CHAPTER 1

INTRODUCTION TO NETWORKING

1.1.Introduction to Computer Network

- **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the sharing of resources among various devices.

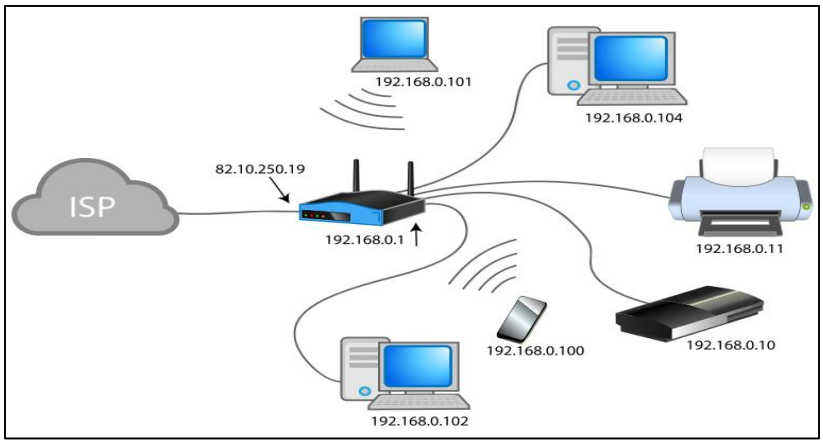


Figure 1. Computer Network Example

1.2.Network Application

- **Resource sharing**: Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model**: Computer networking is used in the server-client model. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium**: Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
- **E-commerce**: Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

1.3.Features of Computer network

- **Communication speed**: Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.
- **File sharing**: File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.
- **Back up and Roll back is easy**: Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

- **Software and Hardware sharing**: We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.
- **Security**: Network allows the security by ensuring that the user has the right to access the certain files and applications.
- **Scalability**: Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But, it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.
- **Reliability**: Computer network can use the alternative source for the data communication in case of any hardware failure.

1.4.Computer Network Architecture

- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.
- In simple terms, we can say that Computer Network Architecture is how computers are organized and how tasks are allocated to the computer.
- The two types of network architectures are used: Peer-To-Peer network and Client/Server network

1.4.1. Peer-To-Peer Network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

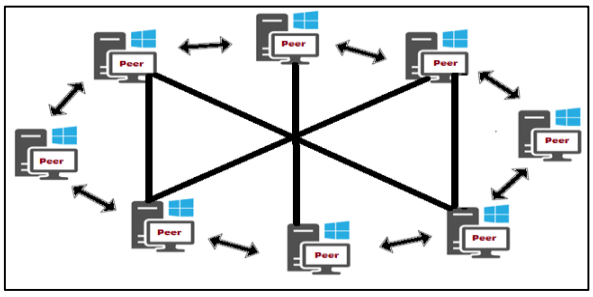


Figure 2. Peer-To-Peer Network

Advantages:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.

- It has a security issue as the device is managed itself.

1.4.2. Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a server while all other computers in the network are called clients.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

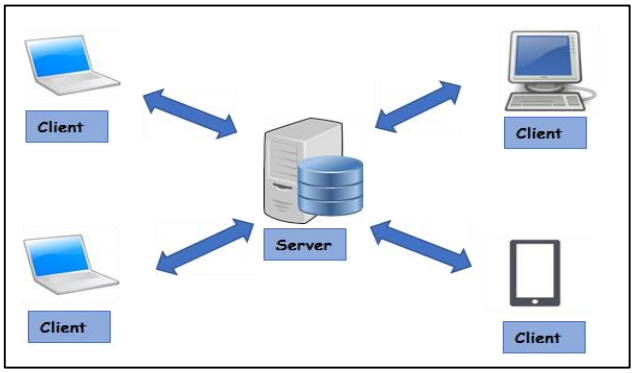


Figure 3. Client/Server Network

Advantages:

- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantage:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

1.5. Network Topology

- Topology defines the structure of the network of how all the components are interconnected to each other.
- Topology can be physical or logical.

1.5.1. Physical topology

- It indicates arrangement of different elements of a network.
- It reflects physical layout of devices and cables to a form a connected network.
- It is concerned with essentials of network ignoring minute details like transfer of data and device type.
- The pattern of arrangement of nodes (computers) and network cables depends on ease of installation and setup of the network.
- It affects cost and bandwidth capacity based on solution of devices.
- It takes into account placement of nodes and distance between them.
- Devices can be arranged to form a ring (Ring Topology) or linearly connected in a line called Bus Topology.

1.5.2. Logical Topology

- Logical Topology reflects arrangement of devices and their communication.
- It is the transmission of data over physical topology.
- It is independent of physical topology, irrespective of arrangements of nodes.
- It is concerned with intricate details of network like type of devices (switches, routers) chosen and their quality, which affect rate and speed of data packets delivery.
- The logical topology ensures optimal flow control that can be regulated within network.
- The data can either flow in a linear pattern called Logical bus or in form of a circle called Logical ring.

1.5.3. Types of Network Topology

1. Bus Topology

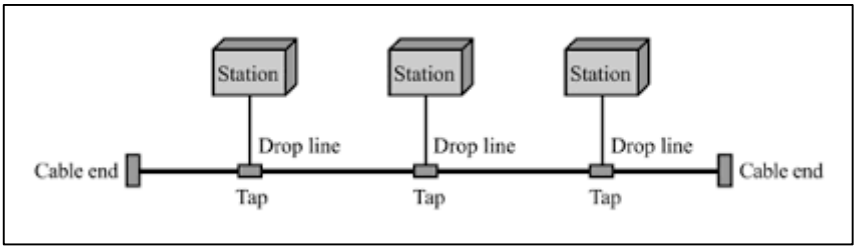


Figure 4. Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a **backbone cable**.
- Each node is either connected to the backbone cable by **drop line** or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (Ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.

- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).
- **CSMA**: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.
- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

Advantages of Bus topology:

- Bus topology is easy to install.
- Because of backbone, less cable is required.
- Number of I/O port required is less. Also the hardware is reduced.
- The backbone can be extended by using repeater.
- Cost of the network is low.

Disadvantages of Bus topology:

- Heavy network traffic can slow a bus considerably.
- Difficult for reconnection, fault isolation or troubleshooting.
- Difficult to add new node/device.
- Failure of backbone affects failure of all devices on the network.

2. Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is token passing. Token is a frame that circulates around the network.
- A token move around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

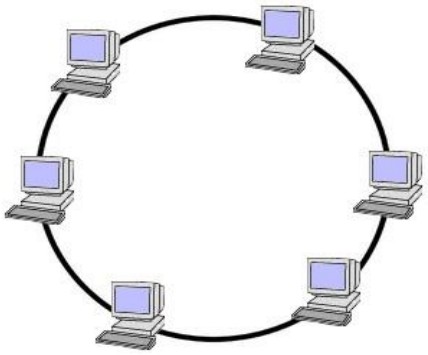


Figure 5. Ring Topology

Advantages:

- A ring is relatively easy to install and reconfigure.
- Link failure can be easily found as each device is connected to its immediate neighbours only.
- Because every node is given equal access to the token no one node can monopolise the network.

Disadvantages:

- Maximum ring length and number of devices is limited.
- Failure of one node on the ring can affect the entire network.
- Adding or removing node disrupts the network.

3. Star Topology

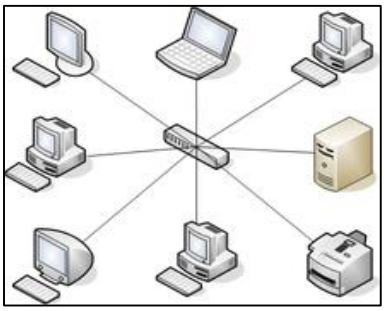


Figure 6. Star Topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a server, and the peripheral devices attached to the server are known as clients.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a physical star topology.
- Star topology is the most popular topology in network implementation.

Advantages:

- Each device needs only one link and one I/O port, which makes star topology less expensive, easy to install and easy to configure.

- Robust topology.
- If any link fails, it does not affect entire network.
- Easy fault identification and fault isolation.
- It is easy to modify and add new nodes to star network without disturbing the rest of the network.

Disadvantages:

- If the central hub fails, the entire network fails to operate.
- Each device requires its own cable segment.
- In hierarchical network, installation and configuration is difficult.

4. Mesh Topology

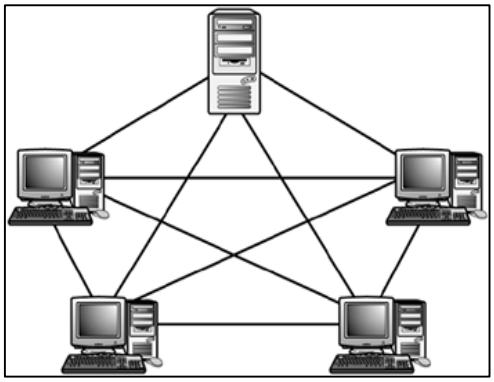


Figure 7. Mesh Topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: Number of cables = (n*(n-1))/2; where n is the number of nodes that represents the network.
- This indicates that each node must have (n-1) I/O ports.

Advantages:

- No traffic because of dedicated link.
- Robust because if one link fails, it does not affect the entire network.
- Privacy and security of data is achieved due to dedicated link.
- Fault identification is easy.

Disadvantages:

- Difficulty of installation and reconfiguration as every node is connected to every other node.
- Costly because of maintaining redundant links.
- The amount of cabling required is large.

5. Hybrid Topology

- The combination of various different topologies is known as **hybrid topology**.
- A hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of HDFC bank and bus topology in another branch of HDFC bank, connecting these two topologies will result in Hybrid topology.

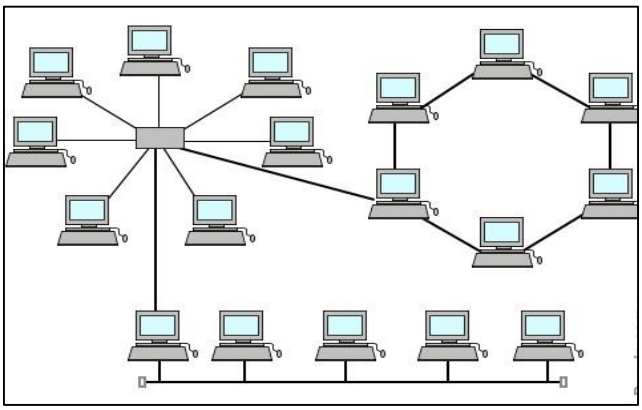


Figure 8. Hybrid Topology

Advantages:

- **Reliable**: If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable**: Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible**: This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective**: Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages:

- **Complex design**: The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub**: The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure**: The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

1.6. Network Hardware Components

1.6.1. Transmission Technology

Broadly speaking, there are two types of links that are in widespread use to transmit data. They are as follows:

1. Broadcast links
2. Point-to-point links

1. Broadcast Networks

- Broadcast networks have a single communication channel that is shared by all the machines on the network.
- The data to be transmitted is converted in small **packet** form.
- Each packet contains address field of the destination station. Upon receiving the packet, a machine checks the address field.
- If the packet is intended for the receiving station, that station processes the packet; if the packet is intended for some other station, it is just ignored.
- It is also possible to send same packets to all stations within a network; it is called as **broadcasting**.
- When data packets are sent to a specific group of stations, it is called as **multicasting**. Multicasting is a selective process.
- Example of broadcasting is Radio and example of multicasting is Email.

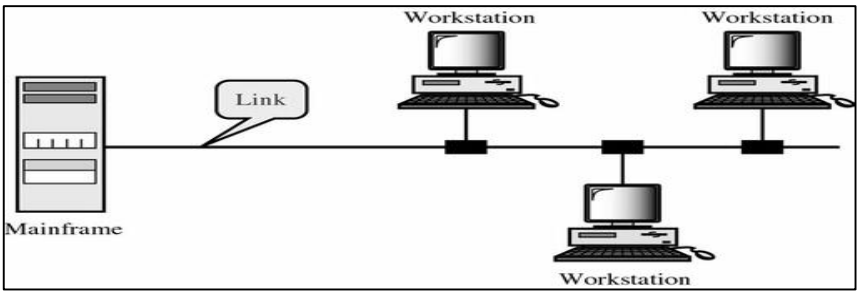


Figure 9. Broadcast Network

2. Point-to-Point Networks

- Point-to-point networks provides a dedicated link between any two stations.
- The data packets are sent from source station to the destination station. Such a transmission is called unicasting.
- Example of point-point network is Telephone.

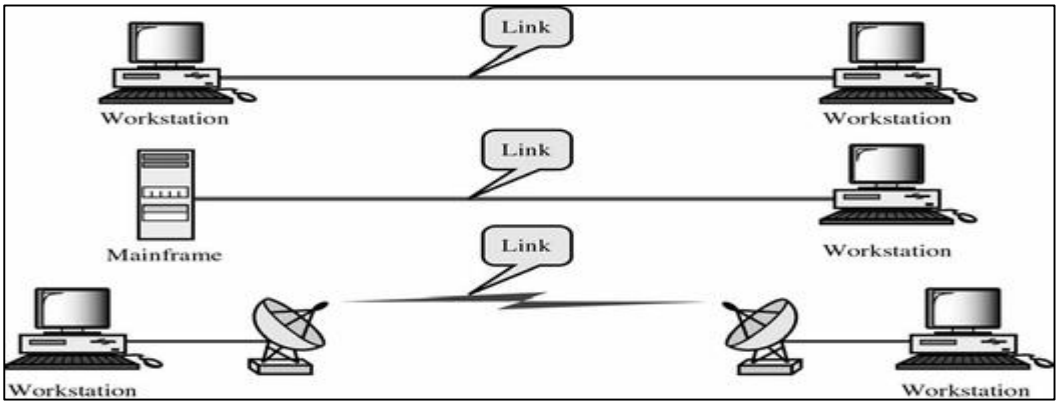


Figure 10. Point-to-Point Network

1.6.2. Transmission Modes

1. Simplex Mode

- In simplex transmission mode, the communication between sender and receiver occurs in only one direction.
- The sender can only send the data, and the receiver can only receive the data.
- The receiver cannot reply to the sender.
- Example: **Keyboard-Monitor Communication**; the keyboard can only send the input to the monitor, and the monitor can only receive the input and display it on the screen. The monitor cannot reply, or send any feedback to the keyboard.

2. Half-Duplex Mode

- The communication between sender and receiver occurs in both directions in half duplex transmission, but only one at a time.
- The sender and receiver can both send and receive the information, but only one is allowed to send at any given time.
- Half duplex is still considered a one-way road, in which a vehicle traveling in the opposite direction of the traffic has to wait till the road is empty before it can pass through.
- For example, in **walkie-talkies**, the speakers at both ends can speak, but they have to speak one by one. They cannot speak simultaneously.

3. Full Duplex Mode

- In full duplex transmission mode, the communication between sender and receiver can occur simultaneously.
- The sender and receiver can both transmit and receive at the same time.
- Full duplex transmission mode is like a two-way road, in which traffic can flow in both directions at the same time.
- For example, in a **telephone conversation**, two people communicate, and both are free to speak and listen at the same time.

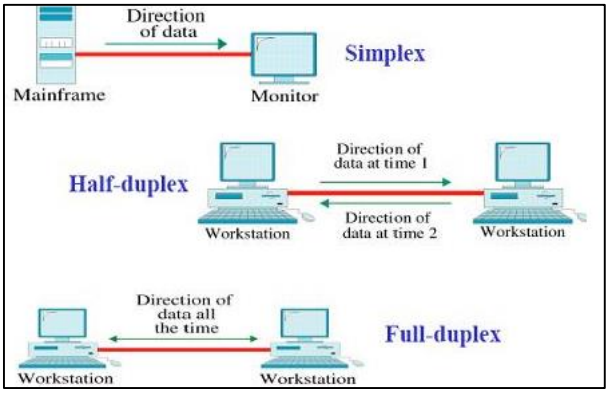


Figure 11. Transmission Modes

1.6.3. Types of Networks

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:

1. LAN (Local Area Network)
2. PAN (Personal Area Network)
3. MAN (Metropolitan Area Network)
4. WAN (Wide Area Network)

1. LAN (Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network. Traditional LANs run at speeds of 10 Mbps to 100 Mbps. Newer LANs operate at upto 10 Gbps.
- Local Area Network provides higher security.

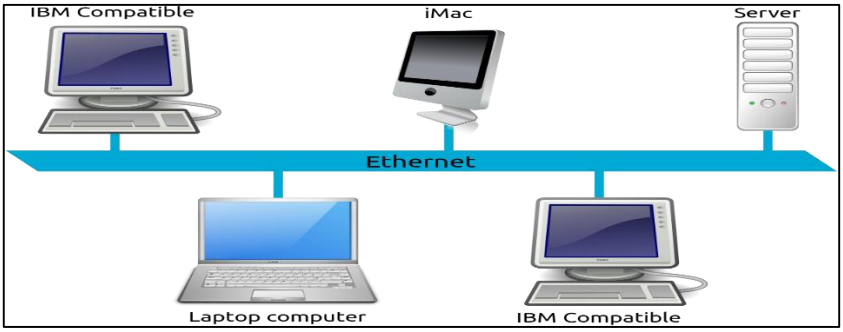


Figure. 12 Local Area Network (LAN)

2. Personal Area Network (PAN)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Thomas Zimmerman was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of 30 feet.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.
- Examples of PAN include Body Area Network, Small Home Office

Figure 13. Personal Area Network (PAN)

3. Metropolitan Area Network (MAN)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, ADSL, etc.
- It has a higher range than Local Area Network(LAN).
- Supports both data and voice.
- Speed: 34 to 150 Mbps

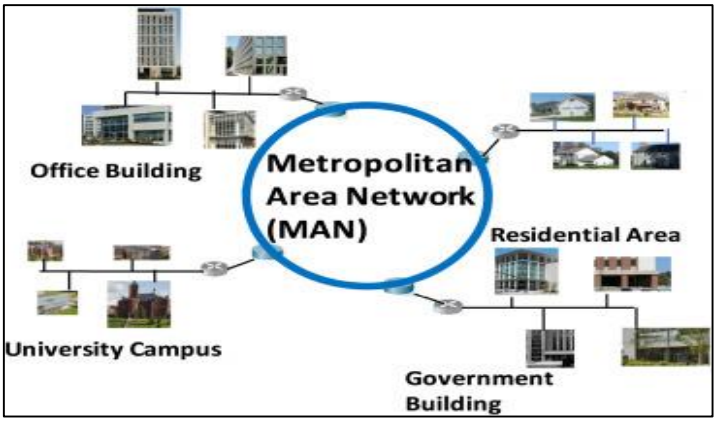


Figure 14. Metropolitan Area Network (MAN)

4. Wide Area Network (WAN)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The Internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

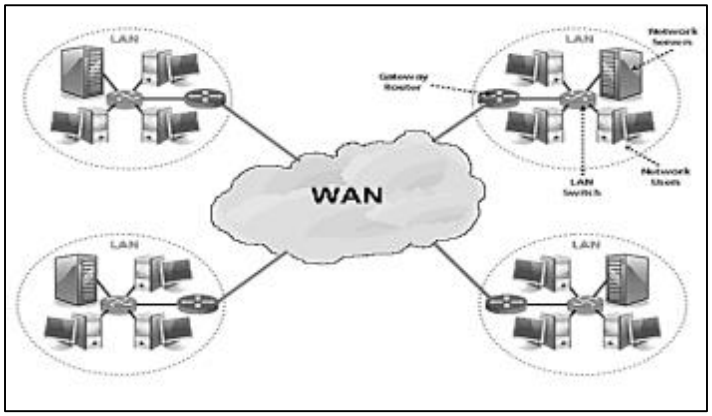


Figure 15. Wide Area Network (WAN)

5. Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, at least it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

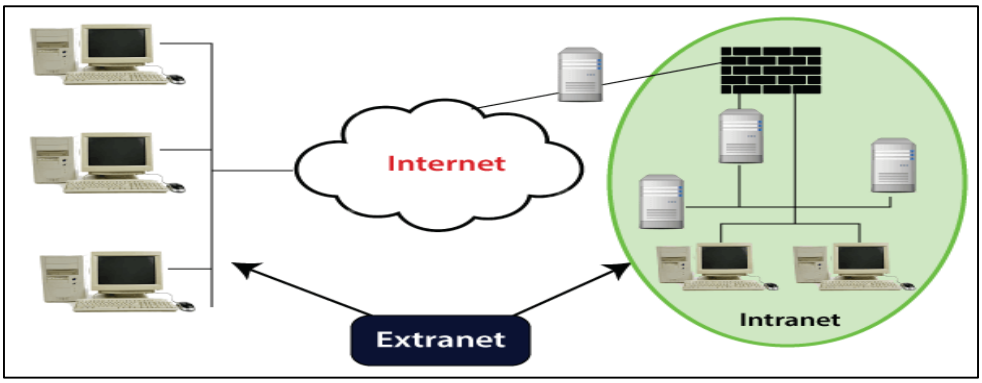


Figure 16. Intranet and Extranet

Comparison of LAN, MAN and WAN

Table 1. Comparison of LAN, MAN and WAN

BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.
Allows	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.

1.6.4 Networking Devices

1. Repeater

- Also called a regenerator.
- Operates only in the physical layer of the ISO-OSI model.
- Simply regenerates the weak signal and transmit the regenerated signal.
- Provides signal amplification.

Figure 17. Repeater

2. Hub

- Also called the central concentrator or controller.
- Operates in the physical layer of the IOS-OSI model.
- It simply transmits the incoming signals to the other media segments.

- Provides central management.
- Do not amplify the incoming signal.

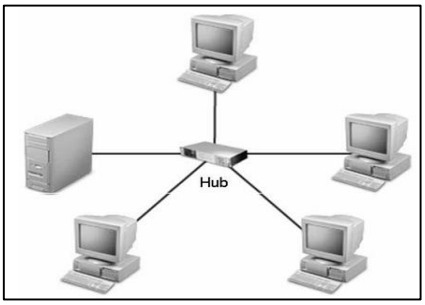


Figure 18. Hub

3. Bridge

- Operates in the data link layer of the ISO-OSI model.
- A bridge connects two or more LANs.
- When a frame arrives, software in the bridge extracts the destination address from the frame header and looks it up in the bridge table to see where to send the frame.
- Can divide the busy network into segments and reduce the network traffic.

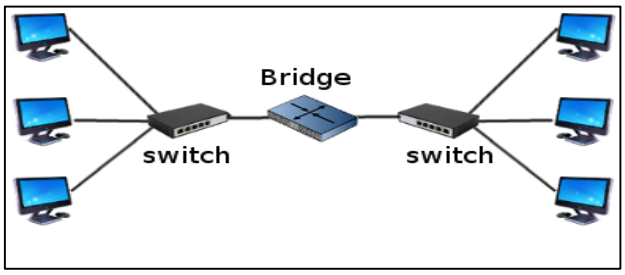


Figure 19. Bridge

4. Switch

- Operates in the data link layer of the ISO-OSI model.
- More efficient than bridging.
- Buffer the incoming packet.
- Check the address and decide the outgoing line.
- Retransmit the packet only if the line is idle.

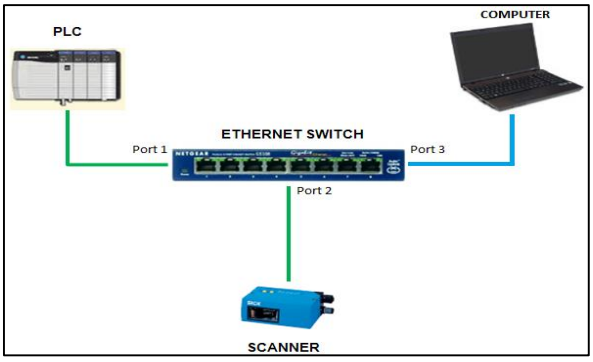


Figure 20. Switch

5. Router

- Operates at the network layer of the ISO-OSI model.
- Interconnects two or more networks which can be heterogeneous.
- They decide on the most efficient path that the packets should take while flowing from one network to another.

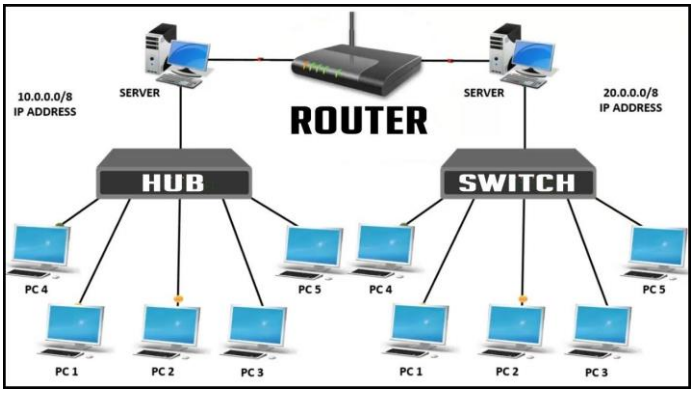


Figure 21. Router

6. Gateway

- Operates at all the seven layers of the ISO-OSI model.
- It is a protocol converter.
- A gateway can accept a packet formatted for one protocol and can convert it into a packet formatted for another protocol before forwarding it.
- Gateway must adjust data rate, size, and data format.
- Gateway is generally a software installed within a router.

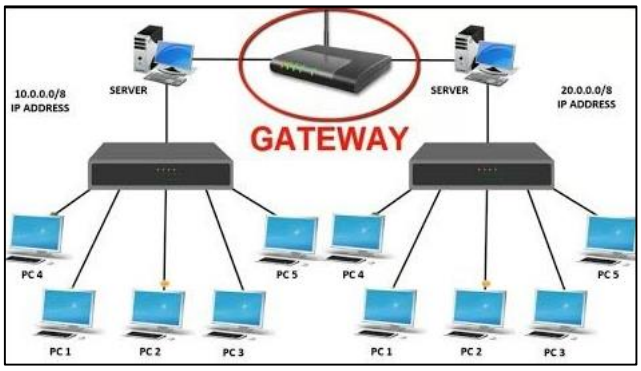


Figure 22. Gateway

1.7. Network Software

- Computer network is designed around the concept of layered protocols or functions. For exchange of data between computers, terminals or other data processing devices, there is data path between two computers, either directly or via a communication network.
- Following factors should be considered:
  1. The source system must either activate the direct data communication path or inform the communication network the identity of the desired destination system.
  2. Provide for standard interface between network functions.
  3. Provide for symmetry in function performed at each node in the network. Each layer performs the same functions as its counterpart in the other node of the network.
- The network software is now highly structured.

1.7.1. Protocol Hierarchies

- Most networks are organized as a series of layers or levels.

- To reduce the design complexity, networks are organized as a series of layer or levels, one above the other as shown in figure 23 below.
- The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network.

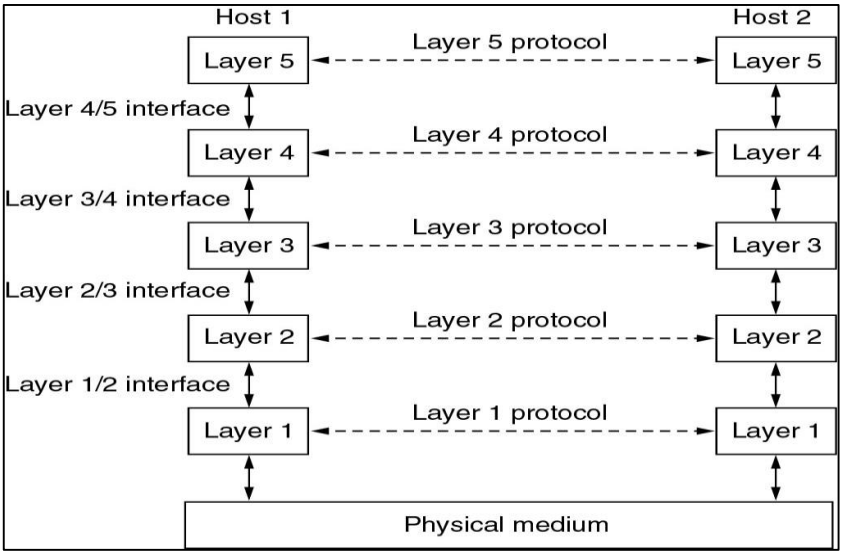


Figure 23. Layers, protocols and interfaces

- The purpose of each layer is to offer certain services to the higher layers.
- Layer n on one machine (sender) carries a conversation with layer n on another machine (receiver).
- The rules and conventions used in this conversation are collectively known as the layer n protocol.
- Basically, a **protocol** is an agreement between the two machines as how communication link should be established, maintained and released.
- If the protocol is violated, the communication will be difficult.
- A five-layer network is shown in figure 23.
- The entities comprising the corresponding layers on different machines are called as **peers**.
- The communication actually takes place between the peers using the protocol.
- The dotted lines in figure shows the virtual communication and the physical communication is shown by solid lines.
- Between each pair of adjacent layers is interface. The **interface** defines which primitive operations and services the lower layer offers to the upper layer.
- A set of layers and protocols is called a **network architecture**.

Advantages of Layered Architecture

- Since the functions of each layers and their interactions are well defined, layered architecture simplifies the design process.
- The layered architecture provides flexibility to modify and develop network services.
- The number of layers, names of the layers, and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer provides certain services to its upper layer.

- The concept of layered architecture redefines the way of conceiving networks. This leads to a considerable cost saving and managerial benefits.
- Addition of new services and management of network infrastructure becomes easy.
- Due to segmentation, it is possible to break complex problems into smaller and more manageable pieces.
- Logical segmentation helps development taking place by different teams.

Disadvantages of Layered Architecture

- Layering is a kind of hiding information.
- It can sometimes result in poor performance.
- We may lose touch with the reality because of layered protocols.

1.7.2. Design Issues for the Layers

The key design issues that occur in computer networking are as follows:

1. **Addressing**
   - Every layer must have ability to identify senders and receivers.
   - Since there are multiple possible destinations, some form of addressing is needed in order to specify a specific destination.
2. **Direction of Transmission**
   - The direction of data transfer is another design issue.
   - Based on the direction of communication, the communication systems are classified as simplex, half-duplex and full-duplex.
3. **Error Control**
   - Since physical communication circuits are not perfect, error control is one of the important design issue.
   - Error detection and correction both are essential.
   - Many error detecting and correcting codes are known, out of which those agreed by the sender and the receiver should be used.
   - The receiver should be able to send proper acknowledgement of message received to the sender.
4. **Avoid Loss of Sequencing**
   - All the communication channels may not be able to preserve the order in which messages are transmitted on it. This may lead to loss of sequencing.
   - To avoid all this, all the messages should be numbered so that they can be put back together at the receiver in the appropriate sequence.
5. **Ability of Receiving Long Messages**
   - Several layers in the network may not be able to process or accept arbitrarily long messages.
   - So a mechanism needs to be developed to disassemble, transmit and then reassemble messages.
6. **To use Multiplexing and Demultiplexing**
   - Multiplexing and demultiplexing is to be used to share same channel by multiple sources simultaneously.
   - It can be used for any layer. Multiplexing is needed in the physical layer.

1.8. Connection Oriented and Connectionless Services

Connection-oriented and Connection-less Services are used to establish connections between two or more devices.

Connection-oriented Services

- In connection oriented service we have to establish a connection before starting the communication.
- When connection is established, we send the message or the information and then we release the connection.
- Connection oriented service is more reliable than connectionless service.
- We can send the message in connection oriented service if there is an error at the receiver's end.
- Example of connection oriented is TCP (Transmission Control Protocol) protocol.

Connection-less Services

- It is similar to the postal services, as it carries the full address where the message (letter) is to be carried.
- Each message is routed independently from source to destination. The order of message sent can be different from the order received.
- In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message.
- Authentication is not needed in this.
- Example of Connectionless service is UDP (User Datagram Protocol) protocol.

Following are the important differences between Connection-oriented and Connection-less Services.

Sr. No.	Key	Connection-oriented Services	Connection-less Services
1	Analogy	Connection-oriented Services are similar to Telephone System.	Connection-less Services are similar to Postal System.
2	Usage	Connection-oriented Services are used in long and steady communication networks.	Connection-less Services are used in volatile networks.
3	Congestion	No Congestion in Connection-oriented Service.	Congestion is quiet possible in Connection-less Services.
4	Reliability	Connection-oriented Service are highly reliable.	In Connection-less Services, no guarantee of reliability.
5	Packet Routing	In Connection-oriented Service, packets follows same route.	In Connection-less Services, packets can follow any route.

1.8.1 Service Primitives

- A service is formally specified by a set of primitives (operations) available to a user process to access the service.
- These primitives tell the service to perform some action or report on an action taken by a peer entity.
- If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls.
- These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.
- The set of primitives available depends on the nature of the service being provided.
- The primitives for connection-oriented service are different from those of connection-less service.
- There are five types of service primitives:
  1. **LISTEN:** When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.
  2. **CONNECT:** It connects the server by establishing a connection. Response is awaited.
  3. **RECIEVE:** Then the RECIEVE call blocks the server.
  4. **SEND:** Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.
  5. **DISCONNECT:** This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.

1.9.Communication between Layers

- A set of layers and protocols is called a network architecture.
- The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.

