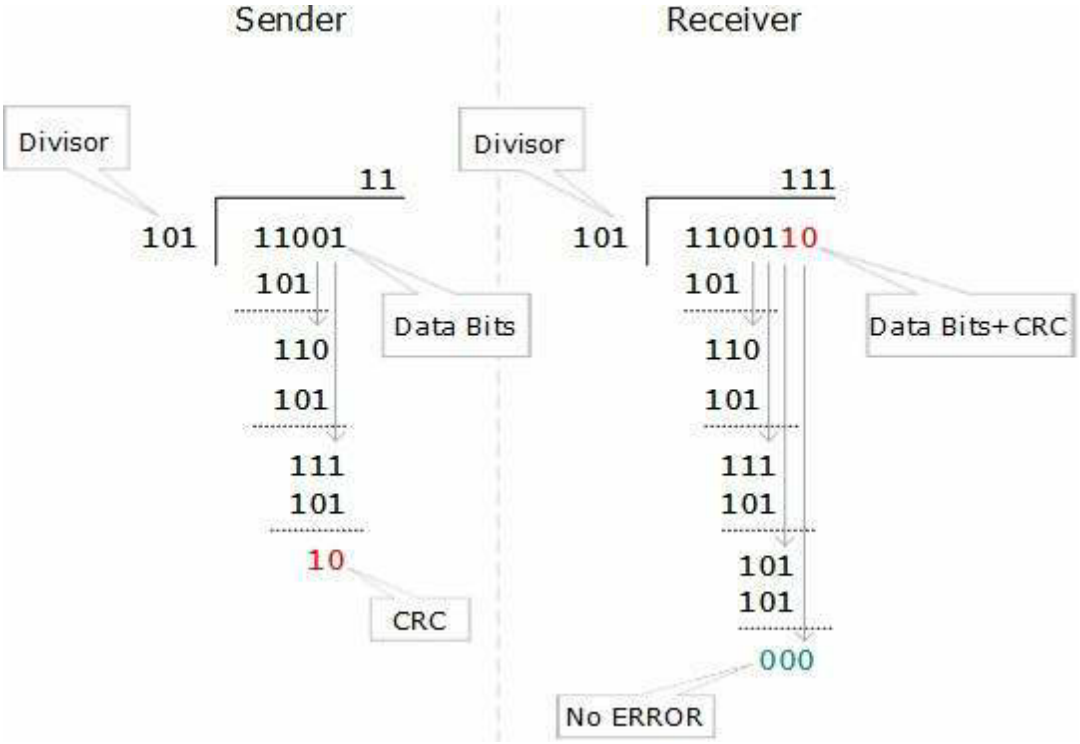


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

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

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



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

Error Correction

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

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

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

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

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit

codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

$$2^r >= m+r+1$$

Hamming Code

Hamming code is technique developed by R.W. Hamming for error correction. This method corrects the error by finding the state at which the error has occurred.

Determining the positions of redundancy bits

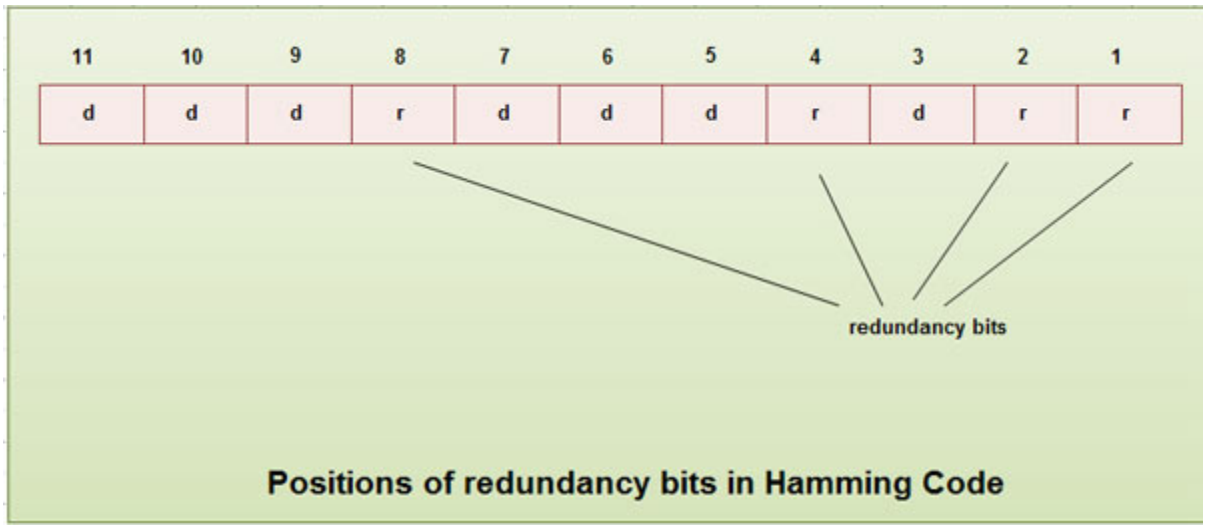
Till now, we know the exact number of redundancy bits required to be embedded with the particular data unit.

We know that to detect errors in a 7 bit code, 4 redundant bits are required.

Now, the next task is to determine the positions at which these redundancy bits will be placed within the data unit.

• These redundancy bits are placed at the positions which correspond to the power of2.

• For example in case of 7 bit data, 4 redundancy bits are required, so making total number of bits as 11. The redundancy bits are placed in position 1, 2, 4 and 8 as shown in fig.



Positions of redundancy bits in Hamming Code

Generating parity information

• In Hamming code, each r bit is the VRC for one combination of data bits. r_1 is the VRC bit for one combination of data bits, r_2 is the VRC for another combination of data bits and so on.

• Each data bit may be included in more than one VRC calculation.

• r_1 bit is calculated using all bits positions whose binary representation includes a 1 in the rightmost position.

• r_2 bit calculated using all the bit positions with a 1 in the second position and so on.

• Therefore the various r bits are parity bits for different combination of bits.

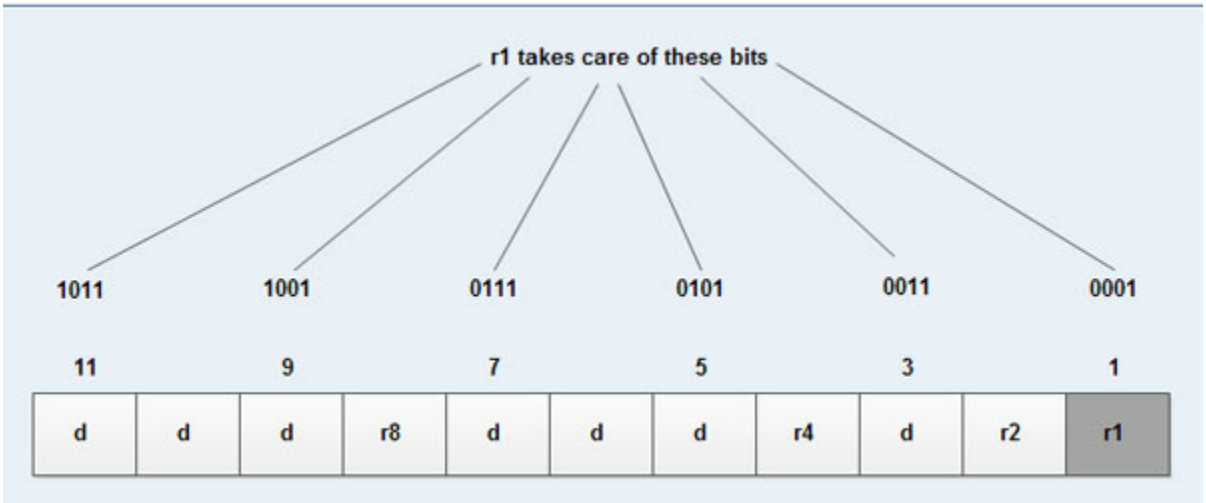
The various combinations are:

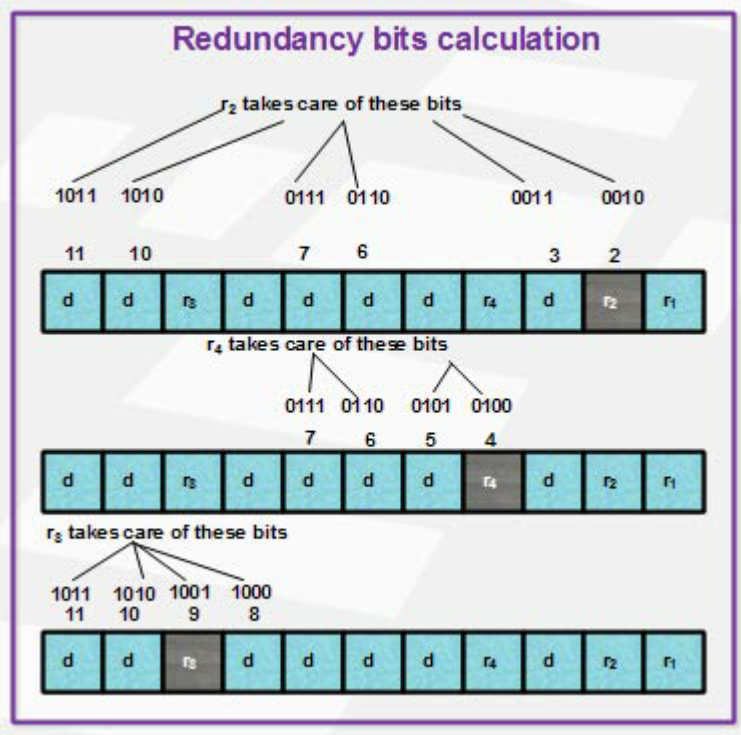
r_1 : bits 1,3,5, 7, 9, 11

r_2 : bits 2, 3, 6, 7, 10, 11

r_4 : bits 4, 5, 6, 7

r_8 : bits 8, 9, 10, 11





Example of Hamming Code Generation

Suppose a binary data 1001101 is to be transmitted. To implement hamming code for this, following steps are used:

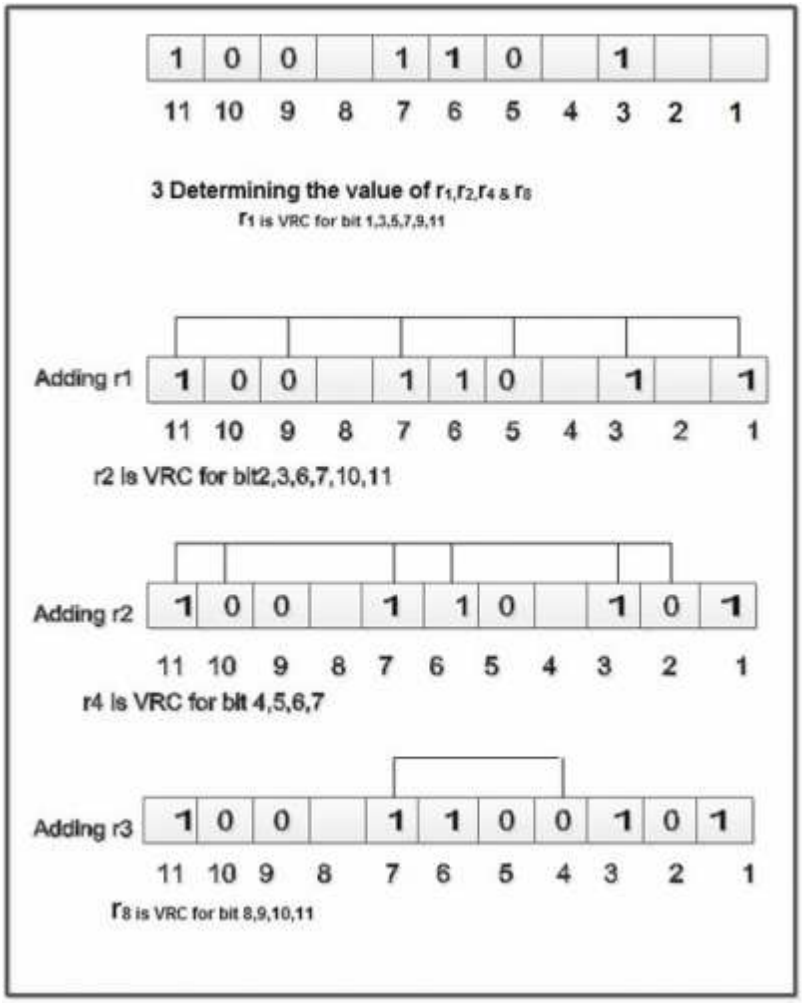
1. Calculating the number of redundancy bits required. Since number of data bits is 7, the value of r is calculated as

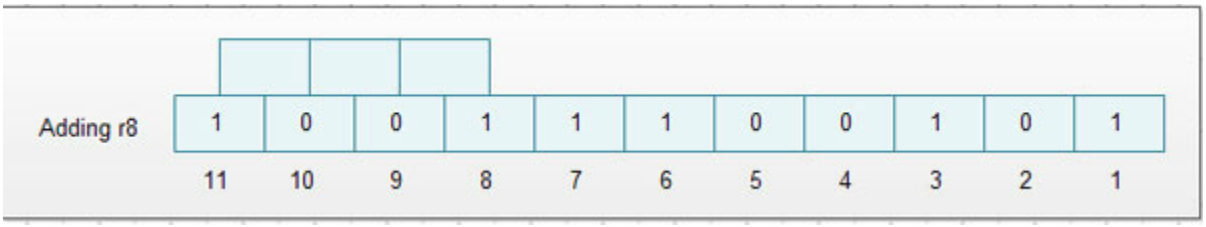
$$2^r \geq m + r + 1$$

$$2^4 \geq 7 + 4 + 1$$

Therefore no. of redundancy bits = 4

2. Determining the positions of various data bits and redundancy bits. The various r bits are placed at the position that corresponds to the power of 2 *i.e.* 1, 2, 4, 8

