KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF COMPUTER SCIENCE, CA & IT

SUBJECT : **INTRODUCTION TO COMPUTER NETWORKS**

SEMESTER : **III** **L T P C**

SUBJECT CODE: **17CSU303** **CLASS** : **II B.Sc.CS A & B** **4 0 0 4**

SYLLABUS

COURSE OBJECTIVE:

This course is to master the fundamentals of data communications networks by gaining knowledge of data transmission concepts, understanding the operation of all seven layers of OSI Model and the protocols used in each layer.

COURSE OUTCOME:

- Describe various transmission media, their comparative study, fiber optics and wireless media
- Describe Categories and topologies of networks (LAN and WAN) Layered architecture (OSI and TCP/IP) and protocol suites.
- Able to analyze datalink or network layer protocols for error detection and correction.
- Deep understanding about details of IP operations in the INTERNET and associated routing principles.

Unit I

Introduction to Computer Networks : Network definition; network topologies; network classifications; network protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite. **Data Communication Fundamentals and Techniques**: Analog and digital signal; data-ratelimits; digital to digital line encoding schemes; pulse code modulation; parallel and serial transmission;

Unit – II

(cont..)digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media.

Networks Switching Techniques and Access mechanisms: Circuit switching; packet switching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

Unit – III

Data Link Layer Functions and Protocol: Error detection and error correction techniques; data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

Unit – IV

Multiple Access Protocol and Networks: CSMA/CD protocols; Ethernet LANS; connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router and gateways; **Networks Layer Functions and Protocols**: Routing; routing algorithms; network layer protocol of Internet- IP protocol, Internet control protocols.

Unit V

Transport Layer Functions and Protocols: Transport services- error and flow control, Connection establishment and release- three way handshake; **Overview of Application layer protocol**: Overview of DNS protocol; overview of WWW &HTTP protocol.

Suggested Readings

1. Forouzan, B. A.(2007). Data Communications and Networking(4th ed.). New Delhi: THM.
2. Tanenbaum, A. S. (2002). Computer Networks (4th ed.). New Delhi: PHI.

WEB SITES

1. en.wikipedia.org/wiki/Internet_protocol_suite
2. http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies
3. www.yale.edu/pclt/COMM/TCPIP.HTM
4. www.w3schools.com/tcpip/default.asp

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)

DEPARTMENT OF COMPUTER SCIENCE, CA & IT

SUBJECT : **INTRODUCTION TO COMPUTER NETWORKS**

SEMESTER : **III** **L T P C**

SUBJECT CODE: **17CSU303** **CLASS** : **II B.Sc.CS A & B** **4 0 0 4**

LECTURE PLAN

Unit I

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	**Introduction to Computer Networks** : Network definition, network topologies	**W1**
2	1	network classifications, network protocol	**T1: 13-15, T1: 19**
3	1	layered network architecture	**T1: 27-28**
4	1	overview of OSI reference model	**T1: 29-33,R1:41**
5	1	overview of TCP/IP protocol suite.	**T1: 42-45,R1:45**
6	1	**Data Communication Fundamentals and Techniques**: Analog and digital signal, data-ratelimits	**T1: 57-58, T1: 85-88**
7	1	digital to digital line encoding schemes	**T1: 101-106**
8	1	pulse code modulation, parallel and serial transmission	**T1: 121-128, T1: 131-132**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 1: 9 hrs	

Unit – II

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	digital to analog modulation	**T1: 141-148**
2	1	multiplexing techniques- FDM, TDM Transmission media.	**T1: 161-179 T1: 191-207,R1:95-99**
3	1	Networks Switching Techniques and access mechanisms: Circuit switching	**T1: 213-218**
4	1	Packet switching	**W2,R1:356-361**

5	1	connectionless datagram switching,	**W3,R1:356-361**
6	1	connection-oriented virtual circuit switching	**W3,R1:356-361**
7	1	dial-up modems	**T1: 248-250**
8	1	digital subscriber line cable TV for data transfer.	**T1: 251-255,** **T1: 257-260**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 2: 9 hrs	

Unit – III

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	**Data Link Layer Functions and Protocol**: Error detection techniques	**T1: 267-269, 272** **R1:209**
2	1	error correction techniques	**T1: 273-274,R1:204**
3	1	data-link control- framing	**T1: 307-308**
4	1	Flow control	**T1: 311,R1:194-201**
5	1	error recovery protocols-	**T1: 312**
6	1	stop and wait ARQ,	**T1: 318-323, W4**
7	1	go-back-n ARQ	**T1: 324-331,W4**
8	1	Point to Point Protocol on Internet.	**T1: 346-355**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 3: 9 hrs	

Unit – IV

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	**Multiple Access Protocol and Networks**: CSMA/CD protocols	**T1: 363-377**
2	1	Ethernet LANS	**T1: 395-402**
3	1	connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router and gateways	**T1: 445-457** **R1:340**
4	1	**Networks Layer Functions and Protocols**: Routing	**T1: 647-655**
5	1	routing algorithms	**T1: 658-684,**

			R1:362-389
6	1	network layer protocol of Internet-	**T1: 579-582**
7	1	IP protocol,	**T1: 582-602**
8	1	Internet control protocols	**T1: 621-627, W5**
9	1	Recapitulation and Discussion of Important Questions	
		Total hours planned for UNIT- 4: 9 hrs	

Unit V

S.No	Lecture Duration (Hours)	Topics to be Covered	Support Materials
1	1	**Transport Layer Functions and Protocols**: Transport services	**T1: 715, W6**
2	1	error control	**T1: 731-734**
3	1	flow control	**T1: 728-730**
4	1	Connection establishment and release	**T1: 703-707**
5	1	Three way handshake	**R1:516-517**
6	1	**Overview of Application layer protocol**: Overview of DNS protocol	**T1: 799-801, 803-805 W7**
7	1	overview of WWW &	**T1: 851-860**
8	1	Overview of HTTP protocol.	**T1: 861-868**
9	1	Recapitulation and Discussion of Important Questions	
10	1	Discussion of Previous year ESE Question Paper	
11	1	Discussion of Previous year ESE Question Paper	
12	1	Discussion of Previous year ESE Question Paper	
		Total hours planned for UNIT- 5: 12 hrs	
		Total No Of Hours Planned: 48 hrs	

Text Book:

T1→Forouzan, B. A.(2007). Data Communications and Networking(4th ed.). New Delhi: THM.

Reference Book:

R1→Tanenbaum, A. S. (2002). Computer Networks(5th ed.). New Delhi: PHI.