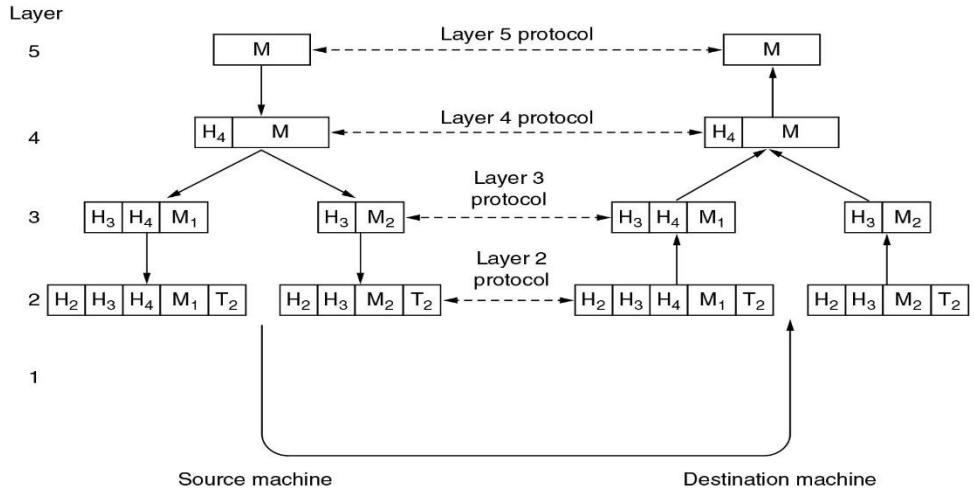


Figure 24. Communication between layers

- A message, M, is produced by an application process running in layer 5 and given to layer 4 for transmission.
- Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3.
- The header includes control information, such as sequence numbers, to allow layer 4 on the destination machine to deliver messages in the right order if the lower layers do not maintain sequence.
- In some layers, headers can also contain sizes, times, and other control fields.
- In many networks, there is no limit to the size of messages transmitted in the layer 4 protocol, but there is nearly always a limit imposed by the layer 3 protocol.
- Consequently, layer 3 must break up the incoming messages into smaller units, packets, pre-pending a layer 3 header to each packet.
- In this example, M is split into two parts, M1 and M2.
- Layer 3 decides which of the outgoing lines to use and passes the packets to layer 2.
- Layer 2 adds not only a header to each piece, but also a trailer, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses.
- None of the headers for layers below (n) are passed up to layer (n).
- The important thing to understand about the figure below is the relation between the virtual and actual communication and the difference between protocols and interfaces.
- The peer processes in layer 4, for example, conceptually think of their communication as being "horizontal," using the layer 4 protocol.
- Each one is likely to have a procedure called something like SendToOtherSide and GetFromOtherSide, even though these procedures actually communicate with lower layers across the 3/4 interface, not with the other side.

1.10. ISO-OSI Reference Model

- OSI stands for **Open System Interconnection**.
- It is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers as shown in figure 26, and each layer performs a particular network function.
- OSI model was developed by the **International Organization for Standardization** (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- Each layer is assigned a particular task. Each layer is self-contained, so that task assigned to each layer can be performed independently.
- The functions of each of the layer in ISO-OSI Reference model are described below.

1. Physical Layer

- It deals with the physical layout of the network.
- It deals with transmitting raw bits (0's and 1's) over the communication channel.

- The design issues here deal with the mechanical, electrical and timing interfaces and the physical transmission medium which lies below the physical layer.

2. Data Link Layer

- It breaks the data into frames and passes it to the network layer.
- It deals with error control mechanism during transmission.
- It deals with the flow control mechanism to prevent the drowning of the slow receiver by the fast transmitter.
- It controls access to the shared medium.

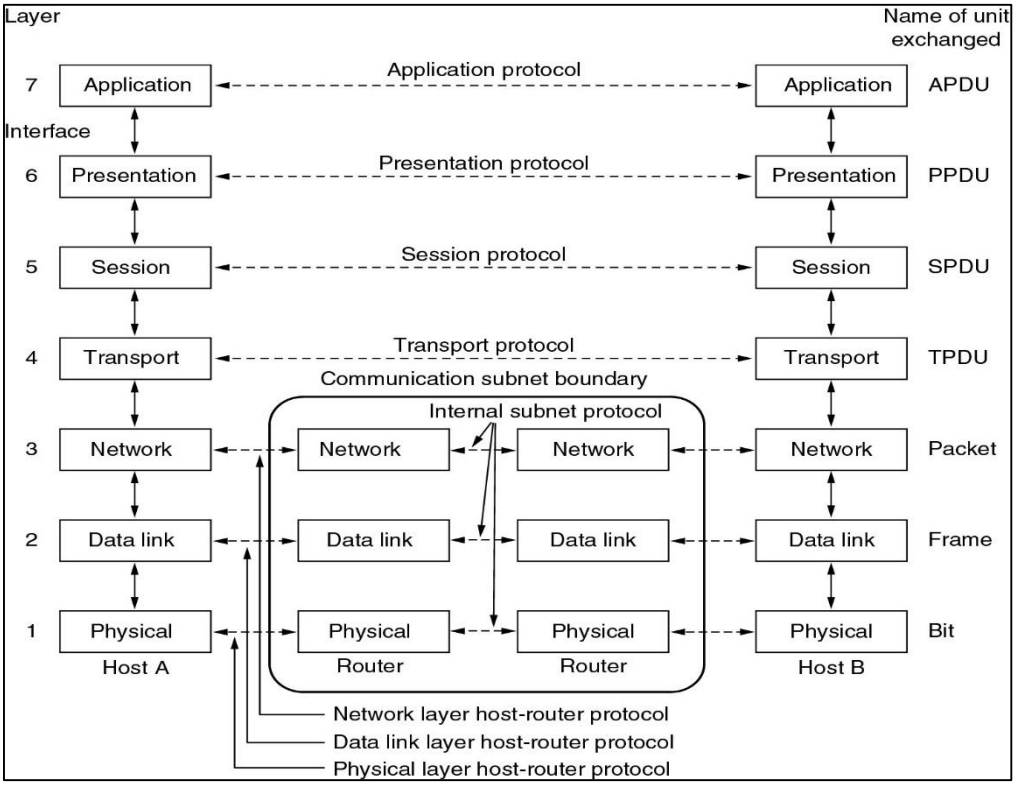


Figure 26. ISO-OSI Reference Model

3. Network Layer

- It determines the network path on which to route the packet.
- Helps to reduce network congestion.
- Establishes virtual circuits.
- Routes frames to other network, resequencing packet transmission when needed.

4. Transport Layer

- Ensures reliability of packet transmission from node to node.
- Ensures data is sent and received in the same order.
- Provides acknowledgment when a packet is received.
- Monitors for packet transmission errors, and resends the damaged packets.

5. Session Layer

- It deals with dialogue control and synchronization to keep track of whose turn is it to transmit.
- It deals with token management to prevent two parties from attempting the same critical operation at the same time.

- It deals with check-pointing long transactions to allow them to continue from where they were after a crash.

6. Presentation Layer

- It deals with syntax of information.
- It deals with semantics of information.
- It deals with compression of information.
- It also deals with encoding of information.

7. Application Layer

- Provides user interfaces.
- Support for services like Email, File transfer, Database Management, Remote File access.

1.9.TCP/IP 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.
- They also offer simple naming and addressing schemes.
- TCP/IP 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.
- Protocols and networks in the TCP/IP model is shown in figure 27.

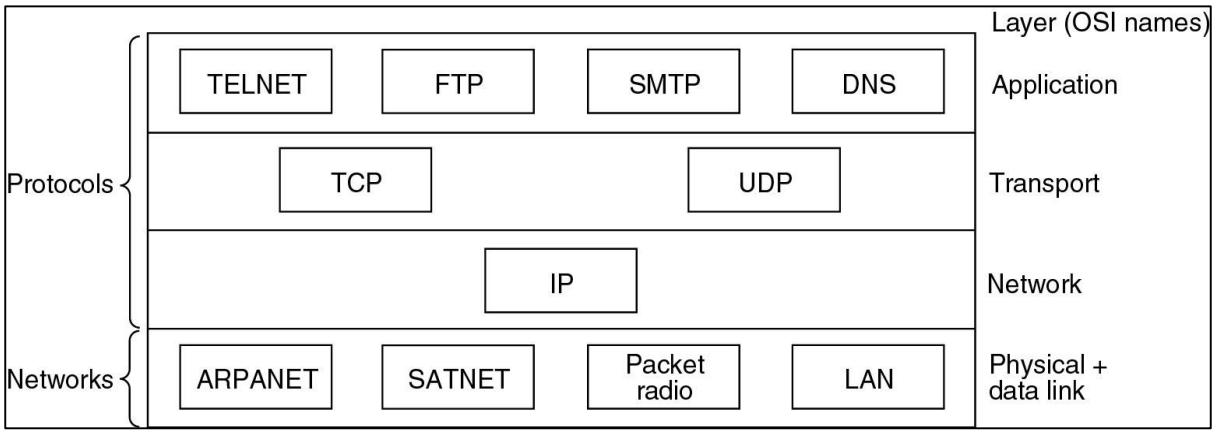


Figure 27. TCP/IP Model

1. Network Access Layer (Host-to-Network Layer)

- A network access layer is the lowest layer of the TCP/IP model.
- A network access layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

- The protocols used by this layer are Ethernet, Token ring, FDDI, X.25, Frame relay.

2. **Internet Layer**
   - It permits hosts to inject packets into the network and make these packets reach their destination.
   - It defines the packet format and protocol called the Internet Protocol (IP).
   - Main focus is on packet routing.
3. **Transport Layer**
   - The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
   - It has two main protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

   TCP
   i. Reliable, connection-oriented.
   ii. Allows byte stream from one machine to be delivered to any other machine on the network.
   iii. Handles error control and flow control.

   UDP
   i. Unreliable, connectionless.
   ii. Used for client-server type queries, where prompt delivery is more than reliability.
   iii. Does not implement flow or error control.
4. **Application Layer**
   - An application layer is the topmost layer in the TCP/IP model.
   - It is responsible for handling high-level protocols, issues of representation.
   - This layer allows the user to interact with the application.
   - When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
   - Contains protocols like FTP, SMTP, HTTP, DNS, Telnet.

1.10. Comparison of OSI and TCP/IP Reference Model

Following are some similarities between OSI Reference Model and TCP/IP Reference Model.

- Both have layered architecture.
- Layers provide similar functionalities.
- Both are protocol stack.
- Both are reference models.

Following are some major differences between OSI Reference Model and TCP/IP Reference Model.

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 guarantee 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 and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not have a problem of fitting the protocols into the model.
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

ಅಅಅಅಅ

CHAPTER 2

PHYSICAL LAYER

2.1. Introduction to Communication System

- **Data** refers to the raw facts that are collected while **information** refers to processed data that enables us to take decisions.
- Example: When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed.
- The word data refers to any information which is presented in a form that is agreed and accepted upon by is creators and users.
- Data Communication is a process of exchanging data or information.
- In case of computer networks this exchange is done between two devices over a transmission medium.
- This process involves a communication system which is made up of hardware and software.
- The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes.
- The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a **Protocol**.

2.1.1. Characteristics of Data Communication

The effectiveness of any data communications system depends upon the following four fundamental characteristics:

1. **Delivery**: The data should be delivered to the correct destination and correct user.
2. **Accuracy**: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
3. **Timeliness**: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4. **Jitter**: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

2.1.2. Components of Data Communication

A Data Communication system has five components as shown in the figure 1 below:

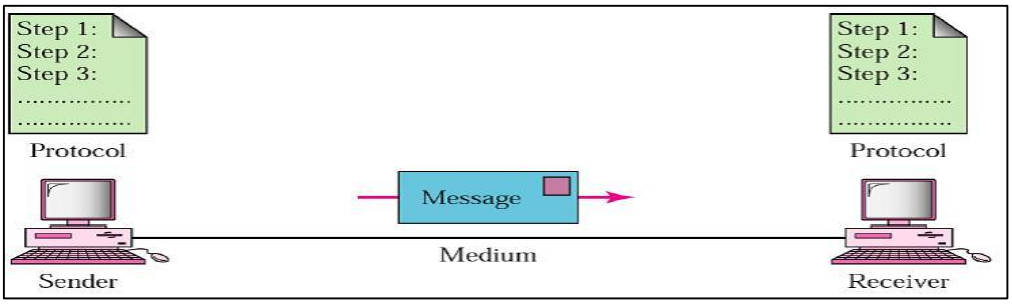


Figure 1. Components of Data Communication

1. **Message**: Message is the information to be communicated by the sender to the receiver.

2. **Sender**: The sender is any device that is capable of sending the data (message).
3. **Receiver**: The receiver is a device that the sender wants to communicate the data (message).
4. **Transmission Medium**: It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
5. **Protocol**: A protocol is a set of rules that governs data communication. A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language.

2.1.3. Data Representation

- Data is collection of raw facts which is processed to deduce information.
- There may be different forms in which data may be represented.
- Some of the forms of data used in communications are as follows:

1. **Text**:
    - Text includes combination of alphabets in small case as well as upper case.
    - It is stored as a pattern of bits.
    - Prevalent encoding system: ASCII, Unicode
2. **Numbers**:
    - Numbers include combination of digits from 0 to 9.
    - It is stored as a pattern of bits.
    - Prevalent encoding system: ASCII, Unicode
3. **Images**:
    - "An image is worth a thousand words" is a very famous saying.
    - In computers, images are digitally stored.
    - A Pixel is the smallest element of an image. To put it in simple terms, a picture or image is a matrix of pixel elements.
    - The pixels are represented in the form of bits.
    - Depending upon the type of image (black & white or colour) each pixel would require different number of bits to represent the value of a pixel.
    - The size of an image depends upon the number of pixels (also called resolution) and the bit pattern used to indicate the value of each pixel.
    - Example: if an image is purely black and white (two colour) each pixel can be represented by a value either 0 or 1, so an image made up of 10 x 10 pixel elements would require only 100 bits in memory to be stored.
    - On the other hand, an image that includes gray may require 2 bits to represent every pixel value (00 - black, 01 – dark gray, 10– light gray, 11 –white). So the same 10 x 10-pixel image would now require 200 bits of memory to be stored.
    - Commonly used Image formats: jpg, png, bmp, etc.
4. **Audio:**
    - Data can also be in the form of sound which can be recorded and broadcasted.
    - Example: What we hear on the radio is a source of data or information.
    - Audio data is continuous, not discrete.
5. **Video:**
    - Video refers to broadcasting of data in form of picture or movie.

2.2. Digital Communication

- The communication that occurs in our day-to-day life is in the form of signals.
- These signals, such as sound signals, generally, are analog in nature.
- When the communication needs to be established over a distance, then the analog signals are sent through wire, using different techniques for effective transmission.
- These analog signals may suffer from many losses such as distortion, interference, and other losses including security breach.
- In order to overcome these problems, the signals are digitized using different techniques. The digitized signals allow the communication to be more clear and accurate without losses.
- The following figure 2 indicates the difference between analog and digital signals. The digital signals consist of 1s and 0s which indicate High and Low values respectively.

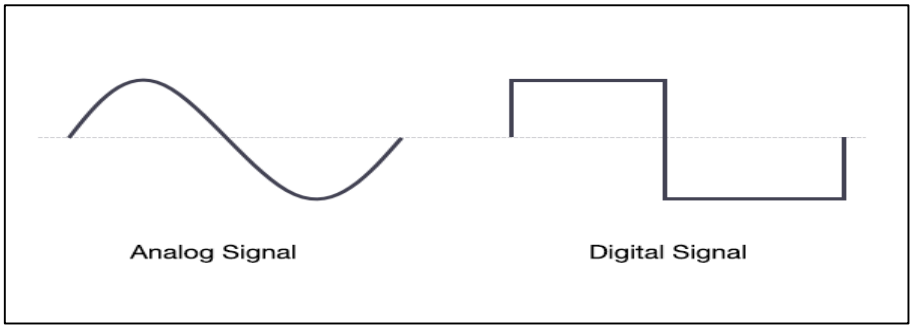


Figure 2. Analog and Digital Signal

- Communication systems that first convert the source output into a binary sequence and then convert that binary sequence into a form suitable for transmission over particular physical media such as cable, twisted wire pair, optical fiber, or electromagnetic radiation through space are called digital communication systems.
- In digital technology, the data are generated and processed in two states: High (represented as 1) and Low (represented as 0). Digital technology stores and transmits data in the form of 1s and 0s.
- Figure 3 is the basic digital communication model.

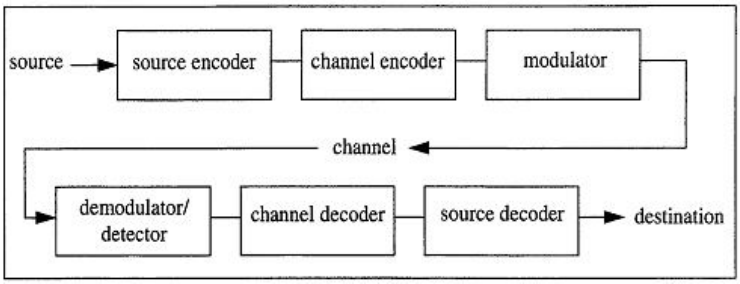


Figure 3. Digital Communication Model

- The first three blocks of the diagram (source encoder, channel encoder, and modulator) together comprise the transmitter.
- The source represents the message to be transmitted which includes speech, video, image, or text data among others.
- If the information has been acquired in analog form, it must be converted into digitized form to make our communication easier.

- This analog to digital conversion (ADC) is accomplished in the source encoder block by placing a binary interface between source and channel.
- The source encoder converts the source output to a binary sequence and the channel encoder (often called a modulator) processes the binary sequence for transmission over the channel.
- The last three blocks consisting of detector/demodulator, channel decoder, and source decoder form the receiver.
- The destination represents the client waiting for the information. This might include a human or a storage device or another processing station.
- In any case, the source decoder's responsibility is to recover the information from the channel decoder and to transform it into a form suitable for the destination.
- This transformation includes digital to analog conversion (DAC) if the destination is a human waiting to hear or view the information or if it is an analog storage device.
- If the destination is a digital storage device, the information will be kept in its digital state without DAC.
- The channel decoder (demodulator) recreates the incoming binary sequence (hopefully reliably), and the source decoder recreates the source output.
- Noise is one of the channel imperfection or impairment in the received signal at the destination.
- There are external and internal sources that cause noise.
- External sources include interference, i.e. interference from nearby transmitted signals (cross talk), interference generated by natural source such as lightning, solar or cosmic radiation, from automobile generated radiation, etc.
- The external noise can be minimised and eliminated by appropriate design of the channel, shielding of cables. Also by digital transmission external noise can be much minimised.
- Internal sources include noise due to random motion and collision of electrons in the conductors, thermal noise due to diffusion and recombination of charge carriers in other electronic devices.
- Internal noise can be minimised by cooling and using digital technology for transmission.
- **Attenuation**: Attenuation is a problem caused by the medium. When the signal is propagating for a longer distance through a medium, depending on the length of the medium the initial power decreases. The loss in initial power is directly proportional to the length of the medium. Using amplifiers, the signal power is strengthened or amplified so as to reduce attenuation. Also, digital signals are comparatively less prone to attenuation than analogue signals.
- **Distortion**: It is also another type of channel problem. When the signal is distorted, the distorted signal may have frequency and bandwidth different from the transmitted signal. The variation in the signal frequency can be linear or non-linear.

2.2.1. Maximum Data Rate of a Channel

- The maximum data rate limit over a medium is decided by following factors:
  1. Bandwidth of channel
  2. Signal levels

3. Channel quality (Level of noise)

- Depending upon the channel type (noiseless channel or noisy channel), the data rate is calculated by two different formulas.
  1. For noiseless channel – Nyquist Bit Rate
  2. For noisy channel – Shannon Capacity

1. Nyquist Bit Rate

- Nyquist bit rate defines the theoretical maximum bit rate for a noiseless channel or ideal channel.
- The formula for maximum bit rate in bits per second (bps) is:

$$\textbf{Maximum Bit Rate} = 2 \times \textbf{BW} \times \log_2 \textbf{L}$$

where, BW = Bandwidth of channel

L = Number of signal levels used to represent data

2. Shannon Capacity

- An ideal noiseless channel never exists. The maximum data rate for any noisy channel is:

$$\textbf{C} = \textbf{BW} \times \log_2 \left(1 + \frac{\textbf{S}}{\textbf{N}}\right)$$

where, C = Channel capacity in bits per second

BW = Bandwidth of channel

$\frac{S}{N}$ = Signal-to-Noise ratio

Q1. Determine the data rate for a noiseless channel having bandwidth of 3kHz and two signal levels are used for signal transmission.

Solution: For a noiseless channel, the maximum data rate is given by Nyquist bit rate as

$$\text{Maximum Bit Rate} = 2 \times \text{BW} \times \log_2 \text{L}$$
$$\text{Maximum Bit Rate} = 2 \times (3 \times 10^3) \times \log_2 2$$
$$\text{Maximum Bit Rate} = 6000\text{bps}$$

Q2. Calculate the bandwidth of a noiseless channel having a maximum bit rate of 12kbps and four signal levels.

Solution: For a noiseless channel, the maximum data rate is given by Nyquist bit rate as

$$\text{Maximum Bit Rate} = 2 \times \text{BW} \times \log_2 \text{L}$$
$$12 \times 10^3 = 2 \times \text{BW} \times \log_2 4$$

$$\text{BW} = \frac{12 \times 10^3}{4} = 3000 \text{ Hz} = 3\text{kHz}$$

Q3. Calculate the capacity of a telephone channel. The channel bandwidth is 3000 Hz and $\frac{S}{N}$ is 3162.

Solution: The telephone channel is a noisy channel.

$$\text{C} = \text{BW} \times \log_2 \left(1 + \frac{\text{S}}{\text{N}}\right)$$
$$\text{C} = 3000 \times \log_2 (1 + 3162) = 34881 \text{ bps}$$

Q4. Calculate the maximum bit rate for a channel having bandwidth 3100 Hz and S/N ratio 20dB.

Solution:

S/N ratio = 20 dB

$$\text{i.e. } 20 \text{ dB} = 10 \log \frac{S}{N}$$

$$\therefore \frac{S}{N} = 10^2 = 100$$

Maximum bit rate for a noisy channel is

$$C = BW \times \log_2\left(1 + \frac{S}{N}\right)$$

$$C = 3100 \times \log_2(1 + 100) = 20640 \text{ bps}$$

2.3. Electromagnetic Spectrum

- Electromagnetic spectrum in simple terms is defined as the range of all types of electromagnetic radiation.
- The electromagnetic spectrum is a range of frequencies, wavelengths and photon energies covering frequencies from below 1 Hz to above 10^{25} Hz corresponding to wavelengths which are a few kilometres to a fraction of the size of an atomic nucleus in the spectrum of electromagnetic waves.
- Generally, in a vacuum electromagnetic waves tend to travel at speeds which is similar to that of light. However, they do so at a wide range of wavelengths, frequencies, and photon energies.
- The electromagnetic spectrum consists of a span of all electromagnetic radiation which further contains many subranges which are commonly referred to as portions.
- These can be further classified as infra-red radiation, visible light or ultraviolet radiation.
- The entire range (electromagnetic spectrum) is given by radio waves, microwaves, infrared radiation, visible light, ultra-violet radiation, X-rays, gamma rays and cosmic rays in the increasing order of frequency and decreasing order of wavelength.
- The type of radiation and their frequency and wavelength ranges are as follows:

Type of Radiation	Frequency Range (Hz)	Wavelength Range
gamma-rays	$10^{20} – 10^{24}$	$< 10^{-12}$ m
x-rays	$10^{17} – 10^{20}$	1 nm – 1 pm
Ultraviolet	$10^{15} – 10^{17}$	400 nm – 1 nm
Visible	$4 – 7.5 \times 10^{14}$	750 nm – 400 nm
near-infrared	$1 \times 10^{14} – 4 \times 10^{14}$	2.5 μm – 750 nm
Infrared	$10^{13} – 10^{14}$	25 μm – 2.5 μm
Microwaves	$3 \times 10^{11} – 10^{13}$	1 mm – 25 μm
radio waves	$< 3 \times 10^{11}$	> 1 mm

- The electromagnetic spectrum can be depicted as follows:

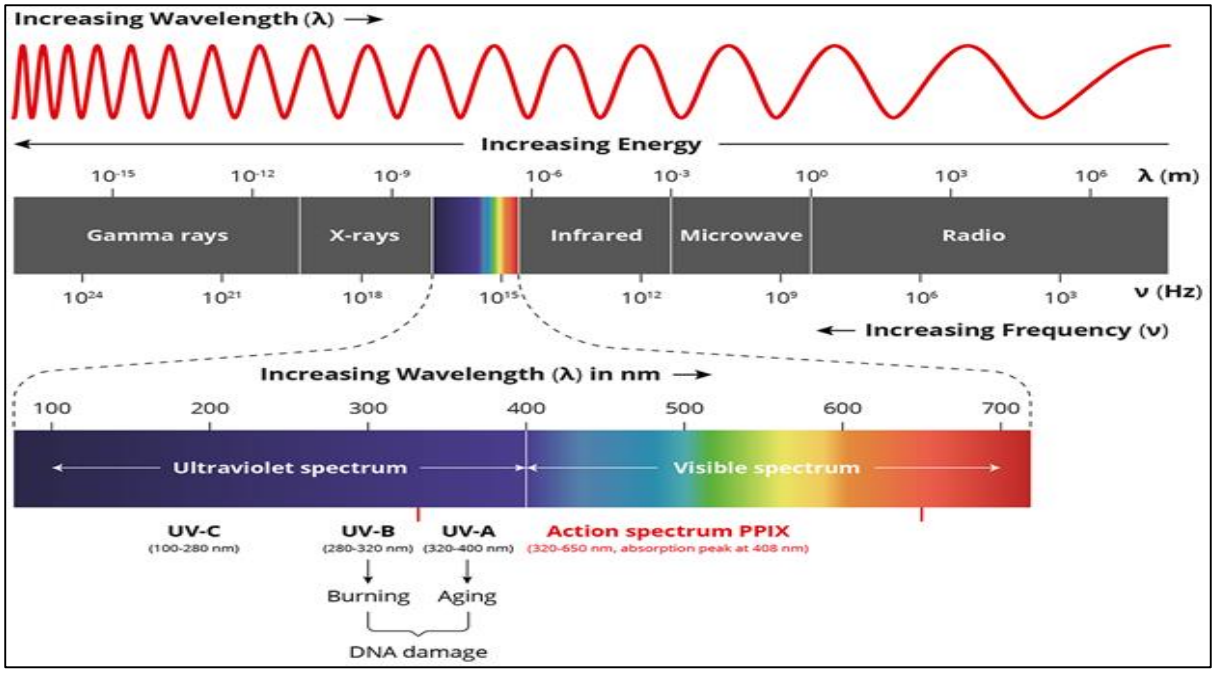


Figure 4. Electromagnetic Spectrum

- We see the uses of the electromagnetic waves in our daily life as:

1. **Radio:** Radio waves are mainly used for TV/mobile communication.
2. **Microwave:** This type of radiation is found in microwaves and helps in cooking at home/office. It is also used by astronomers to determine and understand the structure of nearby galaxies and stars.
3. **Infrared:** It is used widely in night vision goggles. These devices can read and capture the infrared light emitted by our skin and objects with heat.
4. **X-ray:** X-rays can be used in many instances. For example, a doctor can use an x-ray machine to take an image of our bone or teeth. Airport security personnel use it to see through and check bags.
5. **Gamma-ray:** It has a wide application in the medical field. Gamma-ray imaging is used to see inside our bodies.
6. **Ultraviolet:** Sun is the main source of ultraviolet radiation. It causes skin tanning and burns.
7. **Visible:** Visible light can be detected by our eyes. Light bulbs, stars, etc. emit visible light.

2.4. Transmission Media

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN** (Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits are transmitted in the form of electrical signals.
- In a fibre based network, the bits are transmitted in the form of light pulses.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.

- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types: guided (also called wired or bounded) media and unguided (also called wireless or unbounded) media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.

2.4.1 Selection of Transmission Media

The selection of transmission media depends on following factors:

1. Design factors
2. Guided or unguided media

1. Design Factors

Some factors need to be considered for designing the transmission media:

- **Bandwidth**: The greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment**: When the received signal is not identical to the transmitted one, it is due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.
- **Number of receivers**: A guided media is used either for point-to=point link or a shared link with multiple attachments. In multiple attachments, each attachment introduces some attenuation and distortion on the link; this limits the distance and data rate.

Causes of Transmission Impairment:

- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

2. Guided or unguided Media

- Depending on the type of application and geographical situation, suitable guided and unguided media is chosen.
- For long distance point-to-point transmission, guided media are suitable.
- For long distance broadcasting transmission, unguided media like microwave links are suitable.

2.4.2. Guided Transmission Medium

- It is defined as the physical medium through which the signals are transmitted.
- It is also known as Bounded media or wired media.
- Types of Guided Media
  1. Magnetic Media
  2. Twisted Pair
  3. Coaxial Cable
  4. Fiber Optic Cable

1. Magnetic Media

- Data is written on magnetic tape or floppy disk or CD ROM.
- Bandwidth is excellent i.e. upto 19 Gbps.
- Cost effective way to transmit large amount of data.
- High delay in accessing data. It takes minutes to hours to days to physically transport cassette from one location to another.

2. Twisted Pair

- Twisted pair cable is the most common transmission medium for LANs.
- It is comprised of copper wires individually surrounded by a PVC insulating layer and twisted around each other in a spiral.
- The wires are twisted to improve the transmission characteristics by reducing the interference.
- It can be used for either analog or digital transmission.
- Bandwidth depends on the thickness of the wire and the distance travelled.
- Twisted pair is relatively inexpensive and easy to install and terminate.
- There are two types of twisted pair cable: Unshielded twisted pair (UTP) and shielded twisted pair (STP).

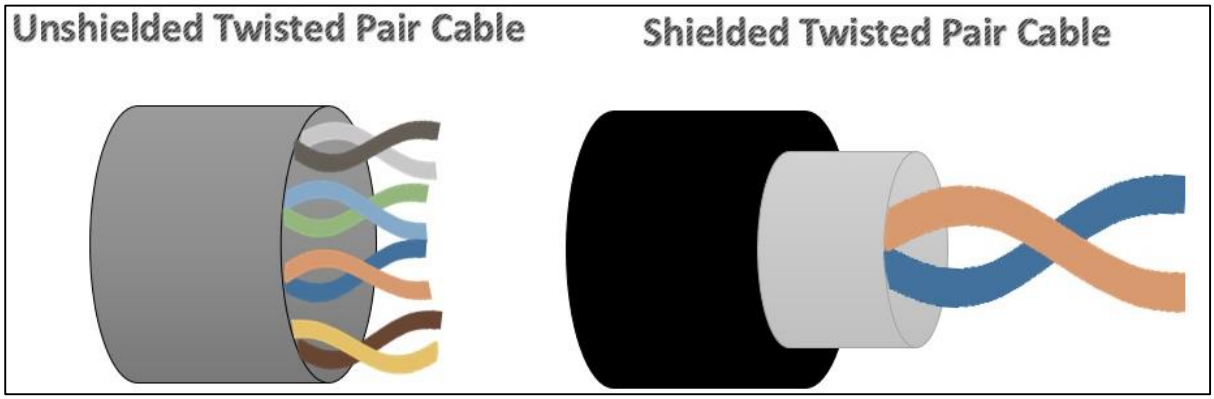


Figure 5. Twisted Pair Cable

Unshielded Twisted Pair (UTP)

- UTP is a set of twisted pairs of cable within a plastic sheet.
- There is no additional shielding for the twisted pairs.
- It is used for telephonic applications.

- UTP has data rate of 10 – 100 Mbps.
- UTP is less expensive than fiber optic cable and coaxial cable.
- Maximum cable segment of UTP is 100 metres.
- UTP cable is very flexible and easy to work.
- UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.
- Most susceptible to electrical interference or crosstalk.

Advantages of UTP

- UTP is easy to terminate.
- Cost of installation is less.

Disadvantages of UTP

- It is very noisy.
- It covers less distance.
- UTP suffers from interference.

Categories of UTP

UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Figure 6. Categories of UTP

Shielded Twisted Pair (STP)

- STP cable consists of twisted pair of wires that are not only individually insulated, but also surrounded by a shield made of a metallic substance such as aluminium foil.
- The shielding also ensures that the electromagnetic field generated in one pair will not interfere with the signal in an adjacent pair.
- STP has data rate of 150 Mbps.
- Maximum cable segment of STP is 500 metres.
- Less susceptible to interference or crosstalk.
- Very easy to install.
- Little costly as compared to UTP.

Advantages of STP

- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of STP

- Difficult to manufacture
- Heavy

3. **Coaxial Cable**
    - Coaxial is called by this name because it contains two conductors that are parallel to each other.
    - Copper is used in this as centre conductor which can be a solid wire or a standard one.
    - It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, braid or both.
    - Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit.
    - The outer conductor is also encased in an insulating sheath.
    - The outermost part is the plastic cover which protects the whole cable.
    - To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector.

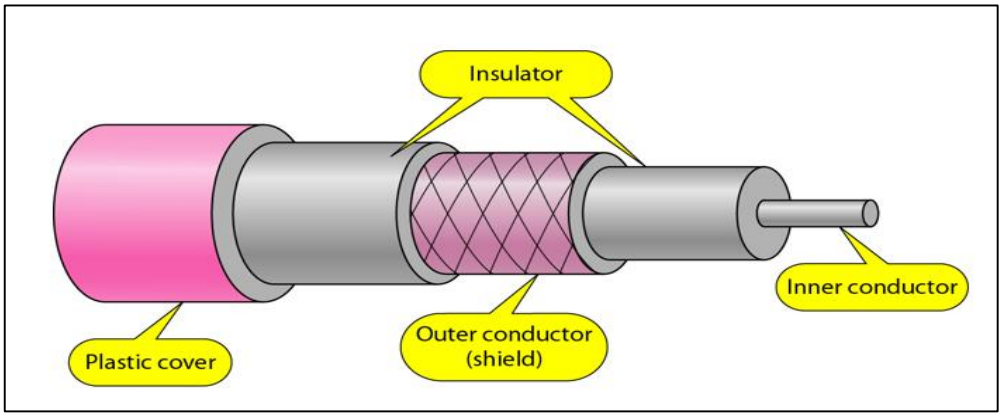


Figure 7. Coaxial Cable

Classification of Coaxial Cable

1. Based on Impedance
    a. 50 Ohm: Used for digital transmission
    b. 75 Ohm: Used for analog transmission
2. Based on Frequency
    a. Baseband 0 – 4 kHz: Used for telephone cabling
    b. Broadband 4 kHz: Used for cable television cabling

Advantages of Coaxial Cable:

- Bandwidth is high.
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.