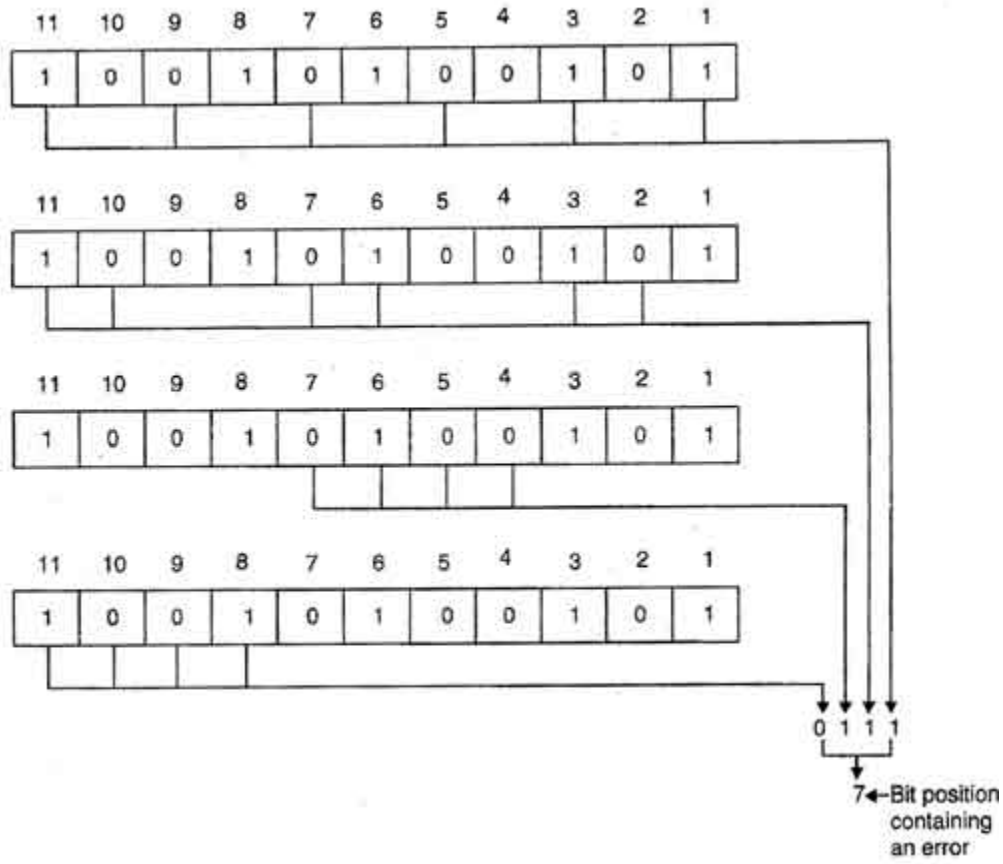




4. Thus data 1 0 0 1 1 1 0 0 1 0 1 with be transmitted.

Error Detection & Correction

Considering a case of above discussed example, if bit number 7 has been changed from 1 to 0.The data will be erroneous.



Data sent: 1 0 0 1 1 1 0 0 1 0 1

Data received: 1 00 1 0 1 00 1 0 1 (seventh bit changed)

The receive takes the transmission and recalculates four new VRCs using the same set of bits used by sender plus the relevant parity (r) bit for each set as shown in fig.

Then it assembles the new parity values into a binary number in order of r position (r_8, r_4, r_2, r_1).

In this example, this step gives us the binary number 0111. This corresponds to decimal 7. Therefore bit number 7 contains an error. To correct this error, bit 7 is reversed from 0 to 1.

Flow Control

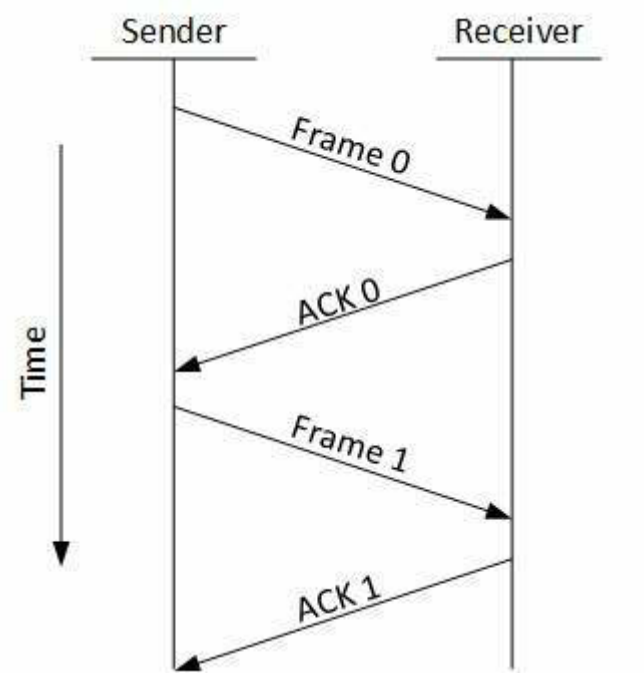
When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or

receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- **Stop and Wait**

  This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



- **Sliding Window**

  In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.In such case, both sender and receiver are equipped with some

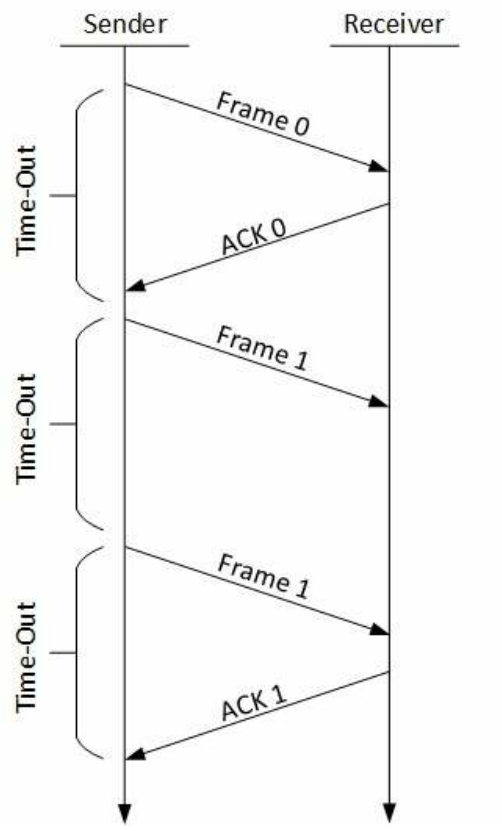
protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

- **Stop-and-wait ARQ**

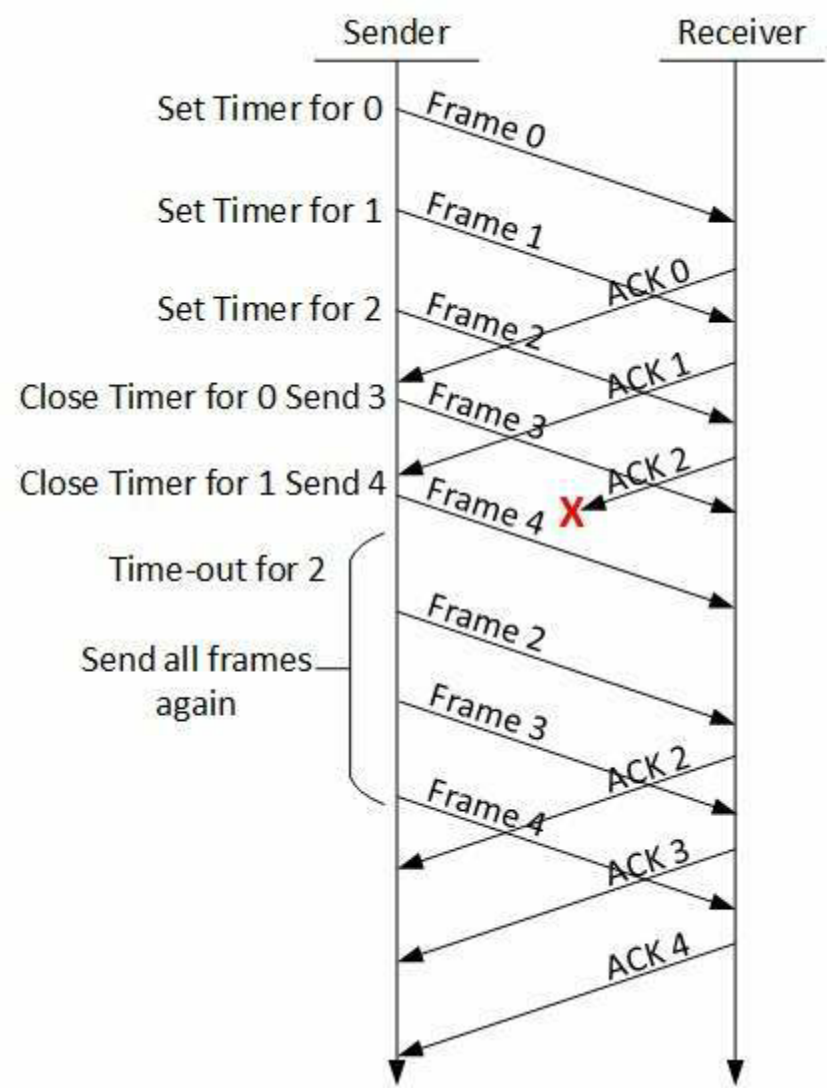


The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

- **Go-Back-N ARQ**

  Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

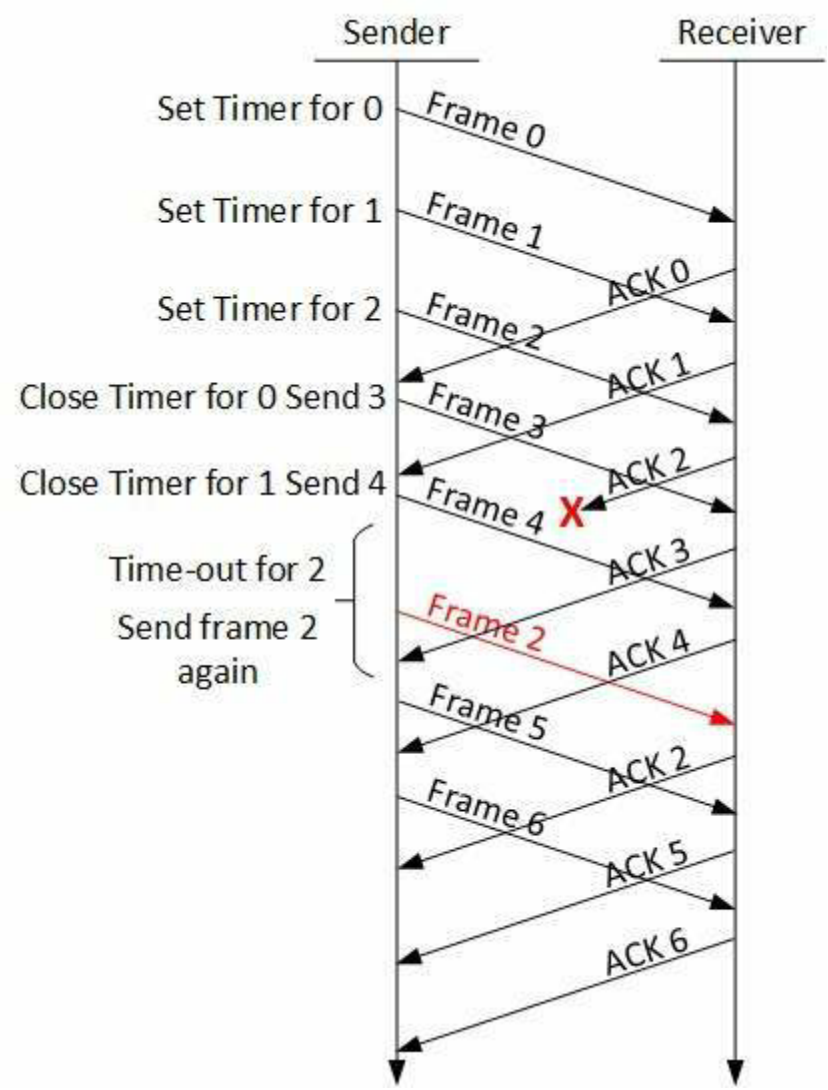


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

- **Selective Repeat ARQ**

  In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

What is piggybacking?

• In all practical situations, the transmission of data needs to be bi-directional. This is called as full-duplex transmission.

• We can achieve this full duplex transmission i.e. by having two separate channels-one for forward data transfer and the other for separate transfer i.e. for acknowledgements

• A better solution would be to use each channel (forward & reverse) to transmit frames both ways, with both channels having the same capacity. If A and B are two users. Then the data frames from A to Bare intermixed with the acknowledgements from A to B.

• One more improvement that can be made is piggybacking. The concept is explained as follows:

In two way communication, Whenever a data frame is received, the received waits and does not send the control frame (acknowledgement) back to the sender immediately.

The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.

This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.

• The major advantage of piggybacking is better use of available channel bandwidth.

The disadvantages of piggybacking are

1. Additional complexity.

2. If the data link layer waits too long before transmitting the acknowledgement, then retransmission of frame would take place.

Sliding Window Protocol

• In sliding window method, multiple frames are sent by sender at a time before needing an acknowledgment.

• Multiple frames sent by source are acknowledged by receiver using a single ACK frame.

Sliding Window

• Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.

• It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.

• Frames may be acknowledged by receiver at any point even when window is not full on receiver side.

• Frames may be transmitted by source even when window is not yet full on sender side.

• The windows have a specific size in which the frames are numbered modulo- n, which means they are numbered from 0 to n-l. For e.g. if n = 8, the frames are numbered 0, 1,2,3,4,5,6, 7, 0, 1,2,3,4,5,6, 7, 0, 1, ...

• The size of window is n-1. For e.g. In this case it is 7. Therefore, a maximum of n-l frames may be sent before an acknowledgment.