Websites:

W1→ https://www.studytonight.com/computer-networks/overview-of-computer-networks

W2→https://www.tutorialspoint.com/data_communication_computer_network/ecomputernotes.com › Computer Networking › Switching

W3→https://thehelios.wordpress.com/tag/connectionless-packet-switching/

W4→https://www.geeksforgeeks.org/stop-and-wait-arq/

W5→https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/

W6→https://www.studytonight.com/computer-networks/osi-model-transport-layer

W7→https://www.geeksforgeeks.org/protocols-application-layer/

UNIT I

SYLLABUS

Introduction to Computer Networks : Network definition; network topologies; network classifications; network protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite. **Data Communication Fundamentals and Techniques**: Analog and digital signal; data-ratelimits; digital to digital line encoding schemes; pulse code modulation; parallel and serial transmission;

INTRODUCTION TO COMPUTER NETWORKS:

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork.

Definition: A set of devices often mentioned as nodes connected by media link is called a Network.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is **Internet.**

NETWORK DEFINITION

A network is a set of devices (often referred to as nodes) connected by communicationlinks. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Data communication:

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

Components:

A data communications system has five components;

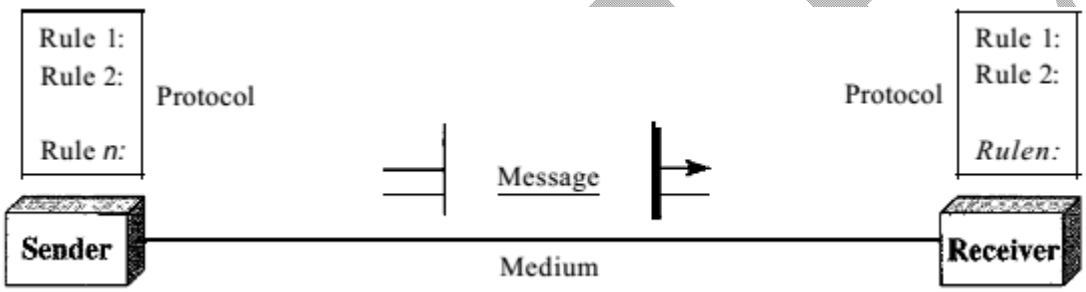
1. Message. The message is the information (data) to be communicated. Popularforms of information include text, numbers, pictures, audio, and video.

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

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

4. Transmission medium. The transmission medium is the physical path by whicha message travels from sender to receiver. Some examples of transmission mediainclude twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

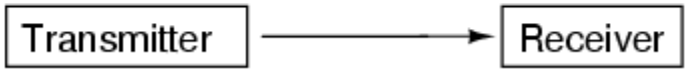
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.



Data Representation
Information today comes in different forms such as text, numbers, images, audio, and video.

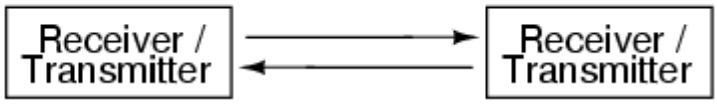
Data Flow
Buses and networks are designed to allow communication to occur between individual devices that are interconnected. The flow of information, or data, between nodes, can take a variety of forms: simplex, half-duplex, or full-duplex.

Simplex communication



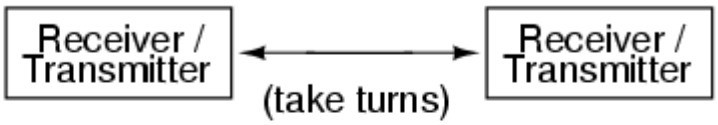
With **simplex communication**, all data flow is unidirectional: from the designated transmitter to the designated receiver.
Keyboard and Monitor is an example of simplex communication.

Duplex communication

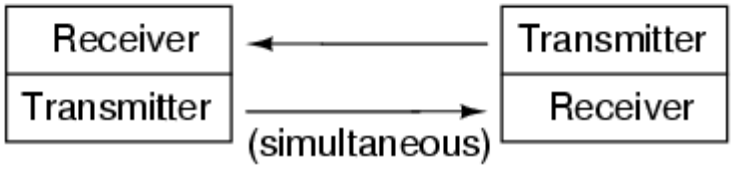


With **duplex communication**, the flow of information is bi-directional for each device. Duplex can be further divided into two sub-categories:

Half-duplex



Full-duplex



In **half-duplex mode**, each station can both transmit and receive, but not at the same time: When one device is sending, the other can only receive, and vice versa.
Example: Walkie-talkies and CB (citizens band) radios,intercom are both half-duplex systems.

In **full-duplex mode** (also called duplex), both stations can transmit and receive simultaneously. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

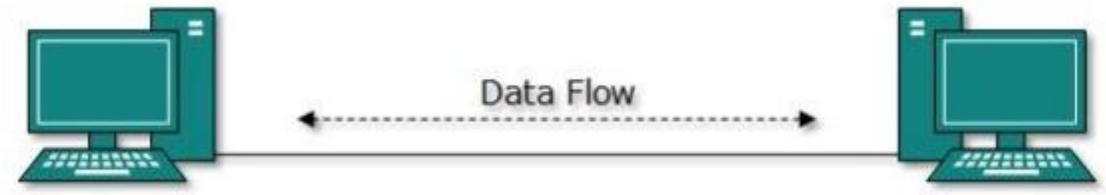
We can use this for multipurpose data communication at the same time like internet, cable TV and phone etc with the same cable.

NETWORK TOPOLOGIES:

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

POINT-TO-POINT

Point-to-point networks contains exactly two hosts (computer or switches or routers or servers) connected back toback using a single piece of cable. Often, the receiving end of one host is connected to sending end of the otherend and vice-versa.

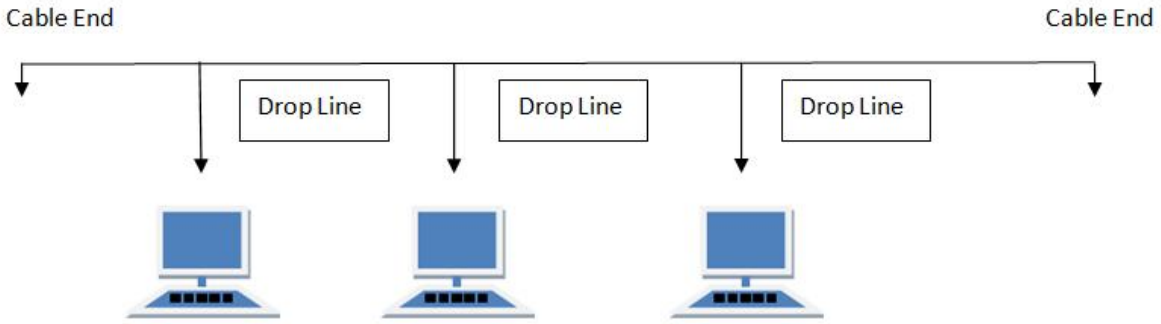


[*Image: Point-to-point Topology*]

If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hostsare unaware of underlying network and see each other as if they are connected directly.

BUS TOPOLOGY

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.