Disadvantages of Coaxial Cable:

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

4. Fiber Optic Cable

- Fiber optic cable consists of bundled fiber strands.
- Each fiber strand has a thin, inner core of optical fiber and a cladding, which is a concentric glass covering, surrounding the core.
- The core and cladding are surrounded by a protective covering.
- Fiber optic cable is able to transmit signals over long distances at very high bandwidth.
- Data is transmitted via pulsing light sent from a laser through the central fiber.
- Cladding reflects light back to the core.
- Plastic coating (or buffer) protects the fiber from damage and moisture.
- Fiber optics is not susceptible to electromagnetic or radio frequency interference.
- Fiber optic cable uses two types of connectors for connection. They are Subscriber Channel (SC) connector and Straight Line (ST) connector.

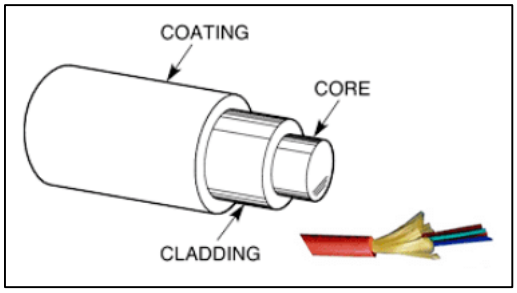


Figure 8. Fiber Optic Cable

Types of Fiber Optic Cable

1. **Single-mode fiber**
   - Have a single strand of glass fiber.
   - Have small core with diameter of 8.3 to 10 microns.
   - Transmit infrared laser light having wavelength 1310 or 1550nm.
   - Bandwidth is nearly infinity.

2. **Multimode fiber**
   - Have a multiple strands of glass fiber.
   - Have larger core with diameter of 62.5 microns i.e. about thickness of human hair.
   - Transmit infrared light having wavelength 850 to 1300nm.
   - Bandwidth is 2 GHz.

Advantages of Fibre Optic Cable

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

Disadvantages of Fiber Optic Cable

- Installation and maintenance is difficult
- Unidirectional light propagation
- High Cost

Comparison of Twisted Pair Cable Vs Coaxial Cable Vs Fiber Optic Cable

Sr. No.	Twisted Pair Cable	Coaxial Cable	Fiber Optic Cable
1	Transmission of signals takes place in the electrical form over metallic conducting wire.	Coaxial cable is used to transmit signal in electrical form over the inner conductor of the cable.	Signal transmission takes place in light forms over a glass fiber.
2	Twisted pair cable can be affected due to external magnetic field.	Coaxial cable is less affected due to external magnetic field.	Fiber optical cable is never affected due to external magnetic field.
3	Twisted pair cable is made up of a pair of insulated copper wire.	Coaxial cable is made up of four components moving from inside to the outside: a solid conductor wire, a layer of insulation, a grounding conductor and a layer of exterior insulation.	Optical cables are made up of very thin optical fibers bundled together into a single cable. The fibers can be made of glass or plastic.
4	Twisted pair cables are comparatively low in price when compared to both Coaxial and Fiber optical cables.	The cost of coaxial cables is higher than that of twisted pair cables.	In general, fiber optic cable is more expensive than copper cable due to its high performance and capacity.
5	Attenuation is very high.	Attenuation is low.	Attenuation is very much low.
6	Installation and implementation of twisted pair cables is simple and easy.	Installation and implementation of coaxial cable is relatively difficult due to the dielectric insulator around the core copper in coaxial cable.	Installation and implementation of optical fiber is difficult. This is due to the fact that they are thin and fragile and therefore requires more care in installation.
7	Low Bandwidth.	Moderately high bandwidth.	They have very high bandwidth.

8	The security of transmitted signal is not guaranteed.	The security of transmitted signal is not guaranteed.	There is increased security in fiber-optic technology and therefore it is hard to tap fiber-optic cables without also disrupting the system.
9	Twisted pair cables are generally used in telephone networks, data networks and cable shielding.	Coaxial cables are used in feedlines connecting radio transmitters and receivers with their antennas, computer network (Internet) connections, digital audio (S/PDIF) and distributing cable television signals.	Fiber optical cable can transmit television, telephone and data at a relatively faster speed when compared to twisted pair and coaxial cable.
10	Common types of twisted pair Ethernet cable include: Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).	Common types of coaxial cable include: Baseband and Broadband	Fiber optic cable can be categorized into Single mode fiber (SMF) and Multimode fiber (MMF).

2.4.3. Unguided Transmission Medium

- It is also referred to as Wireless or Unbounded transmission media.
- No physical medium is required for the transmission of electromagnetic signals.
- The signal is broadcasted through air.
- Less Secure.
- Used for larger distances.
- Types of Guided Media
  1. Radio Waves
  2. Microwave
  3. Infrared
  4. Bluetooth

1. Radio Waves

- These are easy to generate and can penetrate through buildings.
- The sending and receiving antennas need not be aligned.
- Frequency Range:3KHz – 1GHz.
- AM and FM radios and cordless phones use radio waves for transmission.
- Further Categorized as (i) Terrestrial and (ii) Satellite.

2. Microwave

- It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other.
- The distance covered by the signal is directly proportional to the height of the antenna.
- Frequency Range:1GHz – 300GHz.

- These are majorly used for mobile phone communication and television distribution.
- Can pass through thin solids but has difficulty in passing through buildings.

3. **Infrared**
   - Infrared waves are used for very short distance communication.
   - They cannot penetrate through obstacles.
   - This prevents interference between systems.
   - Frequency Range:300GHz – 400THz.
   - It is used in TV remotes, wireless mouse, keyboard, printer, etc.
4. **Bluetooth**
   - It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances.
   - This technology was invented by Ericson in 1994.
   - It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz.
   - Bluetooth lets devices discover and connect to each other (by pairing), and then securely transfer data.
   - Maximum devices that can be connected at the same time are 7.
   - Bluetooth ranges upto 10 meters.
   - It provides data rates upto 1 Mbps or 3 Mbps depending upon the version.
   - The spreading technique which it uses is FHSS (Frequency hopping spread spectrum).
   - A Bluetooth network is called **Piconet** and a collection of interconnected piconets is called **Scatternet**.

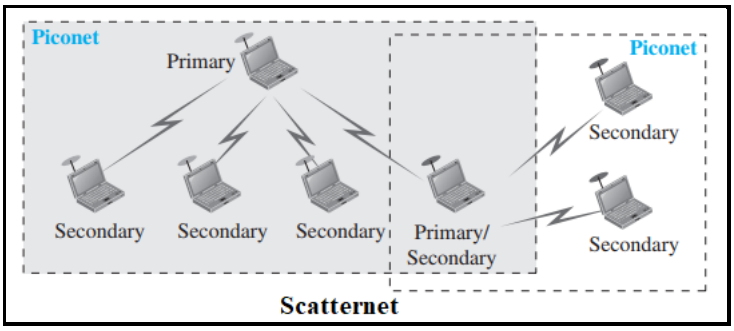


Figure 9. Bluetooth Architecture

Piconet

- Piconet is a type of Bluetooth network that contains **one primary node** called master node and **seven active secondary nodes** called slave nodes.
- Thus, we can say that there are total of 8 active nodes which are present at a distance of 10 metres.
- The communication between the primary and secondary node can be one-to-one or one-to-many.
- Possible communication is only between the master and slave; Slave-slave communication is not possible.

- It also has **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet

- It is formed by using **various piconets**.
- A slave that is present in one piconet can be act as master or we can say primary in other piconet.
- This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave.
- This type of node is called as **bridge node**.
- A station cannot be master in two piconets.

Advantages of Bluetooth:

- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an adhoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages of Bluetooth:

- It can be hacked and hence, less secure.
- It has slow data transfer rate: 3 Mbps.
- It has small range: 10 meters.

2.5. Switching Techniques

- In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.

2.5.1. Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.
- Communication through circuit switching has 3 phases:
    a. Connection establishment

b. Data transfer
c. Connection Release

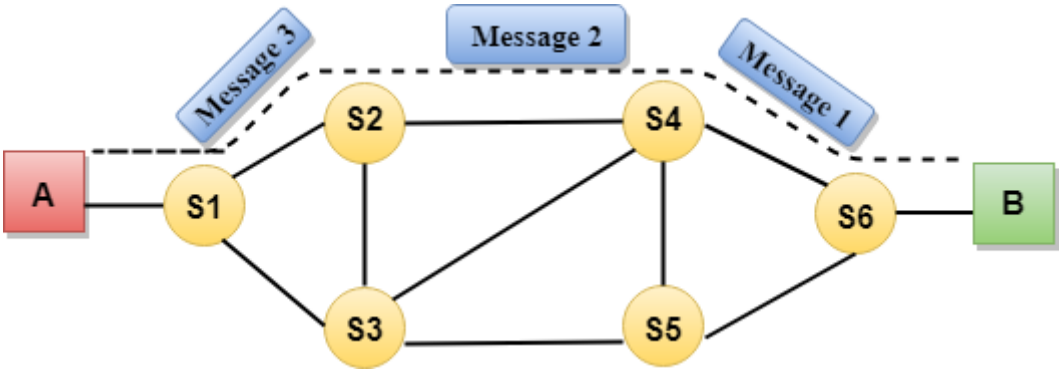


Figure 10. Circuit Switching

Advantages of Circuit Switching

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages of Circuit Switching

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approximately 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

2.5.2. Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message.
- Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward** network.
- Message switching treats each message as an independent entity.

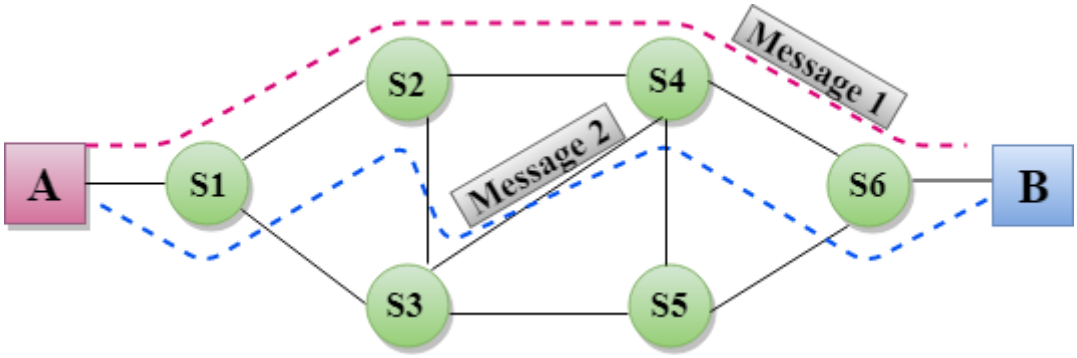


Figure 11. Message Switching

Advantages of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The long delay can occur due to the storing and forwarding facility provided by the message switching technique.

2.5.3. Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

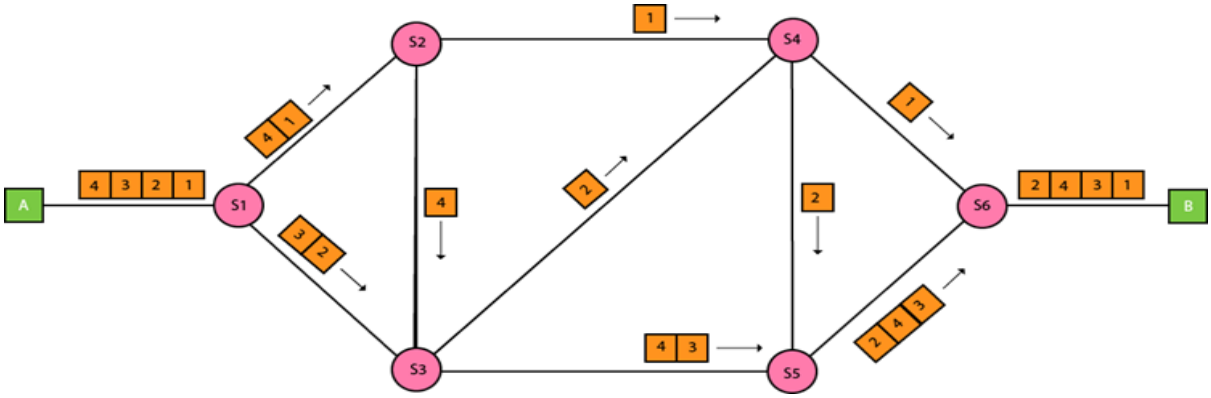


Figure 12. Packet Switching

Approaches of Packet Switching

There are two approaches to Packet Switching:

1. **Datagram Packet switching**
   - It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
   - The packets are reassembled at the receiving end in correct order.
   - In Datagram Packet Switching technique, the path is not fixed.
   - Intermediate nodes take the routing decisions to forward the packets.
   - Datagram Packet Switching is also known as connectionless switching.

2. **Virtual Circuit Switching**
   - Virtual Circuit Switching is also known as connection-oriented switching.
   - In the case of virtual circuit switching, a pre-planned route is established before the messages are sent.
   - Call request and call accept packets are used to establish the connection between sender and receiver.
   - In this case, the path is fixed for the duration of a logical connection.
   - **Let's understand the concept of virtual circuit switching through a diagram:**

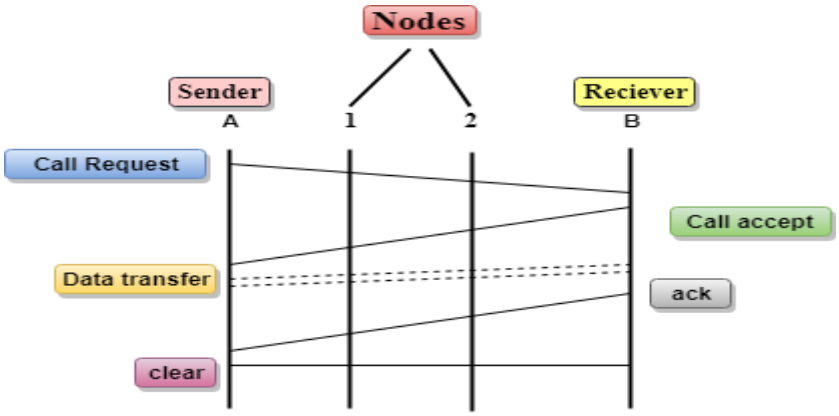


Figure 13. Virtual Circuit Packet Switching

- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Advantages of Packet Switching

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages of Packet Switching

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are not recovered.

ಅಅಅಅಅ

CHAPTER 3

DATA LINK LAYER

3.1. Data Link Layer Design Issues

The functions of the Data Link Layer (DLL) are:

1. **Providing services to the network layer**
   - In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it.
   - The data link layer uses the services offered by the physical layer.
   - The primary function of this layer is to provide a well-defined service interface to network layer above it.
   - The principle service is transferring data from network layer on sending machine to the network layer on destination machine.
   - The services provided for this purpose are:
     a. **Unacknowledged Connectionless Service**: No acknowledgements are used. It is a connectionless service. Example: VoIP
     b. **Acknowledged Connectionless Service**: Acknowledgments are used. It is a connectionless service. Example: Wi-Fi
     c. **Acknowledged Connection-oriented Service**: Acknowledgments are used. It is a connection-oriented service. Example: Telephone
2. **Error control**

   To achieve error control, following techniques are used:

   a. **Acknowledgments**: When the receiver correctly receives the data, it sends an acknowledgement to the sender. (Used in Stop-and-wait protocol)
   b. **Timer**: The sender maintains a timer which is set to a time which is enough for the data to reach the receiver and for the acknowledgement from the receiver to reach back to the sender.
   c. **Sequence Numbers**: Sequence numbers are used by the receiver to decide if they are receiving the new frames or the duplicate frames.
3. **Flow control**
   - A receiving node can receive the frames at a faster rate than it can process the frame.
   - Without flow control, the receiver's buffer can overflow, and frames can get lost.
   - DLL regulates the flow of data so that receivers are not swamped by the fast senders.
4. **Framing**
   - The data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission.
   - Each frame contains a frame header, a payload field for holding the packet, and a frame trailer as shown in figure 1.
   - Frame management forms the heart of what the data link layer does.

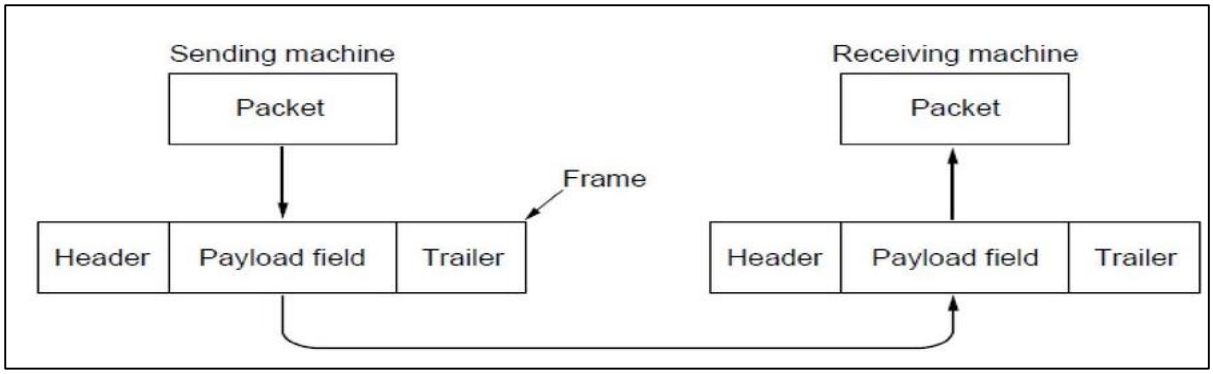


Figure 1. Relationship between packets and frames

Techniques of Framing

a. Character Count

- The first field in the header specifies the number of characters in the frame.
- When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of frame is.
- This technique is shown in figure 2 below for four frames of sizes 5, 5, 8, and 8 characters respectively.

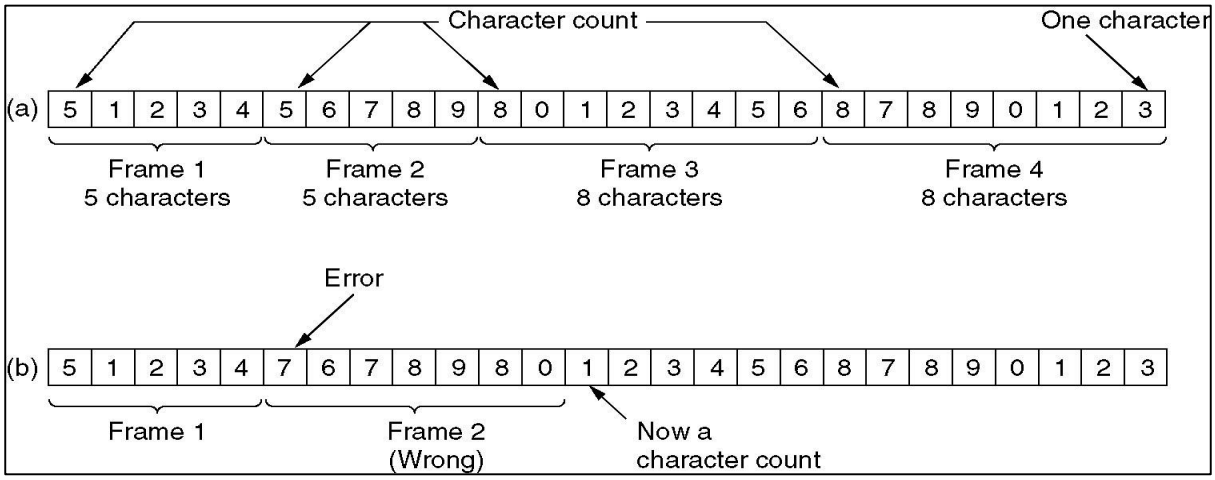


Figure 2. A Character Stream. (a) Without errors (b) With one error

- The trouble with this algorithm is that the count can be garbled by a transmission error. For example, if the character count of 5 in the second frame of figure (b) becomes a 7, the destination will get out of synchronization and will be unable to locate the start of the next frame.

b. Character Stuffing

- Each frame starts with a special start and end bytes (flag bytes). Here, we will image it as same byte, FLAG as shown in figure 3.

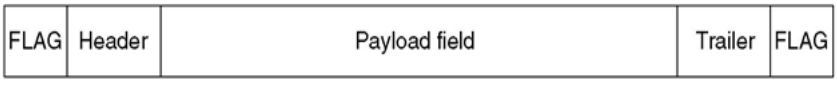


Figure 3. A frame delimited by flag bytes

- After error occurs, it can always find start of next frame.

- If flag byte is already present in the data, insert special escape byte (ESC) before each FLAG in data. Remove it at receiver end. This is called **byte stuffing** or **character stuffing**.
- Probably it won't happen for text data, but could easily happen with binary data.
- If ESC is itself in the data, insert another ESC before it.
- De-stuffing recovers original characters.

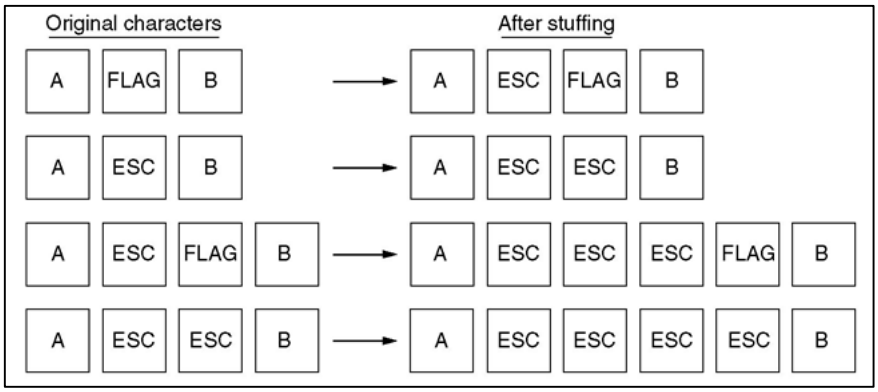


Figure 4. Four examples of byte sequences before and after stuffing

c. Bit Stuffing

- Byte stuffing specifies character format (i.e. 8 bits per character).
- To allow arbitrary number of bits per character, use stuffing at bit-level rather than at byte-stuffing.
- Each frame begins and ends with bit pattern 01111110 (6 1's).
- If five 1's in a row in data, stuff in a bit 0 so that never there will be six 1's in a row.
- Stuff it in always irrespective of whether next bit will be 1 or 0.
- De-stuffer removes the 0's after any five 1's at the receiver end.

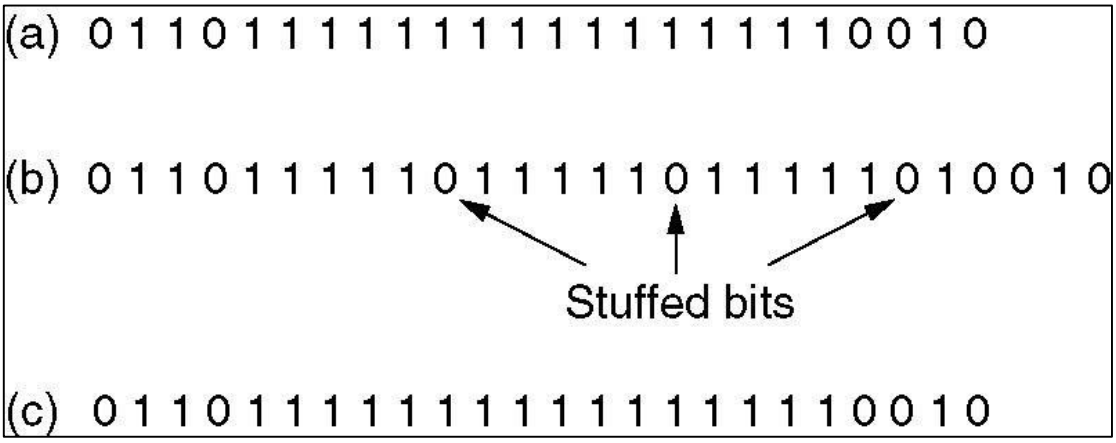


Figure 5. Bit Stuffing

(a) The original data.

(b) The data as they appear on the line.

(c) The data as they are stored in receiver's memory after de-stuffing.

5. Data link layer performs error detection using CRC and error correction using Hamming code.

3.2. Flow Control Techniques

- Flow control is a technique which implies on the data link layer and tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver.
- Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
- So the sending station must not send frame at a rate faster than the receiving station can absorb them.
- Two techniques have been developed to control the flow of data across communication links.
  1. Stop-and wait flow control
  2. Sliding window flow control

1. **Stop-and-wait flow control**

- The sender waits for an acknowledgement from the receiver after every frame, which is transmitted by the sender.
- It indicates the willingness of the receiver to accept another frame by sending back an acknowledgement to the sender.
- The sender must wait until it receives the acknowledgement before sending next frame.
- The receiver thus can stop the flow of data simply by withholding acknowledgement.
- The procedure is illustrated in figure 6.

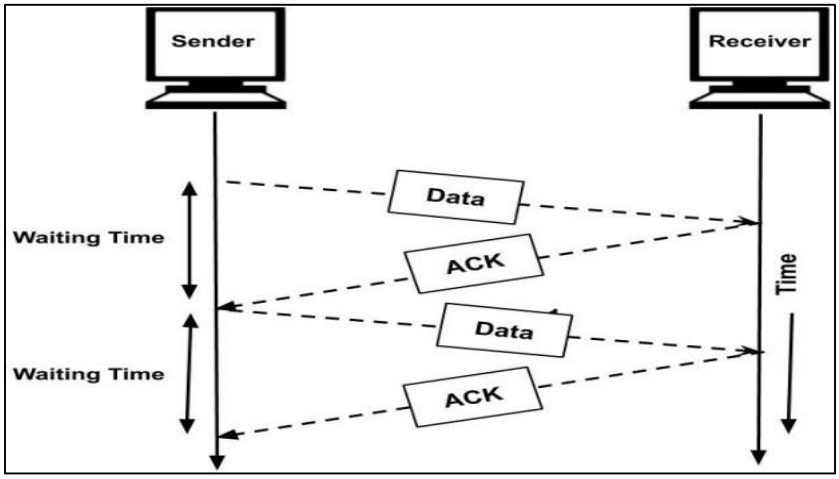


Figure 6. Stop-and-wait Flow Control

Advantage: Simplicity. Each frame is checked and acknowledged before the next frame is sent.

Disadvantage: Inefficiency. Stop-and-wait is slow. Each frame must travel all the way to the receiver and the acknowledgement must travel all the way back to the sender before the next frame can be sent.

2. Sliding window flow control

- In sliding window method of flow control, the sender can transmit several frames before getting the acknowledgement.

- The link can carry several frames at one time and its capacity can be used efficiently.
- The sliding window refers to imaginary boxes at both the sender and the receiver end.
- The window can hold frames at either end and these may be acknowledged at any point without waiting for the window to fill up.
- To keep track of which frames have been transmitted and received, sliding window introduces an identification scheme based on size of the window.
- The frames are numbered from 0 to n-1 and the size of window is also n-1.
- Example: If n=8, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7 and size of window =7.
- Thus, the receiver sends an acknowledgment which includes the number of next frame it expects to receive.

Sender's Window

- At the beginning of transmission, the sender's window contains n-1 frames.
- As the frames are sent out, the left boundary of the window moves inwards shrinking the size of the window.
- Once an acknowledgement arrives, the window expands to allow in a number of new frames equal to number of frames acknowledged by the receiver.

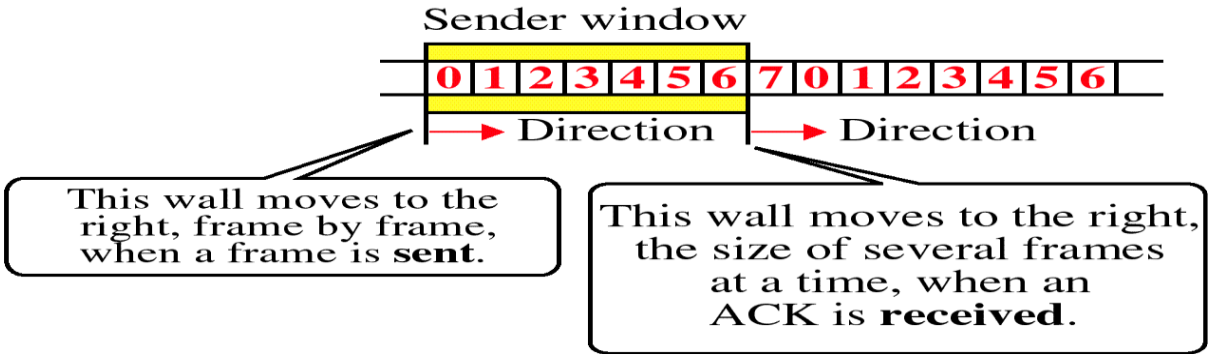


Figure 7. Sender's Window

Receiver's Window

- At the beginning of transmission, the receiver's window contains n-1 spaces for frames.
- As new frames come in, the size of the receiver window shrinks as soon as the acknowledgement is sent.
- The window expands to include spaces for a number of frames equal to the number of frames acknowledged.

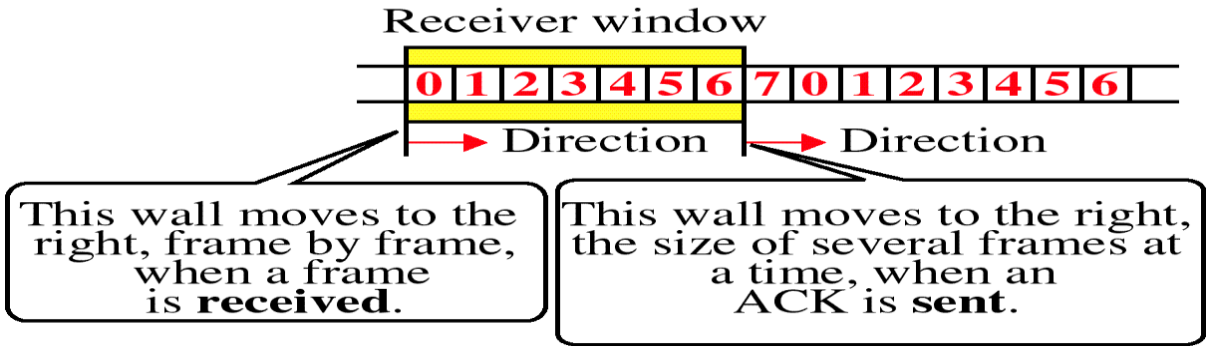


Figure 8. Receiver's Window

Example of Sliding Window Flow Control

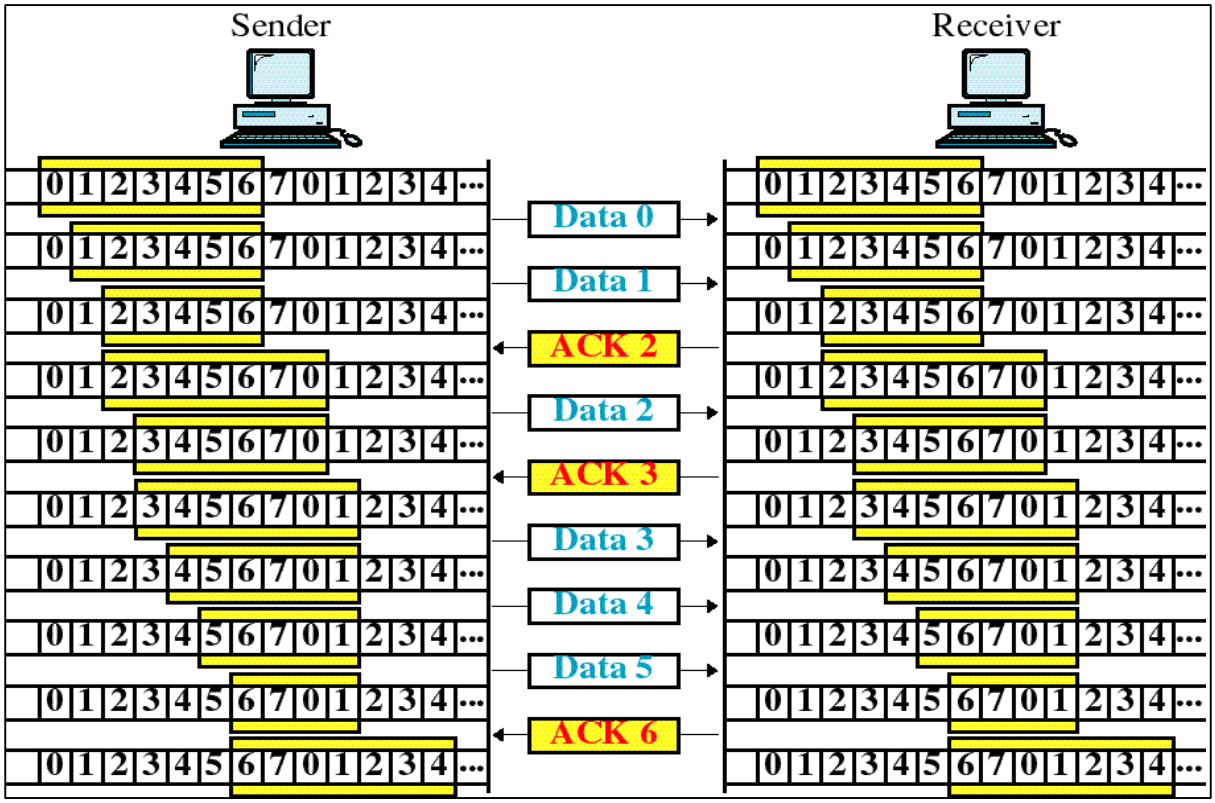


Figure 9. Sliding Window Flow Control

3.3. Error Detection and Correction

Error Detection

- Data can be corrupted during transmission.
- For reliable communication, error must be detected and corrected.
- Whenever an electromagnetic signal flows from one point to another, it is subjected to an interference from heat, magnetism and other forms of electric signals.
- This interference can change the shape of timing of the signal.
- Errors are of 2 types.
  1. Single bit error: Only one bit in the data unit is changed.
  2. Burst error: 2 or more bits in the data unit is changed.
- Cyclic Redundancy Check (CRC) is one of the method used for error detection.