• When the receiver sends an ACK, it includes the number of next frame it expects to receive. For example in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.

Sliding window

Sliding Window on Sender Side

• At the beginning of a transmission, the sender's window contains n-l frames.

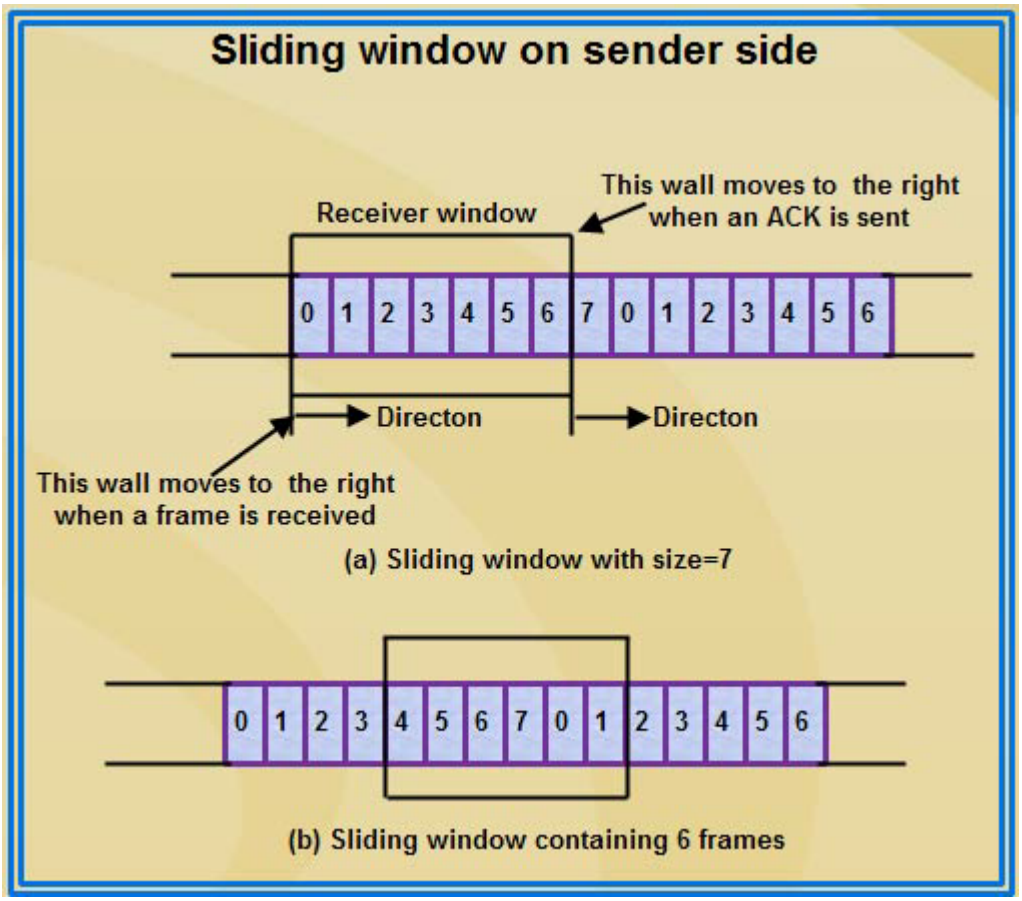
• As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window. This means if window size is w, if four frames are sent by source after the last acknowledgment, then the number of frames left in window is w-4.

• When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.

• For example, Let the window size is 7 (see diagram (a)), if frames 0 through 3 have been sent and no acknowledgment has been received, then the sender's window contains three frames - 4,5,6.

• Now, if an ACK numbered 3 is received by source, it means three frames (0, 1, 2) have been received by receiver and are undamaged.

• The sender's window will now expand to include the next three frames in its buffer. At this point the sender's window will contain six frames (4, 5, 6, 7, 0, 1). (See diagram (b)).



Sliding Window on Receiver Side

• At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.

• As the new frames come in, the size of window shrinks.

• Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must be sent.

• Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.

• As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.

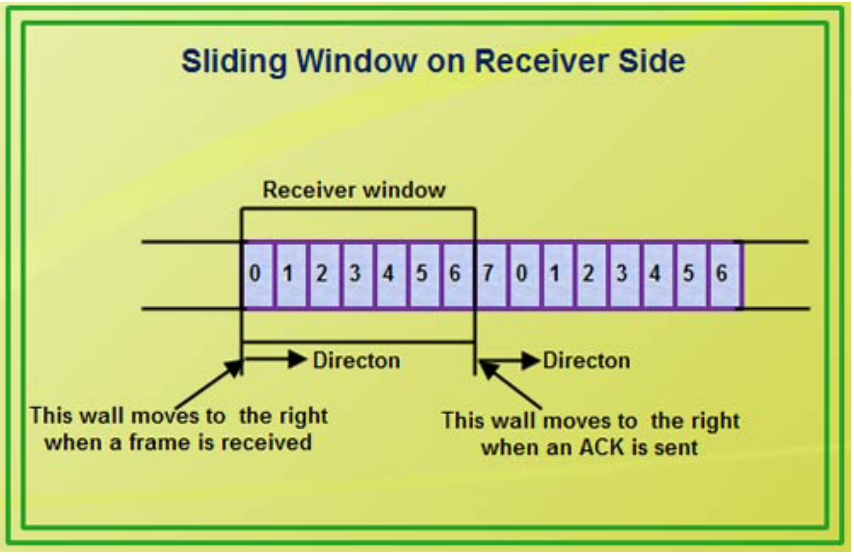
• For example, let the size of receiver's window is 7 as shown in diagram. It means window contains spaces for 7 frames.

• With the arrival of the first frame, the receiving window shrinks, moving the boundary from space 0 to 1. Now, window has shrunk by one, so the receiver may accept six more frame before it is required to send an ACK.

• If frames 0 through 3 have arrived but have DOC been acknowledged, the window will contain three frame spaces.

• As receiver sends an ACK, the window of the receiver expands to include as many new placeholders as newly acknowledged frames.

• The window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of previously acknowledged frame. For *e.g.,* If window size is 7 and if prior ACK was for frame 2 & the current ACK is for frame 5 the window expands by three (5 -2).



• Therefore, the sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.

• The sliding window of the receiver shrinks from left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgement is sent.

MODULE 3

MODULE 3

ALOHA:

- ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel.
- The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.
- A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time.
- In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost.

However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

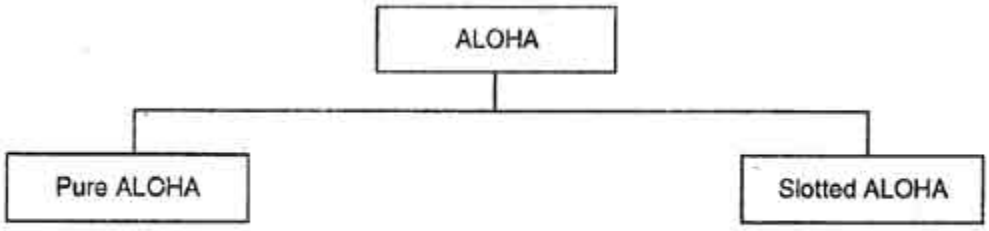
Aloha means "Hello".

Aloha is a **multiple access** protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision.

The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different types of ALOHA:

(i) PureALOHA
(ii) Slotted ALOHA



Types of ALOHA

(i) Pure ALOHA

• **In** pure ALOHA, the stations transmit frames whenever they have data to send.

• When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

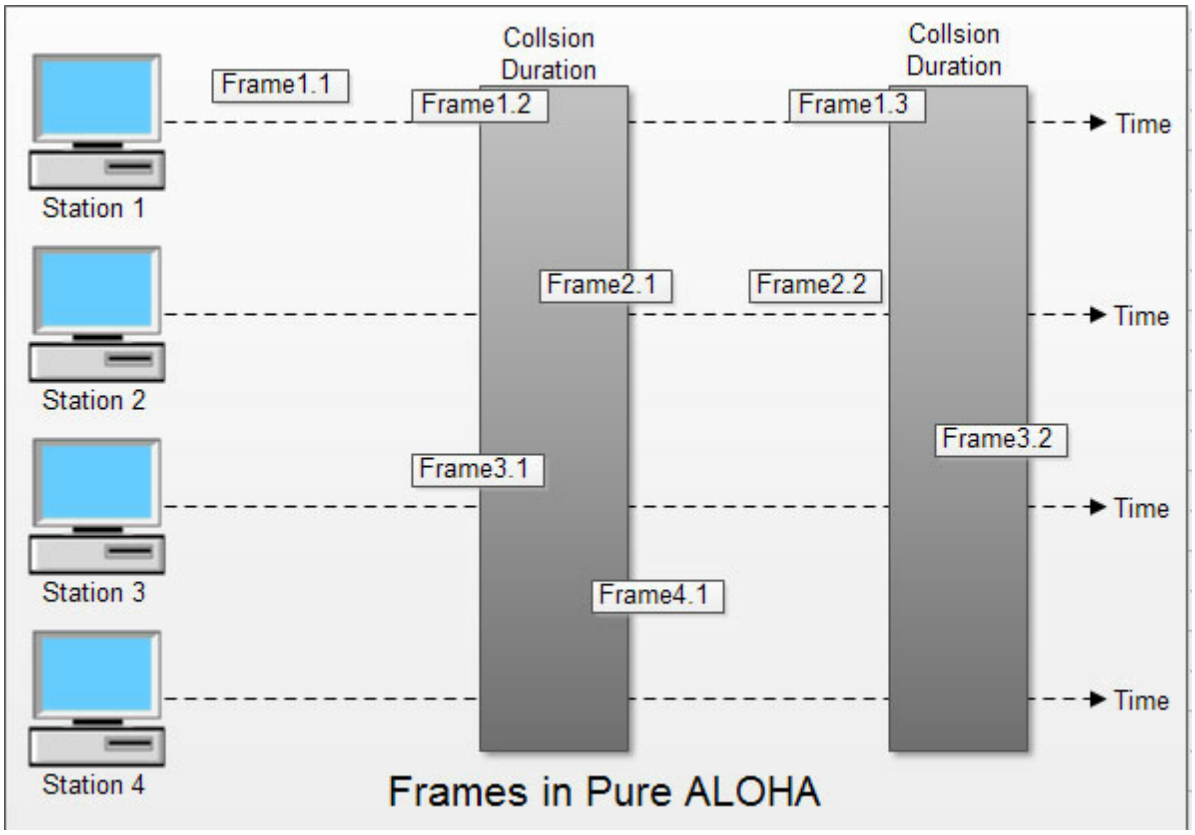
• If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

• If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

• Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random

amount of time before resending its frame. This randomness will help avoid more collisions.

• Figure shows an example of frame collisions in pure ALOHA.



• In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

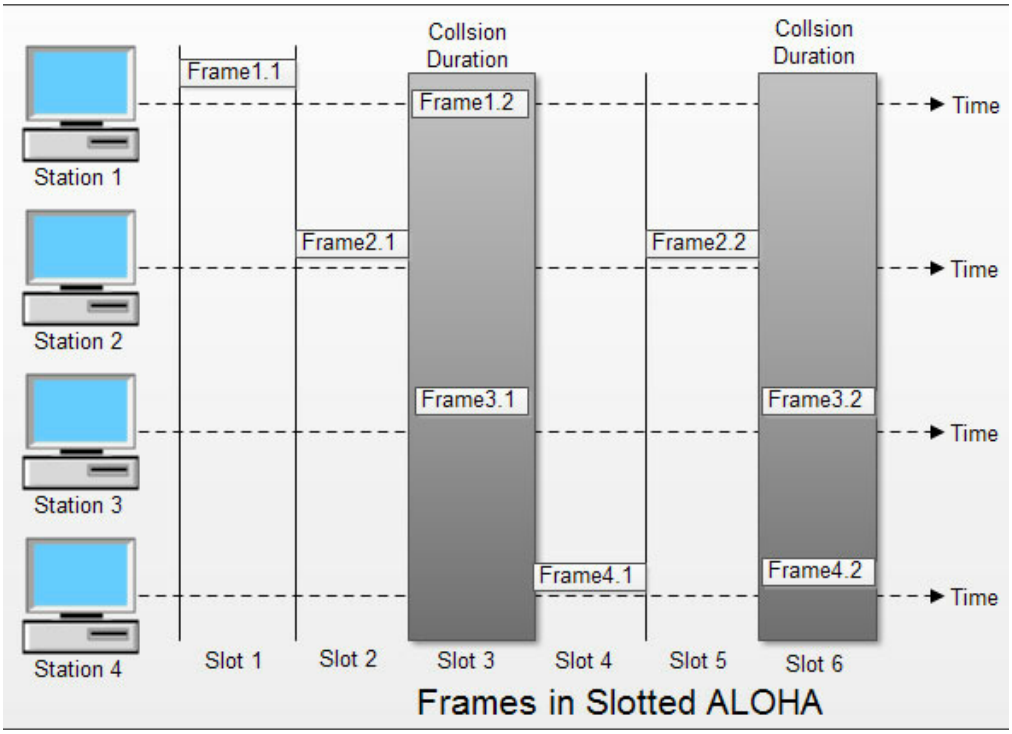
• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

(ii) Slotted ALOHA

• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

• In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.

• The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.



• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.