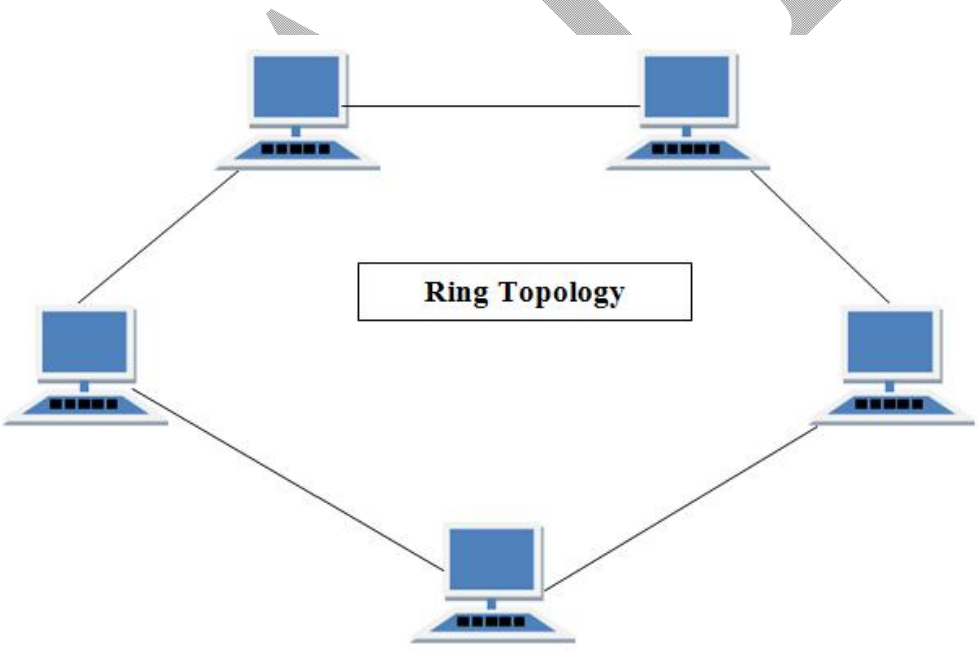
3. Cable has a limited length.
4. It is slower than the ring topology.

RING TOPOLOGY

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.



Advantages of Ring Topology

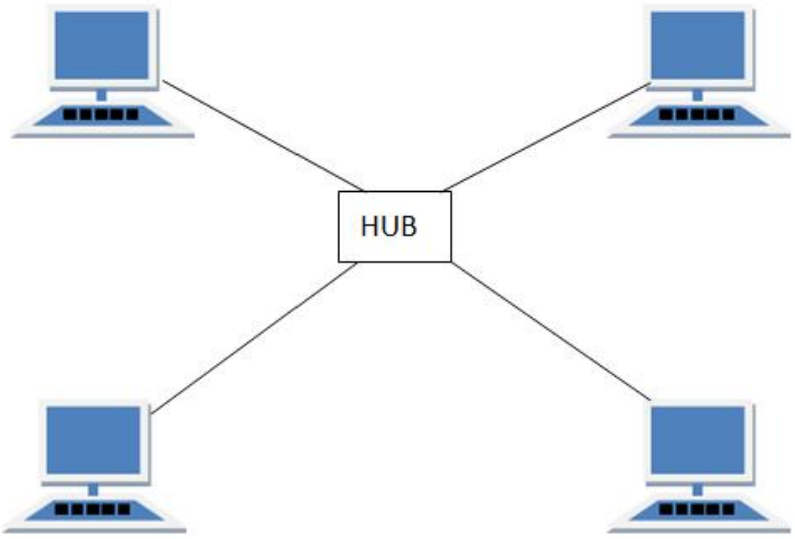
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR TOPOLOGY

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.

3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

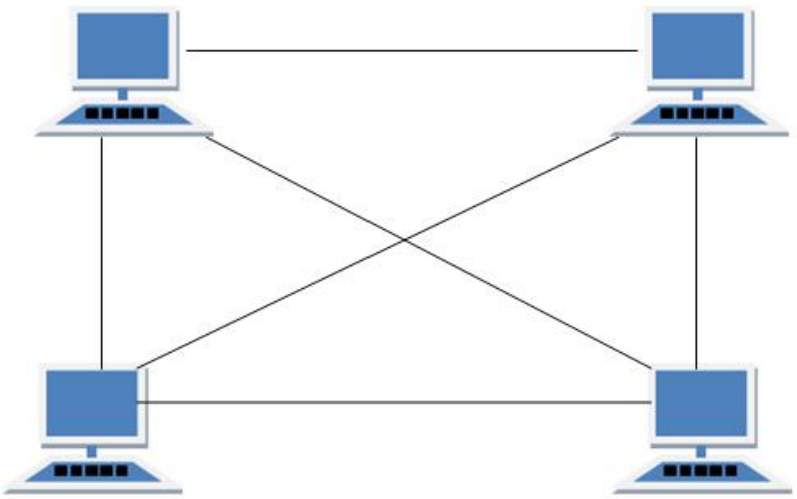
MESH TOPOLOGY

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.
There are two techniques to transmit data over the Mesh topology, they are :

1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.



MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Types of Mesh Topology

1. **Partial Mesh Topology :**In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :**Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.

3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

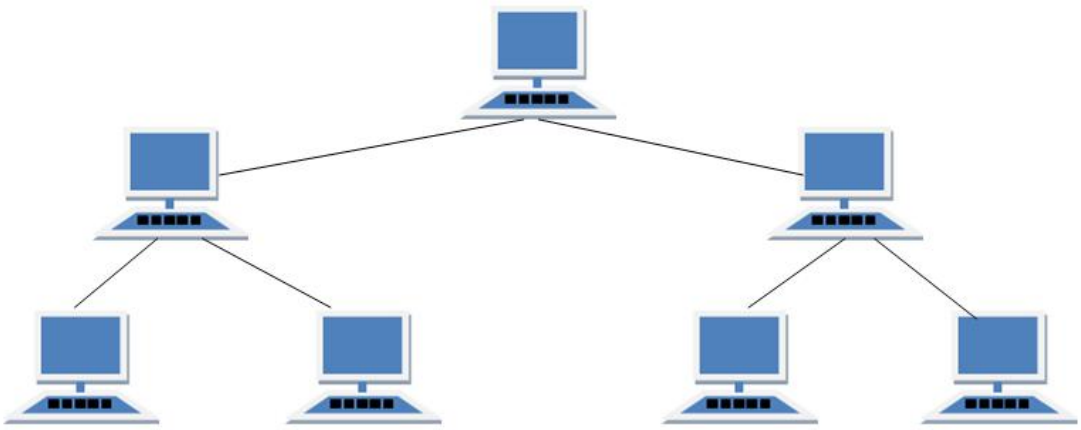
Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Features of Tree Topology