Cyclic Redundancy Check (CRC)

- CRC is one of the most common error detecting codes.
- In CRC, a sequence of redundant bits called CRC remainder is appended to the end of the data unit.
- So the resulting data becomes exactly divisible by a predetermined binary number.
- At the receiver end, the incoming data unit is divided by the same number.
- If at this step, there is no remainder the data unit is assumed error free and is therefore accepted,

- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

CRC Generator and Checker

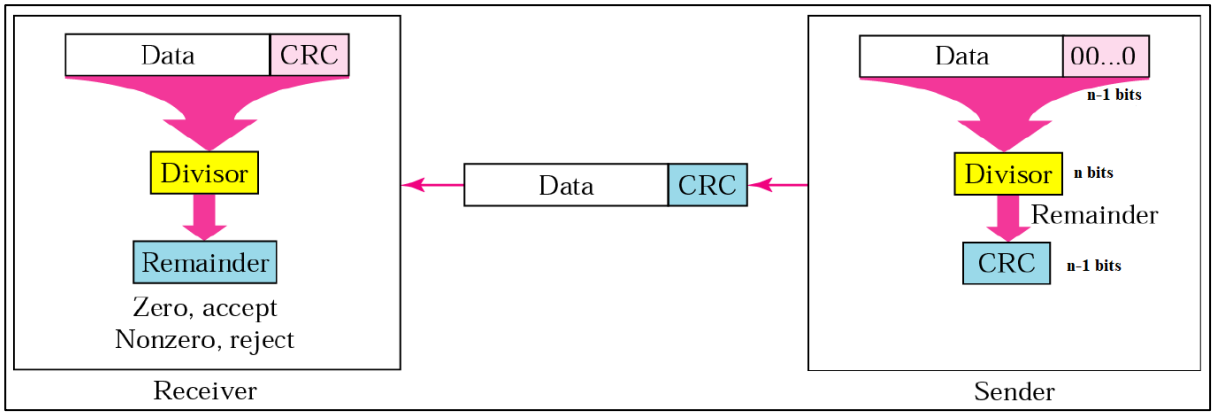


Figure 10. CRC Generator and Checker

The basic steps involved in CRC are:

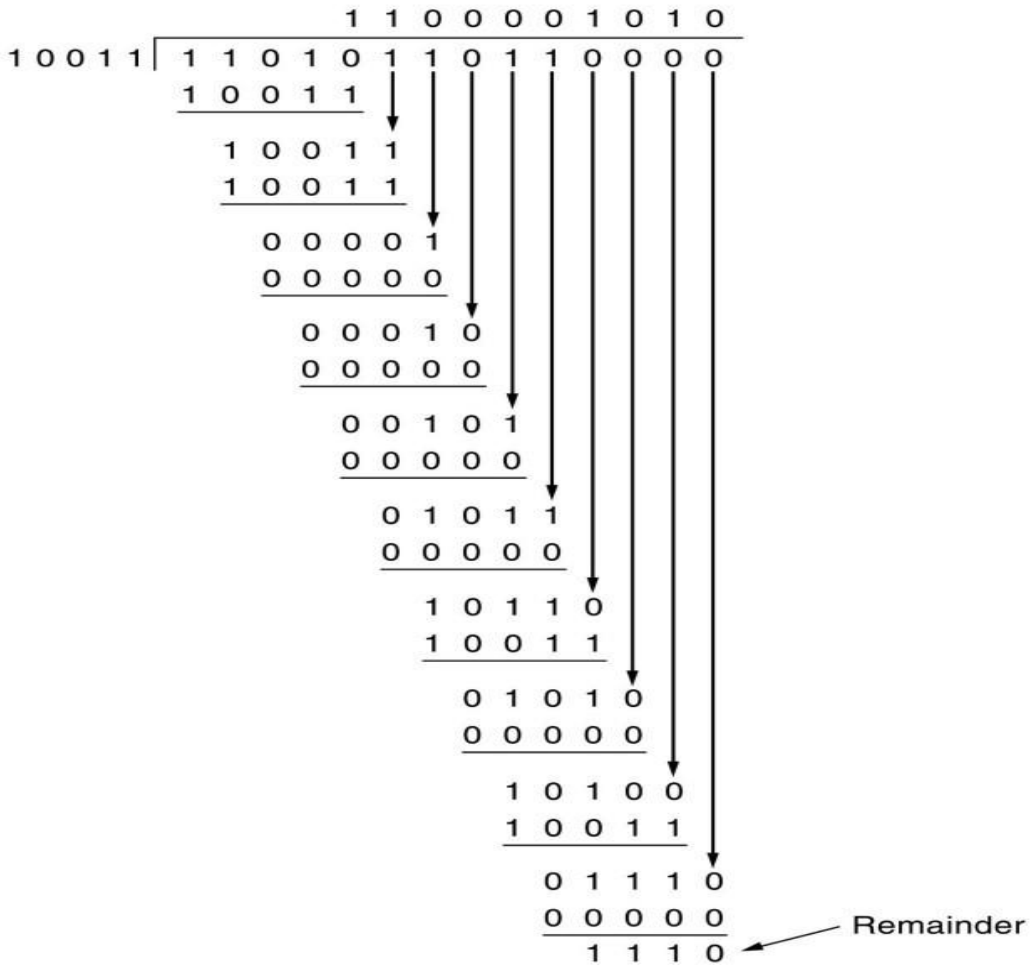
1. A string of n-1 zero's is appended to the data unit.
2. The number 'n' is the number of bits in the predetermined divisor.
3. The newly elongated data unit is divided by the divisor using a process called Binary Division (or XOR division or Modulo-2 division).
4. The remainder resulting from the division is called CRC.
5. The CRC of n-1 bits derived replaces the zeroes at the end of the data.
6. The data unit followed by the CRC arrives at the receiver end.
7. The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder.
8. If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes.
9. If the string has been changed in the transit, the division gives a non-zero remainder and the data unit does not pass.

Q1. A bit stream 1101011011 is transmitted using the standard CRC method. The generator polynomial is x^4+x+1. What is the actual bit string transmitted?

Solution:

- The generator polynomial $G(x) = x^4 + x + 1$ is encoded as 10011.
- Clearly, the generator polynomial consists of 5 bits.
- So, a string of 4 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 1101011011**0000**.

Now, the binary division is performed as-



From here, CRC = 1110.

Now,

- The code word to be transmitted is obtained by replacing the last 4 zeroes of 1101011011**0000** with the CRC.
- Thus, the code word transmitted to the receiver = 1101011011**1110**.

Q2. A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is x^3+1.

1. What is the actual bit string transmitted?
2. Suppose the third bit from the left is inverted during transmission. How will receiver detect this error?

Solution:

Part 1	**Part 2**
• The generator polynomial $G(x) = x^3 + 1$ is encoded as 1001. • Clearly, the generator polynomial consists of 4 bits. • So, a string of 3 zeroes is appended to the bit stream to be transmitted.	According to the question, • Third bit from the left gets inverted during transmission. • So, the bit stream received by the receiver = 10111101100. Now,

<table>
<tr>
<td>

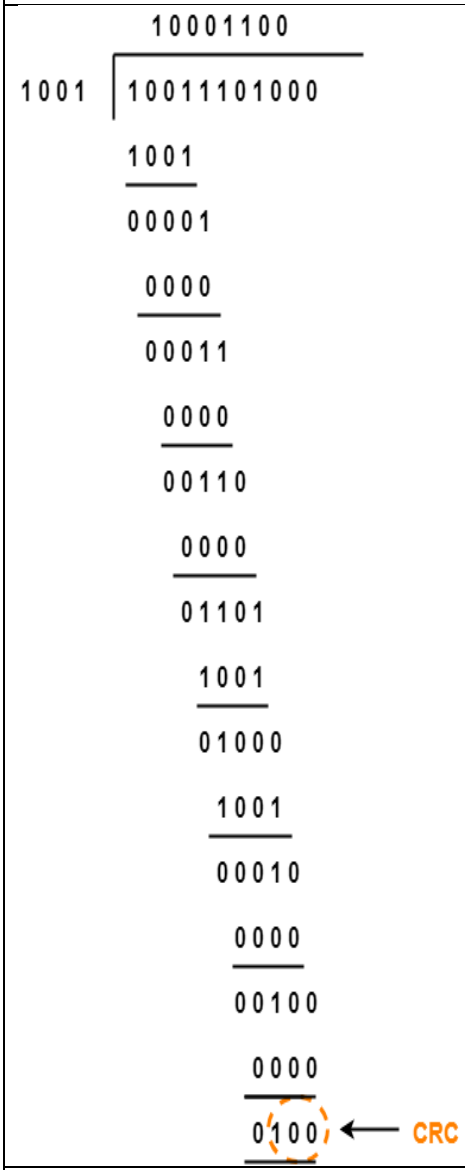
- The resulting bit stream is 10011101**000**.

Now, the binary division is performed as-

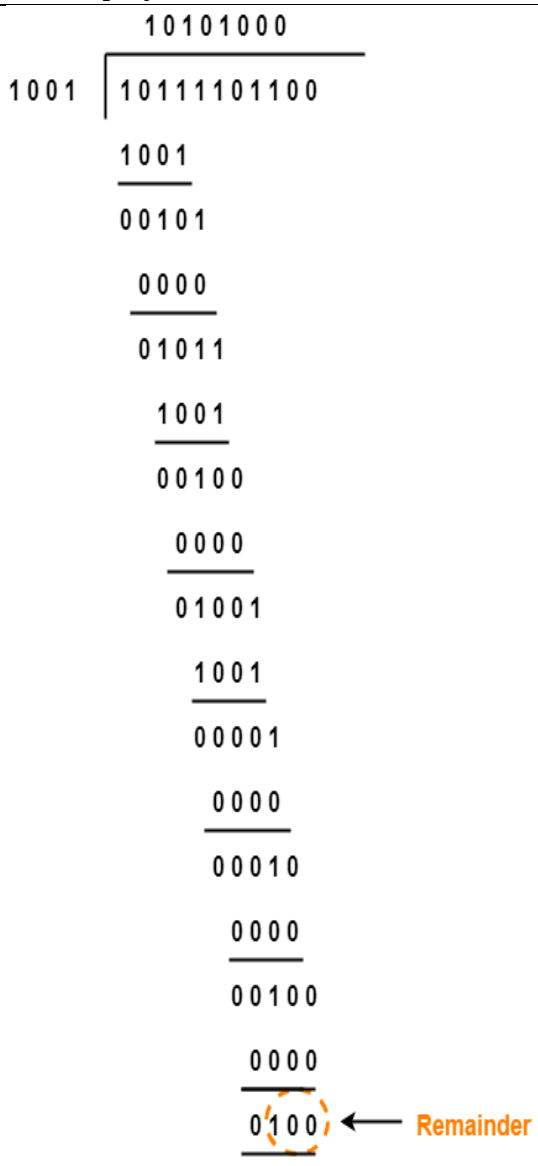
</td>
<td>

- Receiver receives the bit stream = 10111101100.
- Receiver performs the binary division with the same generator polynomial as-

</td>
</tr>
<tr>
<td>



</td>
<td>



</td>
</tr>
<tr>
<td>

From here, CRC = 100.

Now,

- The code word to be transmitted is obtained by replacing the last 3 zeroes of 10011101**000** with the CRC.
- Thus, the code word transmitted to the receiver = 10011101**100**.

</td>
<td>

From here, remainder = 100.

- The remainder obtained on division is a non-zero value.
- This indicates to the receiver that an error occurred in the data during the transmission.
- Therefore, receiver rejects the data and asks the sender for retransmission.

</td>
</tr>
</table>

Error Correction

- Hamming code is an error correcting code.
- Hamming codes are linear block codes.
- Parity bits are used here.
- They are inserted in between the data bits.
- The most commonly used is a 7-bit Hamming code.
- Structure of a 7-bit Hamming code:

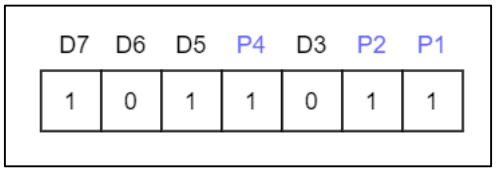


Figure 11. 7-bit Hamming Code Structure (D→ Data bits, P→ Parity bits)

- Parity bits are in position 2^m; where m = 0, 1, 2, ….
- Computing the values of parity bits:

7	6	5	4	3	2	1	←Position
D7	D6	D5	P4	D3	P2	P1	
111	110	101	100	011	010	001	3-bit binary of position no.

- To find P1, select positions that has first bit as 1 from LSB i.e. positions 1,3,5,7.
- To find P2, select positions that has second bit as 1 from LSB i.e. positions 2,3,6,7.
- To find P4, select positions that has third bit as 1 from LSB i.e. positions 4, 5, 6, 7.
- Parity can be even or odd.
  If we want to find even parity, then number of 1's excluding parity bit has to be even. If yes, then the parity bit becomes 0; otherwise the parity bit becomes 1.
  If we want to find odd parity, then number of 1's excluding parity bit has to be odd. If yes, then the parity bit becomes 0; otherwise the parity bit becomes 1.

Q1. A bit word 1011 is to be transmitted. Construct the even parity 7-bit Hamming code for the data.

Solution:

7	6	5	4	3	2	1	←Position
D7	D6	D5	P4	D3	P2	P1	
1	0	1	P4	1	P2	P1	Bits

To find P1, take bits in the position 1, 3, 5, 7. They are P1, 1, 1, 1 respectively.
Given even parity. Therefore, number of 1's need to be even.
Hence, P1 = 1.
To find P2, take bits in the position 2, 3, 6, 7. They are P2, 1, 0, 1 respectively.
Given even parity. Therefore, number of 1's need to be even.
Hence, P2 = 0.
To find P4, take bits in the position 4, 5, 6, 7. They are P4, 1, 0, 1 respectively.
Given even parity. Therefore, number of 1's need to be even.
Hence, P4 = 0.
So, the even parity 7-bit Hamming code for data 1011 is **1010101**.

Q2. Determine which bit is in error in the even parity. Hamming code character is 1100111.

Solution:

7	6	5	4	3	2	1	←Position
D7	D6	D5	P4	D3	P2	P1	
1	1	0	0	1	1	1	Bits

To find P1, take bits in the position 1, 3, 5, 7. They are 1, 1, 0, 1 respectively.
Given even parity. Therefore, number of 1's need to be even.
Hence, P1 = 0. But here P1 =1 is given. Therefore, **P1 bit is in error**.
To find P2, take bits in the position 2, 3, 6, 7. They are 1, 1, 1, 1 respectively.
Given even parity. Therefore, number of 1's need to be even.
Hence, P2 = 1. Therefore, P2 is not in error.
To find P4, take bits in the position 4, 5, 6, 7. They are 0, 0, 1, 1 respectively.
Given even parity. Therefore, number of 1's need to be even.
Hence, P4 = 0. Therefore, P4 is not in error.
So only P1 bit is in error.
Corrected Hamming code character is **1100110**.

3.4. 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:
    1. **Error detection**: The sender and receiver, either both or any, must ascertain that there is some error in the transit.
    2. **Positive ACK**: When the receiver receives a correct frame, it should acknowledge it.
    3. **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.
    4. **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):

1. 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.

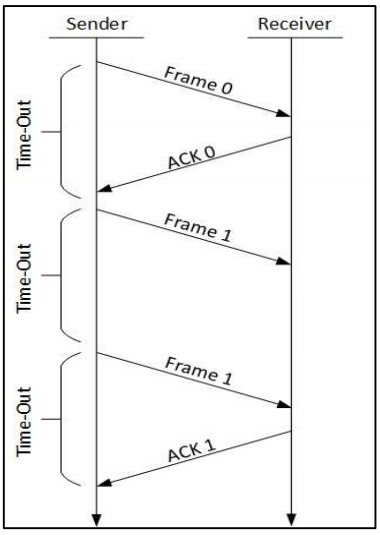


Figure 11. Stop-and-Wait ARQ

2. 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.

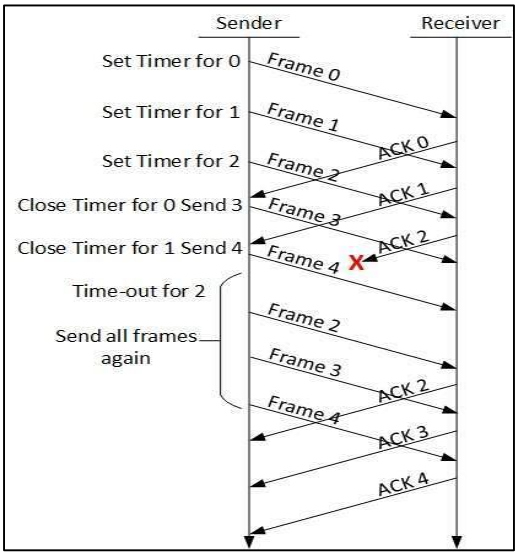


Figure 12. Go-Back-N ARQ

3. 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.

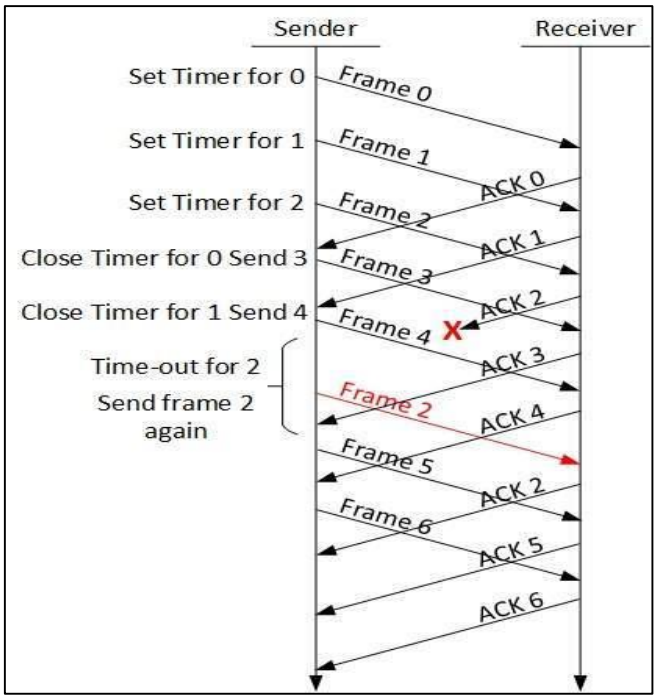


Figure 13. Selective Repeat ARQ

3.5. Elementary Data Link Protocols

In this section, we are going to discuss some elementary data link layer protocols.

3.5.1. Unrestricted Simplex Protocol

- This protocol is the simplest possible protocol.
- The transmission of data takes place in only one direction. So it is a simplex (unidirectional) protocol.
- It is assumed that the network layers of sender and receiver are always ready.
- It is also assumed that the processing time can be ignored and infinite buffer space is available.
- The communication channel is imagined to be noise free, so it does not damage or lose any frames.
- All this is highly unrealistic. This protocol is also called as "**utopia**".
- This protocol consists of two distinct procedures, namely a sender and a receiver.
- The sender runs in the data link layer of the sender machine whereas the receiver runs in the data link layer of the receiver machine.
- No sequence numbers or acknowledgements are used.

3.5.2. Simplex Stop and Wait Protocol

- The most unrealistic restriction in the previous protocol is the assumption that the receiving network layer can process the data with zero processing time.
- In this protocol it is assumed that a finite processing time is essential.
- However, like the unrestricted simplex protocol, the communication channel is assumed to be noise free and the communication is simplex, i.e. only in one direction.
- This protocol deals with the important problem i.e. how to prevent the sender from flooding the receiver with data faster than its processing speed.
- In this protocol, a small dummy frame is sent back from the receiver to the sender to indicate that it can send the next frame.
- The sender sends one frame and then waits for the dummy frame called acknowledgement.
- Once the acknowledgement is received, it sends the next frame. Hence the name stop-and-wait.
- The best thing about this protocol is that the incoming frame is always an acknowledgement.

3.5.3. Simplex Protocol for Noisy Channel

- This is the third protocol in which we go one step ahead and assume that the communication channel is noisy and can introduce errors in the data travelling over it.
- Frames may either be damaged or lost completely.
- In this protocol, the sender waits for a positive acknowledgement before advancing to the next data item.
- So it is called as PAR (Positive Acknowledgement with Retransmission) or ARQ (Automatic Repeat Request).
- Due to retransmission, there is always a possibility of duplication of frames at the receiver.
- To avoid this, the sender puts a sequence number in the header of each frame it sends.
- The receiver can check the sequence number of each arriving frame to check the possible duplication. If the frame is duplicated, then the receiver will discard it.

3.6. Piggybacking

- In all the practical situations, the transmission of data needs to be full-duplex (i.e. bidirectional).
- One way of achieving full duplex transmission is to have two separate channels, one for forward data transfer and the other for reverse transfer for acknowledgements.
- But this will waste the bandwidth of the reverse channel almost entirely.
- A better solution would be to use each channel (forward and reverse) to transmit frames both ways, with both channels having the same capacity.
- Let A and B be the users. Then the data frames from A to B are intermixed with the acknowledgements from A to B.
- One more improvement can be made. When a data frame arrives, the receiver waits, does not send the acknowledgement back immediately.
- The receiver waits until its network layer passes in the next dat packet.

- The acknowledgement is then attached to this outgoing data frame.
- This technique in which the outgoing acknowledgement is delayed temporarily is called as piggybacking.
- **Advantage**: Better utilization of available channel bandwidth.
- **Disadvantage**: If the data link layer waits too long before transmitting acknowledgement, then retransmission of frame would take place.

3.7. Protocol Performance

- Throughput efficiency is the measure of the performance of an ARQ protocol. For any channel a certain bandwidth and bit error rate are specified.
- Throughput efficiency is defined as

$$\eta = \frac{t_f}{t_f + 2t_p}$$

where, t_f = transmission time required to transmit a frame

t_p = propagation time required to reach destination for a transmitted bit

- Frame size N = R x t_f, where R = Data rate

Q1. Calculate the throughput for stop-and-wait flow control mechanism if the frame size is 4800 bits, bit rate is 9600 bps and distance between device is 2000 km. Speed of propagation over the transmission is 200, 000 km/s.

Solution:

Given, Frame size N = 4800 bits

Bit rate R = 9600 bps

Distance D= 2000 km

Speed V= 200,000 km/s

We have, N = R x t_f

$$t_f = \frac{N}{R} = \frac{4800}{9600} = 0.5sec$$

$$t_p = \frac{D}{V} = \frac{2000}{200000} = 0.01\ sec$$

$$\eta = \frac{t_f}{t_f + 2t_p} = \frac{0.5}{0.5 + 2 \times 0.01} = 0.96$$

Therefore, **throughput = 96%**

Q2. A channel has a bit rate of 4 kbps and propagation delay of 20 msec. For what range of frame size does stop and wait gives the efficiency of at least 50%.

Solution:

Given, Bit rate R = 4kbps

Propagation delay t_p= 20 ms

Efficiency $\eta \geq 50$ % i.e. $0.5 \leq \eta \leq 1$

$$\eta = \frac{t_f}{t_f + 2t_p}$$

For η = 0.5 we get, $0.5 = \frac{t_f}{t_f + 2 \times 20 \times 10^{-3}}$

$\therefore 0.5t_f + 20 \times 10^{-3} = t_f$

$\therefore t_f = 40 \times 10^{-3} sec$

We have, N = R x t_f

$\therefore N = 4 \times 10^3 \times 40 \times 10^{-3} = 160\ bits$

Therefore, **frame size = 160 bits**

3.7. High Level Data Link Control (HDLC) Protocol

- HDLC (High-Level Data Link Control) is a bit-oriented code-transparent synchronous data link layer protocol developed by the International Organization for Standardization (ISO).
- HDLC provides both connection-oriented and connectionless service.
- In HDLC, data is organized into a unit (called a frame) and sent across a network to a destination that verifies its successful arrival.
- It supports half-duplex, full-duplex transmission, point-to-point, and multi-point configuration and switched or non-switched channels.

Types of stations for HDLC Protocol:

Primary station:
- It acts as a master and controls the operation.
- Handles error recovery.
- Frames issued by the primary station are called commands.

Secondary station:
- It acts as a slave and operates under the control of the primary station.
- Frames issued by a secondary station are called responses.
- The primary station maintains a separate logical link with each secondary station.

Combined station:
- Acts as both primary and secondary stations.
- It does not rely on others for sending data.

HDLC Data transfer modes:

HDLC communications session can use one of the following connection modes, which determine how the primary and secondary stations interact.

- **Normal Response mode (NRM)**
  i. A secondary station can only transmit when specifically instructed by the primary station in response to polling.
  ii. It is used for both point-to-point and multipoint communications.
  iii. It is an unbalanced configuration and good for multi-point links.
- **Asynchronous Response mode (ARM)**
  i. It is similar to NRM except that the secondary stations can initiate transmissions without direct polling from the primary station.
  ii. Asynchronous Response Mode (ARM) is an unbalanced configuration.
  iii. It has a single primary station and multiple secondary stations.
- **Asynchronous Balanced mode (ABM)**
  i. Asynchronous balanced mode (ABM) is a balanced configuration.
  ii. It uses combined stations.

HDLC Frame Types

In HDLC both data and control messages are carried in a standard format frame. Three classes of frames are used in HDLC.

- **Unnumbered frame (U-frame)**
    i. These are used for functions like link setup and disconnection.
    ii. They do not contain any acknowledgement information, which is used in sequence numbers.
- **Information frame (I-frame)**
    i. These carry the actual information or data from the network layer.
    ii. I-frames can also include flow and error control information piggybacked on data.
- **Supervisory frame (S-frame)**
    i. S-frames, are used for flow and error control whenever piggybacking is impossible or inappropriate, such as when a station does not have data to send.
    ii. S-frames do not have information fields.

HDLC Frame Structure

- HDLC uses synchronous transmission. All transmissions are in the form of frames.
- Figure 14 below shows the format of HDLC frame.
- The flag, address and control bits before the information or data field are known as a header. The FCS and flag fields following the information or data field are referred as a trailer.

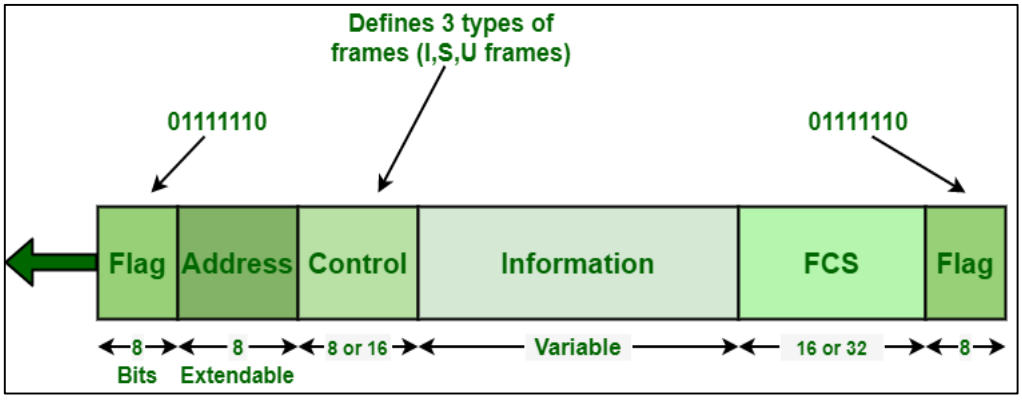


Figure 14. HDLC Frame Structure

- **Flag fields**: It has a unique pattern (i.e. 01111110) at both the ends of the frame structure. It identifies the start and the end of the frame. The length of the flag field is 8 bits.
- **Address field**: Address field states the destination address. The address field is usually 8-bit long, but can be extended.
- **Control field**: Control field contains frame numbers. Also it controls the acknowledgement of frames. Control field is 8 or 16 bit in length.
- **Information (or Data) field**: This field contains the user data received from the network layer. It can be of variable length but in integral number of octets.
- **FCS (Frame Check Sequence)**: FCS is an error detecting code calculated from the remaining bits of the frame. FCS can be 16 or 32 bits long.

3.8. Medium Access Control

The data link layer is the second lowest layer. It is divided into two sublayers −

- The logical link control (LLC) sublayer
- The medium access control (MAC) sublayer

Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

3.9. Channel Allocation Problem

- When there is more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users.
- The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.
- Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.

Channel Allocation Schemes

Channel Allocation may be done using two schemes −

1. Static Channel Allocation
2. Dynamic Channel Allocation

Static Channel Allocation

- In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user.
- For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.
- This scheme is also referred as fixed channel allocation or fixed channel assignment.
- In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel.
- However, it is not suitable in case of a large number of users with variable bandwidth requirements.

Dynamic Channel Allocation

- In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users.
- Instead channels are allotted to users dynamically as needed, from a central pool.
- The allocation is done considering a number of parameters so that transmission interference is minimized.
- This allocation scheme optimises bandwidth usage and results is faster transmissions.
- Dynamic channel allocation is further divided into centralised and distributed allocation.
- Possible assumptions include:
  Station Model: Assumes that each of N stations independently produce frames. Once the frame is generated at the station, the station does nothing until the frame has been successfully transmitted.
  Single Channel Assumption: In this allocation all stations are equivalent and can send and receive on that channel.
  Collision Assumption: If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must be retransmitted. Collisions are only possible error.
  Time can be divided into Slotted or Continuous.
  Stations can sense a channel is busy before they try it.

3.10. ALOHA

- ALOHA is a multiple access protocol for transmission of data via a shared network channel.
- It operates in the medium access control sublayer (MAC sublayer).
- In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy.
- If the channel is idle, then the frames will be successfully transmitted.
- If two frames attempt to occupy the channel simultaneously, collision of frames will occur and the frames will be discarded.
- These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.

Pure ALOHA

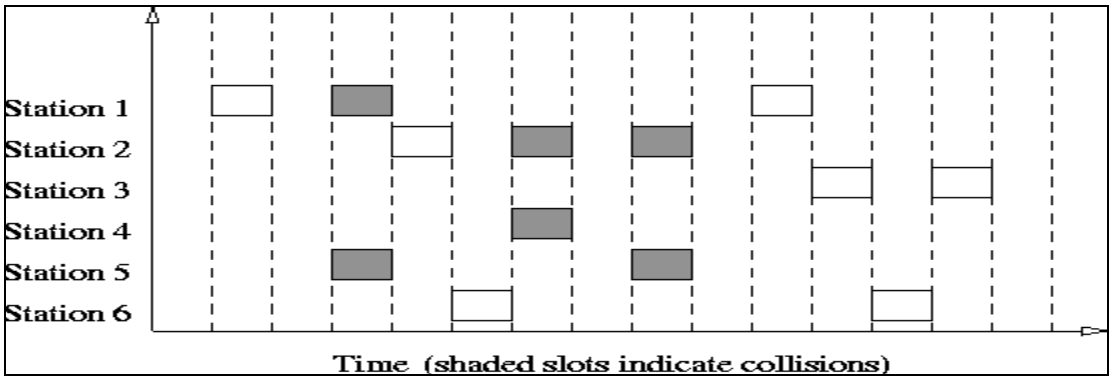


Figure 15. Pure ALOHA

- In pure ALOHA, the time of transmission is continuous.
- Time is not slotted and stations can transmit whenever they want.
- There is high possibility of collision and the colliding frames will be destroyed.
- If frames collide and get destroyed, then the sender waits for random amount of time and resends the frame.

Slotted ALOHA

- Slotted ALOHA reduces the number of collisions and doubles the capacity of pure ALOHA.
- The shared channel is divided into a number of discrete time intervals called slots.
- A station can transmit only at the beginning of each slot.
- However, there can still be collisions if more than one station tries to transmit at the beginning of the same time slot.