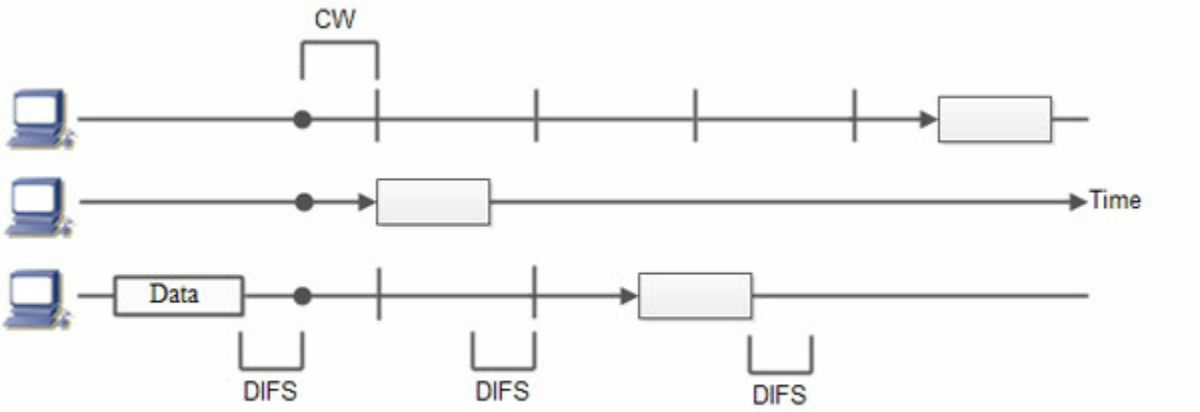
• In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.

• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

Carrier Sense Multiple Access (CSMA)

- **Carrier Sensed Multiple Access (CSMA) :** CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
- Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting.
- MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.
- In other words, a station that wants to communicate "listen" first on the media communication and awaits a "silence" of a preset time (called the Distributed Inter Frame Space or DIFS). After this compulsory period, the station starts a countdown for a random period considered. The maximum duration of this countdown is called the collision window (Window Collision, CW). If no equipment speaks before the end of the countdown, the station simply deliver its package. However, if it is overtaken by another station, it stops immediately its countdown and waits for the next silence. She then continued his account countdown where it left off. This is summarized

in Figure. The waiting time random has the advantage of allowing a statistically equitable distribution of speaking time between the various network equipment, while making little unlikely (but not impossible) that both devices speak exactly the same time. The countdown system prevents a station waiting too long before issuing its package. It's a bit what place in a meeting room when no master session (and all the World's polite) expected a silence, then a few moments before speaking, to allow time for someone else to speak. The time is and randomly assigned, that is to say, more or less equally.



Sharing time with CSMA method.

Again, this is what we do naturally in a meeting room if many people speak exactly the same time, they are realizing account immediately (as they listen at the same time they speak), and they interrupt without completing their sentence. After a while, one of them speaks again. If a new collision occurs, the two are interrupted again and tend to wait a little longer before speaking again.

CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance. CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.

Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.

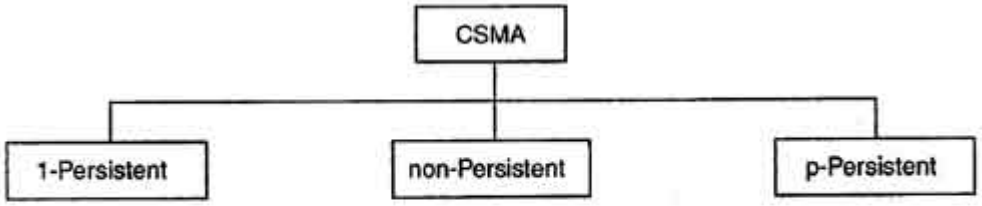
The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.

There Are Three Different Type of CSMA Protocols

(I) I-persistent CSMA

(ii) Non- Persistent CSMA

(iii) p-persistent CSMA



Types of CSMA

(i) I-persistent CSMA

• In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.

• If the channel is busy, the station waits until it becomes idle.

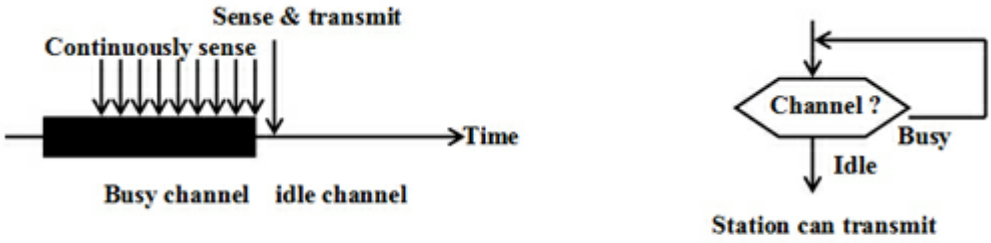
• When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.

• This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

• When the collision occurs, the stations wait a random amount of time and start allover again.

Drawback of I-persistent

• The propagation delay time greatly affects this protocol. Let us suppose, just after the station I begins its transmission, station 2 also became ready to send its data and senses the channel. If the station I signal has not yet reached station 2, station 2 will sense the channel to be idle and will begin its transmission. This will result in collision.



1-persistent CSMA

Even if propagation delay time is zero, collision will still occur. If two stations became .ready in the middle of third station's transmission, both stations will wait until the transmission of first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.

(ii) Non-persistent CSMA

• In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval oftime.
• After this time, it again checks the status of the channel and if the channel is.free it will transmit.

• A station that has a frame to send senses the channel.

• If the channel is idle, it sends immediately.

• If the channel is busy, it waits a random amount of time and then senses the channel again.

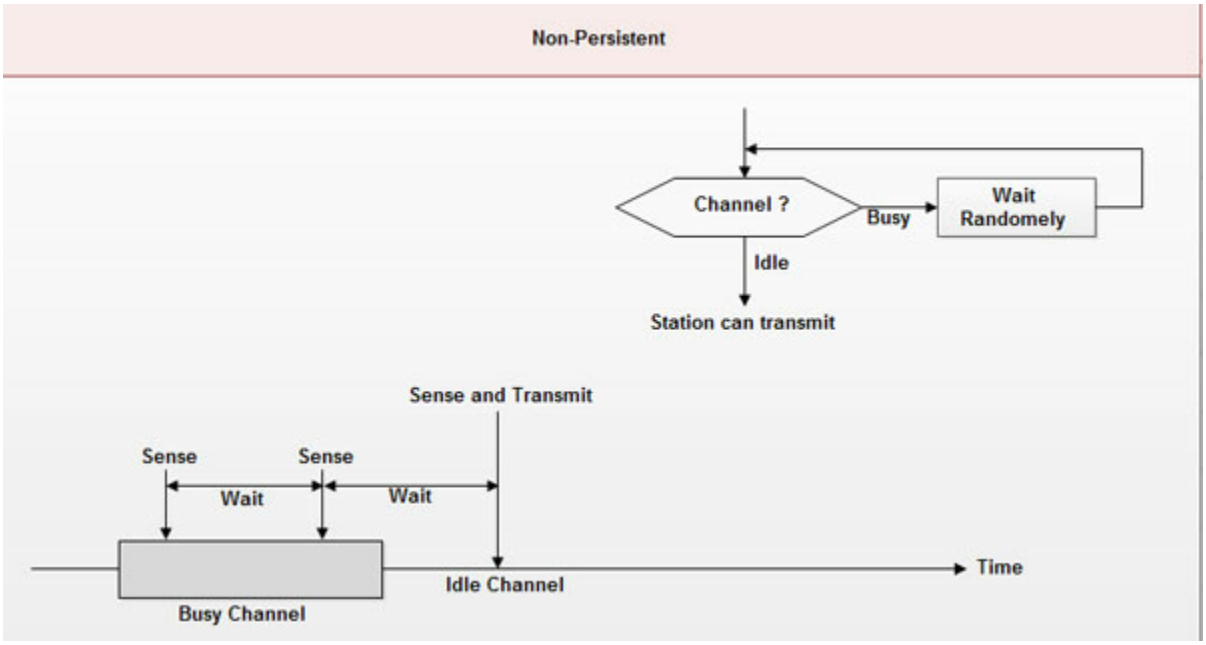
• In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantage of non-persistent

• It reduces the chance of collision because the stations wait a random amount of time. It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Disadvantage of non-persistent

• It reduces the efficiency of network because the channel remains idle when there may be stations with frames to send. This is due to the fact that the stations wait a random amount of time after the collision.



(iii) p-persistent CSMA

• This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.

• Whenever a station becomes ready to send, it senses the channel.

• If channel is busy, station waits until next slot.

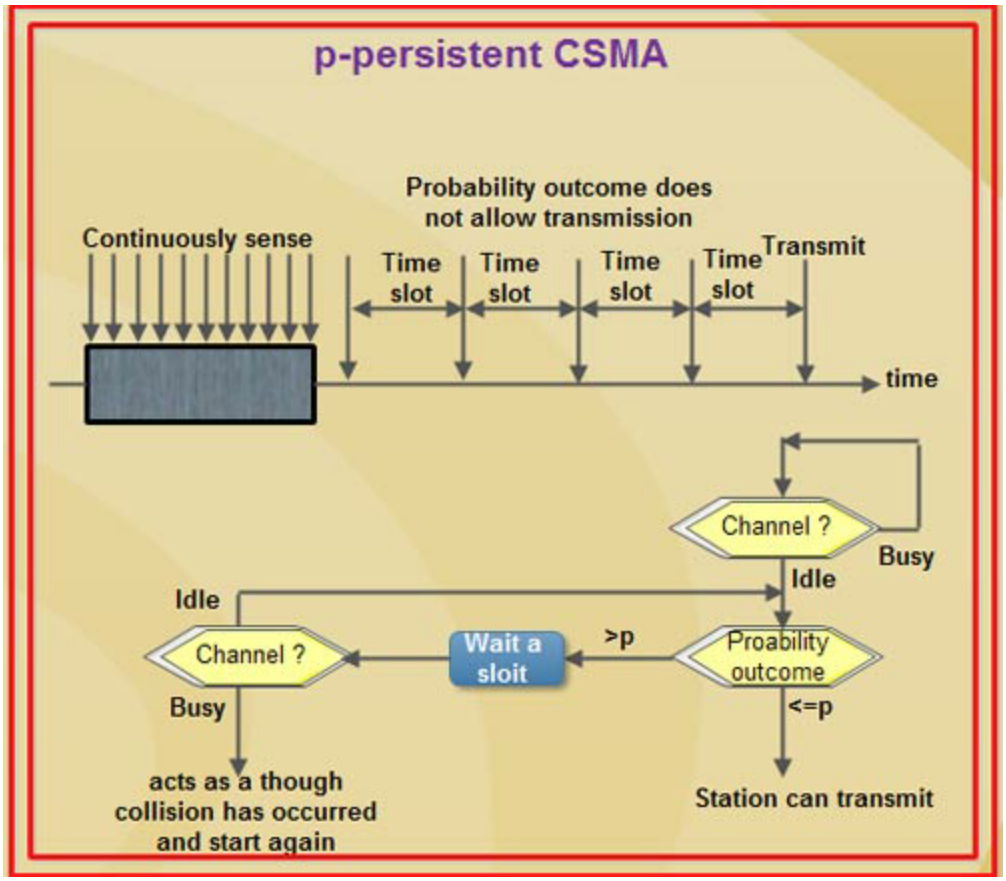
• If channel is idle, it transmits with a probability p.

• With the probability q=l-p, the station then waits for the beginning of the next time slot.

• If the next slot is also idle, it either transmits or waits again with probabilities p and q.

• This process is repeated till either frame has been transmitted or another station has begun transmitting.

• In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.



Advantage of p-persistent

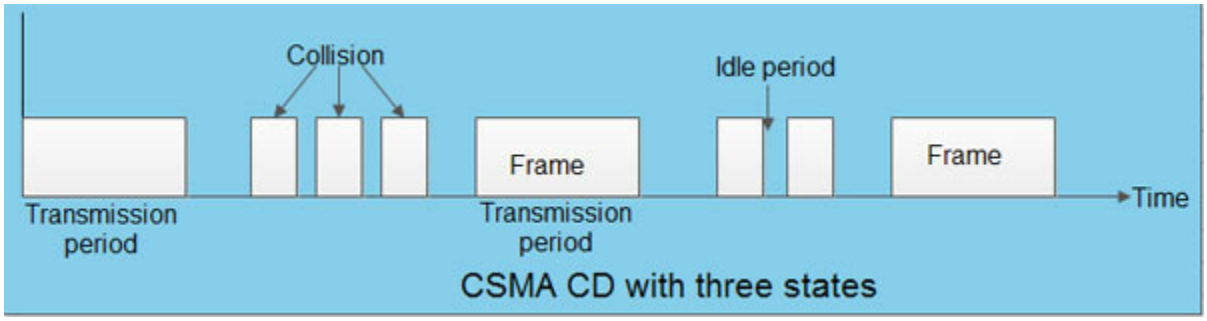
• It reduces the chance of collision and improves the efficiency of the network.