1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

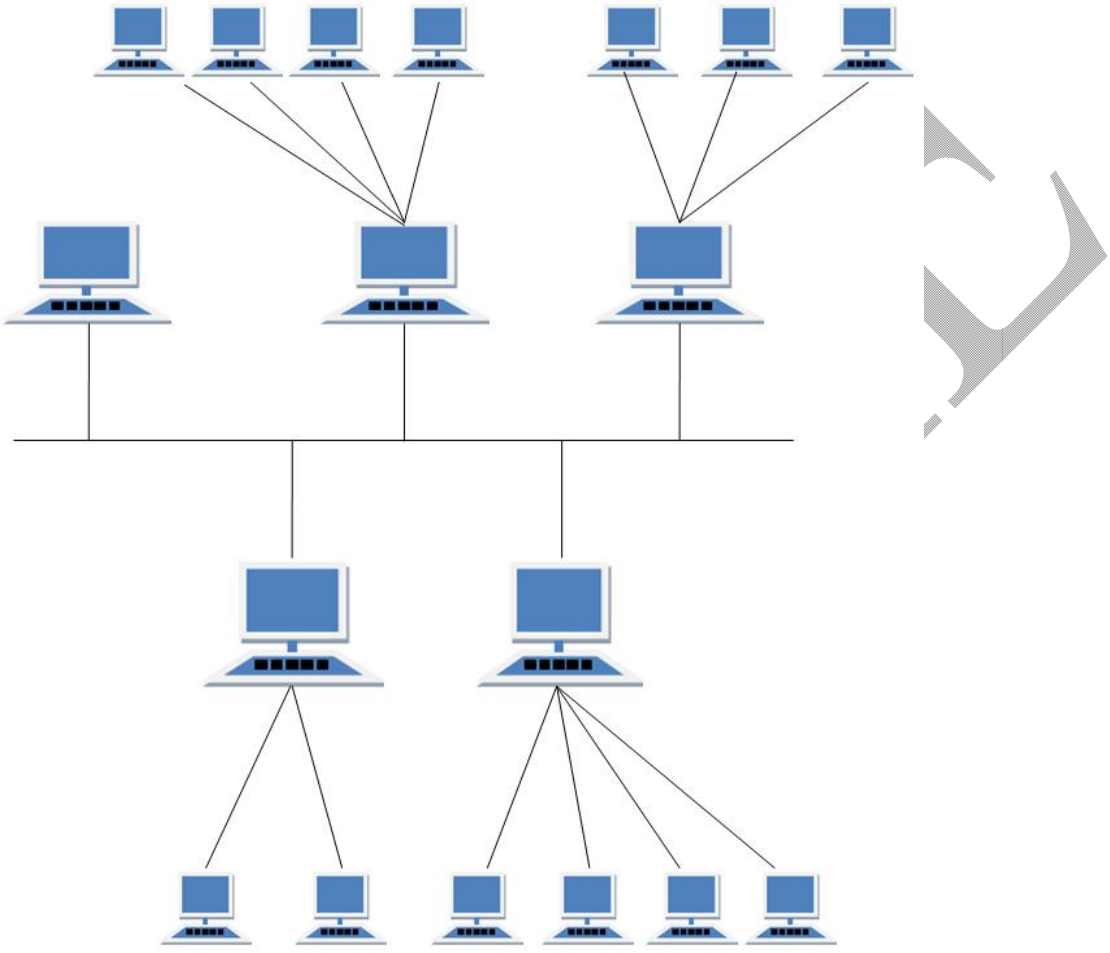
1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included



Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

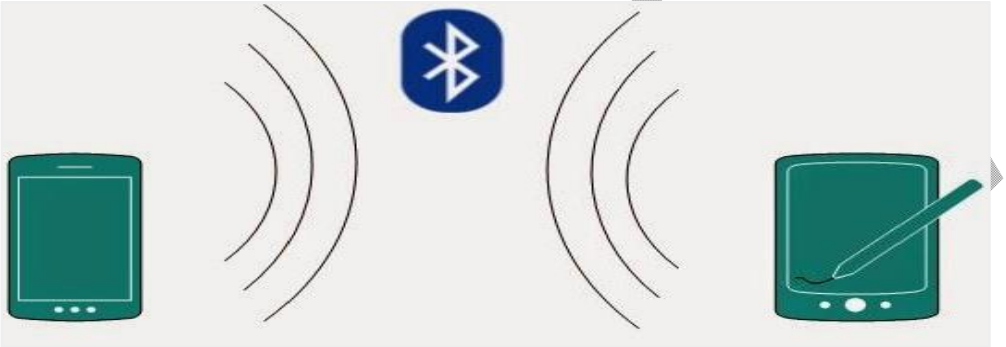
1. Complex in design.
2. Costly.
3.

NETWORK CLASSIFICATIONS

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the Internet itself, covering the whole geographical world, i.e. the Earth.

Personal Area Network

A Personal Area Network or simply PAN, is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes for example.

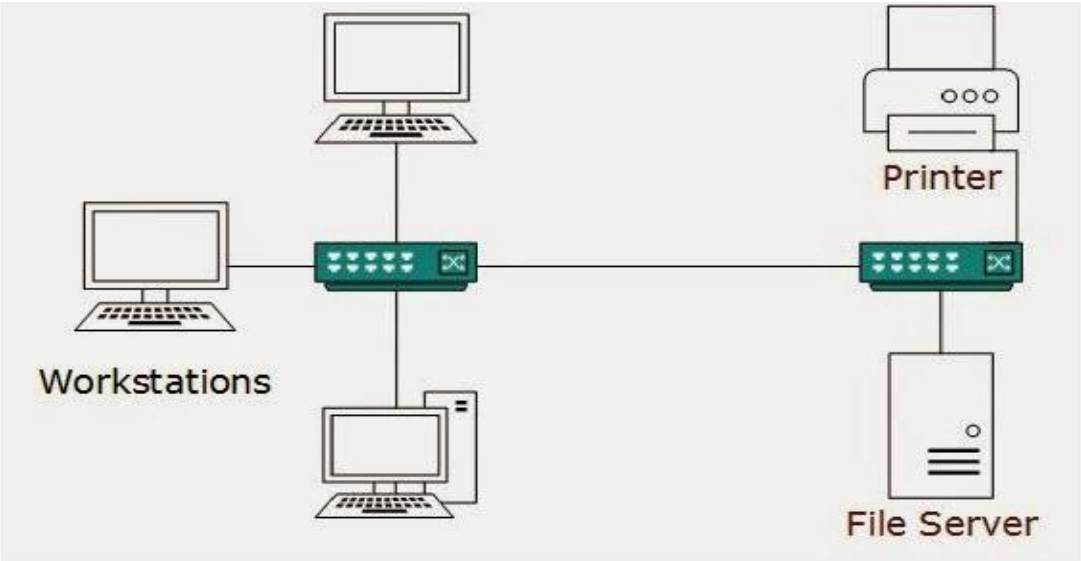


Piconet is an example Bluetooth enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network. Usually, Local Area Network covers an organization's offices, schools, college/universities etc. Number of systems may vary from as least as two to as much as 16 million

LAN provides a useful way of sharing resources between end users. Resources like Printers, File Servers, Scanners and internet is easy sharable among computers.