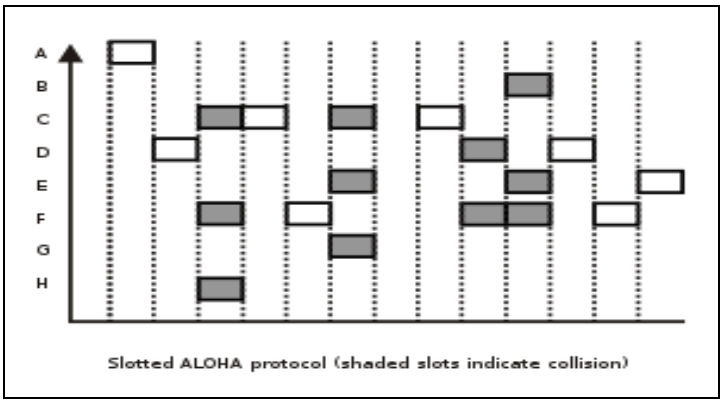


Figure 16. Slotted ALOHA

Efficiency of ALOHA

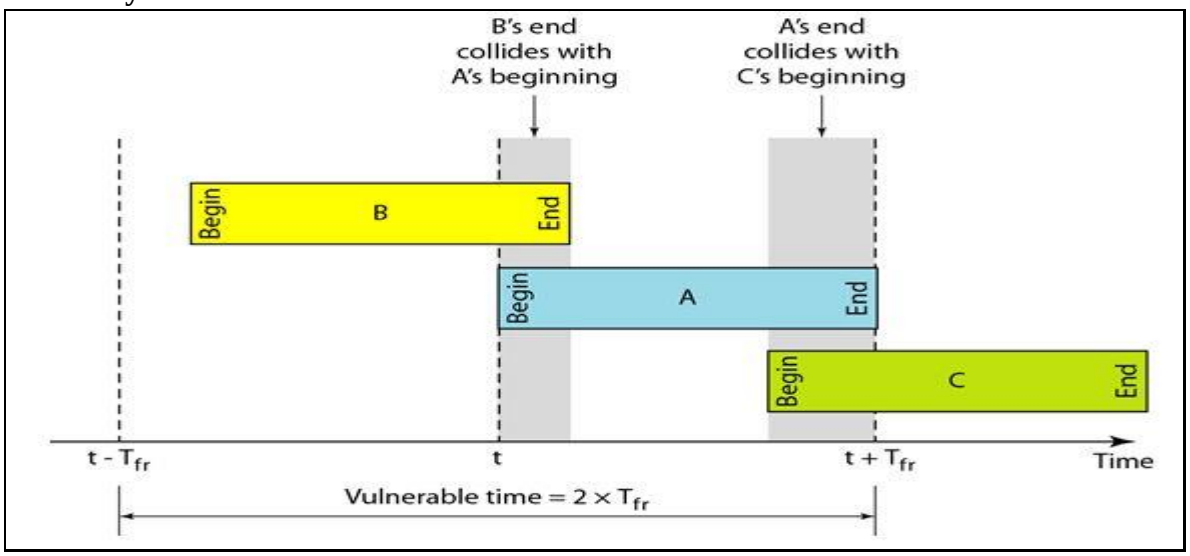


Figure 17. Vulnerable Time of Frame A

- Station A sends a frame at time t.
- Now imagine station B has already sent a frame between t - T_{fr} and t. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame. On the other hand, suppose that station C sends a frame

between t and t + T_{fr}. Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.

Terms Used

- Frame Time: Time required to transmit a frame
- G: Average number of new + old frames generated per frame time.
  (Old frames are the frames which have to be retransmitted due to collision)
- S: Average number of new frames generated per frame time
- P_0: Probability that the frame does not suffer collision.
- VP (Vulnerable Period): Time for which a station should not transmit anything to avoid collision with the shaded frame.
- For pure ALOHA, vulnerable period = 2 time slots.
- For slotted ALOHA, vulnerable period = 1 time slot.
- (This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. In slotted ALOHA, frame can start at only two times t - T_{fr} and t. If the frame B start at time t - T_{fr}, it will not collide with frame A. If the frame B start at time t - T_{fr}, it will collide with frame A. Therefore, collision can take place in only one time slot.)

Derivation:

At low load, S ≈ 0 and G ≈ 0.

∴ S = G

At high load, $S = G.P_0$ ……..(I)

According to Poisson distribution formula

$P_k = \frac{e^{-m}m^k}{k!}$, where m is the mean and k is the random variable

For k = 0, $P_0 = e^{-m}$

∴ $S = G.\ e^{-m}$ ……. (II)

For pure ALOHA,

VP = 2 time slots

∴ m = 2G

Putting m = 2G in equation (II), we get

$S = G.\ e^{-2G}$

Differentiating w.r.t G and equate it to zero

$\frac{dS}{dG} = \frac{d}{dG}(G.\ e^{-2G}) = 0$

$G\ e^{-2G}(-2) + e^{-2G}(1) = 0$

$e^{-2G}(1 - 2G) = 0$

∴ (1-2G) = 0

∴ G = 0.5

At G = 0.5, $S_{max} = G.\ e^{-2G} = 0.5\ e^{-2x0.5}$

∴ $S_{max} = 0.184$

∴ $\boldsymbol{\eta_{max} = 0.184 \times 100 = 18.4\%}$

For slotted ALOHA,

VP = 1 time slot

$\therefore$ m = G

Putting m = G in equation (II), we get

$S = G.\ e^{-G}$

Differentiating w.r.t G and equate it to zero

$\frac{dS}{dG} = \frac{d}{dG}(G.\ e^{-G}) = 0$

$G\ e^{-G}(-1) + e^{-G}(1) = 0$

$e^{-2G}(1 - G) = 0$

$\therefore (1-G) = 0$

$\therefore G = 1$

At G = 1, $S_{max} = G.\ e^{-G} = 1e^{-1}$

$\therefore S_{max} = 0.368$

$\therefore \boldsymbol{\eta_{max} = 0.368 \times 100 = 36.8\%}$

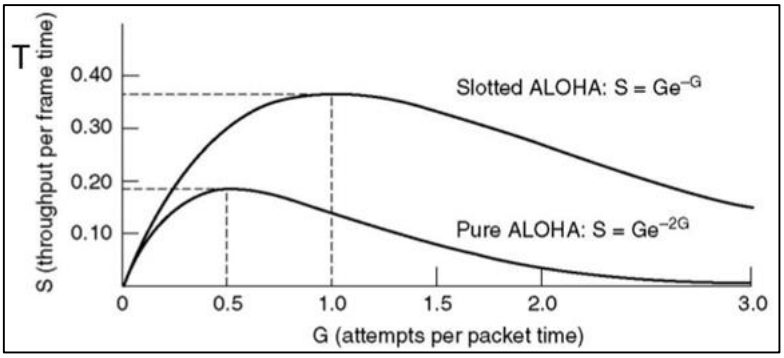


Figure 18. Efficiency of ALOHA

Difference Between Pure ALOHA and Slotted ALOHA

Pure ALOHA	Slotted ALOHA
Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
Vulnerable time in which collision may occur = 2 x T	Vulnerable time in which collision may occur = T
Probability of successful transmission of data packet = $G \times e^{-2G}$	Probability of successful transmission of data packet = $G \times e^{-G}$
Maximum efficiency = 18.4% (Occurs at G = 1/2)	Maximum efficiency = 36.8% (Occurs at G = 1)
The main advantage of pure ALOHA is its simplicity in implementation.	The main advantage of slotted ALOHA is that it reduces the number of collisions to half and doubles the efficiency of pure aloha.

Q1. A group of N stations share 100 Kbps slotted ALOHA channel. Each station output a 500 bits frame on an average of 5000ms even if previous one has not been sent. What is the required value of N?

Solution:

Throughput of One Station

Throughput of each station
= Number of bits sent per second
= 500 bits / 5000ms
= 500 bits / (5000 x 10^{-3} sec)
= 100 bits/sec

Throughput of Slotted ALOHA

Throughput of slotted ALOHA
= Efficiency x Bandwidth
= 0.368 x 100 Kbps
= 36.8 Kbps

Total Number of Stations

Throughput of slotted aloha = Total number of stations x Throughput of each station
Substituting the values, we get-
36.8 Kbps = N x 100 bits/sec
∴ N = 368
Thus, required value of **N = 368**.

Q2. A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces:
a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second.

Solution:

The frame transmission time is 200/200 kbps or 1 ms.
a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or S = 0.135 (13.5 percent). This means that the throughput is 1000 × 0.135 = 135 frames. Only 135 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or S = 0.184 (18.4 percent). This means that the throughput is 500 × 0.184 = 92 frames. Only 92 frames out of 500 will probably survive.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or S = 0.152 (15.2 percent). This means that the throughput is 250 × 0.152 = 38 frames. Only 38 frames out of 250 will probably survive.

Q3. A slotted ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces:
a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second.

Solution:
The frame transmission time is 200/200 kbps or 1 ms.
a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G\times e^{-G}$ or S = 0.368 (36.8 percent). This means that the throughput is 1000 × 0.368 = 368 frames. Only 368 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G\times e^{-G}$ or S = 0.303 (30.3 percent). This means that the throughput is 500 × 0.303 = 151 frames. Only 151 frames out of 500 will probably survive.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/2). In this case $S = G\times e^{-G}$ or S = 0.195 (19.5 percent). This means that the throughput is 250 × 0.195 = 49 frames. Only 49 frames out of 250 will probably survive.

3.11. CSMA (Carrier Sense Multiple Access) Protocol

Carrier Sense: A station can sense the channel to see if anyone is using it. If the channel is being used, then the station will not attempt to use the channel.

Types:
(a) 1-Persistent CSMA
(b) Non-persistent CSMA
(c) p- Persistent CSMA
(d) CSMA/CD

(a) 1-Persistent CSMA

- When a station needs to send data, it first listens to the channel.
- If the channel is busy, the station waits till the channel becomes free.
- When the channel becomes free, a station can transmit a frame.
- A collision occurs when two stations detect an idle channel at the same time abd simultaneously send frames.
- If a collision occurs, the station waits a random amount of time and starts all over again.
- It is called 1-persistent as the station will transmit with a probability of 1, when it finds the channel idle.

Drawbacks

- Propagation Delay: It is possible that just after a station begins transmitting, another station becomes ready to send and it will sense the channel. If the first station's signal has not yet reached the 2nd station, the 2nd station will sense an idle channel and will begin sending its data. This will lead to a collision.
- Assume that station 2 and station 3 are waiting for station 1 to finish its transmission. Immediately after station 1 finishes transmitting, both station 2 and station 3 begin transmitting at the same time thus leading to a collision.

Advantage

- Due to carrier sense property, 1-persistent CSMA gives better performance than the ALOHA systems.

(b) Non-persistent CSMA

- A station senses the channel when it wants to send data.
- If the channel is idle, the station begins sending the data.
- However, if the channel is busy, the station does not continually sense the channel like 1-persistent CSMA. Instead, it waits a random period of time and then checks the channel again.

Disadvantage

- This leads to longer delays than 1-persistent CSMA.

Advantage

- This algorithm leads to better channel utilization.

(c) p-persistent CSMA

- It is used for slotted channels.
- When a station becomes ready to send, it senses the channel.
- If channel is idle, station transmits within that slot with a probability p and defers from sending with a probability q = 1- p.
- If p > q, then the station transmits, else if p < q, then the station does not transmit and waits till the next slot and again checks if p > q or p < q.
- This process is repeated until either the frame has been transmitted or another station has started transmitting.

3.12. CSMA/CD (Carrier Sense Multiple Access with Collison Detection)

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer.
- It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free.
- The collision detection technology detects collisions by sensing transmissions from other stations.
- On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

Algorithms

The algorithm of CSMA/CD is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
- If a collision is detected, the station starts the collision resolution algorithm.
- The station resets the retransmission counters and completes frame transmission.

The algorithm of Collision Resolution is:

- The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.

- The station increments the retransmission counter.
- If the maximum number of retransmission attempts is reached, then the station aborts transmission.
- Otherwise, the station waits for a back-off period which is generally a function of the number of collisions and restart main algorithm.

Frame format of CSMA/CD

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

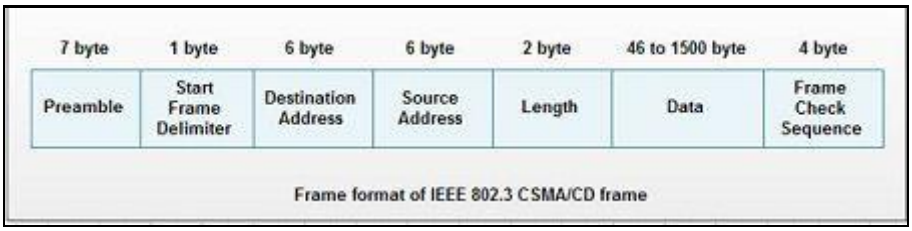


Figure 19. CSMA/CD Frame Format

1. **Preamble**: It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating 0s 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 four-byte field contains CRC for error detection.

Q1. A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including (including the delays in the devices and ignoring the time needed to send a jamming) is 25.6 μs, what is the minimum size of the frame?

Solution:

Propagation delay $T_p = 25.6$ μs

Bandwidth = 10 Mbps

Frame transmission time $T_{fr} = 2 \times T_p = 2 \times 25.6$ μs = 51.2 μs

Minimum frame size = Bandwidth x T_{fr} = 10 Mbps x 51.2 μs

= **512 bits = 64 bytes**

Q2. Consider a CSMA/CD network that transmits data at a rate of 100 Mbps over a 1km cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, what is the signal speed (km/sec) in the cable?

Solution:

Bandwidth = 100 Mbps

Distance = 1 km

Minimum frame size = 1250 bytes

Minimum frame size = Bandwidth x T_{fr} = 100 Mbps x T_{fr}

$\therefore 1250 \times 8 = 100 \times 10^6 \times T_{fr}$

$\therefore T_{fr} = \frac{1250 \times 8}{10^8} = \mathbf{1 \times 10^{-4} sec}$

Frame transmission time T_{fr} = 2 x T_p

$T_p = \frac{T_{fr}}{2} = \frac{1 \times 10^{-4}}{2} = \mathbf{5 \times 10^{-5}\ sec}$

Speed = $\frac{\text{Distance}}{\text{Time}} = \frac{1\text{ km}}{5 \times 10^{-5}\text{ sec}} = \mathbf{20000\ km/sec}$

3.13. Ethernet 802.3

- Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies which are allowed.
- Ethernet generally uses Bus Topology.
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.
- For Ethernet, the protocol data unit is Frame since we mainly deal with DLL.
- In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.
- Manchester Encoding Technique is used in Ethernet where 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition and **Baud rate = 2 x Bit rate**.
- Ethernet LANs consist of network nodes and interconnecting media or link. The network nodes can be of two types:
- **Data Terminal Equipment (DTE):** Generally, DTEs are the end devices that convert the user information into signals or reconvert the received signals. DTEs devices are: personal computers, workstations, file servers or print servers also referred to as end stations. These devices are either the source or the destination of data frames.
- **Data Communication Equipment (DCE):** DCEs are the intermediate network devices that receive and forward frames across the network. They may be either standalone devices such as repeaters, network switches, routers or maybe communications interface units such as interface cards and modems. The DCE performs functions such as signal conversion, coding and may be a part of the DTE or intermediate equipment.

IEEE 802.3 Frame Format

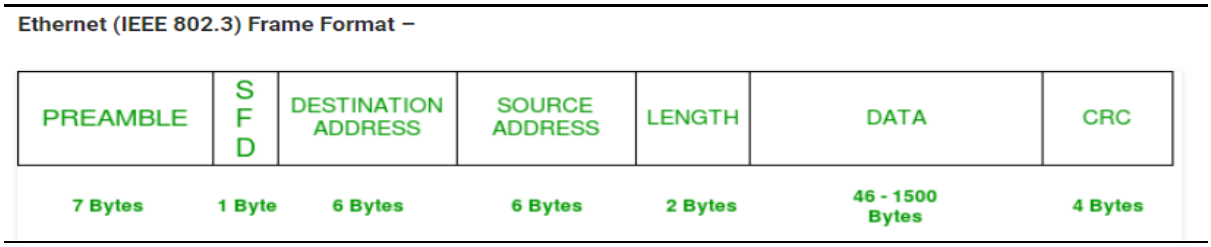
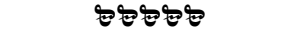


Figure 20. Ethernet Frame Format

- **Preamble**: It is the starting field that provides alert and timing pulse for transmission. It is of 7 bytes.
- **Start of Frame Delimiter**: It is a 1-byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address**: It is a 6-byte field containing physical address of destination stations.
- **Source Address**: It is a 6-byte field containing the physical address of the sending station.
- **Length**: Length is a 2-byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.
- **Data**: This is a variable sized field that carries the data from the upper layers. The maximum size of data field is 1500 bytes. **Padding of 0's is done** to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC is 4-byte field. CRC stands for cyclic redundancy check. It contains the error detection information.



CHAPTER 4

NETWORK LAYER

4.1 Network Layer Design Issues

Network layer is majorly focused on getting packets from the source to the destination, routing, error handling and congestion control. It is the lowest layer that deals with end-to-end transmission.

The network layer comes with some design issues described as follows:

1. Store and Forward packet switching

- The host sends the packet to the nearest router. This packet is stored there until it has fully arrived.
- Once the link is fully processed by verifying the checksum, then it is forwarded to the next router till it reaches the destination. This mechanism is called "Store and Forward packet switching."

2. Services provided to Transport Layer

- Through the network/transport layer interface, the network layer transfers its services to the transport layer. But before providing these services to the transport layer, following goals must be kept in mind:
  a. Offering services must not depend on router technology.
  b. The transport layer needs to be protected from the type, number and topology of the available router.
  c. The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections
- These services are described below:
  a. **Connectionless** – The routing and insertion of packets into subnet is done individually. No added setup is required.
  b. **Connection-Oriented** – Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service

- Packet are termed as "datagrams" and corresponding subnet as "datagram subnets".
- When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via a few protocol.
- Each data packet has destination address and is routed independently irrespective of the packets.

4. Implementation of Connection Oriented service

- To use a connection-oriented service, first we establish a connection, use it and then release it.
- In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.

It can be done in either two ways:

a. **Circuit Switched Connection:** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
b. **Virtual Circuit Switched Connection**: The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

4.2 Difference between Circuit Switching and Packet Switching

BASIS FOR COMPARISON	CIRCUIT SWITCHING	PACKET SWITCHING
Orientation	Connection oriented.	Connectionless.
Purpose	Initially designed for Voice communication.	Initially designed for Data Transmission.
Flexibility	Inflexible, because once a path is set all parts of a transmission follows the same path.	Flexible, because a route is created for each packet to travel to the destination.
Order	Message is received in the order, sent from the source.	Packets of a message are received out of order and assembled at the destination.
Technology/Approach	Circuit switching can be achieved using two technologies, either Space Division Switching or Time-Division Switching.	Packet Switching has two approaches Datagram Approach and Virtual Circuit Approach.
Layers	Circuit Switching is implemented at Physical Layer.	Packet Switching is implemented at Network Layer.

4.3 Difference between Virtual Circuit and Datagram Network

Sr. No.	Key	Virtual Circuits	Datagram Networks
1	Definition	Virtual Circuit is the connection oriented service in which there is a implementation of resources like buffers, CPU, bandwidth, etc., used by virtual circuit for a data transfer session.	Datagram is the connection less service where no such resources are required for the data transmission.
2	Path	In Virtual circuits as all the resources and bandwidth get reserved before the transmission, the path which is utilized or followed by first data packet would get fixed and all other data packets will use the same path and consume same resources.	In Datagram network, the path is not fixed as data packets are free to decide the path on any intermediate router on the go by dynamically changing routing tables on routers.

3	Header	As there is same path followed by all the data packets, a common and same header is being used by all the packets.	Different headers with information of other data packet is being used in Datagram network.
4	Complexity	Virtual Circuit is less complex as compared to that of Datagram network.	Datagram network are more complex as compared to Virtual circuit.
5	Reliability	Due to fixed path and assurance of fixed resources, Virtual Circuits are more reliable for data transmission as compared to Datagram network.	Datagram network due to dynamic resource allocation and follow dynamic path is more prone to error and is less reliable than Virtual circuits.
6	Example and Cost	Virtual circuits are costlier in installation and maintenance and are widely used by ATM (Asynchronous Transfer Mode) Network, which is used for the Telephone calls.	Datagram network are cheaper as compared to the Virtual Circuits and are mainly used by IP network, which is used for Data services like Internet.

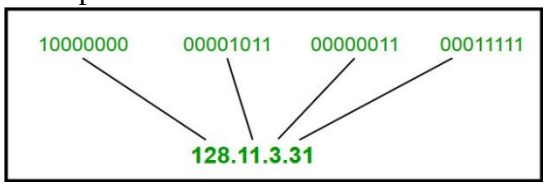
4.4 Communication Primitives

Data is transported over a network by three simple methods i.e. Unicast, Broadcast, and Multicast.

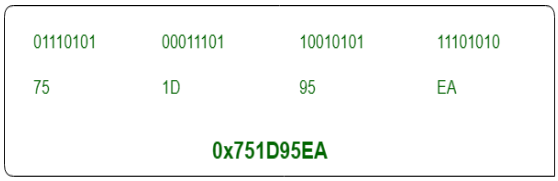
- **Unicast**: From one source to one destination i.e. One-to-One. **Example**: Telephone call
- **Broadcast**: From one source to all possible destinations i.e. One-to-All
  Example: Cable Television
- **Multicast**: From one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many. **Example**: Email

4.5 IPv4 Addressing

- The IPv4 address is a 32-bit number that uniquely identifies a network interface on a system.
- An IP address can be written in three notations; dotted-decimal, binary and hexadecimal. Among these types, dotted-decimal is the most popular and frequently used method for writing an IP address.
- An IPv4 address written in decimal digits is divided into four 8-bit fields that are separated by periods. Each 8-bit field represents a byte of the IPv4 address.
- This form of representing the bytes of an IPv4 address is often referred to as the dotted-decimal format.
  Example:



Dotted Decimal Notation



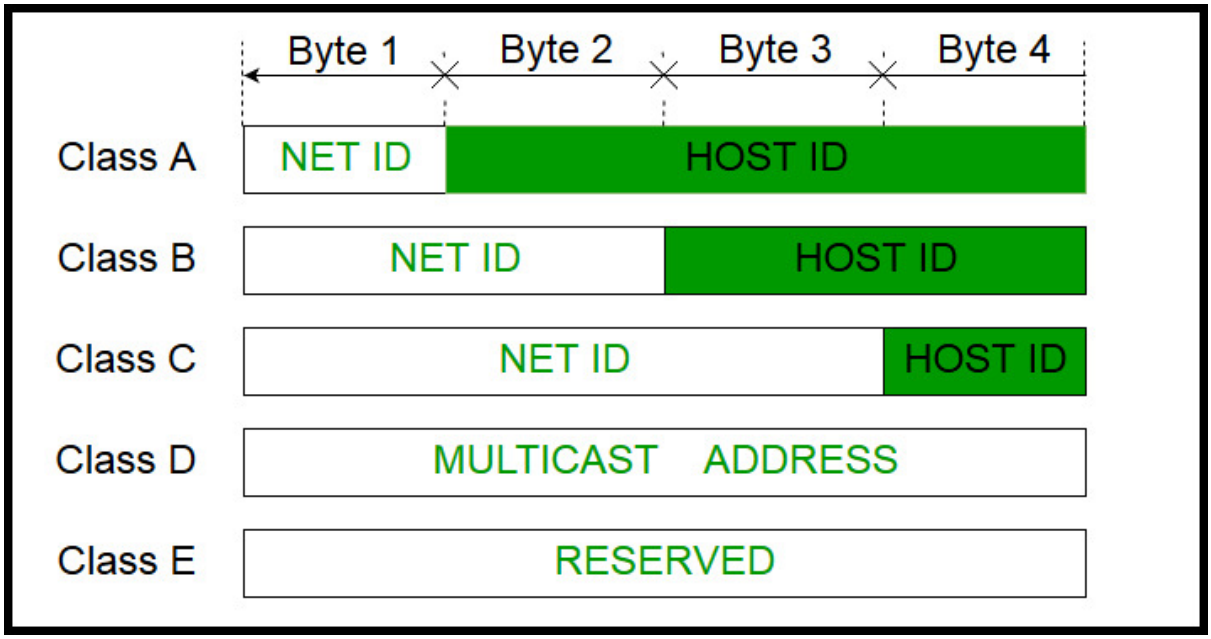
Hexadecimal Notation

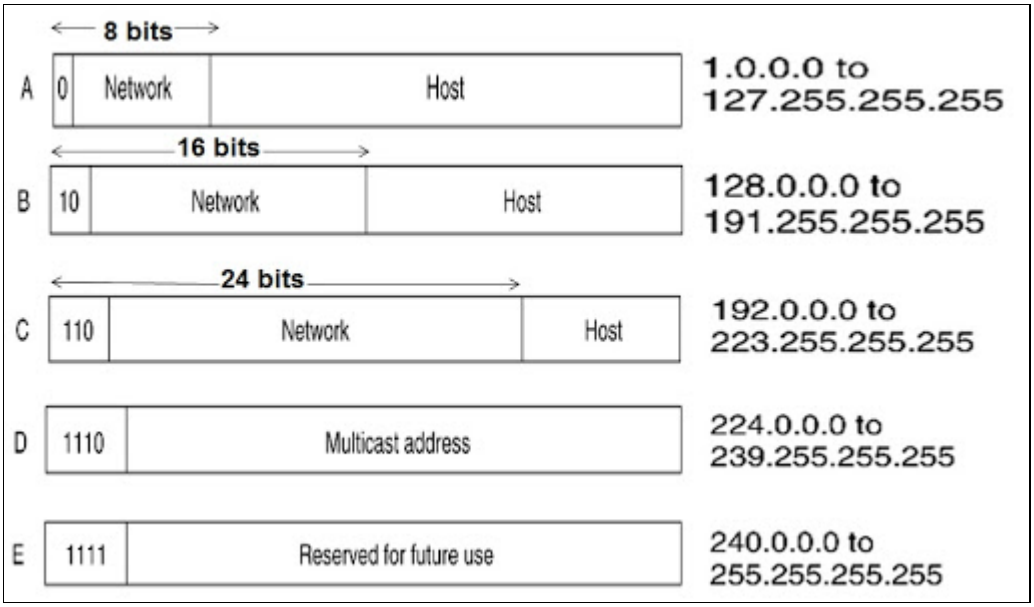
Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

4.5.1 Classfull IP Addressing

- The 32 bit IP address is divided into five sub-classes.
- These are:
  - Class A
  - Class B
  - Class C
  - Class D
  - Class E
- Each of these classes has a valid range of IP addresses.
- Classes D and E are reserved for multicast and experimental purposes respectively.
- The order of bits in the first octet determine the classes of IP address.
- IPv4 address is divided into two parts:
  - **Network ID**
  - **Host ID**
- The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class.
- Each ISP or network administrator assigns IP address to each device that is connected to its network.
- IP addresses are globally managed by **Internet Assigned Numbers Authority(IANA)** and **regional Internet registries(RIR).**
- While finding the total number of host IP addresses, **two** IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the **network number** and whereas the last IP address is reserved for **broadcast IP**.





CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Range of special IP addresses:

- 169.254.0.0 – 169.254.0.16: Link local addresses
- 127.0.0.0 – 127.0.0.8: Loop-back addresses
- 0.0.0.0 – 0.0.0.8: used to communicate within the current network.

Problems with Classfull Addressing:

- The problem with this Classfull addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations.
- Class D addresses are used for multicast routing and are therefore available as a single block only.
- Class E addresses are reserved.

Since there are these problems, Classfull networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993.

4.5.2 Classless Addressing

- To reduce the wastage of IP addresses in a block, we use sub-netting.
- What we do is that we use host id bits as net id bits of a Classfull IP address.
- We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28.
- Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

Subnetting:

- Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called **subnetting**.
- It is also called as subnet routing or subnet addressing.
- It is a practice that is widely used when classless addressing is done.

Benefits of Subnetting

- Reduced network traffic
- Optimized network performance
- Simplified network management

Masking:

- A process that extracts the address of the physical network from an IP address is called masking.
- If we do the subnetting, then masking extracts the subnetwork address from an IP address.
- To find the subnetwork address, two methods are used. They are boundary level masking and non-boundary level masking.
- In boundary level masking, two masking numbers are considered (i.e. 0 or 255). In non-boundary level masking, other value apart from 0 and 255 are considered.

Rules for boundary level masking:

- In this mask number is either 0 or 255.
- If the mask number is 255 in the mask IP address, then the IP address is repeated in the subnetwork address.
- If the mask number is 0 in the mask IP address, then the 0 is repeated in the subnetwork address.

Rules for non-boundary level masking:

- In this mask number is greater than 0 and less than 255.
- If the mask number is 255 in the mask IP address, then the IP address is repeated in the subnetwork address.
- If the mask number is 0 in the mask IP address, then the 0 is repeated in the subnetwork address.
- For any other mask numbers, bitwise AND operator is used. Bitwise ANDing is done in between mask number (byte) and IP address (byte).

The **default mask** in different classes are:

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

Example 1: Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).
Solution: The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Example 2: Find the subnetwork address for the following.

Sr. No.	IP Address	Mask	**Subnetwork Address**
1	140.11.36.22	255.255.255.0	140.11.36.0
2	120.14.22.16	255.255.128.0	120.14.0.0
3	141.181.14.16	255.255.224.0	141.181.0.0
4	200.34.22.156	255.255.255.240	200.34.22.144
5	125.35.12.57	255.255.0.0	125.35.0.0

How to do Logical AND on Calculator.
1. Turn ON the calculator.
2. Change the mode to Base-N.
3. Select the Base as per the given question on Calculator (i.e. DEC or HEX or BIN).
4. Enter the corresponding number from IP address and press = sign.
5. Then, press SHIFT + 3, and select the AND operation and then enter the corresponding number from the mask.
6. Press = sign and get the result.

Example 3: Find the class of the following IP address.

Sr. No.	IP Address	**Class**
1	1.22.200.10	**Class A**
2	241.240.200.2	**Class E**
3	227.3.6.8	**Class D**
4	180.170.0.2	**Class B**

Example 4: Find the netid and hostid for the following.

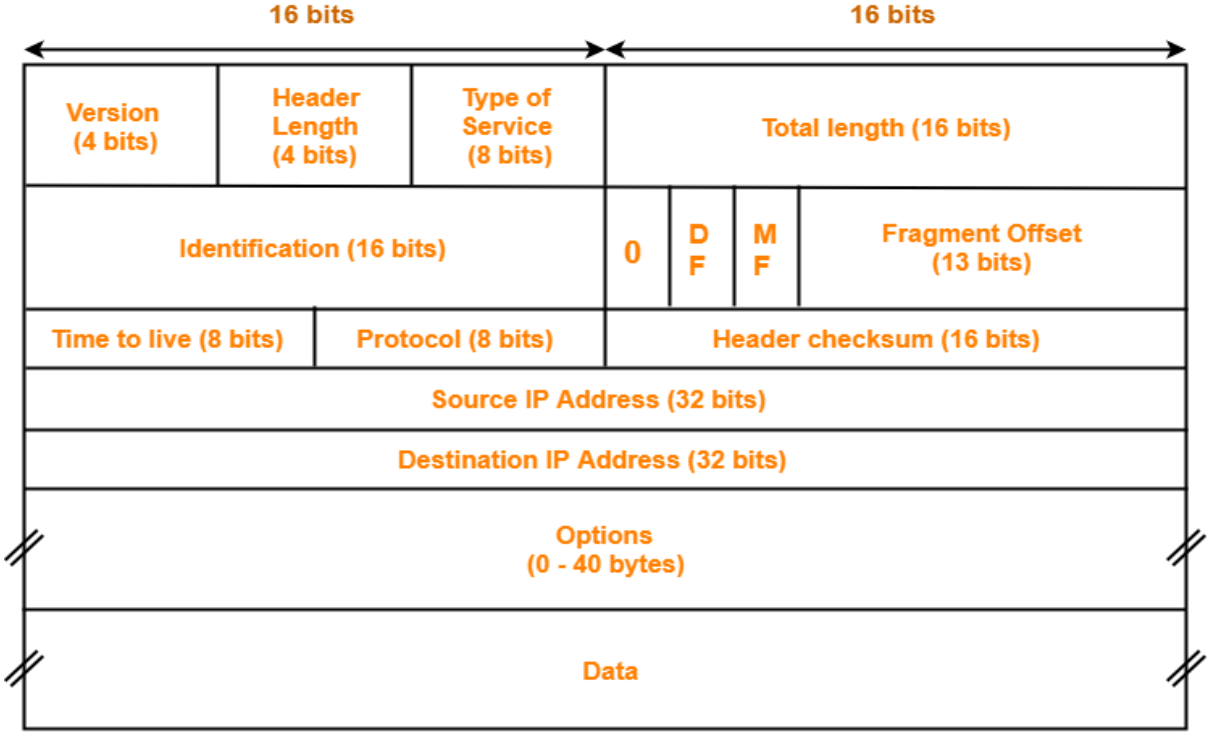
Sr. No.	IP Address	**Class**	**Netid**	**hostid**
1	19.34.21.5	**Class A**	**19**	**34.21.5**
2	190.13.70.10	**Class B**	**190.13**	**70.10**
3	246.3.4.10	**Class E**	**No netid and No hostid because Class E IP addresses are reserved.**	
4	201.2.4.2	**Class C**	**201.2.4**	**2**

4.6 IPv4 Protocol

- The IP (Internet Protocol) is a protocol that uses datagrams to communicate over a packet-switched network, such as the Internet.
- The IP protocol operates at the network layer protocol of the OSI reference model and is a part of a suite of protocols known as TCP/IP.
- The Internetwork Protocol (IPv4) provides a best effort network layer service connecting endpoints (computers, phones, etc.) to form a computer network.
- In IPv4, each endpoint is identified by one or more globally unique IP addresses.
- The network layer PDUs are known as either "packets" or "datagrams".
- Each packet carries the source IP address of the sending endpoint and also the address of the intended recipient endpoint (or a group destination address). Other protocol information is also carried.
- The IP network service transmits datagrams between routers (intermediate nodes) using IP routers.
- An IP network normally uses a dynamic routing protocol to find alternate routes whenever a link becomes unavailable.
- This provides considerable robustness from the failure of either links or routers, but is unable to guarantee reliable delivery.