CSMA/CD

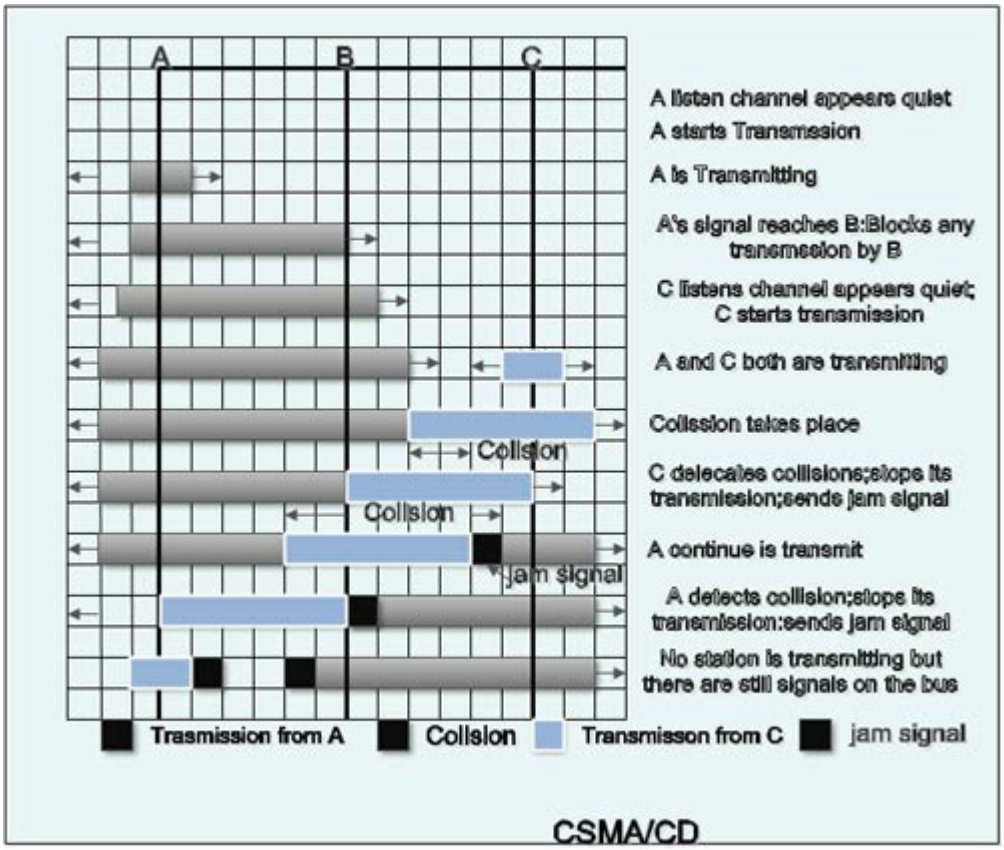
- To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA / CD):
- CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA.
- If the channel is busy, the station waits. it listens at the same time on communication media to

ensure that there is no collision with a packet sent by another station.

- In a collision, the issuer immediately cancel the sending of the package. This allows to limit the duration of collisions: we do not waste time to send a packet complete if it detects a collision.
- After a collision, the transmitter waits again silence and again, he continued his hold for a random number; but this time the random number is nearly double the previous one: it is this called back-off (that is to say, the "decline") exponential.
- In fact, the window collision is simply doubled (unless it has already reached a maximum). From a packet is transmitted successfully, the window will return to its original size.
- Again, this is what we do naturally in a meeting room if many people speak exactly the same time, they are realizing account immediately (as they listen at the same time they speak), and they interrupt without completing their sentence. After a while, one of them speaks again.
- If a new collision occurs, the two are interrupted again and tend to wait a little longer before speaking again.

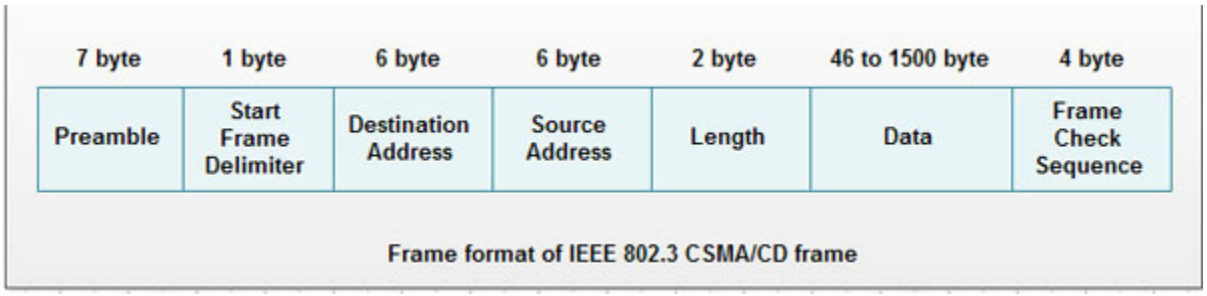


The entire scheme of CSMA/CD is depicted in the fig.



Frame format of CSMA/CD

The frame format specified by IEEE 802.3 standard contains following fields.



7 byte	1 byte	6 byte	6 byte	2 byte	46 to 1500 byte	4 byte
Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	Data	Frame Check Sequence

Frame format of IEEE 802.3 CSMA/CD frame

1. **Preamble**: It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating Os and 1s. The purpose is to provide alert and timing pulse.

2. **Start Frame Delimiter (SFD)**: It is one byte field with unique pattern: 10 10 1011. It marks the beginning of frame.

3. **Destination Address (DA)**: It is six byte field that contains physical address of packet's destination.

4. **Source Address (SA)**: It is also a six byte field and contains the physical address of source or last device to forward the packet (most recent router to receiver).

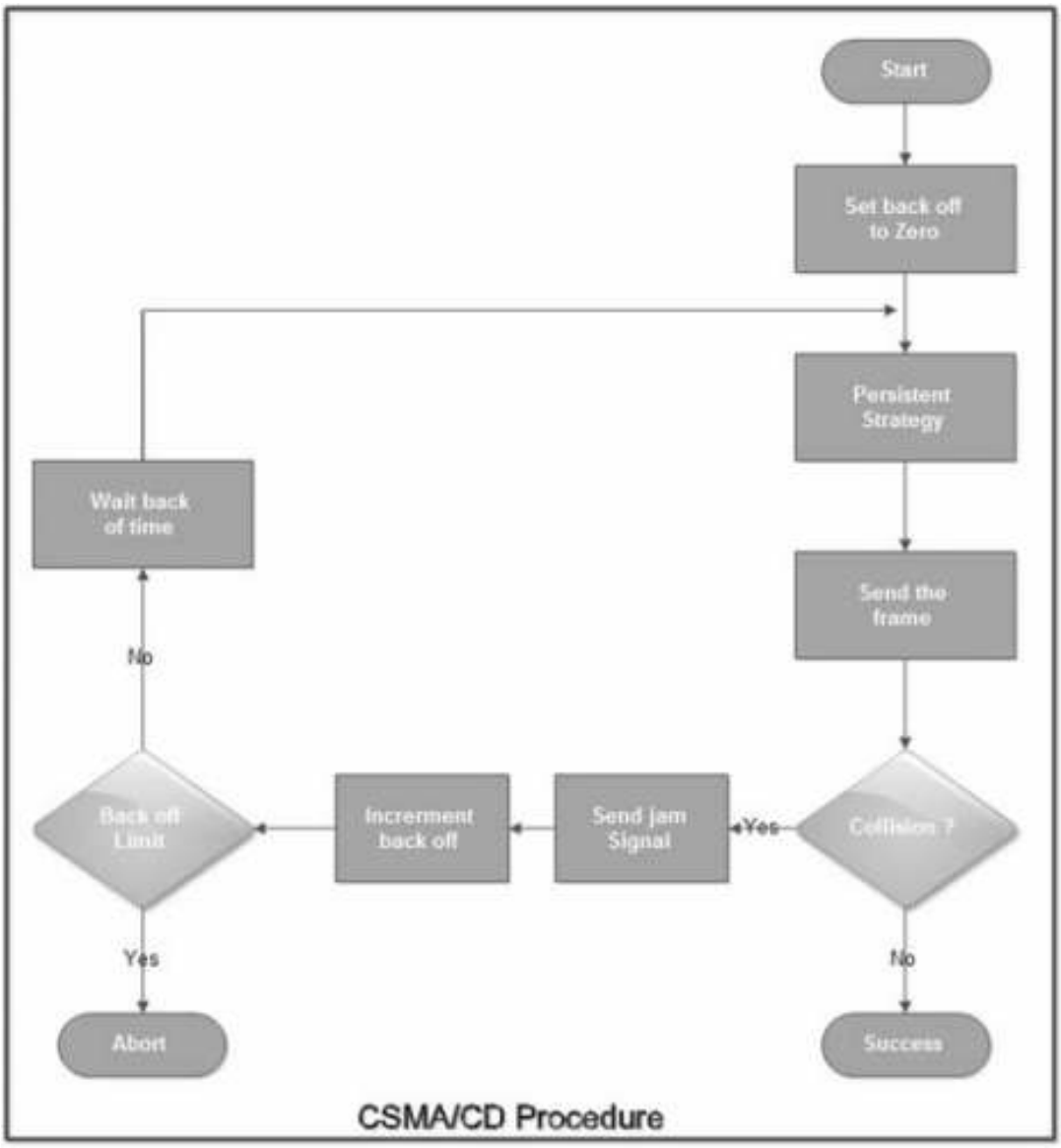
5. **Length**: This two byte field specifies the length or number of bytes in data field.

6. **Data**: It can be of 46 to 1500 bytes, depending upon the type of frame and the length of the information field.

7. **Frame Check Sequence (FCS)**: This for byte field contains CRC for error detection.

CSMA/CD Procedure:

Fig. Shows a flow chart for the *CSMA/CD* protocol.



CSMA/CD Procedure

Explanation:

• The station that has a ready frame sets the back off parameter to zero.

• Then it senses the line using one of the persistent strategies.

• If then sends the frame. If there is no collision for a period corresponding to one complete frame, then the transmission is successful.

• Otherwise the station sends the jam signal to inform the other stations about the collision.

• The station then increments the back off time and waits for a random back off time and sends the frame again.

• If the back off has reached its limit then the station aborts the transmission.

• *CSMA/CD* is used for the traditional Ethernet.

• *CSMA/CD* is an important protocol. IEEE 802.3 (Ethernet) is an example of *CSMNCD.* It is an international standard.

Ethernet

Ethernet(pronounced "eether net") is a local area network, connecting computers together with cables so the computers can share information.

Within each main branch of the network, Ethernet can connect up to 1,024 personal computers and workstations.

In effect

• most landlines are sold with an installed Ethernet network adapter but not a WiFi card;

• reliability and throughput of a wired network are far superior to WiFi;

• securing the network is wired trivial since there will be nothing really configure, or at most a firewall (or firewall) and antivirus. It will be complex secure the wireless network.

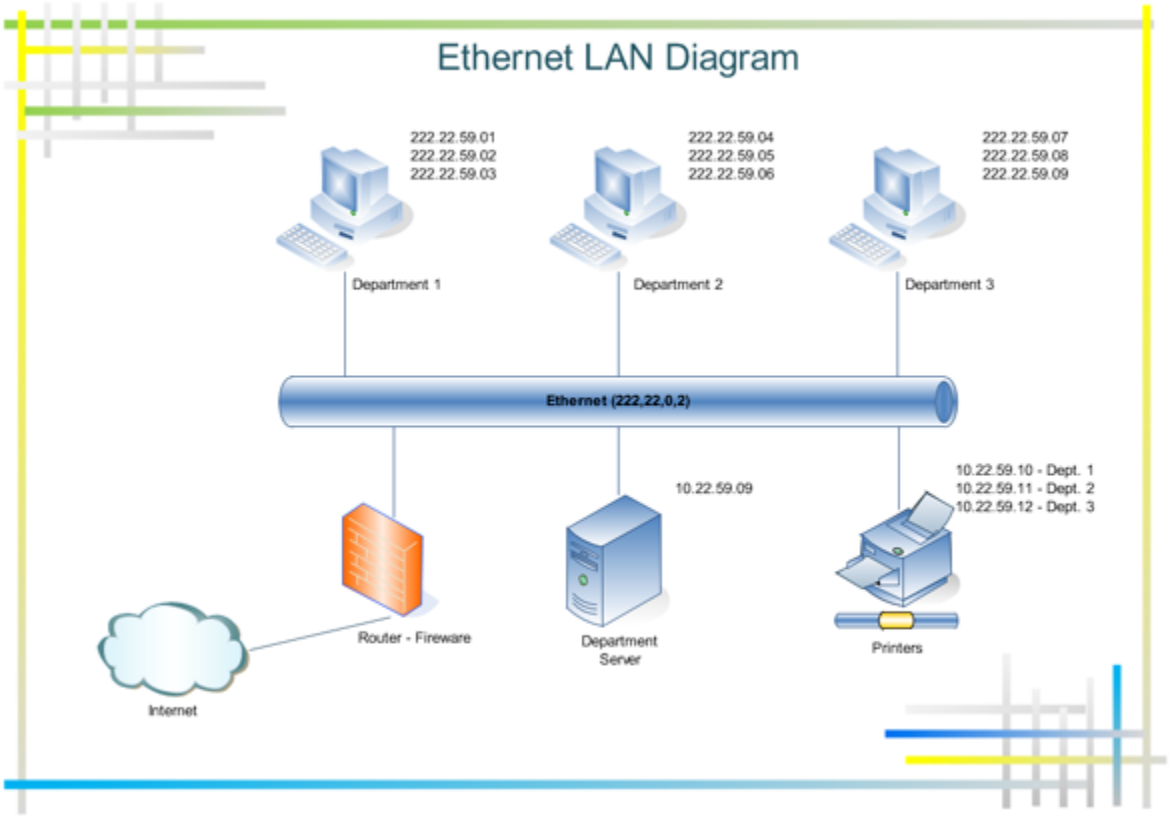
Switching of Ethernet gave birth to two types Half Duplex and Full Duplex Ethernet.

Auto detection mechanism

It also has the mechanism of auto detection which is built in with the ability to assess of rate of exchange; also it decides with which mode of transmission it will go Full Duplex or Half.

In Full Duplex, the data can be sent and received at the same time. The reception and transmission takes place simultaneously and hence the speed of data transfer increases. The data travels between source node and destination node. There is no occurrence of collision when it comes to full duplex Ethernet

The speeds of the Ethernet Network differ and continue to evolve in their own ways with the hike of technology. Rate of transmission of data differ in 10Base2, 10base5, 10BaseT and 10Base TX owing to the speed variation, wire material been used and the length of the transmission wire transmitting the signals and information.