Local Area Networks are composed of inexpensive networking and routing equipment. It may contains local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and generally do not involve heavy routing. LAN works under its own local domain and controlled centrally.

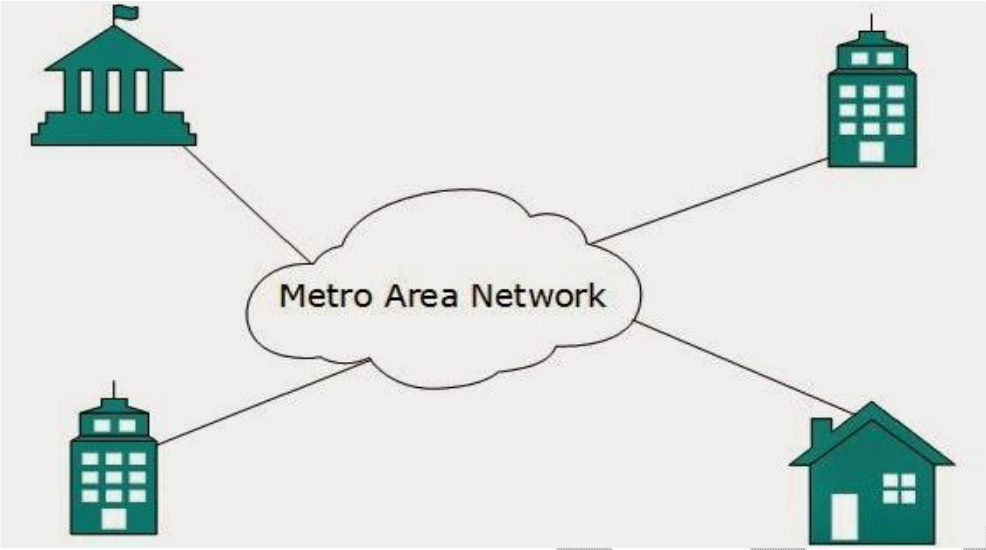
LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology while Token-ring is rarely seen.

LAN can be wired or wireless or in both forms at once.

Metropolitan Area Network

MAN, generally expands throughout a city such as cable TV network. It can be in form of Ethernet, Token-ring, ATM or FDDI.

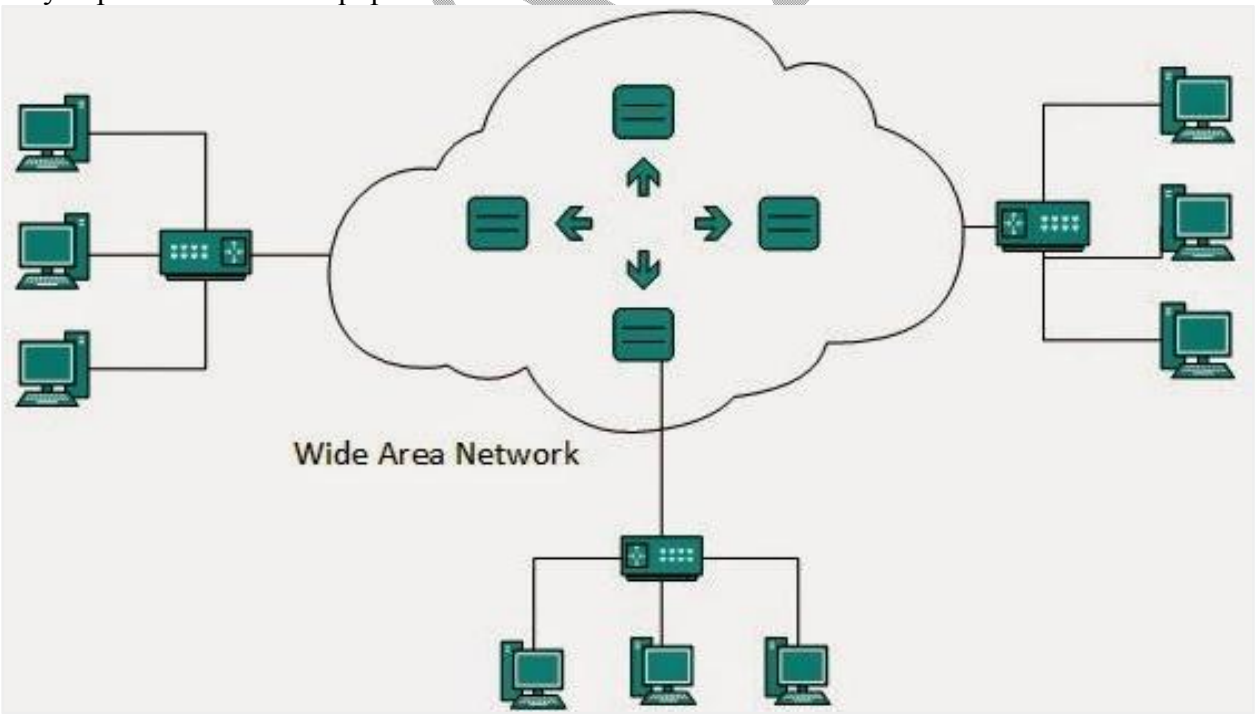
Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a City.



Backbone of MAN is high-capacity and high-speed fiber optics. MAN is works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or Internet.

Wide Area Network

As name suggests, this network covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provides connectivity to MANs and LANs. Equipped with very high speed backbone, WAN uses very expensive network equipment.



WAN may use advanced technologies like Asynchronous Transfer Mode (ATM), Frame Relay and SONET. WAN may be managed under by more than one administration.

Internetwork

A network of networks is called internetwork, or simply Internet. It is the largest network in existence on this planet. Internet hugely connects all WANs and it can have connection to LANs and Home networks. Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses www, ftp, email services, audio and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by some client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very lownetwork protocol; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite.