IPv4 Packet Header

The following diagram represents the IPv4 header.



IPv4 Header

Let's walk through all these fields:

- **Version**
  i. Version is a 4-bit field that indicates the IP version used.
  ii. The most popularly used IP versions are version-4 (IPv4) and version-6 (IPv6).

iii. Only IPv4 uses the above header. So, this field always contains the decimal value 4.

- **Header Length**
  i. This field is also called the **Internet Header Length (IHL)**.
  ii. Header length is a 4-bit field that contains the length of the IP header. So, the range of decimal values that can be represented is [0, 15].
  iii. It helps in knowing from where the actual data begins.
  iv. The length of IP header always lies in the range 20 bytes to 60 bytes.
  v. So, to represent the header length, we use a scaling factor of 4.
  vi. In general, Header length = Header length field value x 4 bytes
- **Type of Service**
  i. Type of service is 8-bit field that is used for Quality of Service (QoS).
  ii. The datagram is marked for giving a certain treatment using this field.
- **Total Length**
  i. Total length is a 16-bit field that contains the total length of the datagram (in bytes).
  ii. Total length = Header length + Payload length
  iii. Minimum total length of datagram = 20 bytes (20-bytes header + 0-byte data)
  iv. Maximum total length of datagram = Maximum value of 16-bit word = 65535 bytes
- **Identification**
  i. Identification is a 16-bit field.
  ii. It is used for the identification of the fragments of an original IP datagram.
- **IP Flags**
  i. The first bit is always set to 0.
  ii. The second bit is called the **DF (Don't Fragment)** bit and indicates that this packet should not be fragmented.
  iii. The third bit is called the **MF (More Fragments)** bit and is set on all fragmented packets except the last one.
- **Fragment Offset**
  i. Fragment Offset is a 13-bit field.
  ii. It indicates the position of a fragmented datagram in the original unfragmented IP datagram.
  iii. The first fragmented datagram has a fragment offset of zero.
- **Time to Live**
  i. Time to live (TTL) is 8-bit field.
  ii. It indicates the maximum number of hops a datagram can take to reach the destination.
  iii. The main purpose of TTL is to prevent the IP datagrams from looping around forever in a routing loop.
  iv. The value of TTL is decremented by 1 when
    - Datagram takes a hop to any intermediate device having network layer.
    - Datagram takes a hop to the destination.
  v. If the value of TTL becomes zero before reaching the destination, then datagram is discarded.

- **Protocol**
    i. Protocol is an 8-bit field.
    ii. It tells the network layer at the destination host to which protocol the IP datagram belongs to.
    iii. Protocol number of ICMP is 1, IGMP is 2, TCP is 6 and UDP is 17.
- **Header Checksum**
    i. This 16-bit field is used to store a checksum of the header.
    ii. The receiver can use the checksum to check if there are any errors in the header.
- **Source IP Address**
    i. Source IP Address is a 32-bit field.
    ii. It contains the logical address of the sender of the datagram.
- **Destination IP Address**
    i. Destination IP Address is a 32-bit field.
    ii. It contains the logical address of the receiver of the datagram.
- **Options**
    i. Options is a field whose size vary from 0 bytes to 40 bytes.
    ii. This field is used for several purposes such as- Record route, Source routing, Padding.

4.7 Network Address Translation

- Network Address Translation (NAT) a way to map multiple local private addresses to a public one before transferring the information.
- Organizations that want multiple devices to employ a single IP address use NAT.

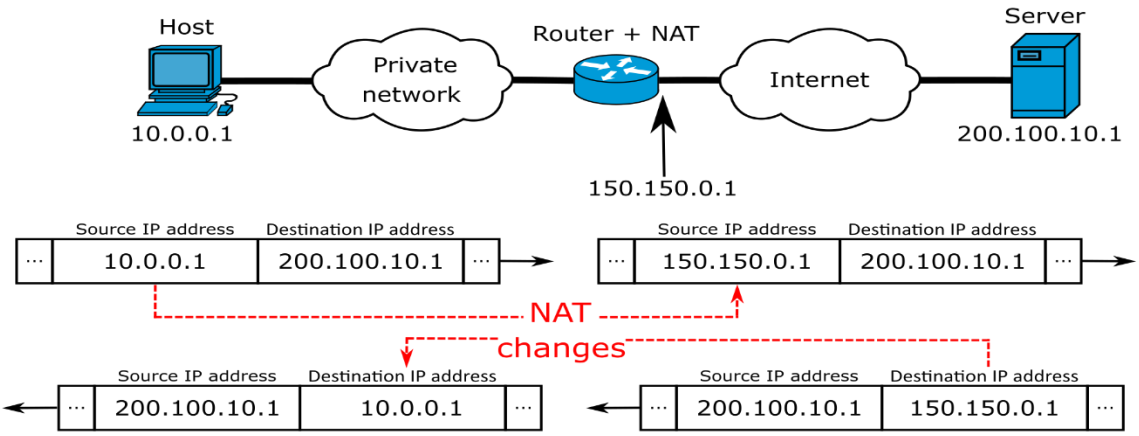
How NAT works?

- When computers and servers within a network communicate, they need to be identified to each other by a unique address, known as IP address. This was named IPv4.
- IP address is of 32 bits and so over 4 billion IP addresses can be generated which sounds a lot, and it really is not considering how fast the world of computers and the internet has grown.
- To circumvent this problem, a temporary solution was produced known as NAT.
- NAT resulted in two types of IP addresses, public and private.
- A range of private addresses were introduced, which anyone could use, as long as these were kept private within the network and not routed on the internet. The range of private addresses known as RFC 1918 are;
  Class A 10.0.0.0 - 10.255.255.255
  Class B 172.16.0.0 - 172.31.255.255
  Class C 192.168.0.0 - 192.168.255.255
- NAT allows you to use these private IP address on the internal network.
- So within your private network you would assign a unique IP address to all your computers, servers and other IP driven resources, usually done via DHCP.
- Another company can use the same private IP addresses as well, as long as they are kept internal to their network.
- So two companies maybe using the same range of IP addresses but because they are private to their network, they are not conflicting with each other.

- However, when internal hosts do need to communicate to the public network (Internet), then this is where a public address comes into the picture. This address usually purchased from an ISP is a routable public address everyone can see, which would represent your network gateway. This public address would be **unique**; no one else would use this address.

Example:

- When a host on the internal network with an internal IP address does need to communicate outside it's private network, it would use the public IP address on the network's gateway to identify itself to the rest of the world, and this translation of converting a private IP address to public is done by NAT.
- For example, a computer on an internal address of 10.0.0.1 wanted to communicate with a web server somewhere on the internet, NAT would translate the address 10.0.0.1 to the company's public address, let's call this 150.150.0.1, so that the internal address is identified as the public address when communicating with the outside world.
- This has to be done because when the web server somewhere on the internet was to reply to this internal computer, it needs to send this to a unique and routable address on the internet, the public address.
- It cannot use the original address of 10.0.0.1, as this is private, none routable and hidden from the outside world. This address, of 150.150.0.1 would be the address of the public address for that company and can be seen by everyone.
- Now the web server would reply to that public address, 150.150.0.1.
- NAT would then use its records to translate the packets received from the web server that was destined to 150.150.0.1 back to the internal network address of 10.0.0.1, and to the computer who requested the original info, will receive the requested packets.



NAT Types

There are three different types of NATs. People use them for different reasons, but they all still work as a NAT.

1. Static NAT

In this, a single private IP address is mapped with single Public IP address, i.e., a private IP address is translated to a public IP address. It is used in Web hosting.

2. Dynamic NAT

Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses. This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

3. PAT

PAT stands for port address translation. It's a type of dynamic NAT, but it bands several local IP addresses to a singular public one. Organizations that want all their employees' activity to use a singular IP address use a PAT, often under the supervision of a network administrator.

4.8 Routing Algorithms

- One of the functions of the network layer is to route the packets from the source machine to the destination machine.
- The major area of the network layer design includes the algorithms which choose the routes and the data structures which are used.
- **Routing algorithm** is a part of network layer software which is responsible for deciding the route/path over which a packet is to be sent.

Types of Routing Algorithms

- **Static Routing or Non-Adaptive Routing**
  i. It follows user defined routing and routing table is not changed until network administrator changes it.
  ii. Static Routing uses simple routing algorithms and provides more security than dynamic routing.
- **Dynamic Routing or Adaptive Routing**
  i. As the name suggests, dynamic routing changes the routing table once any changes to network occurs or network topology changes.
  ii. During network change, dynamic routing sends a signal to router, recalculates the routes and send the updated routing information.

Sr. No.	Key	Static Routing	Dynamic Routing
1	**Routing pattern**	In static routing, user defined routes are used in routing table.	In dynamic routing, routes are updated as per the changes in network.
2	**Routing Algorithm**	No complex algorithm used to figure out shortest path.	Dynamic routing employs complex algorithms to find the shortest routes.
3	**Security**	Static routing provides higher security.	Dynamic routing is less secure.
4	**Automation**	Static routing is a manual process.	Dynamic routing is an automatic process.
5	**Applicability**	Static routing is used in smaller networks.	Dynamic routing is implemented in large networks.

6	**Protocols**	Static routing may not follow any specific protocol.	Dynamic routing follows protocols like BGP, RIP and EIGRP.
7	**Additional Resources**	Static routing does not require any additional resources.	Dynamic routing requires additional resources like memory, bandwidth etc.

4.8.1 Shortest Path Algorithm

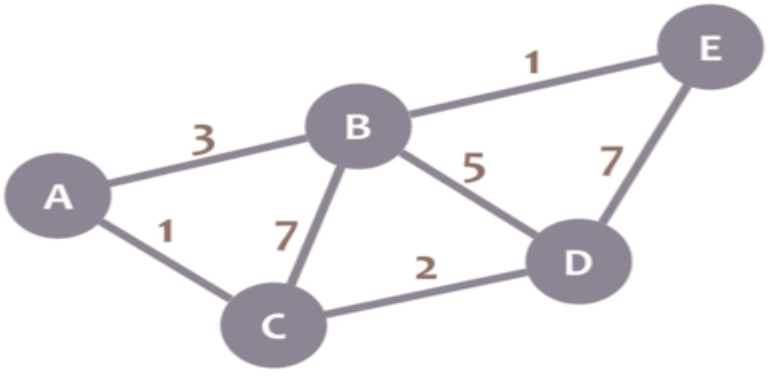
- In shortest path algorithm, the path length between each node is measured as a function of distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, etc.
- By changing the weighing function, the algorithm then computes the shortest path measured according to any one of a number of criteria or a combination of criteria.
- For this a graph of subnet is drawn with each node of graph representing a router and each arc of the graph representing a communication link.
- Each link has a cost associated with it.
- To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.
- Dijkstra's algorithm and Bellman Ford algorithm are used for computing the shortest path between two nodes of a graph.

Dijkstra's Algorithm:

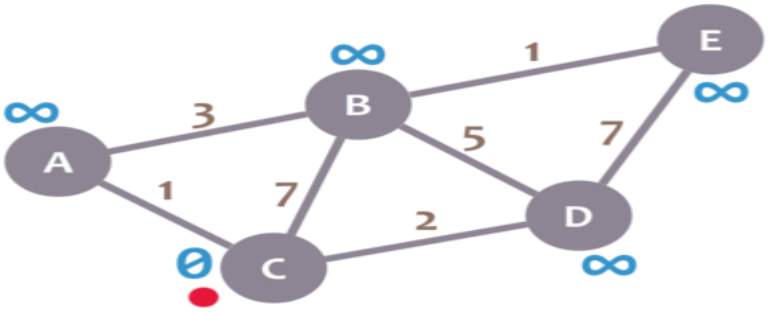
- Dijkstra's Algorithm allows you to calculate the shortest path between one node (you pick which one) and every other node in the graph.
- Here's a description of the algorithm:
  1. Mark your selected initial node with a current distance of 0 and the rest with infinity.
  2. Set the non-visited node with the smallest current distance as the current node C.
  3. For each neighbour N of your current node C: add the current distance of C with the weight of the edge connecting C-N. If it's smaller than the current distance of N, set it as the new current distance of N.
  4. Mark the current node C as visited.
  5. If there are non-visited nodes, go to step 2.

Example 1:

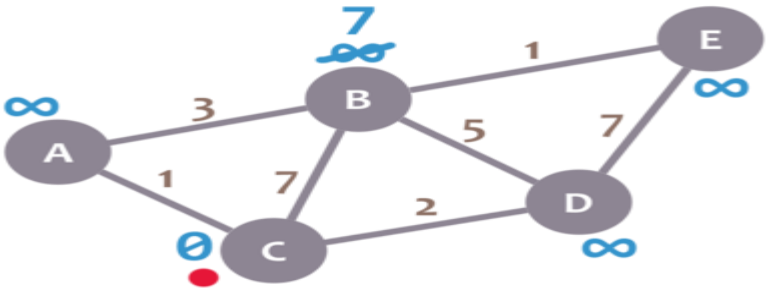
Let's calculate the shortest path between node C and the other nodes in our graph:



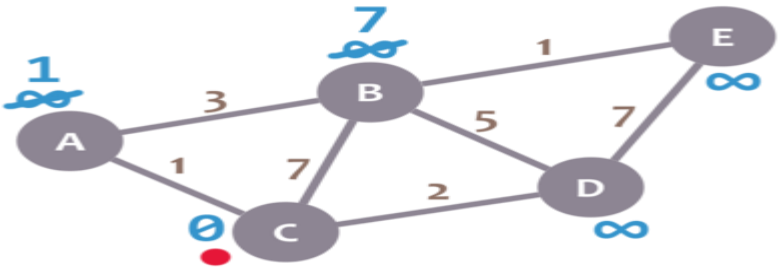
During the algorithm execution, we'll mark every node with its *minimum distance* to node C (our selected node).
For node C, this distance is 0. For the rest of nodes, as we still don't know that minimum distance, it starts being infinity (∞):



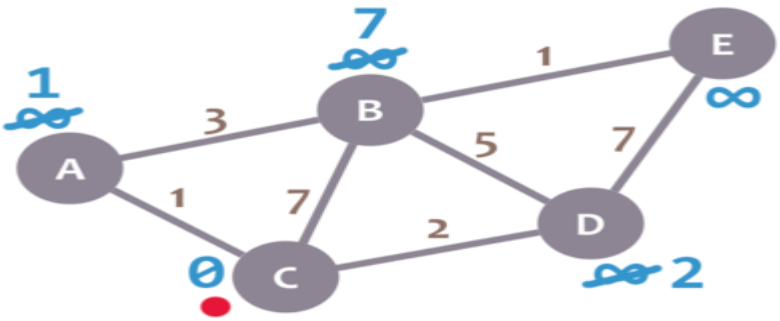
We'll also have a *current node*. Initially, we set it to C (our selected node). In the image, we mark the current node with a red dot.
Now, we check the neighbours of our current node (A, B and D) in no specific order. Let's begin with B. We add the minimum distance of the current node (in this case, 0) with the weight of the edge that connects our current node with B (in this case, 7), and we obtain 0 + 7 = 7. We compare that value with the minimum distance of B (infinity); the lowest value is the one that remains as the minimum distance of B (in this case, 7 is less than infinity):



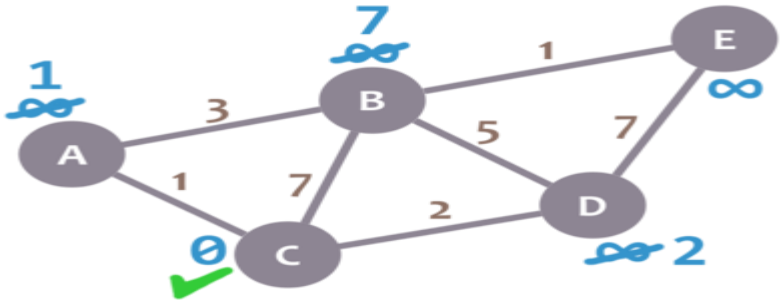
Now, let's check neighbour A. We add 0 (the minimum distance of C, our current node) with 1 (the weight of the edge connecting our current node with A) to obtain 1. We compare that 1 with the minimum distance of A (infinity), and leave the smallest value:



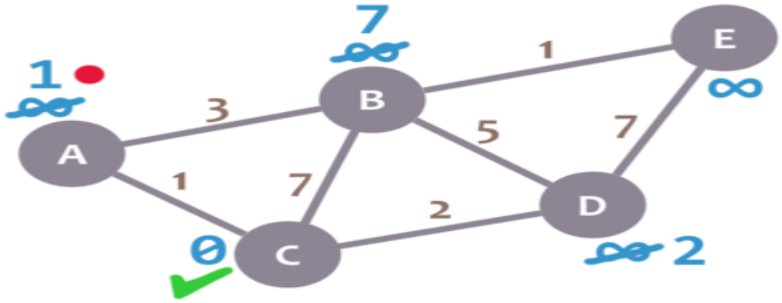
Repeat the same procedure for D:



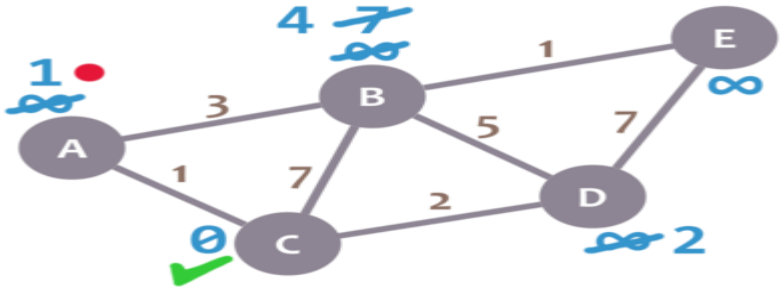
We have checked all the neighbours of C. Because of that, we mark it as *visited*. Let's represent visited nodes with a green check mark:



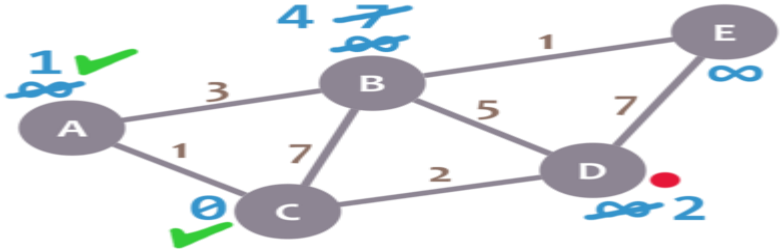
We now need to pick a new *current node*. That node must be the unvisited node with the smallest minimum distance (so, the node with the smallest number and no check mark). That's A. Let's mark it with the red dot:



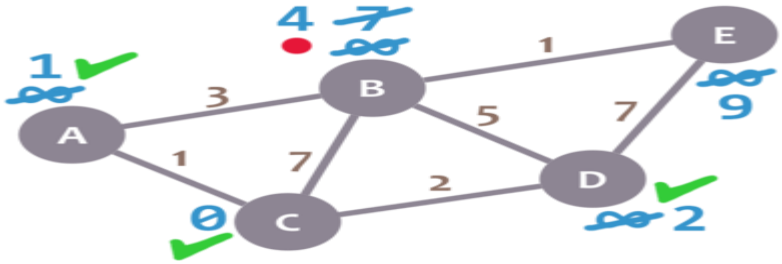
And now we repeat the algorithm. We check the neighbours of our current node, ignoring the visited nodes. This means we only check B.
For B, we add 1 (the minimum distance of A, our current node) with 3 (the weight of the edge connecting A and B) to obtain 4. We compare that 4 with the minimum distance of B (7) and leave the smallest value: 4.



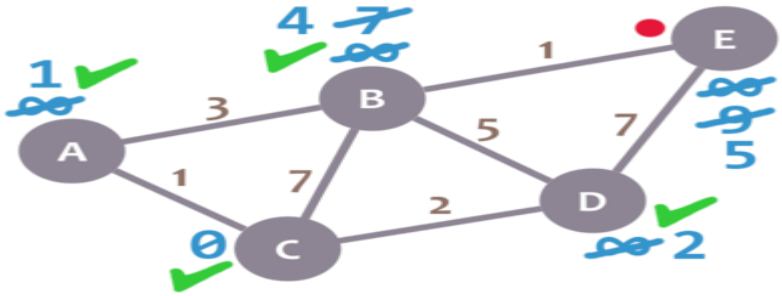
Afterwards, we mark A as visited and pick a new current node: D, which is the non-visited node with the smallest current distance.



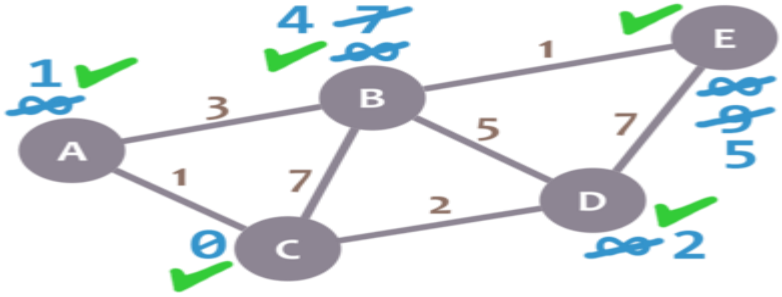
We repeat the algorithm again. This time, we check B and E.
For B, we obtain 2 + 5 = 7. We compare that value with B's minimum distance (4) and leave the smallest value (4). For E, we obtain 2 + 7 = 9, compare it with the minimum distance of E (infinity) and leave the smallest one (9).
We mark D as visited and set our current node to B.



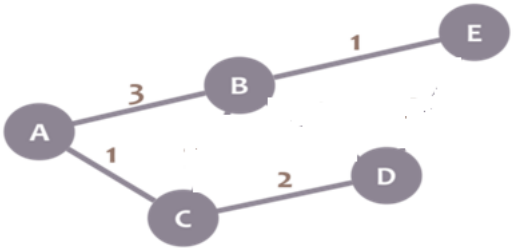
We only need to check E. 4 + 1 = 5, which is less than E's minimum distance (9), so we leave the 5. Then, we mark B as visited and set E as the current node.



E doesn't have any non-visited neighbours, so we don't need to check anything. We mark it as visited.



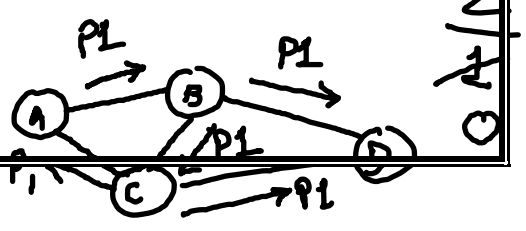
As there are not unvisited nodes, we're done!
The minimum distance of each node now actually represents the minimum distance from that node to node C (the node we picked as our initial node)!



4.8.2 Flooding

- Flooding is the static routing algorithm. In this algorithm, every incoming packet is sent on all outgoing lines except the line on which it has arrived.
- One major problem of this algorithm is that it generates a large number of duplicate packets on the network.
- Several measures are takes to stop the duplication of packets. These are:

[1] One solution is to include a **hop counter** in the header of each packet. This counter is decremented at each hop along the path. When this counter reaches zero the packet is discarded. Ideally, the hop counter should become zero at the destination hop,



indicating that there are no more intermediate hops and destination is reached. This requires the knowledge of exact number of hops from a source to destination.

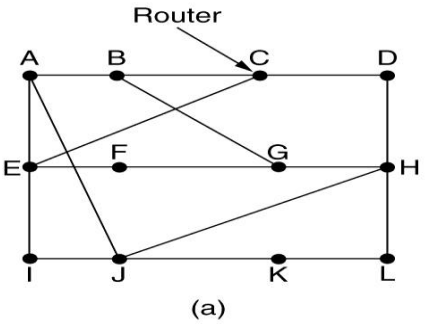
[2] Another technique is to **keep the track of the packet** that have been flooded, to avoid sending them a second time. For this, the source router put a sequence number in each packet it receives from its hosts. Each router then needs a list per source router telling which sequence numbers originating at that source have already been seen. If an incoming packet is on the list, it is not flooded.

[3] Another solution is to use **selective flooding.** In selective flooding the routers do not send every incoming packet out on every output line. Instead packet is sent only on those lines which are approximately going in the right direction.

4.8.3 Distance Vector Routing

- A distance vector routing algorithm operates by having each router maintain a table (i.e., a vector) giving the best known distance to each destination and which link to use to get there.
- These tables are updated by exchanging information with the neighbors.
- Eventually, every router knows the best link to reach each destination.
- The distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford routing algorithm**, after the researchers who developed it (Bellman, 1957; and Ford and Fulkerson, 1962).
- It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP.
- In distance vector routing, each router maintains a routing table indexed by, and containing one entry for each router in the network.
- This entry has two parts: the **preferred outgoing line** to use for that destination and an estimate of **the distance** to that destination.
- The distance might be measured as the number of hops or using another metric, as we discussed for computing shortest paths.
- The router is assumed to know the "distance" to each of its neighbors.
- If the metric is hops, the distance is just one hop.
- If the metric is propagation delay, the router can measure it directly with special **ECHO** packets that the receiver just timestamps and sends back as fast as it can.
- As an example, assume that delay is used as a metric and that the router knows the delay to each of its neighbors.
- Once every T msec, each router sends to each neighbor a list of its estimated delays to each destination.
- It also receives a similar list from each neighbor.
- Imagine that one of these tables has just come in from neighbor X, with X_i being X's estimate of how long it takes to get to router i.
- If the router knows that the delay to X is m msec, it also knows that it can reach router i via X in $X_i + m$ msec.
- By performing this calculation for each neighbor, a router can find out which estimate seems the best and use that estimate and the corresponding link in its new routing table.
- Note that the old routing table is not used in the calculation.

- This updating process is illustrated in Figure below. Part (a) shows a network. The first four columns of part (b) show the delay vectors received from the neighbors of router *J*.
- *A* claims to have a 12-msec delay to *B*, a 25-msec delay to *C*, a 40-msec delay to *D*, etc.
- Suppose that *J* has measured or estimated its delay to its neighbors, *A*, *I*, *H*, and *K*, as 8, 10, 12, and 6 msec, respectively.



(a)

To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	—
K	24	22	22	0	6	K
L	29	33	9	9	15	K

JA delay is 8 | JI delay is 10 | JH delay is 12 | JK delay is 6

Vectors received from J's four neighbors

New routing table for J

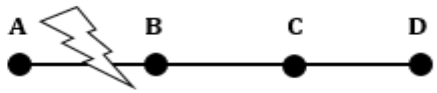
(b)

- Consider how *J* computes its new route to router *G*.
- It knows that it can get to *A* in 8 msec, and furthermore *A* claims to be able to get to *G* in 18 msec, so *J* knows it can count on a delay of 26 msec to *G* if it forwards packets bound for *G* to A.
- Similarly, it computes the delay to G via I, H, and K as 41 (31 + 10), 18 (6 + 12), and 37 (31 + 6) msec, respectively. The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 msec and that the route to use is via H.
- The same calculation is performed for all the other destinations, with the new routing table shown in the last column of the figure.

4.8.4 Count to Infinity Problem

- One of the important issue in Distance Vector Routing is Count to Infinity Problem.
- Count to infinity is just another name for a routing loop.
- In distance vector routing, routing loops usually occur when an interface goes down.
- It can also occur when two routers send updates to each other at the same time.

Link Between A & B is Broken



	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

- Imagine a network with a graph as shown in the above figure.
- As you see in this graph, there is only one link between A and the other parts of the network.
- Now imagine that the link between A and B is cut.
- At this time, B corrects its table.
- After a specific amount of time, routers exchange their tables, and so B receives C's routing table.
- Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A).
- B receives this table and thinks there is a separate link between C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said).
- Once again, routers exchange their tables.
- When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).
- This process loops until all nodes find out that the weight of link to A is infinity.
- This situation is shown in the table below.

	B	**C**	**D**
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	.....	....	....
∞	∞	∞	∞

- In this way, Distance Vector Algorithms have a slow convergence rate.

Solution to Count to Infinity Problem

1. **Split Horizon**: Here, when a router sends a routing update to its neighbors, it does not send those routes it learned from each neighbor back to that neighbor.
2. **Split Horizon with Poison Reverse**: In this variation of split horizon, when a router sends a routing update to its neighbors, it sends those routes it learned from each neighbor back to that neighbor with infinite cost information to make sure that the neighbour does not use that route.

4.8.5. Link State Routing

- Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

- The three keys to understand the Link State Routing algorithm:

[1] **Knowledge about the neighborhood**: Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.

[2] **Flooding**: Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.

[3] **Information sharing**: A router sends the information to every other router only when the change occurs in the information.

- Link State Routing has two phases:

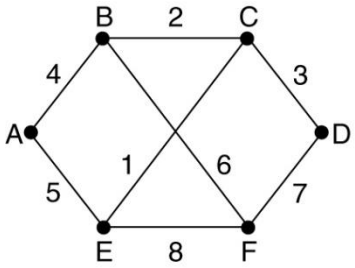
[1] Reliable Flooding

Initial state: Each node knows the cost of its neighbors.
Final state: Each node knows the entire graph.

[2] Route Calculation

Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

- Heavy traffic is created in Line state routing due to Flooding.
- Flooding can cause an infinite looping, this problem can be solved by using Time-to-leave field.



(a)

Link State Packets

A		B		C		D		E		F	
Seq.		Seq.		Seq.		Seq.		Seq.		Seq.	
Age		Age		Age		Age		Age		Age	
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

(b)

4.8.6Distance Vector Routing Vs Link State Routing

Distance vector	Link state
sends the entire routing table	sends only link state information
slow convergence	fast convergence
susceptible to routing loops	less susceptible to routing loops
updates are sometimes sent using broadcast	always uses multicast for the routing updates
doesn't know the network topology	knows the entire network topology
simpler to configure	can be harder to configure
examples: RIP, IGRP	examples: OSPF, IS-IS

4.9 Protocols

4.9.1 ARP Protocol

- **Address Resolution Protocol (ARP)** is an important protocol of the network layer in the OSI model, which helps find the MAC (Media Access Control) address given the system's IP address.

- The ARP's main task is to convert the 32-bit IP address (for IPv4) to a 48-bit MAC address.
- This protocol is mostly used to determine the hardware (MAC) address of a device from an IP address.
- It is also used when one device wants to communicate with some other device on a local network.
- All OS in an IPv4 network keep an ARP cache.
- When the host requests a MAC address to send a packet to another host in the LAN, it checks its ARP cache to check that the MAC address translation already presents.

Important ARP terms:

- **ARP Cache**: After resolving the MAC address, the ARP sends it to the cache stored in a table for future reference. The subsequent communications can use the MAC address from the table.
- **ARP Cache Timeout**: It is the time for which the MAC address in the ARP cache can reside.
- **ARP request**: Broadcasting a packet over the network to validate whether we came across the destination MAC address or not.
- **ARP response/reply**: The MAC address response that the source receives from the destination aids in further communication of the data.

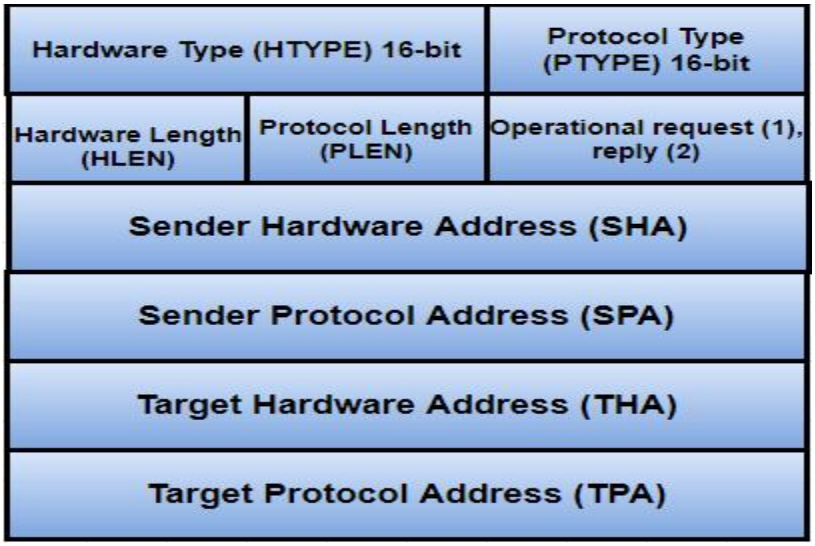
Address Resolution Methods

Association between a protocol address and a hardware address is known as **binding**.

There are three techniques used for this purpose:

- **Table lookup** - Bindings stored in memory with protocol address as the key. It uses the data link layer checks the protocol address to find the hardware address.
- **Dynamic**–This type of network messaging method is used for "just-in-time" resolution. Data link layer sends message requests in a hardware address. Destination responds.
- **Closed-form computation**–In this method, a protocol address is based on a hardware address. Data link layer derives the hardware address from the protocol address.

ARP Header



- **Hardware Type–**It is 1 for Ethernet.
- **Protocol Type–**It is a protocol used in the network layer.
- **Hardware Address Length–**It is the length in bytes so that it would be 6 for Ethernet.
- **Protocol Address Length** – Its value is 4 bytes.
- **Operation Code** indicates that the packet is an ARP Request (1) or an ARP Response (2).
- **Senders Hardware Address** – It is a hardware address of the source node.
- **Senders Protocol Address** -It is a layer 3 address of the source node.
- **Target Hardware Address** – It is used in a RARP request, which response impact both the destination's hardware and layer 3 addresses.
- **Target Protocol Address** – It is used in an ARP request when the response carries both layer 3 addresses and the destination's hardware.