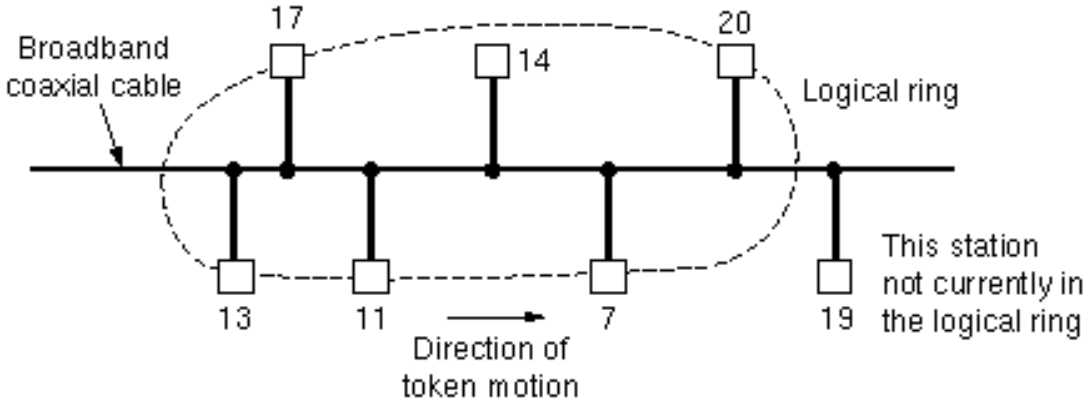
Token Bus :

- In token bus network station must have possession of a token before it can transmit on the network.
- The IEEE 802.4 Committee has defined token bus standards as broadband networks, as opposed to Ethernet's baseband transmission technique.
- The topology of the network can include groups of workstations connected by long trunk cables.
- These workstations branch from hubs in a star configuration, so the network has both a bus and star topology.
- Token bus topology is well suited to groups of users that are separated by some distance.
- IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology.
- The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

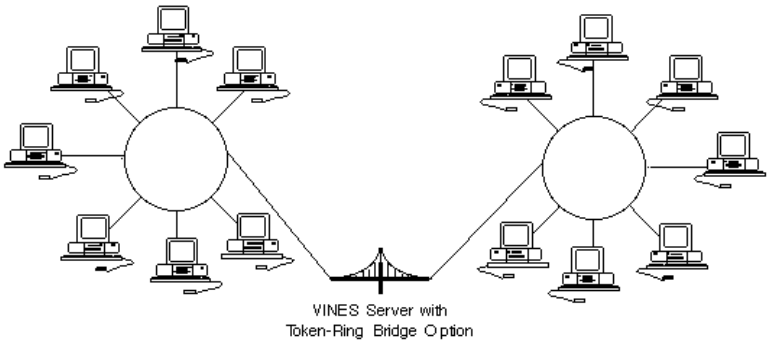
- The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring.

- The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.

- While token bus is used in some manufacturing environments, Ethernet and token ring standards have become more prominent in the office environment.

- 

Two token Ring with Bridge Option

- 

Network Interfacing Devices

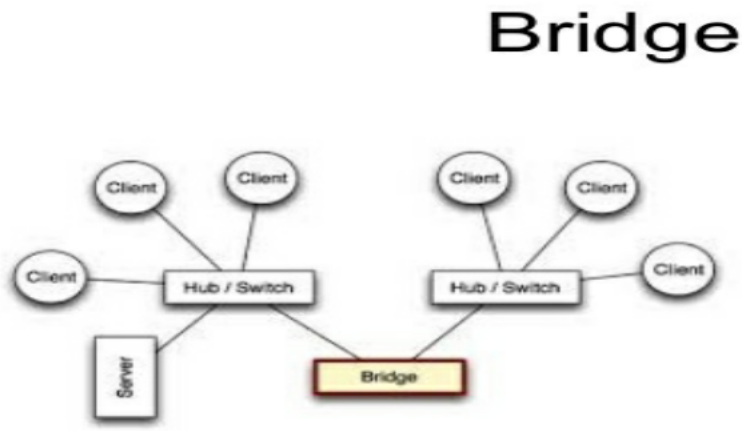
Hubs/Repeaters are used to connect together two or more network segments of any media type. In larger design, signal quality begins to deteriorate as segment exceeds their maximum length. A hub provides the signal amplification required to allow a segment to be extended a greater distance.

Passive hub simply forwards any data packets they receive over one port from one workstation to all their

remaining ports. Active hubs, also sometimes referred to as "multiport repeaters", regenerate the data bits in order to maintain a strong signal.

Bridges: The bridge function is to connect separate homogeneous networks. Bridges map the Ethernet address of the nodes residing on each network segment and allow only necessary traffic to pass through the bridge. When a packet is received by the bridge, the bridge determines the destination and source segments.

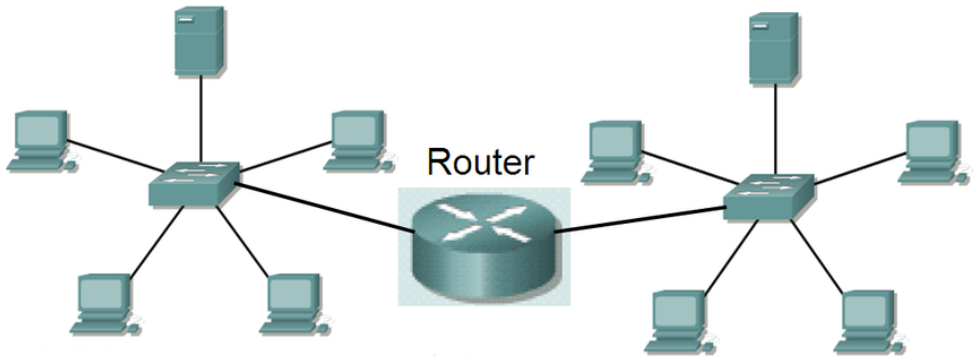
If the segments are different, then the packet is "forwarded" to the correct segment. Bridges are also called "store-and-forward" device because they look at the whole Ethernet packet before making filtering or forwarding decisions.



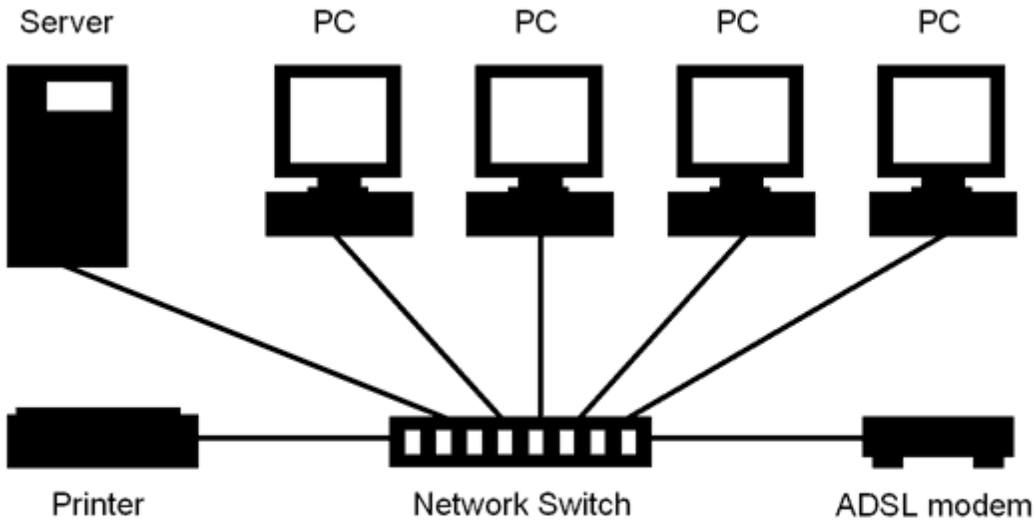
Router: Routing achieved commercially popularity in the mid – 1980s – at a time when large-scale Internetworking began to replace the fairly simple, homogeneous environments. Routing is the act of moving information across an Internetwork from a source to a destination. It is often contrasted with bridging, which perform a similar function.

Routers use information within each packet to route it from one LAN to another, and communicate with each other and share information that allows them to determine the best route through a complex

network of many LANs.



Switches: LAN switches are an expansion of the concept in LAN bridging, which controls data flow, handles transmission errors, provides physical addressing, and manages access to the physical medium. Switches provide these functions by using various link-layer protocols. LAN switches can link four, six, ten or more networks together. A store-and-forward switch, on the other hand, accepts and analyses the entire packet before forwarding it to its destination.

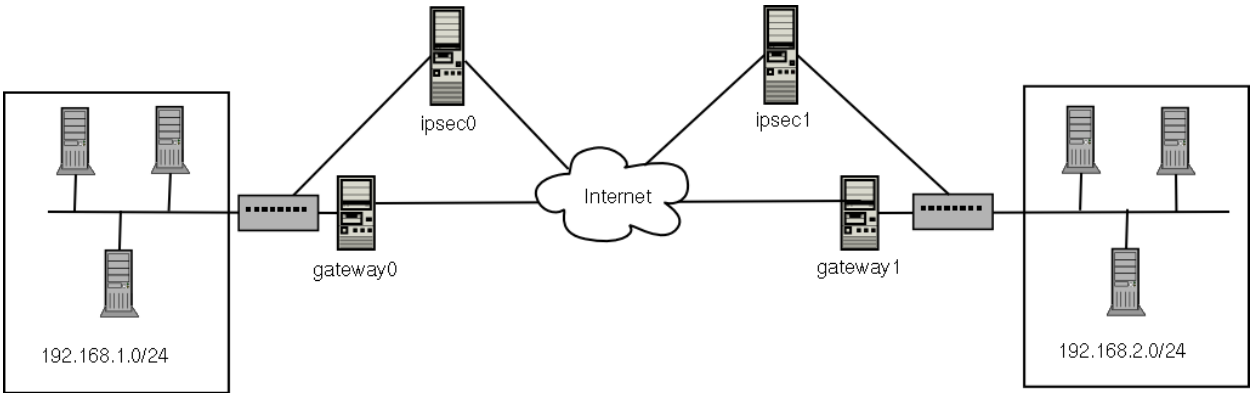


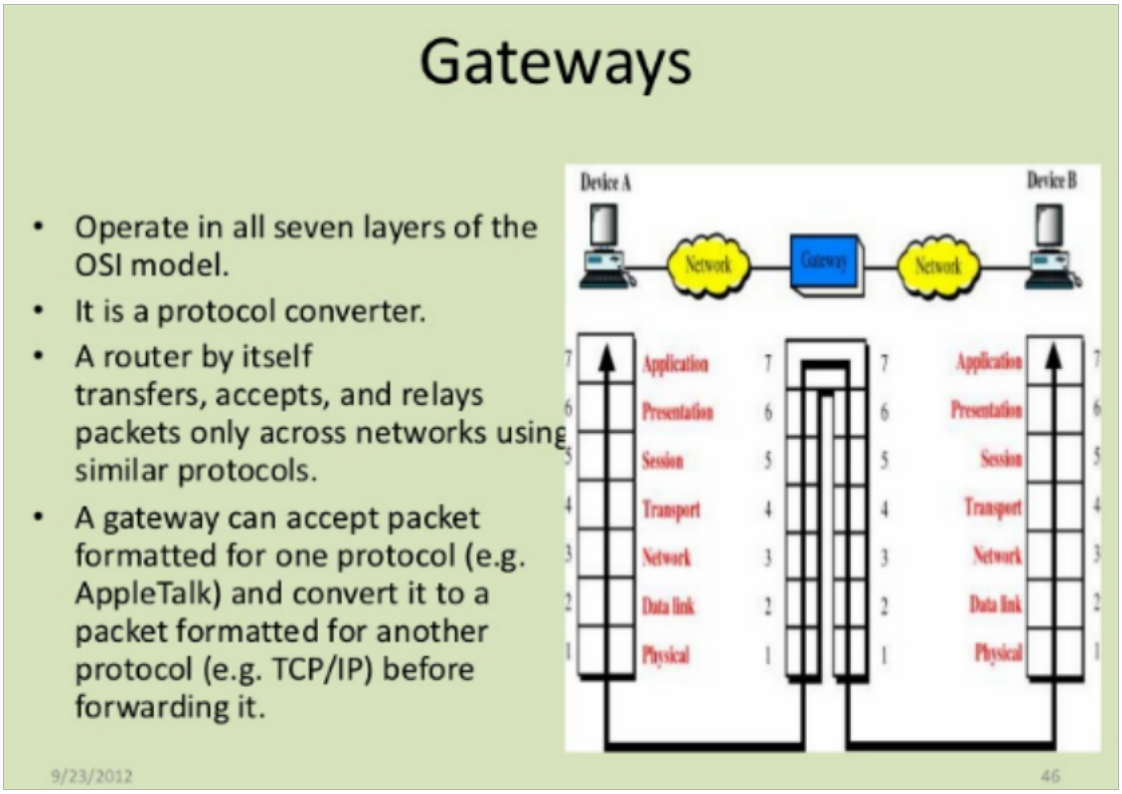
Example 1: A wired client-server network

Gateway: A computer that controls the traffic of your LAN or your ISP receives is a Gateway. A server serves as a Gateway, the gateway also works as a firewall and a proxy server. A Gateway is a device such as a mini or microcomputer capable of operating on a stand alone basis but which also provides connection for communication with the other computers and access to shared resources.

Normally a gateway is associated with a router. A router is a device that lets you know the next network data should be sent to next. A router can be connected to more than one network at a time. A gateway is

associated with a router because a router which uses headers and forwarding tables to figure out where packets or data is sent provides the path through which information is sent in and out a gateway.





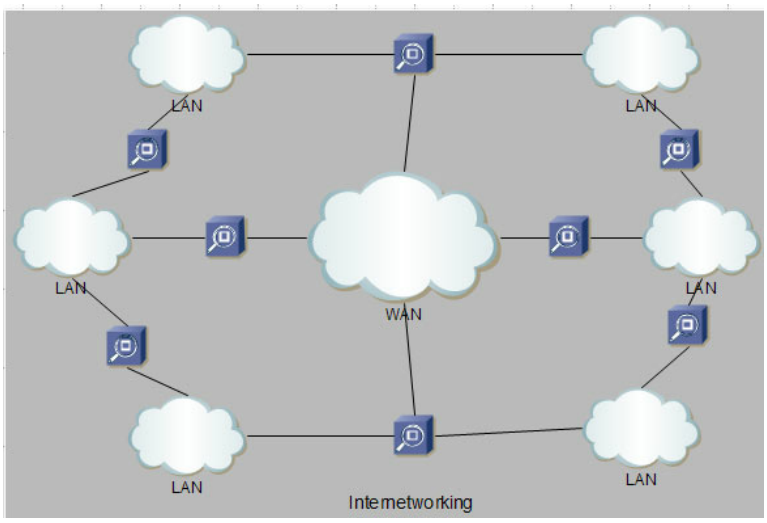
MUDULE 5

MUDULE 5

Internetworking

In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking.