NETWORK PROTOCOLS

Network protocols are formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network. Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

Network protocols incorporate all the processes, requirements and constraints of initiating and accomplishing communication between computers, servers, routers and other network enabled devices. Network protocols must be confirmed and installed by the sender and receiver to ensure network/data communication and apply to software and hardware nodes that communicate on a network. There are several broad types of networking protocols, including:

Network communication protocols example:

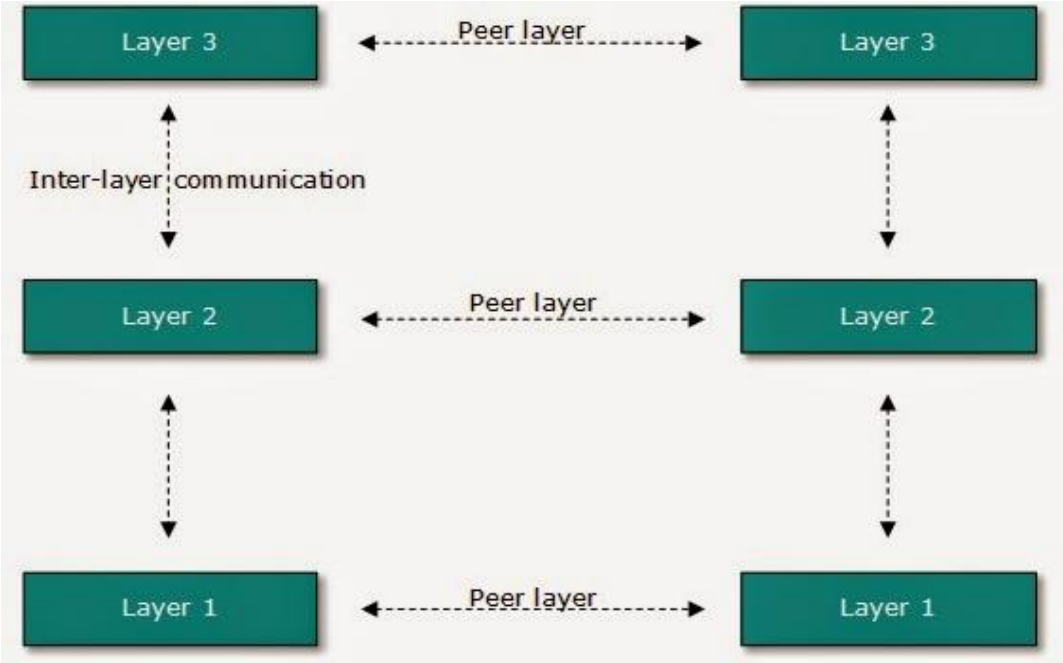
Basic data communication protocols, such as TCP/IP and HTTPNetwork securityprotocols: Implement security over network communications and include HTTPS, SSL and SFTP.

Network management protocols: Provide network governance and maintenance and include SNMP and ICMP.

LAYERED NETWORK ARCHITECTURE

In layered architecture of Network Models, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

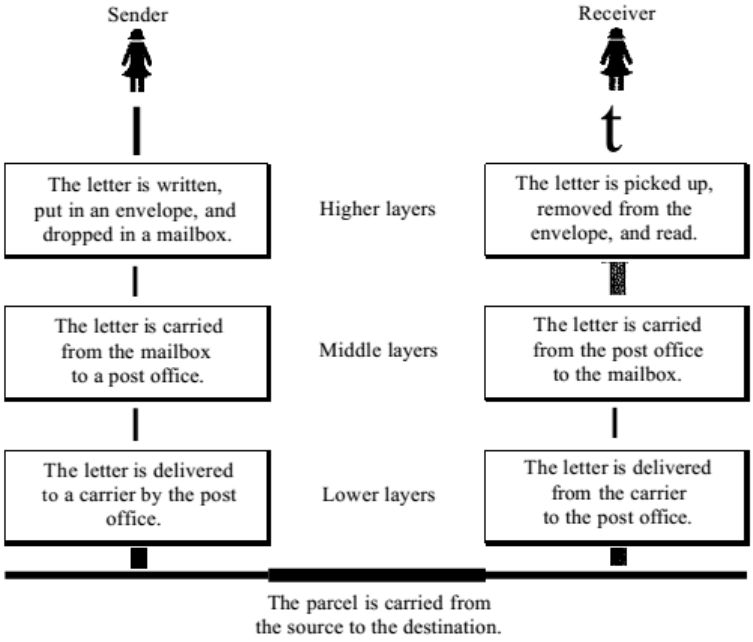
In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by top most layer it is then passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and pass on to lower layer. If the task is initiated by lowest most layer the reverse path is taken.



Every layer clubs together all procedures, protocols, methods which it requires to execute its piece of task. All layers identify their counterparts by means of encapsulation header and tail.

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal maiLThe process of sending a letter to a friend would be complex if there were no services available from the post office. Figure 2.1 shows the steps in this task.

Figure 2.1 *Tasks involved in sending a letter*



Sender, Receiver, and Carrier In Figure 2.1 we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site
Let us first describe, in order, the activities that take place at the sender site.o Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

o Middle layer. The letter is picked up by a letter carrier and delivered to the post office.
o Lower layer. The letter is sorted at the post office; a carrier transports the letter.

On the Way The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

o Lower layer. The carrier transports the letter to the post office.

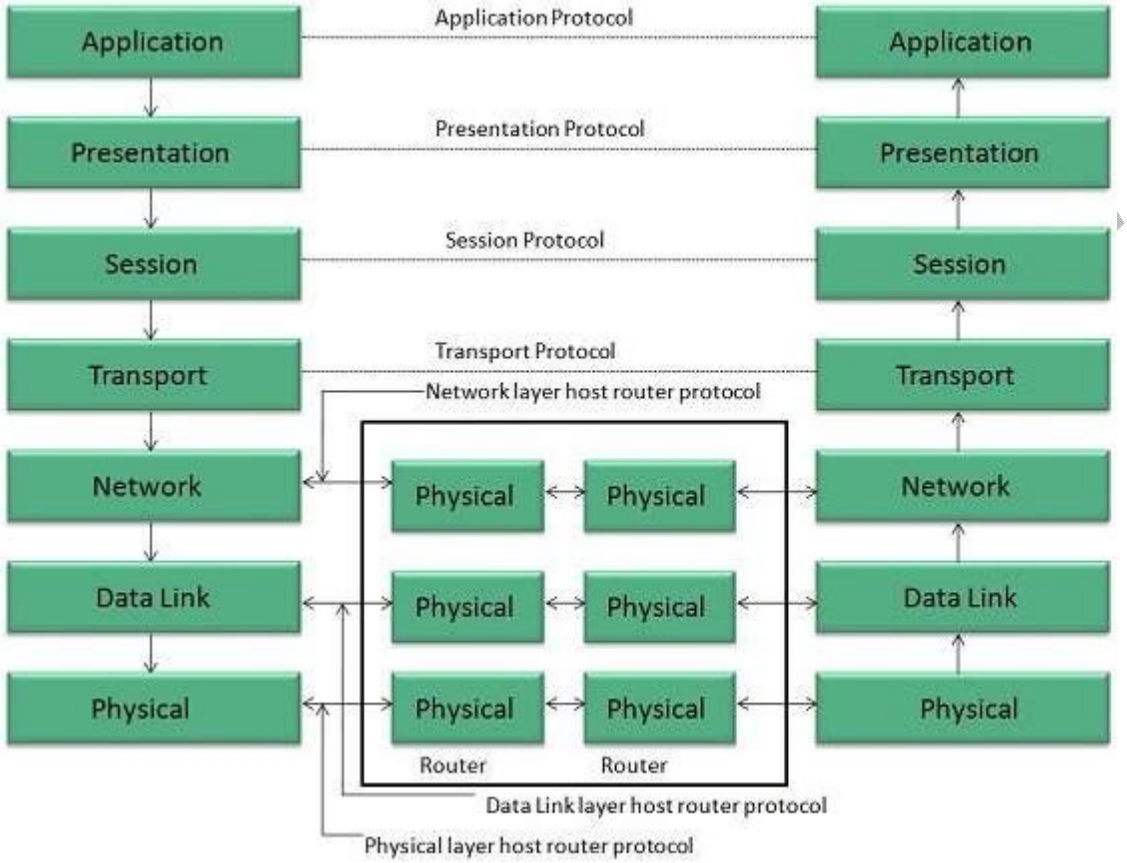
o Middle layer. The letter is sorted and delivered to the recipient's mailbox.