4.9.2 RARP Protocol

- RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol (ARP) table or cache.
- A network administrator creates a table in a local area networks gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses.
- When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address.
- Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.
- RARP is available for Ethernet, Fiber Distributed-Data Interface, and token ring LANs.

RARP	ARP
RARP stands for Reverse Address Resolution Protocol	ARP stands for Address Resolution Protocol
In RARP, we find our own IP address	In ARP, we find the IP address of a remote machine

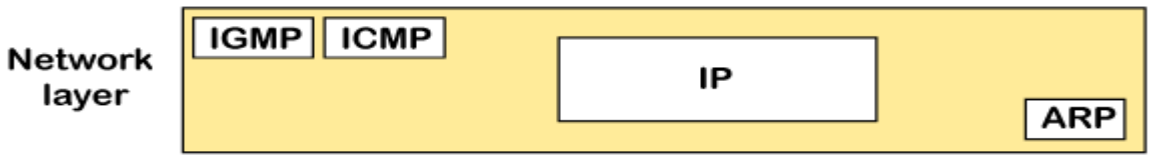
The MAC address is known and the IP address is requested	The IP address is known, and the MAC address is being requested
It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses

4.9.3. ICMP

- The ICMP stands for Internet Control Message Protocol.
- It is a network layer protocol.
- It is used for error handling in the network layer, and it is primarily used on network devices such as routers.
- As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.
- For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.
- The IP protocol does not have any error-reporting or error-correcting mechanism, so it uses a message to convey the information.
- For example, if someone sends the message to the destination, the message is somehow stolen between the sender and the destination. If no one reports the error, then the sender might think that the message has reached the destination. If someone in-between reports the error, then the sender will resend the message very quickly.

Position of ICMP in the network layer

The ICMP resides in the IP layer, as shown in the below diagram.



Messages

The ICMP messages are usually divided into two categories:

ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

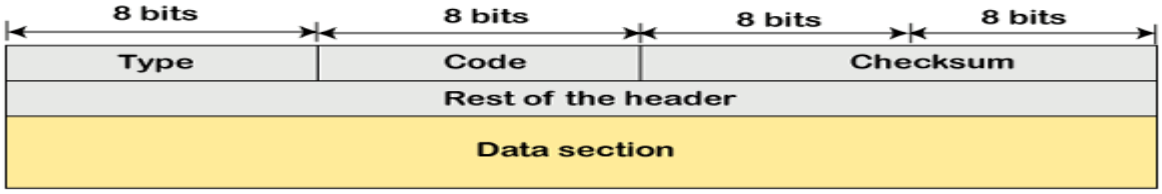
Error-reporting messages: The error-reporting message means that the router encounters a problem when it processes an IP packet then it reports a message.

Query messages: The query messages are those messages that help the host to get the specific information of another host. For example, suppose there are a client and a server, and the client wants to know whether the server is live or not, then it sends the ICMP message to the server.

ICMP Message Format

The message format has two things; one is a category that tells us which type of message it is. If the message is of error type, the error message contains the type and the code. The type defines the type of message while the code defines the subtype of the message.

The ICMP message contains the following fields:



- **Type:** It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
- **Code:** It is an 8-bit field that defines the subtype of the ICMP message
- **Checksum:** It is a 16-bit field to detect whether the error exists in the message or not.

4.9.4 IGMP

- The Internet Group Management Protocol (IGMP) is a protocol that allows several devices to share one IP address so they can all receive the same data.
- IGMP is a network layer protocol used to set up multicasting on networks that use the Internet Protocol version 4 (IPv4).
- Specifically, IGMP allows devices to join a multicasting group.
- Multicasting is when a group of devices all receive the same messages or packets. Multicasting works by sharing an IP address between multiple devices.

How does IGMP work?

- Computers and other devices connected to a network use IGMP when they want to join a multicast group.
- A router that supports IGMP listens to IGMP transmissions from devices in order to figure out which devices belong to which multicast groups.
- IGMP uses IP addresses that are set aside for multicasting.
- Multicast IP addresses are in the range between 224.0.0.0 and 239.255.255.255. (In contrast, anycast networks can use any regular IP address.)
- Each multicast group shares one of these IP addresses.
- When a router receives a series of packets directed at the shared IP address, it will duplicate those packets, sending copies to all members of the multicast group.
- IGMP multicast groups can change at any time. A device can send an IGMP "join group" or "leave group" message at any point.
- IGMP works directly on top of the Internet Protocol (IP).
- Each IGMP packet has both an IGMP header and an IP header.
- Just like ICMP, IGMP does not use a transport layer protocol such as TCP or UDP.

IGMP Messages

The IGMP protocol allows for several kinds of IGMP messages:

- **Membership reports**: Devices send these to a multicast router in order to become a member of a multicast group.
- **"Leave group" messages**: These messages go from a device to a router and allow devices to leave a multicast group.
- **General membership queries**: A multicast-capable router sends out these messages to the entire connected network of devices to update multicast group membership for all groups on the network.
- **Group-specific membership queries**: Routers send these messages to a specific multicast group, instead of the entire network.

IGMPv1 Header

- The IGMP header has a total length of 64 bits.
- The first 8 bits always specify the protocol version IGMPv1 and the type of message.
- There are two options for the field (type): "1" (for membership requests) and "2" (for notifications about multicast data streams).
- Bits 8 to 15 follow, but they have no function and only consist of zeros.
- The first 32-bit block ends with a checksum.
- If it is an IGMP notification package, the 32 bit-long group address will follow.

IGMPv1 header				
Bits	**0–3**	**4–7**	**8–15**	**16–31**
0	Version	Type	Unused	Checksum
32	Group address			

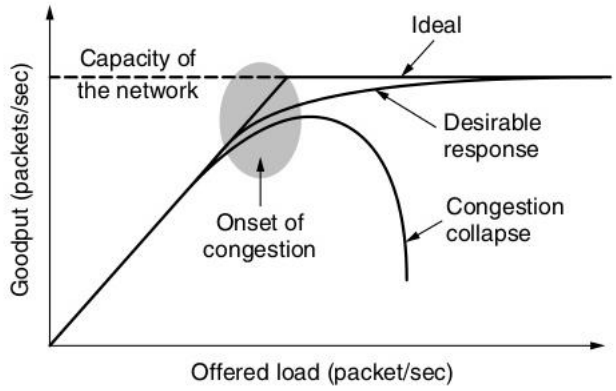
IGMPv2 Header

IGMPv2 header			
Bits	**0–7**	**8–15**	**16–31**
0	Type	Max. response time	Checksum
32	Group address		

- The header line starts similarly to the first log version, but without specifying the version number.
- The possible **type codes** are "0x11" (for requests), "0x16" (for notifications), and "0x17" (for leave messages). For **backwards compatibility**, there is also the code "0x12" for IGMPv1 notifications.
- Bits 8 to 15 receive a concrete function in IGMPv2 – at least for membership requests – and define the **maximum response time allowed**.
- This is followed by the checksum (16 bits) and the group address (32 bits), which in turn has the protocol-typical form 0.0.0.0 for general requests.

4.10 Congestion Control

- Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called **congestion**.
- The network and transport layers share the responsibility for handling congestion.
- Since congestion occurs within the network, it is the network layer that directly experiences it and must ultimately determine what to do with the excess packets.
- However, the most effective way to control congestion is to reduce the load that the transport layer is placing on the network.
- This requires the network and transport layers to work together.
- Figure below depicts the onset of congestion.



- When the number of packets hosts send into the network is well within its carrying capacity, the number delivered is proportional to the number sent. If twice as many are sent, twice as many are delivered.
- However, as the offered load approaches the carrying capacity, bursts of traffic occasionally fill up the buffers inside routers and some packets are lost.
- These lost packets consume some of the capacity, so the number of delivered packets falls below the ideal curve. The network is now congested.
- Unless the network is well designed, it may experience a **congestion collapse**, in which performance plummets as the offered load increases beyond the capacity.
- This can happen because packets can be sufficiently delayed inside the network that they are no longer useful when they leave the network.

4.10.1 Flow Control Vs Congestion Control

Sr. NO.	FLOW CONTROL	CONGESTION CONTROL
1.	In flow control, Traffics are controlled which flow from sender to a receiver.	In this, Traffics are controlled entering to the network.
2.	Data link layer and Transport layer handle it.	Network layer and Transport layer handle it.
3.	In this, Receiver's data is prevented from being overwhelmed.	In this, Network is prevented from congestion.
4.	In flow control, Only sender is responsible for the traffic.	In this, Transport layer is responsible for the traffic.

5.	In this, Traffic is prevented by slowly sending by the sender.	In this, Traffic is prevented by slowly transmitting by the transport layer.
6.	In flow control, buffer overrun is restrained in the receiver.	In congestion control, buffer overrun is restrained in the intermediate systems in the network.

4.10.2 Congestion Control Techniques

Congestion control techniques can be broadly classified into two categories:

1. Open loop congestion control
2. Closed loop congestion control

1. **Open Loop Congestion Control**

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control:

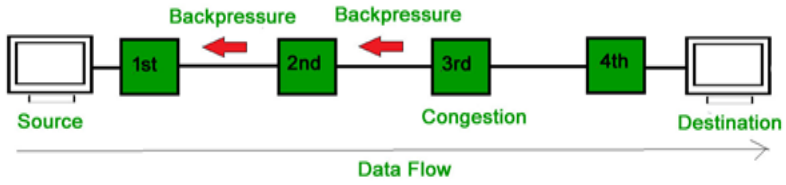
1. **Retransmission Policy:**
   - It is the policy in which retransmission of the packets are taken care.
   - If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.
   - This transmission may increase the congestion in the network.
   - To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.
2. **Window Policy:**
   - The type of window at the sender side may also affect the congestion.
   - Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side.
   - This duplication may increase the congestion in the network and making it worse.
   - Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.
3. **Discarding Policy:**
   - A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packets and also able to maintain the quality of a message.
   - In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.
4. **Acknowledgment Policy:**
   - Since acknowledgement are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion.
   - Several approaches can be used to prevent congestion related to acknowledgment.
   - The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet.
   - The receiver should send an acknowledgment only if it has to send a packet or a timer expires.
5. **Admission Policy:**

- In admission policy, a mechanism should be used to prevent congestion.
- Switches in a flow should first check the resource requirement of a network flow before transmitting it further.
- If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

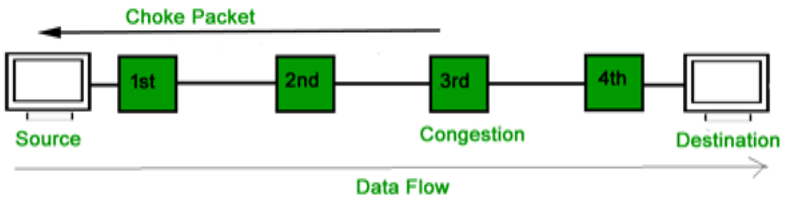
2. Close Loop Congestion Control

Closed loop congestion control technique is used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. **Backpressure:**
   - Backpressure is a technique in which a congested node stops receiving packet from upstream node.
   - This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes.
   - Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow.
   - The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



   - In above diagram the 3rd node is congested and stops receiving packets, as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly, 1st node may get congested and informs the source to slow down.
2. **Choke Packet Technique:**
   - Choke packet technique is applicable to both virtual networks as well as datagram subnets.
   - A choke packet is a packet sent by a node to the source to inform it of congestion.
   - Each router monitors its resources and the utilization at each of its output lines.
   - Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic.
   - The intermediate nodes through which the packets have travelled are not warned about congestion.



3. **Implicit Signalling:**
    - In implicit signalling, there is no communication between the congested nodes and the source.
    - The source guesses that there is congestion in a network.
    - For example, when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.
4. **Explicit Signalling**:
    - In explicit signalling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion.
    - The difference between choke packet and explicit signalling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique.
    - Explicit signalling can occur in either forward or backward direction.

Open Loop Congestion Control Vs Closed Loop Congestion Control

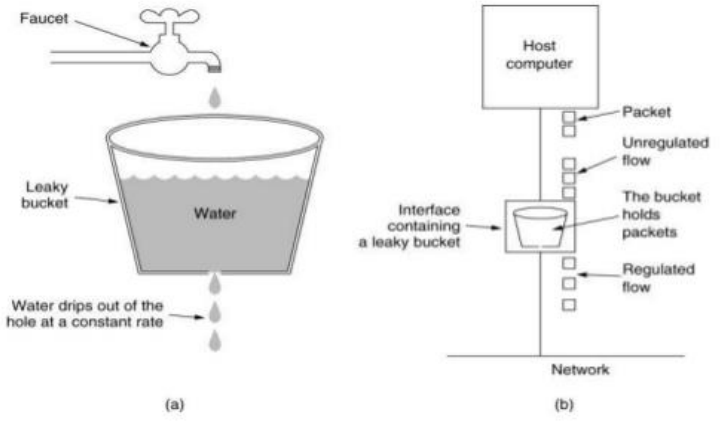
Points	**Open Loop Congestion Control**	**Closed Loop Congestion Control**
Function	In this method, policies are used to prevent the congestion before it happens.	This method try to remove the congestion after it happens.
Structure	It has simple structure.	It has complex structure.
Stability	It is stable method.	This method can cause stability problem.
Cost	Cost is low.	Cost is high.
Accuracy	Accuracy is low.	Accuracy is high.
Feedback	This method does not utilize runtime feedback from the system.	This method uses feedback to make corrections at runtime.
Resistance of Disturbance	Resistance of Disturbance is low.	Resistance of Disturbance is high.
Speed	It has low speed.	It has high speed.
Regulate	It is easy to regulate.	It is hard to regulate.
Mechanisms	a. Retransmission policy b. Window policy c. Acknowledgment policy d. Discarding policy e. Admission policy	a. Back pressure b. Choke point c. Implicit signalling d. Explicit signalling

4.10.3 Traffic Shaping

- One of the reason behind the congestion is **Bursty Traffic**.
- Traffic Shaping is also known as Packet Shaping.
- It is an **Open Loop Control**.
- Traffic shaping is the technique of delaying and restricting certain packets travelling through a network to increase the performance of packets that have been given priority.
- Traffic shaping is a mechanism to control the amount and rate of the traffic sent to the network.
- The two traffic shaping techniques are Leaky Bucket and Token Bucket.

4.10.3.1 Leaky Bucket Algorithm

1. It is a traffic shaping mechanism.
2. A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.



(a) A leaky bucket with water. (b) a leaky bucket with packets.

3. Imagine a bucket with a small hole at the bottom.
4. 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.
5. Thus, the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.
6. Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.
7. The same concept can be applied to packets in the network.
8. Consider the data is coming from the source at variable speeds.
9. 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.
10. If a leaky bucket algorithm is used, the data flow will be 8 Mbps for 9 seconds. Thus, constant flow is maintained.

Leaky Bucket Implementation

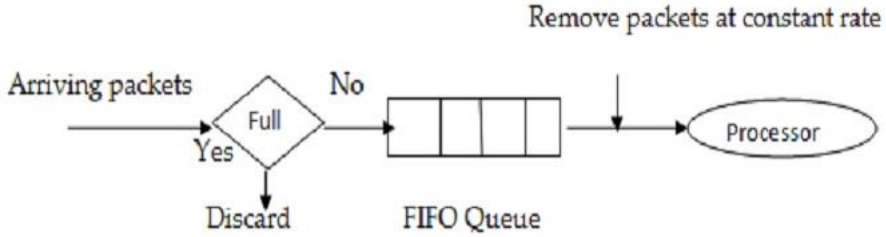


Figure The implementation of leaky bucket

1. Figure above shows the implementation of Leaky Bucket Principle.
2. A FIFO queue is used for holding the packets.
3. Implementation of leaky bucket is done under two different operating conditions.

a. Fixed Size Packets

- If the arriving packets are of fixed size, then the process removes a fixed number of packets from the queue at each tick of the clock.

- Example: Cells in ATM Network

b. Variable Size Packets

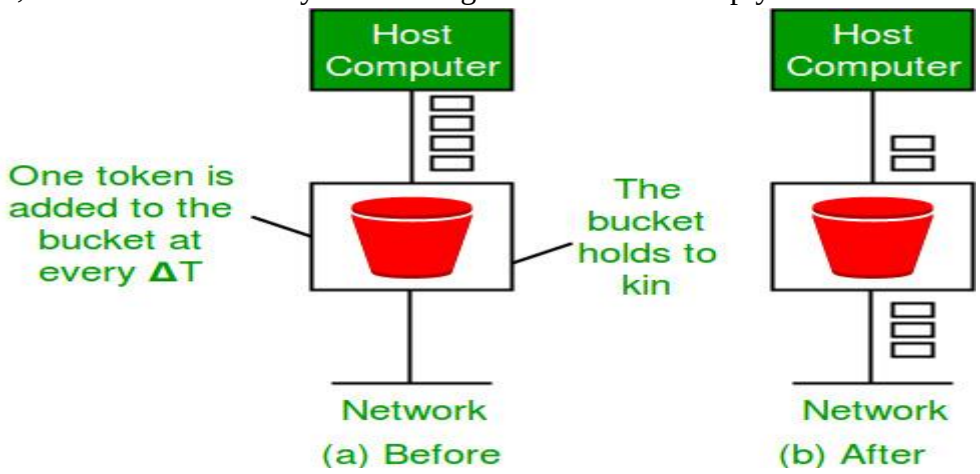
- If the arriving packets are of different size, then the fixed output rate will not be based on the number of departed packets.
- Instead it will be based on the number of departing bytes or bits.

Leaky Bucket Algorithm

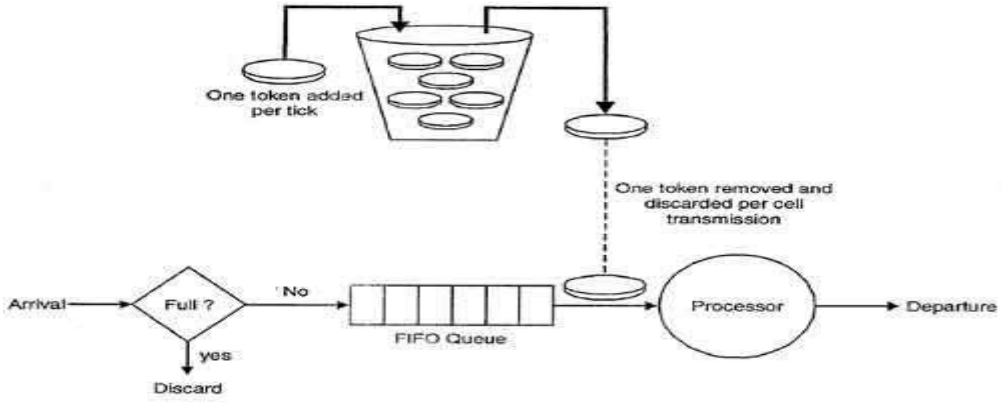
1. Initialize the counter to 'n' at every tick of clock.
2. If n is greater than the size of packet in the front of queue, send the packet into the network and decrement the counter by size of packet.
3. Repeat the step until n is less than the size of packet.
4. Reset the counter and go to step 1.

4.10.3.2 Token Bucket Algorithm

1. The leaky bucket algorithm allows only an average (constant) rate of data flow.
2. Its major problem is that it cannot deal with bursty data.
3. A leaky bucket algorithm does not consider the idle time of the host.
4. For example, if the host was idle for 10 seconds and now it is willing to send data at a very high speed for another 10 seconds, the total data transmission will be divided into 20 seconds and average data rate will be maintained.
5. The host is having no advantage of sitting idle for 10 seconds.
6. To overcome this problem, **a token bucket** algorithm is used.
7. A token bucket algorithm allows bursty data transfers.
8. A token bucket algorithm is a modification of leaky bucket in which leaky bucket contains tokens.
9. In this algorithm, a token(s) are generated at every clock tick.
10. For a packet to be transmitted, system must remove token(s) from the packet.
11. Thus, a token bucket algorithm allows idle hosts to accumulate credit for the future in form of tokens.
12. For example, if a system generates 100 tokens in one clock tick and the host is idle for 100 ticks. The bucket will contain 10,000 tokens.
13. Now, if the host wants to send bursty data, it can consume all 10,000 tokens at once for sending 10,000 cells or bytes.
14. Thus, a host can send bursty data as long as bucket is not empty.



Implementation of Token Bucket



Token bucket algorithm

1. Figure above shows the implementation of Token Bucket.
2. The token bucket can be easily implemented with a counter.
3. The token is initialized to zero.
4. Each time a token is added, the counter is incremented by 1 and each time a unit of data is dispatched, the counter is decremented by 1.
5. If the counter contains zero, the host cannot send any data.

Leaky Bucket Algorithm Vs Token Bucket Algorithm

Sr. No.	Leaky Bucket Algorithm	Token Bucket Algorithm
1	It is token independent.	It is token dependent.
2	If bucket is full, then packet or data is discarded.	If bucket is full, then tokens are discarded, but not the token.
3	Packets are transmitted continuously.	Packets can only be transmitted if there are enough tokens.
4	It sends the packet at constant rate.	It allows large bursts to be sent at faster rate after that constant rate.
5	It does not save token.	It saves tokens to send large bursts.

4.10.4 Quality of Service (QoS) Parameters

- In one word, Quality of Service (QoS) can be referred as **efficiency**. We define Quality of Service as "How well or efficiently data transmissions are taking place".
- So the question arises "How can we improve our network's efficiency?" or "How can we improve our Quality of Service?".
- It can be achieved by managing data traffic which results in reduced packet loss, latency, and jitter on the respective network.
- This is all done by setting up priorities for specific types of data that traverse through the network.
- QoS can be measured quantitatively by using several parameters

1. **Packet loss**: It happens when the network links become congested and the routers and switches start dropping the packets. When these packets are dropped during real-time communication, such as audio or video, these sessions can experience jitter and gaps in speech.
2. **Jitter**: It occurs as the result of network congestion, timing drift, and route changes. And also, too much jitter can degrade the quality of audio communication.

3. **Latency**: It is the time delay, which is taken by a packet to travel from its source to its destination. For a great system, latency should be as low as possible, ideally, it should be close to zero.
4. **Bandwidth**: It is the capacity of a network channel to transmit maximum possible data through the channel in a certain amount of time. QoS optimizes a network by managing its bandwidth and setting the priorities for those applications which require more resources as compared to other applications.
5. **Mean opinion score:** It is a metric for rating the audio quality which uses a five-point scale, with a five indicating the highest or best quality.

ꕥꕥꕥꕥꕥ

CHAPTER 5

TRANSPORT LAYER

5.1 Introduction

- The transport layer is a 4th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
- The transport layer protocols are implemented in the end systems but not in the network routers.
- A computer network provides more than one protocol to the network applications. For example, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.
- All transport layer protocols provide multiplexing/demultiplexing service.
- It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.
- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.

5.2 Services provided by the Transport Layer

- The services provided by the transport layer are similar to those of the data link layer.
- The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks.
- The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- **End-to-end delivery**: The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.
- **Addressing**: According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
- **Reliable delivery**: The transport layer provides reliability services by retransmitting the lost and damaged packets. The reliable delivery has four aspects: Error control, Sequence control, Loss control and Duplication control

- **Flow control**: Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the **sliding window protocol** that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.
- **Multiplexing**: The transport layer uses the multiplexing to improve transmission efficiency. Multiplexing can occur in two ways**:**
  1. **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.
  2. **Downward multiplexing**: Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

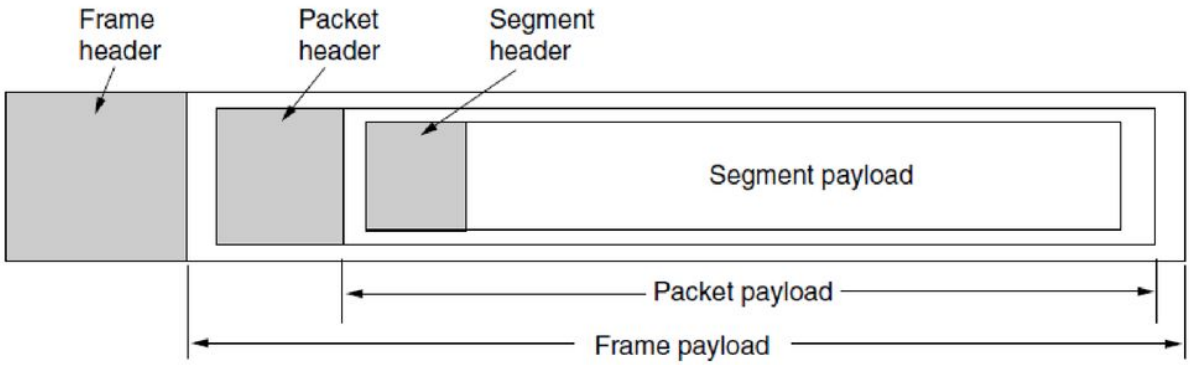
5.3 Transport Layer Service Primitives

- A service in a computer network consists of a set of primitives.
- A primitive is nothing but an operation.
- Transport layer primitives allow the transport user such as application programs to access the transport service.
- Primitive asks the service to do some action or to report on an action.
- Primitives can be considered as system calls.
- The primitive varies for different services.
- The following are some of the primitives used in transport layer:

Primitive	**TPDU Sent**	**Meaning**
LISTEN	None	Block until some process tries to connect
CONNECT	Connection Request	Actively attempt to establish connection
SEND	Data	Send data
RECEIVE	None	Block until a data TPDU arrives
DISCONNECT	Disconnect Request	Release the connection

- To see how these primitives might be used, consider an application with a server and a number of remote clients.
- To start with, the server executes a LISTEN primitive, typically by calling a library procedure that makes a system call that blocks the server until a client turns up.
- When a client wants to talk to the server, it executes a CONNECT primitive. The transport entity carries out this primitive by blocking the caller and sending a packet to the server.
- Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.
- For lack of a better term, we will use the term segment for messages sent from transport entity to transport entity.

- TCP, UDP and other Internet protocols use this term. Some older protocols used the ungainly name TPDU (Transport Protocol Data Unit).
- Thus, segments (exchanged by the transport layer) are contained in packets (exchanged by the network layer). In turn, these packets are contained in frames (exchanged by the data link layer).
- When a frame arrives, the data link layer processes the frame header and, if the destination address matches for local delivery, passes the contents of the frame payload field up to the network entity.
- The network entity similarly processes the packet header and then passes the contents of the packet payload up to the transport entity. This nesting is illustrated in figure below.



- Getting back to our client-server example, the client's CONNECT call causes a CONNECTION REQUEST segment to be sent to the server.
- When it arrives, the transport entity checks to see that the server is blocked on a LISTEN (i.e., is interested in handling requests). If so, it then unblocks the server and sends a CONNECTION ACCEPTED segment back to the client. When this segment arrives, the client is unblocked and the connection is established.
- Data can now be exchanged using the SEND and RECEIVE primitives.
- When a connection is no longer needed, it must be released to free up table space within the two transport entities.
- Disconnection has two variants: asymmetric and symmetric.
- In the asymmetric variant, either transport user can issue a DISCONNECT primitive, which results in a DISCONNECT segment being sent to the remote transport entity. Upon its arrival, the connection is released.
- In the symmetric variant, each direction is closed separately, independently of the other one. When one side does a DISCONNECT, that means it has no more data to send but it is still willing to accept data from its partner. In this model, a connection is released when both sides have done a DISCONNECT.
- A state diagram for connection establishment and release for these simple primitives is given in figure below.

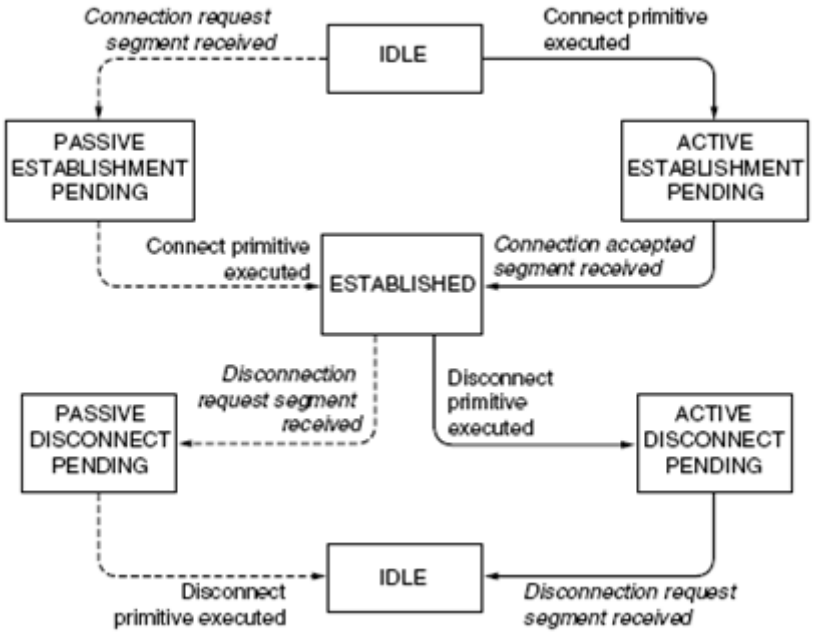


Figure. State diagram for a simple connection management scheme. Transitions labelled in italics are caused by packet arrivals. The solid lines show the client's state sequence. The dashed lines show the server's state sequence.

5.4 Berkeley Sockets

- Sockets are a service provided by transport layer.
- A socket is one endpoint of a two-way communication link between two programs running on the network.
- Berkeley Socket is an application programming interface (API) for Internet Socket and UNIX domain sockets.
- It is used for inter-process communication (IPC).
- It is commonly implemented as a library of linkable modules.
- Primitive used in Berkeley Socket:

Primitives	Meaning
SOCKET	Create a New Communication Endpoint.
BIND	Attach a Local Address to a SOCKET.
LISTEN	Shows the Willingness to Accept Connections.
ACCEPT	Block the Caller until a Connection Attempt Arrives.
CONNECT	Actively Attempt to Establish a Connection.
SEND	Send Some Data over Connection.
RECEIVE	Receive Some Data from the Connection.
CLOSE	Release the Connection.

Socket Programming

Server Side:

- Server startup executes SOCKET, BIND and LISTEN primitives.
- LISTEN primitive allocate queue for multiple simultaneous clients.
- Then it uses ACCEPT to suspend server until request.
- When client request arrives, ACCEPT returns.

- Start new socket (thread or process) with same properties as original, this handles the request, server goes on waiting on original socket.
- If new request arrives while spawning thread for this one, it is queued.
- If queue full, it is refused.

Client side:

- It uses SOCKET primitives to create.
- Then use CONNECT to initiate connection process.
- When this returns, the socket is open.
- Both sides can now SEND, RECEIVE.
- Connection not released until both sides do CLOSE.
- Typically, client does it, server acknowledges.

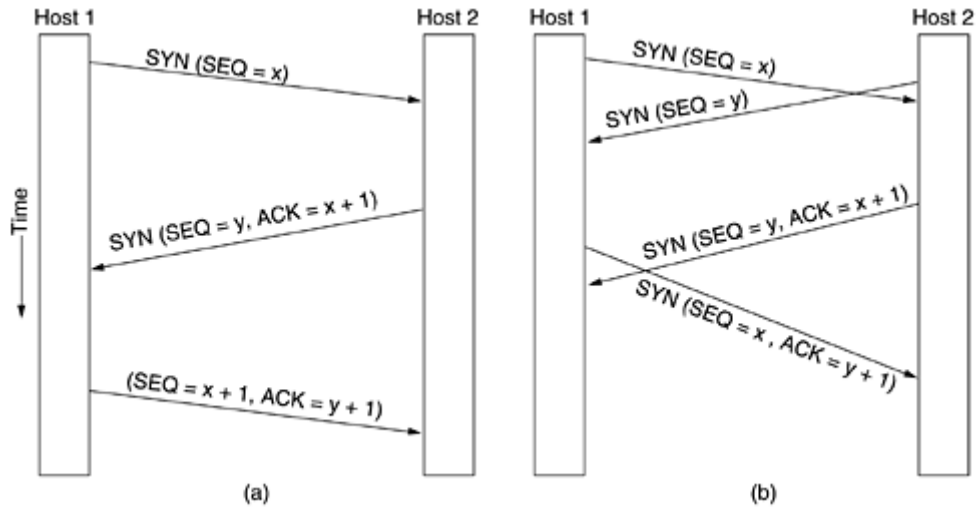
5.5 TCP

- TCP (Transmission Control Protocol) was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork.
- An internetwork differs from a single network because different parts may have wildly different topologies, bandwidth, delays, packet sizes, and other parameters.
- TCP was designed to dynamically adapt to properties of the internetwork and to be robust in the face of many kinds of failures.
- TCP service is obtained by both the sender and receiver creating end points, called sockets.
- Each socket has a socket number (address) consisting of the IP address of the host and a 16-bit number local to that host, called a **port**.
- A port is the TCP name for a TSAP (Transport Service Access Point).
- For TCP service to be obtained, a connection must be explicitly established between a socket on the sending machine and a socket on the receiving machine.
- All TCP connections are full duplex and point-to-point. Full duplex means that traffic can go in both directions at the same time. Point-to-point means that each connection has exactly two end points.
- TCP does not support multicasting or broadcasting.
- The basic protocol used by TCP entities is the sliding window protocol.
- When a sender transmits a segment, it also starts a timer. When the segment arrives at the destination, the receiving TCP entity sends back a segment (with data if any exist, otherwise without data) bearing an acknowledgement number equal to the next sequence number it expects to receive.
- If the sender's timer goes off before the acknowledgement is received, the sender transmits the segment again.