- Internetworking started as a way to connect disparate types of computer networking technology.
- Computer network term is used to describe two or more computers that are linked to each other.
- When two or more computer networks or computer network segments are connected using devices such as a router then it is called as computer internetworking.
- Internetworking is a term used by Cisco. Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or Internetworking.
-



There are three variants of internetwork or **Internetworking**, depending on who administers and who participates in them :

1. **Extranet**
2. **Intranet**
3. **Internet**

Extranet :

An extranet is a **network of internetwork or Internetworking** that is limited in scope to a **single organisation or entity** but which also has **limited connections** to the networks of one or more other usually, but not necessarily, trusted organizations or entities .

Technically, an **extranet may also be categorized as a MAN, WAN**, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

Intranet :

An intranet is a set of **interconnected networks or Internetworking**, using the I**nternet Protocol** and uses **IP-based tools** such as **web browsers** and **ftp tools**, that is under the control of a **single administrative entity.** T

hat administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise. A large intranet will typically have its **own web server** to provide users with browseable information.

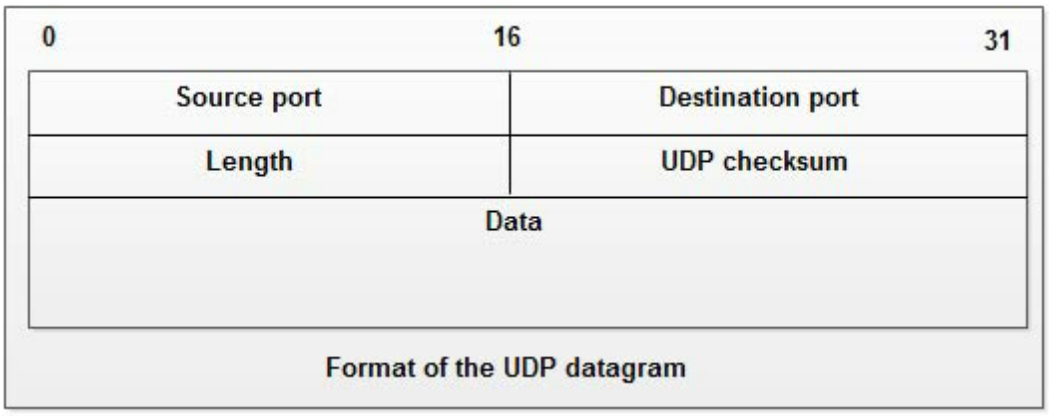
Internet : A specific **Internetworking**, consisting of a **worldwide interconnection** of governmental, academic, public, and private networks based upon the Advanced Research Projects Agency Network (**ARPANET)** developed by ARPA of the U.S. **Department of Defense** also **home** to the **World Wide Web (WWW)** and referred to as the '**Internet**' with a capital 'I' to distinguish it from other generic internetworks. Participants in the Internet, or their service providers, use IP Addresses obtained from address registries that control assignments.

Datagrams

A datagram is a unit of transfer assoicated with networking. A datagram has the following characteristics:

- Data is transmitted from source to destination without guarantee of delivery
- Data is frequently divided into smaller pieces and transmitted without a defined route or guaranteed order of delivery

General format of a Datagram packet



Format of the UDP datagram

Following is a brief description of each field:

Source Port This is the port number of the application that is originating the user data.

Destination Port This is the port number pertaining to the destination application.

Length This field describes the total length of the UDP datagram, including both data and header

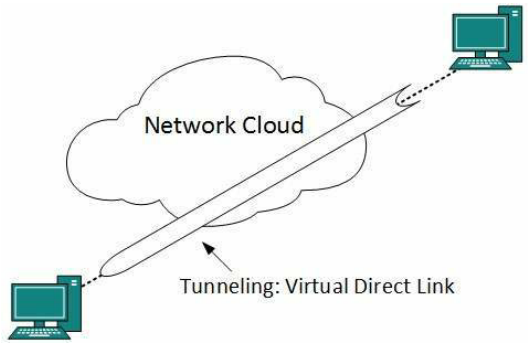
Information.

UDP Checksum Integrity checking is optional under UDP. If turned on, both ends of the communications channel use this field for data integrity checks.

Tunneling

If they are two geographically separate networks, which want to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.

Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends.



When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel its tag is removed and delivered to the other part of the network.

Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.

Packet Fragmentation

- Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes.
- A data packet can have more or less packet length depending upon the application.
- If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally.
- If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.
- If a packet with DF (don't fragment) bit set to 1 comes to a router which can not handle the packet because of its length, the packet is dropped.

- When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way.
- If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

Routing

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes.

A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination,

Types of Routing

- **Distance Vector Routing Protocol**

  Distance Vector is simple routing protocol which takes routing decision on the number of hops between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build up their network topology based on the advertisements of their peer routers,

  For example Routing Information Protocol (RIP).

- **Link State Routing Protocol**

  Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the states of links of all the routers in a network. This technique helps routes build a common graph of the entire network. All routers then calculate their best path for routing purposes .for example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS).

Distance Vector Routing

Distance Vector Routing is one of the two types of routing protocols in which each router informs its

neighbor of its routing table.

Distance Vector protocols judge best path on how far the objective is. Distance can be leaps or a combination of metrics calculated to represent the distance value.

Routing Information Protocol (RIP v1 and v2) and Interior Gateway Routing Protocol (IGRP C developed by Cisco) are some of the IP Distance Vector routing protocols which are still being used.

A very simple distance-vector routing protocol works as follows:

1. A first, the router makes a list of which networks are achievable for it, and how many hops it will cost. In this way two or more networks are connected to this router. There would be only one hop for this network. This table is known as routing table.

2. Secondly the routing table is joint with other routers on each of the connected networks through some particular inter-router protocol. This data is only joint in between physically connected routers, so routers on other networks are not accessed by the new routing tables yet.

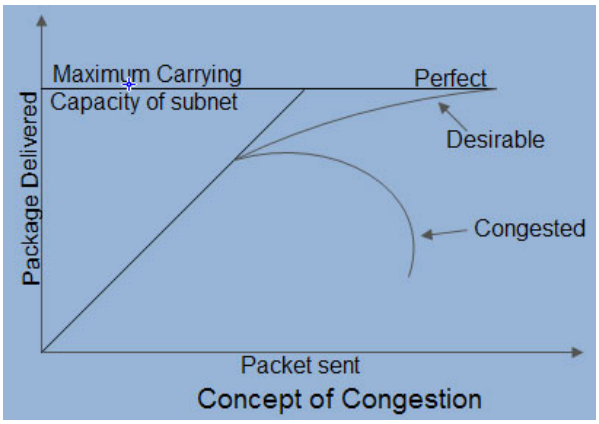
3. The new routing table is made originating on the directly configured network interfaces with the inclusion of the new information received from all the other routers.

4. All the corrupt routing paths are then cleansed out from the newly made routing table. If there are two similar paths to the same network then only the one with the smallest and the briefest hop-count is kept.

What is Congestion Control?

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.)

In other words when too much traffic is offered, congestion sets in and performance degrades sharply

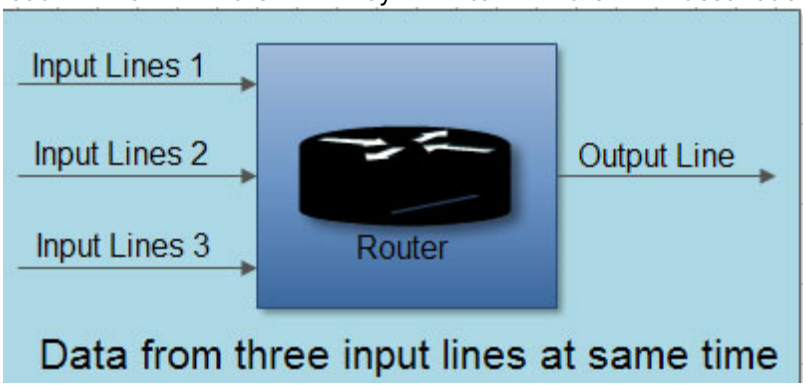


Concept of Congestion

Causing of Congestion:

The various causes of congestion in a subnet are:

1.The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the problem. This is because, by the time packets reach front of the queue, they have already timed out (as they waited the queue). When timer goes off source transmits duplicate packet that are also added to the queue. Thus same packets are added again and again, increasing the load all the way to the destination.



2.The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).

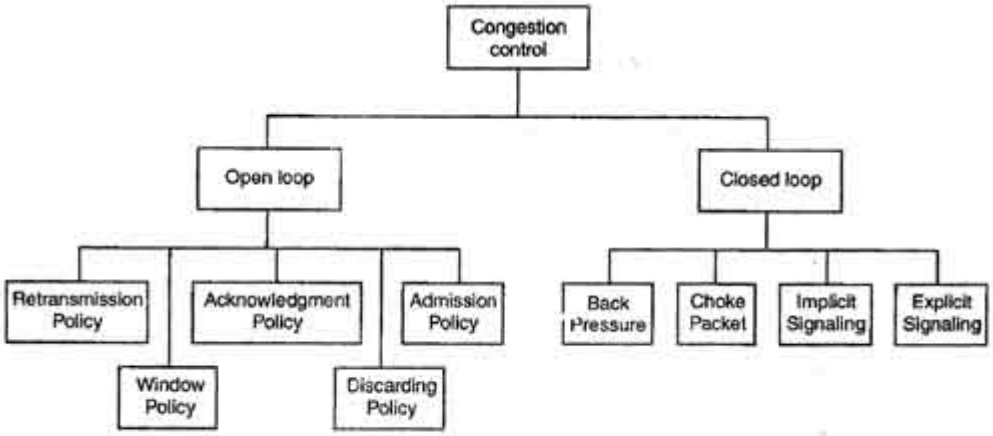
3.The routers' buffer is too limited.

4.Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.

5.Congestion is also caused by slow links. This problem will be solved when high speed links are used. But it is not always the case. Sometimes increase in link bandwidth can further deteriorate the congestion problem as higher speed links may make the network more unbalanced.Congestion can make itself worse. If a route!" does not have free buffers, it start ignoring/discarding the newly arriving packets. When these packets are discarded, the sender may retransmit them after the timer goes off. Such packets are transmitted by the sender again and again until the source gets the acknowledgement of these packets. Therefore multiple transmissions of packets will force the congestion to take place at the sending end.

How to correct the Congestion Problem:

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



Types of Congestion Control Methods

These two categories are:

1. Open loop

2. Closed loop

Open Loop Congestion Control

• In this method, policies are used to prevent the congestion before it happens.

• Congestion control is handled either by the source or by the destination.

• The various methods used for open loop congestion control are:

1. Retransmission Policy

• The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.

• However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.

• The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

2. Window Policy

• To implement window policy, selective reject window method is used for congestion control.

• Selective reject method sends only the specific lost or damaged packets.

3. Acknowledgement Policy

• The acknowledgement policy imposed by the receiver may also affect congestion.

• If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.

• Acknowledgments also add to the traffic load on the network. Thus, by sending fewer acknowledgements we can reduce load on the network.

4. Discarding Policy

• A router may discard less sensitive packets when congestion is likely to happen.

• Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.

5. Admission Policy

• An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual circuit networks.

• Switches in a flow first check the resource requirement of a flow before admitting it to the network.

• A router can deny establishing a virtual circuit connection if there is congestion in the "network or if there is a possibility of future congestion.

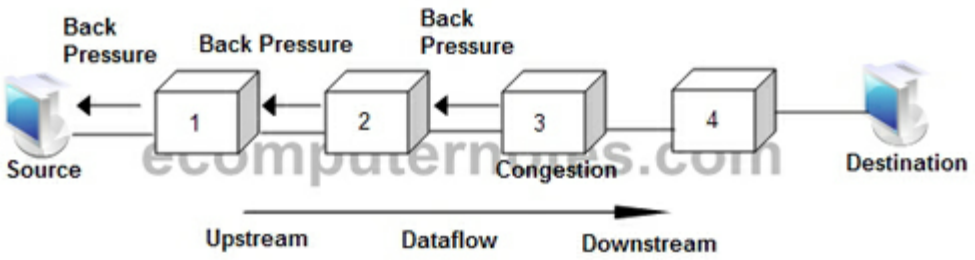
Closed Loop Congestion Control

• Closed loop congestion control mechanisms try to remove the congestion after it happens.

• The various methods used for closed loop congestion control are:

1. Backpressure

• Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.



Backpressure Method

• The backpressure technique can be applied only to virtual circuit networks. In such virtual circuit each node knows the upstream node from which a data flow is coming.

• In this method of congestion control, the congested node stops receiving data from the immediate upstream node or nodes.

• This may cause the upstream node on nodes to become congested, and they, in turn, reject data from their upstream node or nodes.

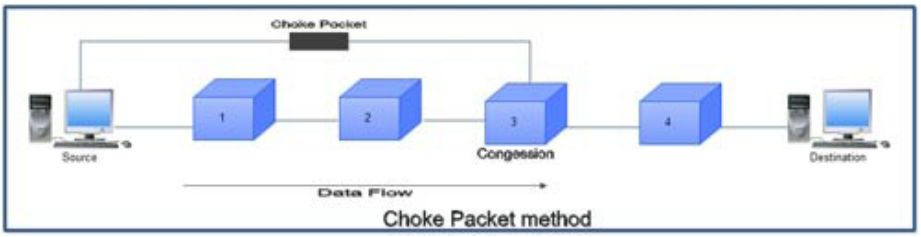
• As shown in fig node 3 is congested and it stops receiving packets and informs its upstream node 2 to slow down. Node 2 in turns may be congested and informs node 1 to slow down. Now node 1 may create congestion and informs the source node to slow down. In this way the congestion is alleviated. Thus, the pressure on node 3 is moved backward to the source to remove the congestion.