o Higher layer. The receiver picks up the letter, opens the envelope, and reads it.

OVERVIEW OF OSI REFERENCE MODEL

OSI is acronym of **Open System Interface**. This model is developed by the **International organization of Standardization (ISO)** and therefore also referred as **ISO-OSI** Model.

The OSI model consists of seven layers as shown in the following diagram. Each layer has a specific function, however each layer provide services to the layer above.



Physical Layer

The Physical layer is responsible for the following activities:

- Activating, maintaining and deactivating the physical connection.
- Defining voltages and data rates needed for transmission.
- Converting digital bits into electrical signal.
- Deciding whether the connection is simplex, half duplex or full duplex.

Data Link Layer

The data link layer performs the following functions:

- Performs synchronization and error control for the information which is to be transmitted over the physical link.
- Enables error detection, and adds error detection bits to the data which are to be transmitted.

Network Layer

Following are the functions of Network Layer:

- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- To divide the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

Transport Layer

The Transport layer performs the following functions:

- It decides if the data transmission should take place on parallel paths or single path.
- It performs multiplexing, splitting on the data.
- It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

The Transport Layer guarantees transmission of data from one end to other end.

Session Layer

The Session layer performs the following functions:

- Manages the messages and synchronizes conversations between two different applications.
- It controls logging on and off, user identification, billing and session management.

Presentation Layer

The Presentation layer performs the following functions:

- This layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

Application Layer

The Application layer performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.

OSI Model

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers:

- **Application Layer**: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.
- **Presentation Layer**: This layer defines how data in the native format of remote host should be presented in the native format of host.
- **Session Layer**: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
- **Transport Layer**: This layer is responsible for end-to-end delivery between hosts.

- **Network Layer**: This layer is responsible for address assignment and uniquely addressing hosts in a network.
- **Data Link Layer**: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
- **Physical Layer**: This layer defines the hardware, cabling wiring, power output, pulse rate etc.

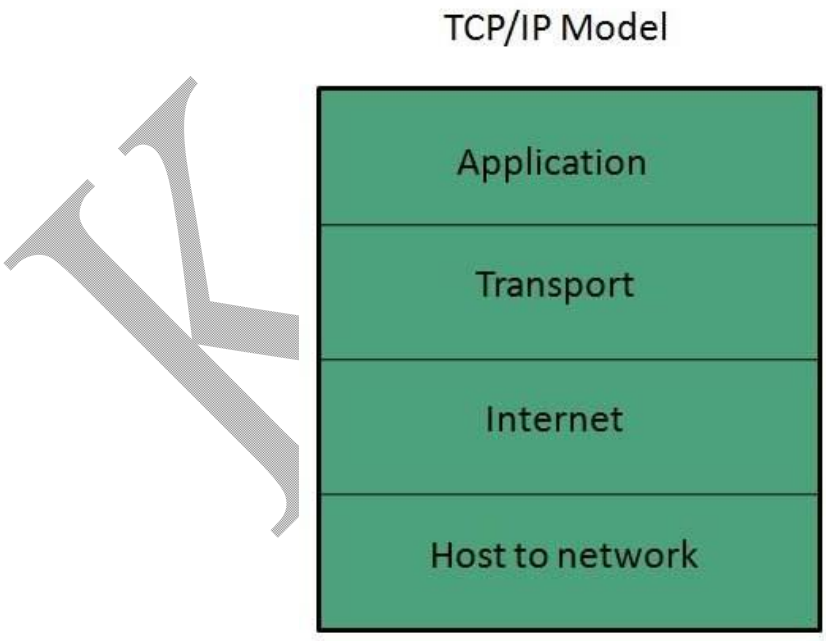
OVERVIEW OF TCP/IP PROTOCOL SUITE

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what Internet uses for all its communication. Internet is independent of its underlying network architecture so is its Model.

TCP/IP Model

TCP/IP model is practical model and is used in the Internet. TCP/IP is acronym of Transmission Control Protocol and Internet Protocol.

The **TCP/IP** model combines the two layers (Physical and Data link layer) into one layer i.e. **Host-to-Network** layer. The following diagram shows the various layers of TCP/IP model:



Application Layer

This layer is same as that of the OSI model and performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.

Protocols used: TELNET, FTP, SMTP, DN, HTTP, NNTP are the protocols employed in this layer.

Transport Layer

It does the same functions as that of transport layer in OSI model. Here are the key points regarding transport layer:

- It uses **TCP** and **UDP** protocol for end to end transmission.
- TCP is reliable and **connection oriented protocol.**
- TCP also handles flow control.
- The UDP is not reliable and a **connection less protocol** also does not perform flow control.

Protocols used: TCP/IP and **UDP** protocols are employed in this layer.

Internet Layer

The function of this layer is to allow the host to insert packets into network and then make them travel independently to the destination. However, the order of receiving the packet can be different from the sequence they were sent.

Protocols used: Internet Protocol (IP) is employed in Internet layer.