TCP Connection Establishment

- Connections are established in TCP by means of the three-way handshake process.
- To establish a connection, one side, say, the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a specific source or nobody in particular.

- The other side, say, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (e.g., a password).
- The CONNECT primitive sends a TCP segment with the SYN bit on and ACK bit off and waits for a response.
- When this segment arrives at the destination, the TCP entity there checks to see if there is a process that has done a LISTEN on the port given in the Destination port field.
- If not, it sends a reply with the RST bit on to reject the connection.
- If some process is listening to the port, that process is given the incoming TCP segment.
- It can then either accept or reject the connection.
- If it accepts, an acknowledgement segment is sent back.
- The sequence of TCP segments sent in the normal case is shown in figure (a) below.



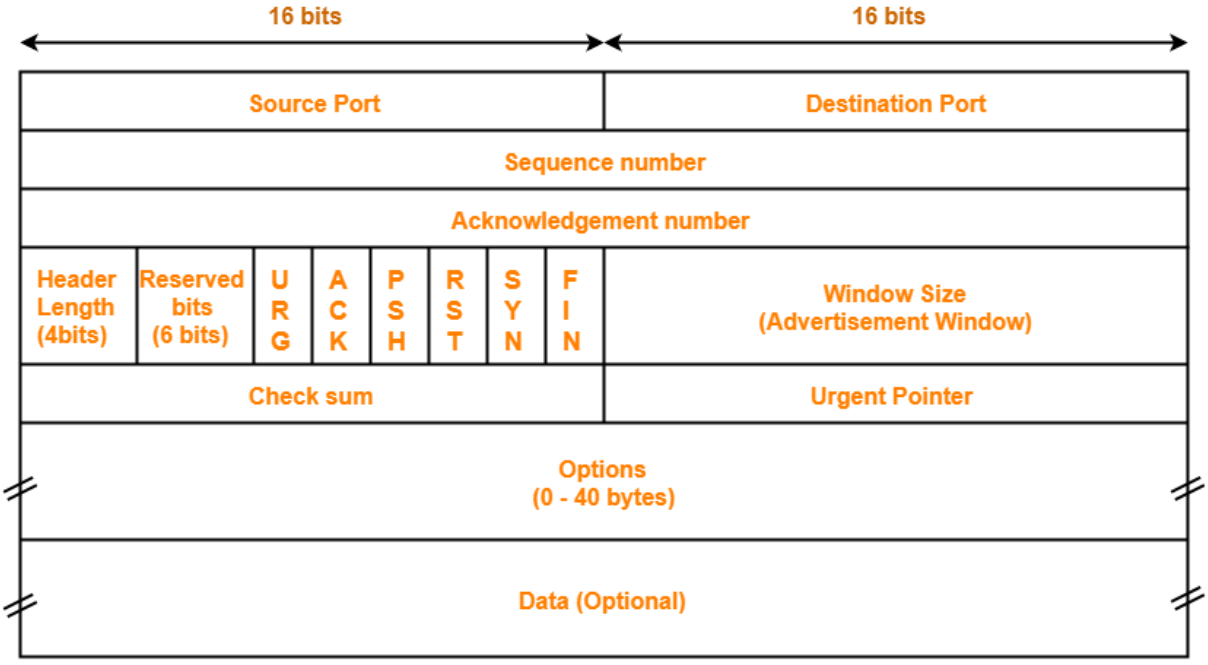
- Note that a *SYN* segment consumes 1 byte of sequence space so that it can be acknowledged unambiguously.
- In the event that two hosts simultaneously attempt to establish a connection between the same two sockets, the sequence of events is as illustrated in figure (b).
- The result of these events is that just one connection is established, not two because connections are identified by their end points.

TCP Connection Release

- TCP connections are full duplex.
- Each simplex connection is released independently of its sibling.
- To release a connection, either party can send a TCP segment with the *FIN* bit set, which means that it has no more data to transmit.
- When the *FIN* is acknowledged, that direction is shut down for new data.
- Data may continue to flow indefinitely in the other direction, however.
- When both directions have been shut down, the connection is released.
- Normally, four TCP segments are needed to release a connection, one *FIN* and one *ACK* for each direction.
- However, it is possible for the first *ACK* and the second *FIN* to be contained in the same segment, reducing the total count to three.

- If a response to a *FIN* is not forthcoming within two maximum packet lifetimes, the sender of the *FIN* releases the connection.
- The other side will eventually notice that nobody seems to be listening to it anymore and will time out as well.
- While this solution is not perfect, given the fact that a perfect solution is theoretically impossible, it will have to do. In practice, problems rarely arise.

TCP Segment Header



TCP Header

- Every segment begins with a fixed-format, **20-byte** header.
- **Source Port**: 16-bit field. Identifies the host process on the sender machine.
- **Destination Port**: 16-bit field. Identifies the host process on the receiver machine. The source port and the destination port together uniquely identify the connection.
- **Sequence Number**: 32-bit field. It is the sequence number of the first data byte in this segment. If SYN bit is set, the sequence number is the initial sequence number and the first data byte is the initial sequence number + 1.
- **Acknowledgement Number**: 32-bit field. If ACK bit is set, this field contains the value of the next sequence number the receiver is expecting to receive.
- **Header Length**: 4-bit field. It tells how many 32-bit words are contained in the TCP header. This field really indicates the start of the data within the segment, measured in 32-bit words.
- Next there is a 6-bit field which is kept for future use.
- **Flags**:
  1. URG: 1-bit. The URG bit is set to 1 if the urgent pointer is in use.
  2. ACK: 1-bit. ACK is set to 1 if the acknowledgement number is valid.
  3. PSH: 1-bit. It is the push flag which indicates the pushed data.
  4. RST: 1-bit. The reset flag is used to reset the connection.
  5. SYN: 1-bit. The SYN bit is used to establish connections.

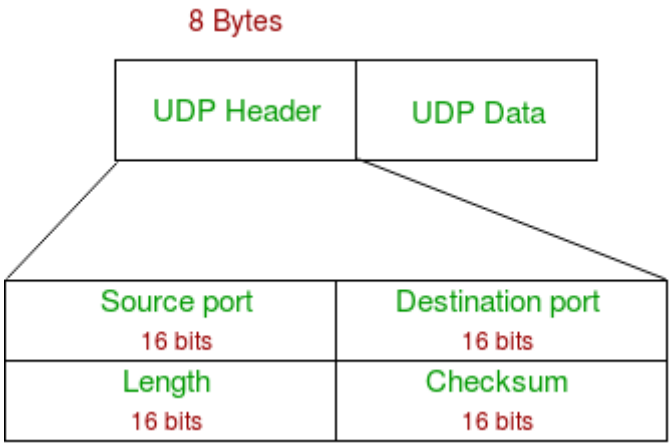
6. FIN: 1-bit. The Finish flag is set to 1 to release the connection. It specifies that the sender has no more data to transmit.

- **Window Size**: 16-bit field. It signifies the number of data bytes that the receiver is willing to accept.
- **Checksum**: 16-bit field. Checksum is used for error control. It verifies the integrity of data in the TCP payload. Sender adds CRC checksum to the checksum field before sending the data. Receiver rejects the data that fails the CRC check.
- **Urgent Pointer**: 16-bit field. It indicates how much data in the current segment counting from the first data byte is urgent. Urgent pointer added to the sequence number indicates the end of urgent data byte. This field is considered valid and evaluated only if the URG bit is set to 1.
- **Options**: Options field is used for several purposes. The size of options field varies from 0 bytes to 40 bytes. Options field is generally used for the following purposes: Time stamp, Window size extension, Parameter negotiation, Padding

5.6 UDP

- **User Datagram Protocol (UDP)** is a Transport Layer protocol.
- UDP is a part of Internet Protocol suite, referred as UDP/IP suite.
- Unlike TCP, it is **unreliable and connectionless protocol.** So, there is no need to establish connection prior to data transfer.
- For the real-time services like computer gaming, voice or video communication, live conferences; we need UDP.
- Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets.
- There is no error checking in UDP, so it also saves bandwidth.
- User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

UDP Header



1. **Source Port:** Source Port is 2 Byte long field used to identify port number of source.
2. **Destination Port:** It is 2 Byte long field, used to identify the port of destined packet.
3. **Length:** Length is the length of UDP including header and the data. It is 16-bits field.

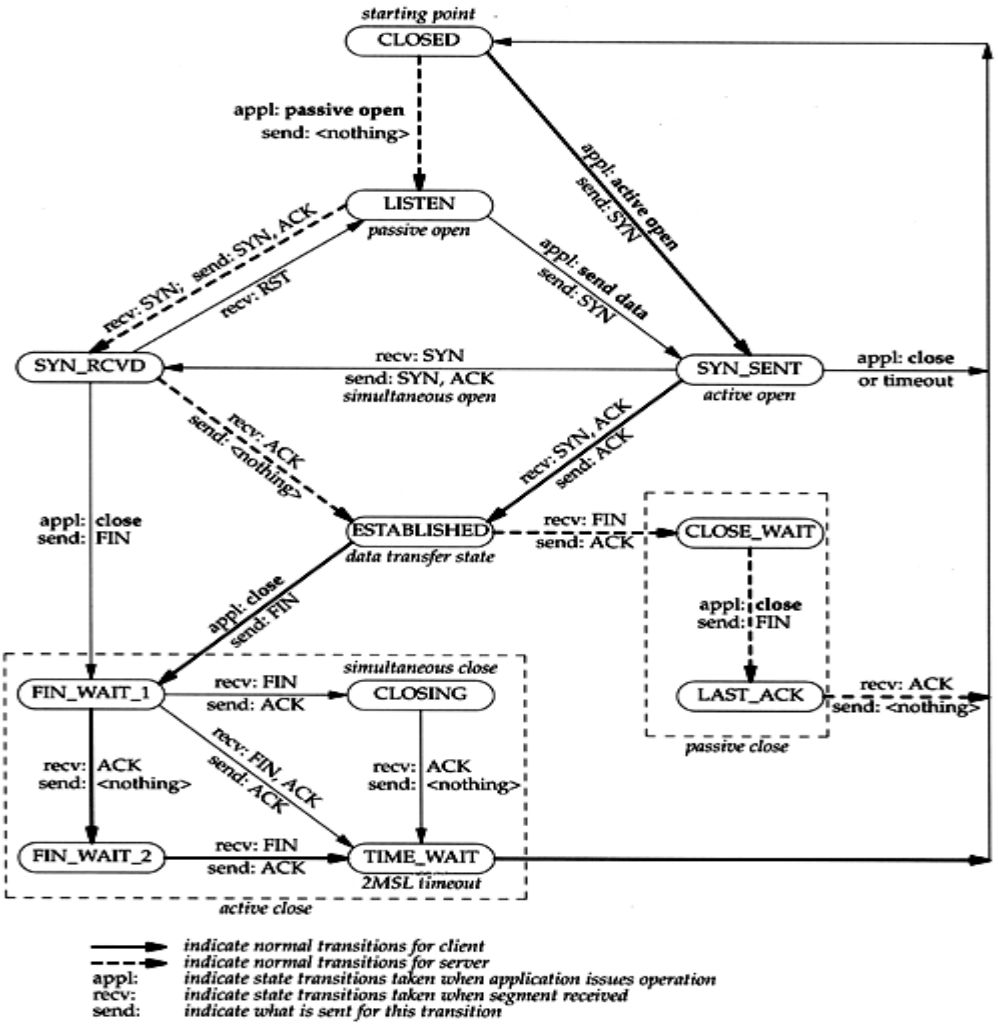
4. **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

TCP Vs UDP

	TCP	**UDP**
Full form	It stands for **Transmission Control Protocol**.	It stands for **User Datagram Protocol**.
Type of connection	It is a connection-oriented protocol, which means that the connection needs to be established before the data is transmitted over the network.	It is a connectionless protocol, which means that it sends the data without checking whether the system is ready to receive or not.
Reliable	TCP is a reliable protocol as it provides assurance for the delivery of data packets.	UDP is an unreliable protocol as it does not take the guarantee for the delivery of packets.
Speed	TCP is slower than UDP as it performs error checking, flow control, and provides assurance for the delivery of	UDP is faster than TCP as it does not guarantee the delivery of data packets.
Header size	The size of TCP is 20 bytes.	The size of the UDP is 8 bytes.
Acknowledgment	TCP uses the three-way-handshake concept. In this concept, if the sender receives the ACK, then the sender will send the data. TCP also has the ability to resend the lost data.	UDP does not wait for any acknowledgment; it just sends the data.
Flow control mechanism	It follows the flow control mechanism in which too many packets cannot be sent to the receiver at the same time.	This protocol follows no such mechanism.
Error checking	TCP performs error checking by using a checksum. When the data is corrected, then the data is retransmitted to the receiver.	It does not perform any error checking, and also does not resend the lost data packets.
Applications	This protocol is mainly used where a secure and reliable communication process is required, like military services, web browsing, and e-mail.	This protocol is used where fast communication is required and does not care about the reliability like VoIP, game streaming, video and music streaming, etc.

5.7 TCP State Transition Diagram

- A TCP connection goes through a series of states during its lifetime.
- Figure below shows the state transition diagram.
- Each state transition is indicated by an arrow, and the associated label indicates associated events and actions.
- Connection establishment begins in the CLOSED state and proceeds to the ESTABLISHED state.
- Connection termination goes from the ESTABLISHED state to the CLOSED state.
- The normal transitions for a client are indicated by thick solid lines, and the normal transitions for a server are denoted by dashed lines.
- Thus when a client does an active open, it goes from the CLOSED state, to SYN_SENT, and then to ESTABLISHED.
- The server carrying out a passive open goes from the CLOSED state, to LISTEN, SYN_RCVD, and then to ESTABLISHED.
- The client normally initiates the termination of the connection by sending a FIN.
- The associated state trajectory goes from the ESTABLISHED state, to FIN_WAIT_1 while it waits for an ACK, to FIN_WAIT_2while it waits for the other side's FIN, and then to TIME WAIT after it sends the final ACK.
- When the TIME_WAIT 2MSL period expires, the connection is closed.



1. **LISTEN** represents waiting for a connection request from any remote TCP and port.
2. **SYN_SENT** represents waiting for a matching connection request after having sent a connection request.
3. **SYN_RECEIVED** represents waiting for a confirming connection request acknowledgment after having both received and sent a connection request.
4. **ESTABLISHED** represents an open connection, data received can be delivered to the user. The normal state for the data transfer phase of the connection.
5. **FIN_WAIT_1** represents waiting for a connection termination request from the remote TCP, or an acknowledgment of the connection termination request previously sent.
6. **FIN_WAIT_2** represents waiting for a connection termination request from the remote TCP.
7. **CLOSE_WAIT** represents waiting for a connection termination request from the local user.
8. **CLOSING** represents waiting for a connection termination request acknowledgment from the remote TCP.
9. **LAST_ACK** represents waiting for an acknowledgment of the connection termination request previously sent to the remote TCP (which includes an acknowledgment of its connection termination request).
10. **TIME_WAIT** represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request.
11. **CLOSED** represents no connection state at all.

5.8 TCP Timers

Timers used by TCP to avoid excessive delays during communication are called as TCP Timers. The 4 important timers used by a TCP implementation are:

1. Time Out Timer

- Sender starts a time out timer after transmitting a TCP segment to the receiver.
- If sender receives an acknowledgement before the timer goes off, it stops the timer.
- If sender does not receive any acknowledgement and the timer goes off, then **TCP Retransmission** occurs.
- Sender retransmits the same segment and resets the timer.
- The value of time out timer is dynamic and changes with the amount of traffic in the network.
- Time out timer is also called as **Retransmission Timer**.

2. Time Wait Timer

- Sender starts the time wait timer after sending the ACK for the second FIN segment.
- It allows to resend the final acknowledgement if it gets lost.
- It prevents the just closed port from reopening again quickly to some other application.
- It ensures that all the segments heading towards the just closed port are discarded.
- The value of time wait timer is usually set to twice the lifetime of a TCP segment.

3. Keep Alive Timer

- Each time server hears from the client, it resets the keep alive timer to 2 hours.

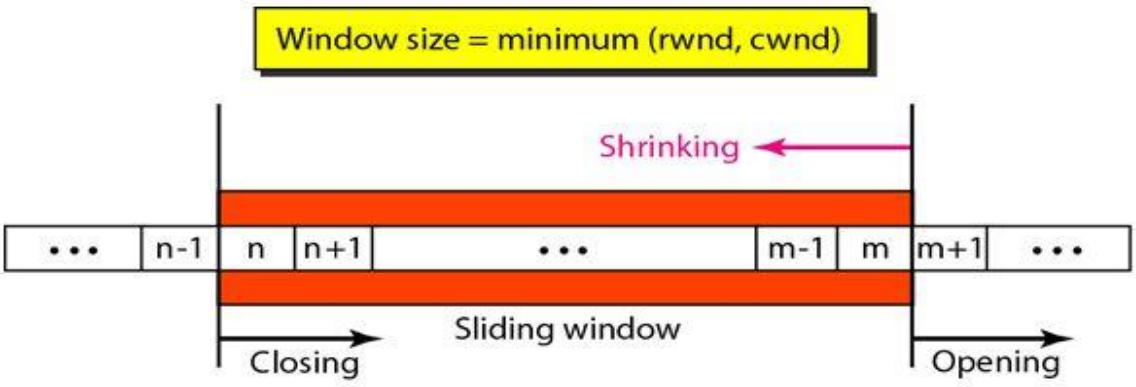
- If server does not hear from the client for 2 hours, it sends 10 probe segments to the client.
- These probe segments are sent at a gap of 75 seconds.
- If server receives no response after sending 10 probe segments, it assumes that the client is down.
- Then, server terminates the connection automatically.

4. Persistent Timer

- TCP uses a persistent timer to deal with a zero-widow-size deadlock situation.
- It keeps the window size information flowing even if the other end closes its receiver window.
- Sender starts the persistent timer on receiving an ACK from the receiver with a zero window size.
- When persistent timer goes off, sender sends a special segment to the receiver.
- This special segment is called as probe segment and contains only 1 byte of new data.
- Response sent by the receiver to the probe segment gives the updated window size.
- If the updated window size is non-zero, it means data can be sent now.
- If the updated window size is still zero, the persistent timer is set again and the cycle repeats.

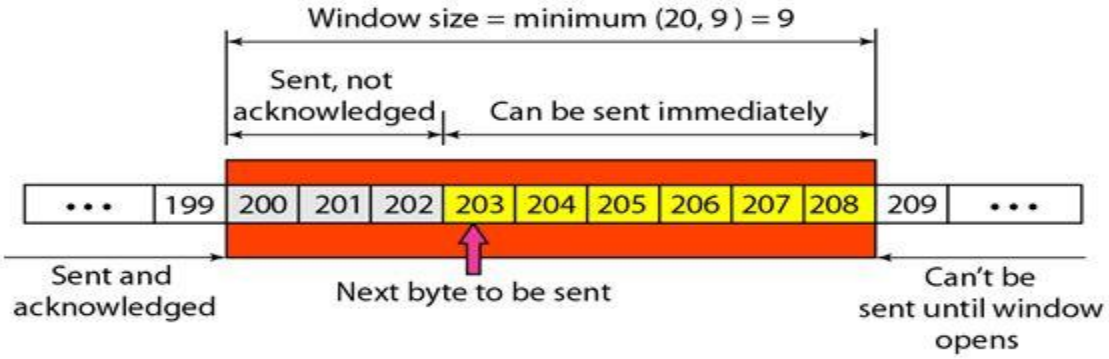
5.9 TCP Flow Control (Sliding Window)

- TCP uses a sliding window to handle flow control.
- The sliding window protocol used by TCP, however, is something between the Go-Back-N and Selective Repeat sliding window.
- There are two big differences between this sliding window and the one we used at the data link layer. First, the sliding window of TCP is byte-oriented but data link layer sliding window is frame-oriented. Second, the TCP's sliding window is of variable size and the data link layer was of fixed size.
- The following figure shows the sliding window in TCP.



- The window spans a portion of the buffer containing bytes received from the process.
- The bytes inside the window are the bytes that can be in transit; they can be sent without worrying about acknowledgment.
- The imaginary window has two walls: one left and one right.
- The window is opened, closed, or shrunk.

- These three activities, as we will see, are in the control of the receiver (and depend on congestion in the network), not the sender.
- The sender must obey the commands of the receiver in this matter.
- Opening a window means moving the right wall to the right. This allows newer bytes in the buffer that are eligible for sending.
- Closing the window means moving the left wall to the right. This means that some bytes have been acknowledged and the sender need not worry about them anymore.
- Shrinking the window means moving the right wall to the left. This is not allowed in some implementations because it means revoking the eligibility of some bytes for sending.
- The size of the window at one end is determined by the lesser of two values: receiver window (rwnd) or congestion window (cwnd).
- The receiver window is the value advertised by the opposite end in a segment containing acknowledgment. It is the number of bytes the other end can accept before its buffer overflows and data are discarded.
- The congestion window is a value determined by the network to avoid congestion.
- The following figure shows an unrealistic example of a sliding window.



- The sender has sent bytes up to 202. We assume that cwnd is 20 (in reality this value is thousands of bytes).
- The receiver has sent an acknowledgment number of 200 with an rwnd of 9 bytes (in reality this value is thousands of bytes).
- The size of the sender window is the minimum of rwnd and cwnd, or 9 bytes.
- Bytes 200 to 202 are sent, but not acknowledged.
- Bytes 203 to 208 can be sent without worrying about acknowledgment.
- Bytes 209 and above cannot be sent.

Features of TCP sliding window are as follows:

- The size of the window is the lesser of rwnd and cwnd.
- The source does not have to send a full window's worth of data.
- The window can be opened or closed by the receiver, but should not be shrunk.
- The destination can send an acknowledgment at any time as long as it does not result in a shrinking window.
- The receiver can temporarily shut down the window; the sender, however, can always send a segment of 1 byte after the window is shut down.

5.10 TCP Congestion Control: Slow Start

- TCP slow start is an algorithm which balances the speed of a network connection.
- Slow start gradually increases the amount of data transmitted until it finds the network's maximum carrying capacity.
- One of the most common ways to optimize the speed of a connection is to increase the speed of the link (i.e. increase the amount of bandwidth). However, any link can become overloaded if a device tries to send out too much data.
- Oversaturating a link is known as congestion, and it can result in slow communications or even data loss.
- Slow start prevents a network from becoming congested by regulating the amount of data that's sent over it.
- It negotiates the connection between a sender and receiver by defining the amount of data that can be transmitted with each packet, and slowly increases the amount of data until the network's capacity is reached.
- This ensures that as much data is transmitted as possible without clogging the network.

How TCP slow start works

- TCP slow start is one of the first steps in the congestion control process.
- It balances the amount of data a sender can transmit (known as the congestion window) with the amount of data the receiver can accept (known as the receiver window).
- The lower of the two values becomes the maximum amount of data that the sender is allowed to transmit before receiving an acknowledgment from the receiver.

Step-by-step, here's how slow start works:

1. A sender attempts to communicate to a receiver. The sender's initial packet contains a small congestion window, which is determined based on the sender's maximum window.

2. The receiver acknowledges the packet and responds with its own window size. If the receiver fails to respond, the sender knows not to continue sending data.

3. After receiving the acknowledgement, the sender increases the next packet's window size. The window size gradually increases until the receiver can no longer acknowledge each packet, or until either the sender or the receiver's window limit is reached.

Once a limit has been determined, slow start's job is done. Other congestion control algorithms take over to maintain the speed of the connection.

Example of TCP slow start

Content providers often adjust their slow start window to maximize performance. The initial congestion window parameter (initcwnd) can have a significant impact on the speed of a network. When the receiver has to send fewer acknowledgments to the sender, more data can be transmitted faster.

Most large CDN (Content Delivery Network) providers default to an initcwnd of 10, meaning the CDN will transmit 10 packets before requesting an acknowledgment. A good balance will be determined by the type of data transmitted and the general speed of the network.

Benefits of TCP slow start

Slow start ensures the speed and integrity of a network while protecting content providers and consumers.

1. **Users experience uninterrupted connections** since packets are no longer dropped due to congestion.
2. **Users also experience faster downloads** since slow start finds and uses the maximum connection speed.
3. **Enterprises see less network congestion** since slow start regulates bandwidth and prevents the sender from having to continuously retransmit data.

ꕥꕥꕥꕥꕥ

CHAPTER 6

APPLICATION LAYER

6.1 Domain Name System (DNS)

- DNS is a host name to IP address translation service.
- DNS is a distributed database implemented in a hierarchy of name servers.
- It is an application layer protocol for message exchange between clients and servers.

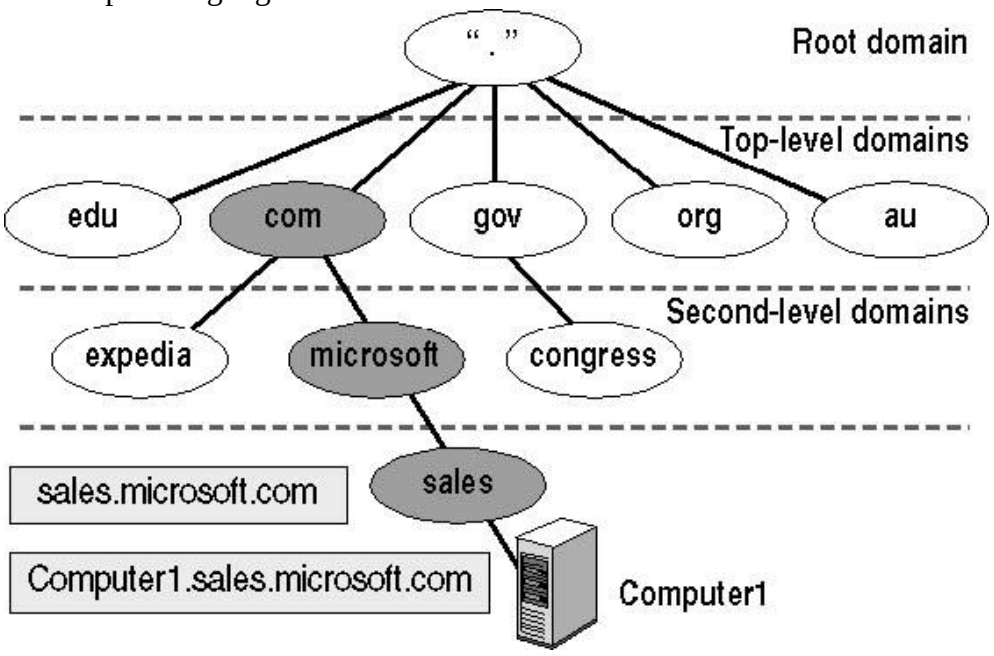
Requirement

- Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static, therefore a mapping is required to change the domain name to IP address.
- So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain:

There are various kinds of DOMAIN:

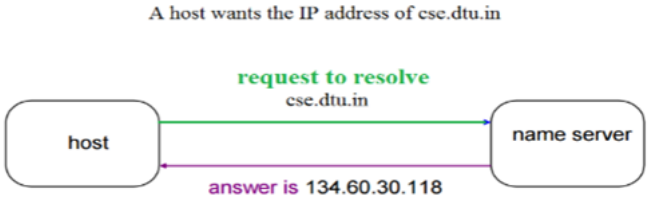
- **Generic domain**: .com (commercial) .edu (educational) .mil(military) .org (non-profit organization) .net (similar to commercial) all these are generic domain.
- **Country domain**: .in (india) .us .uk
- **Inverse domain** if we want to know what is the domain name of the website i.e. IP to domain name mapping. So DNS can provide both the mapping. For example, to find the IP addresses of www.google.com then we have to type
  nslookup www.google.com



It is very difficult to find out the IP address associated to a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delay for that to happen organization of database is very important.

- **DNS record**: Domain name, IP address, what is the validity?, what is the time to live ? and all the information related to that domain name. These records are stored in tree like structure.
- **Namespace**: Set of possible names, flat or hierarchical. In a flat name space, a name is a sequence of characters without structure. In hierarchical name space, each name consists of several parts. First part defines the nature of the organization, second part defines the name of an organization, third part defines department of the organization, and so on. Naming system maintains a collection of bindings of names to values. Given a name, a resolution mechanism returns the corresponding value.
- **Name server**: It is an implementation of the resolution mechanism.

Name to Address Resolution:



- The host request the DNS name server to resolve the domain name.
- And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

Hierarchy of Name Servers

- **Root name servers**: It is contacted by name servers that cannot resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.
- **Top level server**: It is responsible for com, org, edu, etc. and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.
- **Authoritative name servers:** This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative IP address.

6.2 HTTP

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP transfers the files from one host to another host. HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP data is transferred between client and server. The HTTP messages are sent from the client to the server and from server to the client.

Features of HTTP:

1. **Connectionless protocol**: HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
2. **Media independent**: HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
3. **Stateless**: HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.

- **Request Message:** The request message is sent by the client that consists of a request line, headers, and sometimes a body.
- **Response Message:** The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

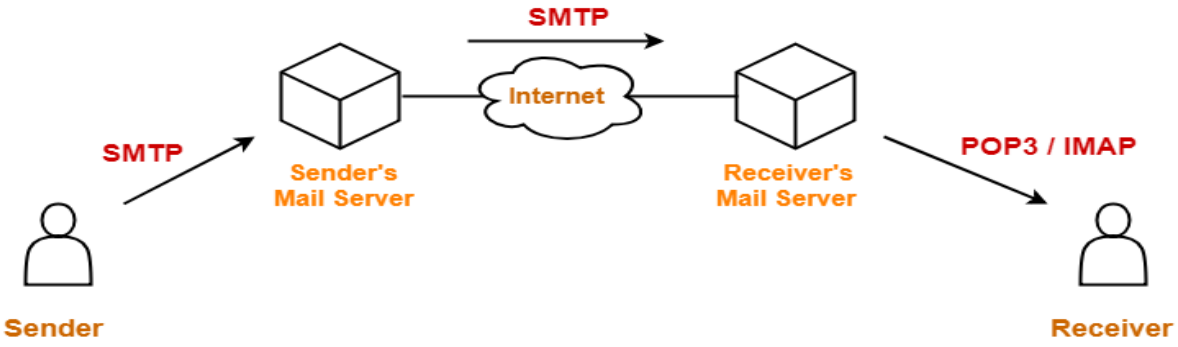
6.3 SMTP

- SMTP is short for Simple Mail Transfer Protocol.
- It is an application layer protocol.
- It is used for sending the emails efficiently and reliably over the internet.
- SMTP is a push protocol.
- SMTP uses TCP at the transport layer.
- SMTP uses port number 25.
- SMTP uses persistent TCP connections, so it can send multiple emails at once.
- SMTP is a connection oriented protocol.
- SMTP is a stateless protocol.

Working

- SMTP server is always on a listening mode.
- Client initiates a TCP connection with the SMTP server.
- SMTP server listens for a connection and initiates a connection on that port.
- The connection is established.

- Client informs the SMTP server that it would like to send a mail.
- Assuming the server is OK, client sends the mail to its mail server.
- Client's mail server uses DNS to get the IP Address of receiver's mail server.
- Then, SMTP transfers the mail from sender's mail server to the receiver's mail server.



While sending the mail, SMTP is used two times-

1. Between the sender and the sender's mail server.
2. Between the sender's mail server and the receiver's mail server.

To receive or download the email,

1. Another protocol is needed between the receiver's mail server and the receiver.
2. The most commonly used protocols are POP3 and IMAP.

6.4 Telnet

- Telnet is short for Terminal Network.
- Telnet is a client-server application that allows a user to log onto remote machine and lets the user to access any application on the remote computer.
- Telnet uses NVT (Network Virtual Terminal) system to encode characters on the local system.
- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- Telnet is a protocol that provides a general, bi-directional, 8-bit byte oriented communications facility.
- Many application protocols are built upon the Telnet protocol.
- Telnet services are used on Port 23.

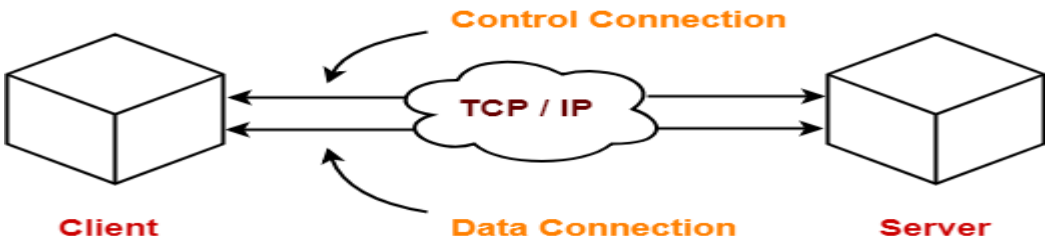
6.5 FTP

- FTP is short for File Transfer Protocol.
- It is an application layer protocol.
- It is used for exchanging files over the internet.
- It enables the users to upload and download the files from the internet.
- FTP uses TCP at the transport layer.
- FTP uses port number 21 for control connection.
- FTP uses port number 20 for data connection.
- FTP uses persistent TCP connections for control connection.
- FTP uses non-persistent connections for data connection.
- FTP is a connection oriented protocol.

- Emails can't be sent using FTP.
- FTP can transfer one file at a time.
- FTP is a statefull protocol.

Working

- FTP establishes two TCP connections between the client and the server.
- One connection is used for transferring data.
- Other connection is used for transferring control information.



6.6 DHCP

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol).
- DHCP automates and centrally manages these configurations.
- There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.
- DHCP can be implemented on local networks as well as large enterprise networks.
- DHCP is the default protocol used by the most routers and networking equipment.
- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.
- DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.
- DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.

- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

ಔಔಔಔಔ