2. Choke Packet

• In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.

• Here, congested node does not inform its upstream node about the congestion as in backpressure method.

• In choke packet method, congested node sends a warning directly to the source station *i.e.* the intermediate nodes through which the packet has traveled are not warned.



Choke Packet method

3. Implicit Signaling

• In implicit signaling, there is no communication between the congested node or nodes and the source.

• The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.

• On sensing this congestion, the source slows down.

• This type of congestion control policy is used by TCP.

4. Explicit Signaling

• In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.

• Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data .

• Explicit signaling can occur in either the forward direction or the backward direction .

• In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down.

• In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.

Congestion control algorithms

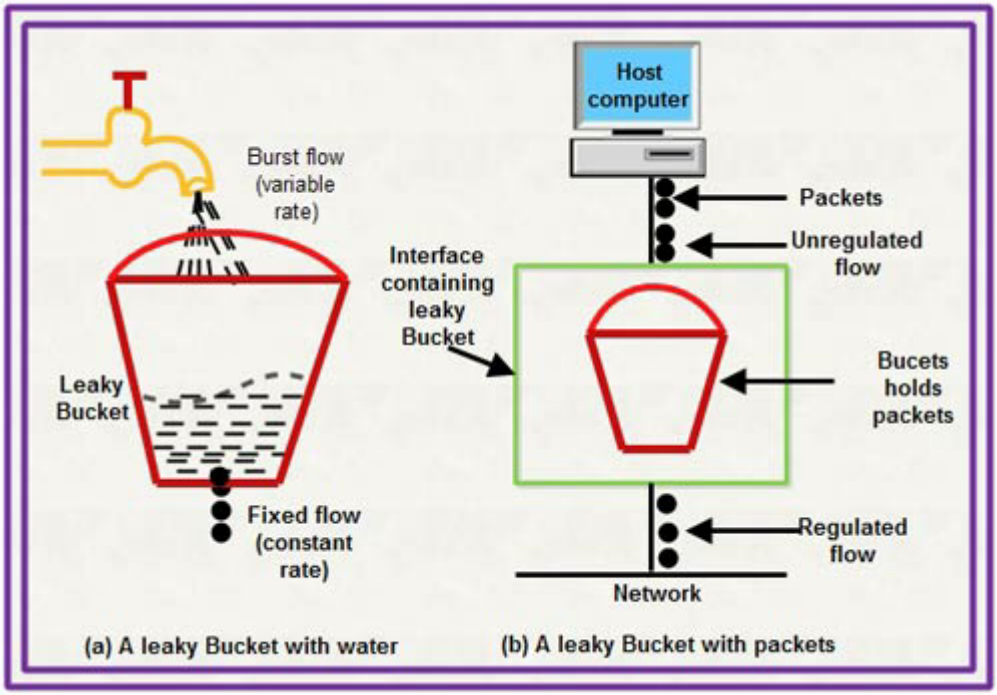
1. Leaky Bucket Algorithm

• It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.

• A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.

• Imagine a bucket with a small hole at the bottom.

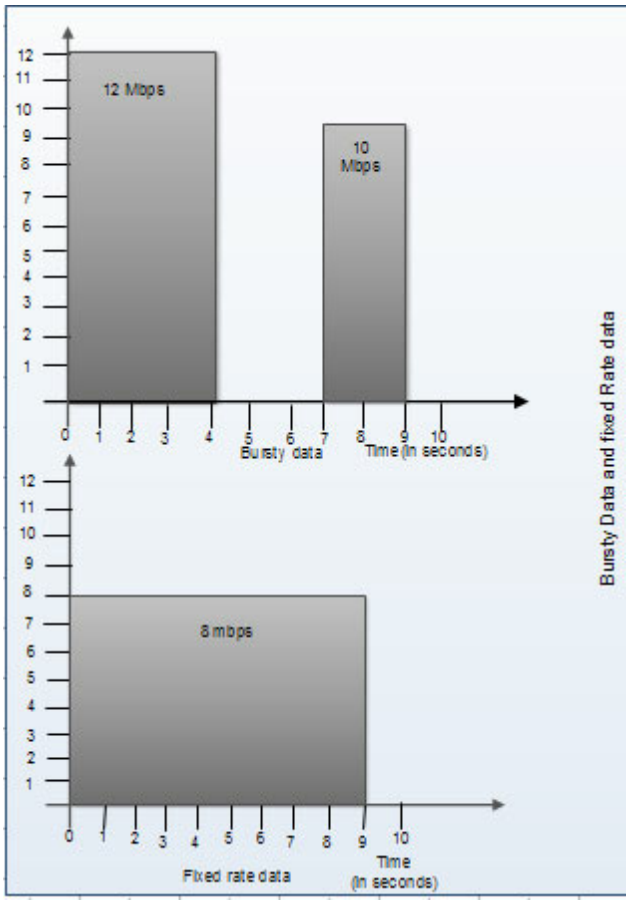
• The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate. Thus (as long as water is present in bucket), the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.



• Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.

• The same concept can be applied to packets in the network. Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 12 Mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 10 Mbps for 2 seconds. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.

If a leaky bucket algorithm is used, the data flow will be 8 Mbps for 9 seconds. Thus constant flow is maintained.


12 Mbps
10 Mbps
Bursty data
Time (In seconds)
8 mbps
Fixed rate data
Time (In seconds)
Bursty Data and fixed Rate data

Edit	TCP	UDP
Acronym for	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Use by other protocols	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.

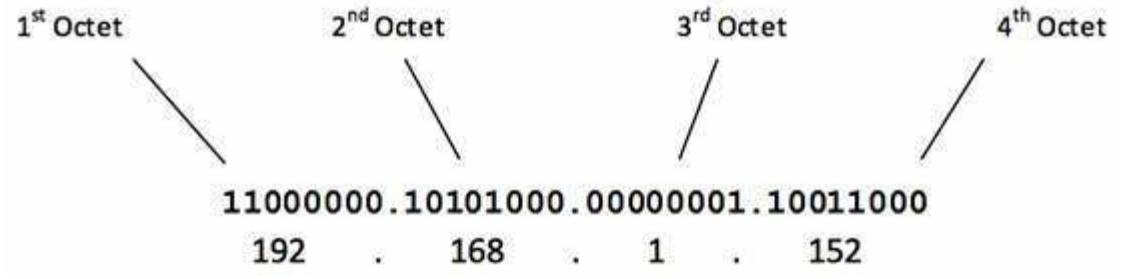
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.
Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.

IP Address

IP address is a unique logical address assigned to a machine over the network. An IP address exhibits the following properties:

- IP address is the unique address assigned to each host present on Internet.
- IP address is 32 bits (4 bytes) long.
- IP address consists of two components: **network component** and**host component**.
- Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example 137.170.4.124

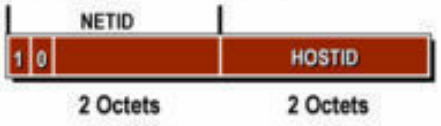
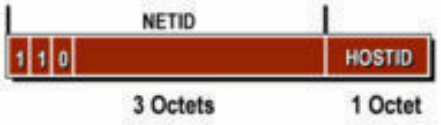
- The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



- The number of networks and the number of hosts per class can be derived by this formula:

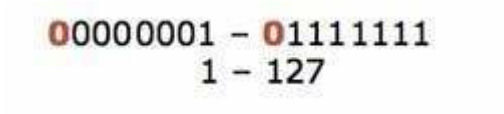
Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits – 2

- When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class	First Octet Range	Max Hosts	Format
A	1-126	16M	
B	128-191	64K	
C	192-223	254	
D	224-239	N/A	
E	240-255	N/A	

Class A Address

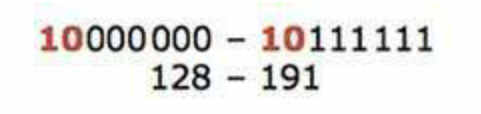
The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.



Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

Class B Address

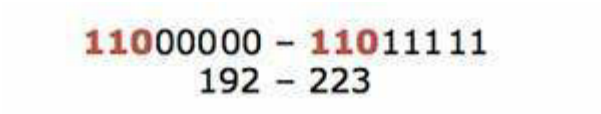
An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.



Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class C Address

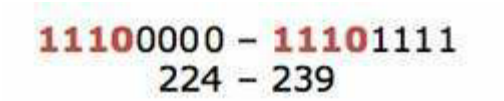
The first octet of Class C IP address has its first 3 bits set to 110, that is:



Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:



Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

DNS

Domain Name System helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

Domain Name System Architecture

The Domain name system comprises of **Domain Names, Domain Name Space, Name Server** that have been described below:

Domain Names

Domain Name is a symbolic string associated with an IP address. There are several domain names available; some of them are generic such as **com, edu, gov, net** etc, while some country level domain names such as **au, in, za, us** etc.

The following table shows the **Generic** Top-Level Domain names:

Domain Name	**Meaning**
Com	Commercial business

Edu	Education
Gov	U.S. government agency
Int	International entity
Mil	U.S. military
Net	Networking organization
Org	Non profit organization

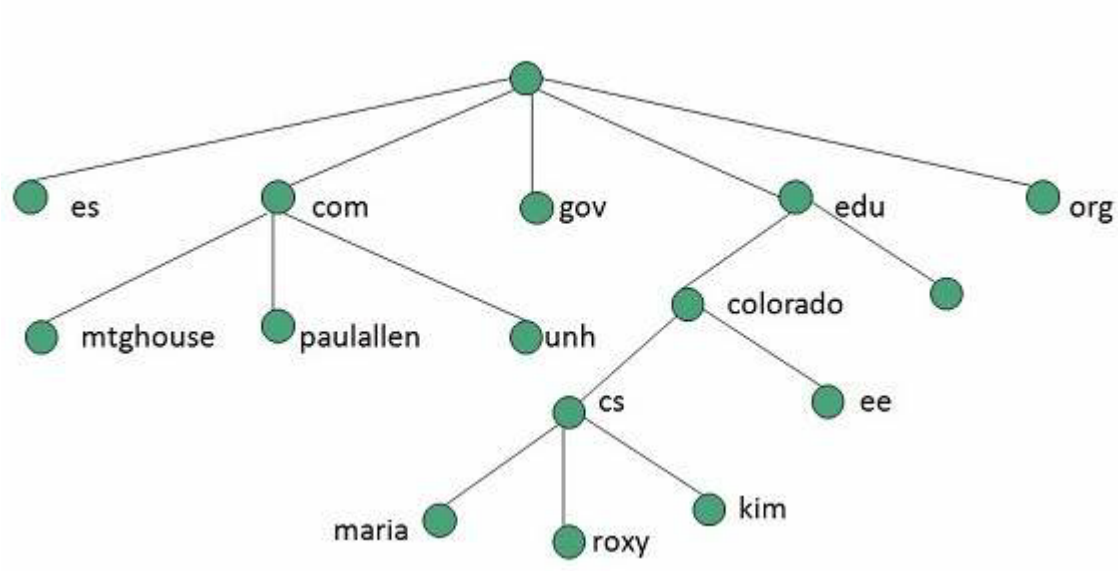
The following table shows the **Country top-level** domain names:

Domain Name	**Meaning**
au	Australia
in	India
cl	Chile
fr	France
us	United States
za	South Africa
uk	United Kingdom

jp	Japan
es	Spain
de	Germany
ca	Canada
ee	Estonia
hk	Hong Kong

Domain Name Space

The domain name space refers a hierarchy in the internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy:



In the above diagram each subtree represents a domain. Each domain can be partitioned into sub domains and these can be further partitioned and so on.

Name Server

Name server contains the DNS database. This database comprises of various names and their corresponding IP addresses. Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.

- Hierarchy of server is same as hierarchy of names.
- The entire name space is divided into the zones

DNS Working

DNS translates the domain name into IP address automatically. Following steps will take you through the steps included in domain resolution process:

- When we type **www.facebook.com** into the browser, it asks the local DNS Server for its IP address.

  Here the local DNS is at ISP end.

- When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
- The root DNS server replies with delegation that **I do not know the IP address of www. facebook.com but know the IP address of DNS Server.**
- The local DNS server then asks the com DNS Server the same question.
- The **com** DNS Server replies the same that it does not know the IP address of www. **facebook**.com but knows the address of facebook.com.
- Then the local DNS asks the facebook.com DNS server the same question.
- Then facebook.com DNS server replies with IP address of www.facebook.com.

- Now, the local DNS sends the IP address of www.facebook.com to the computer that sends the request.

What is FTP?

- One of the most popular uses of the Internet is to download files - that is, transfer files from a computer on the Internet to your computer.
- Many thousands of files are downloaded every day from the Internet. Most of these files are downloaded using the Internet's File Transfer Protocol, commonly referred to as FTP.
- This protocol can also be used to upload files from your computer to another computer on the Internet.
- File Transfer Protocol is a standard network protocol used to exchange and manipulate files over a TCP/IP-based network, such as the Internet.
- FTP is built on client-server architecture

Features of FTP

The basic features of FTP are:

1. Data representation

• FTP handles three types of data representations-ASCII (7 bit), EBCDIC (8-bit) and 8-binary data.

• The **ASCII file** is the default format for transferring text files

2. File organization and Data structures

• FTP supports both unstructured and structured file.

4. Error control

• Since TCP is used for data transfer no additional error recovery mechanism is required.

5. Access control

• File access protection is done using login procedure with login name and password.

FTP operation

• FTP uses client/server model for communication.

• Two TCP connections are used for file transfer.

• On one connection control signals (commands and responses) are exchanged and the other connection is used for actual data transfer. These two connections are called control connection and data connection respectively.