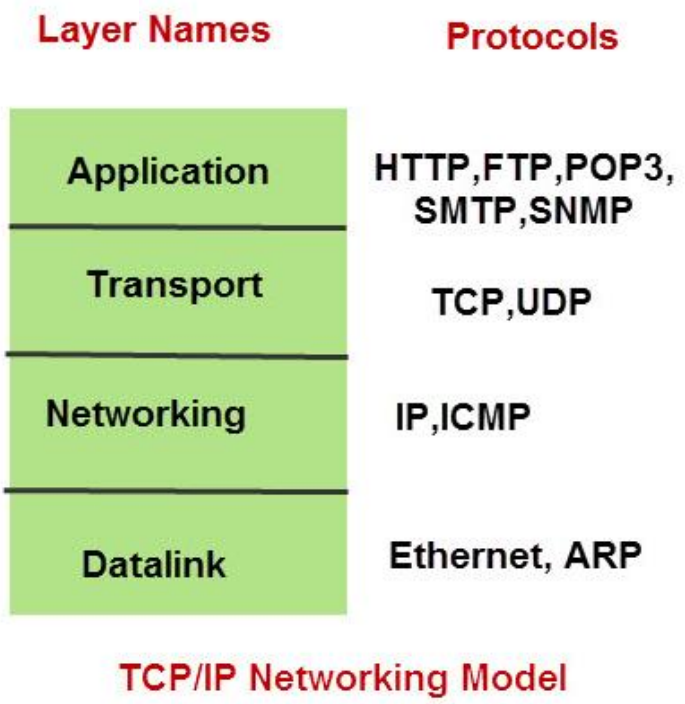
Host-to-Network Layer

This is the lowest layer in TCP/IP model. The host has to connect to network using some protocol, so that it can send IP packets over it. This protocol varies from host to host and network to network.

The TCP/IP Protocol Suite

The TCP/IP protocol suite consists of many protocols that operate at one of 4 layers.

The protocol suite is named after two of the most common protocols – **TCP** (transmission Control Protocol) and **IP** (internet Protocol).



TCP/IP Networking Model

TCP/IP was designed to be independent of networking Hardware and should run across any connection media.

The earliest use, and the most common use is over **Ethernet networks.**

Ethernet is a **2 layer protocol/standard** covering the **physical and data link layer**, shown in the diagram above.

HTTP (hypertext transfer protocol) -This is the workhorse of the Web.

SMTP,POP3,IMap4 – These are email protocols

TCP (Transmission control protocol) is a connection orientated protocol and is used to provides a reliable end to end connection.

UDP (used datagram protocol) is connection less protocol and doesn't guarantee delivery.

Applications will choose which transmission protocol to use based on their function. HTTP, POP3, IMAP4, SMTP and many more use TCP.

UDP is used more in utility applications like DNS, RIP (routing information protocol), DHCP.

IP (Internet Protocol) – This is the main networking protocol. There are two version of IP (IPv4 and IPV6).

ARP (address resolution Protocol) -Translates an IP address to a MAC or physical address.(IP4 networks)

DATA COMMUNICATION FUNDAMENTALS AND TECHNIQUES:

One of the major functions of the physical layer is to move data in the form of electromagnetic signals across a transmission medium.
To be transmitted, data must be transformed to electromagnetic signals.
Analog and digital signal
Both data and the signals that represent them can be either **analog or digital** in form.

ANALOG AND DIGITAL DATA

Data can be analog or digital.
The term **analog data** refers to information that is continuous;
When someone speaks, an analog wave is created in the air. This can be captured by amicrophone and converted to an analog signal or sampled and converted to a digitalsignal.

Digital data refers to information that has discrete states. Analog data, such as the sounds made by a human voice, take on continuous values.

Digital data take on discrete values. For example, data are stored in computermemory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

ANALOG AND DIGITAL SIGNALS

When data is sent over physical medium it needs to be first converted into electromagnetic signals. Data itself canbe analog such as human voice, or digital such as file on the disk. Data (both analog and digital) can berepresented in digital or analog signals.

Digital Signals
Digital signals are discrete in nature and represents sequence of voltage pulses. Digital signals are used withinthe circuitry of a computer system.

An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value *A* to value *B,* it passes through and includes an infinite number of values along its path.

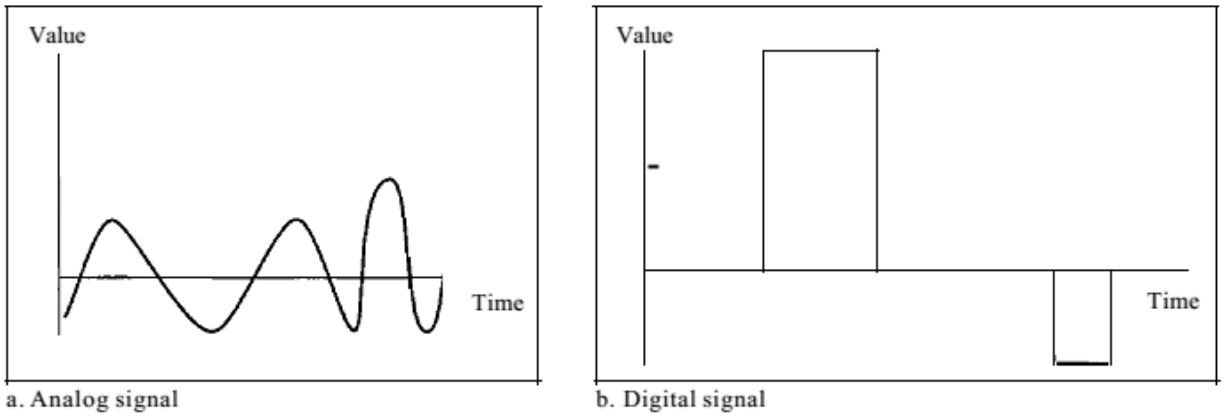
Analog Signals

Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves.

A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.

Analog and Digital Signals:

Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value *A* to value *B,* it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and O. The simplest way to show signals is by plotting them on a pair of perpendicular axes. The vertical axis represents the value or strength of a signal. The horizontal axis represents time. Figure below illustrates an analog signal and a digital signal. The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal, however, demonstrate the sudden jump that the signal makes from value to value.



a. Analog signal b. Digital signal

Comparison of analog and digital signals

Periodic and Nonperiodic Signals:

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

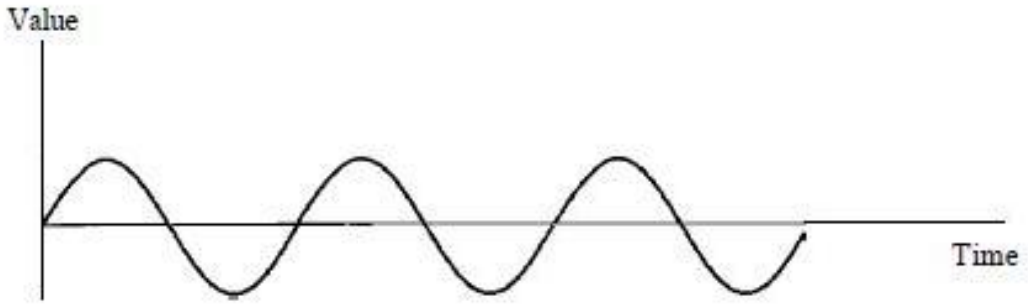
PERIODIC ANALOG SIGNALS:

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

Sine Wave

The sine wave is the most fundamental form of a periodic analog signal. When we visualize it as a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow. Figure below shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.

A sine wave

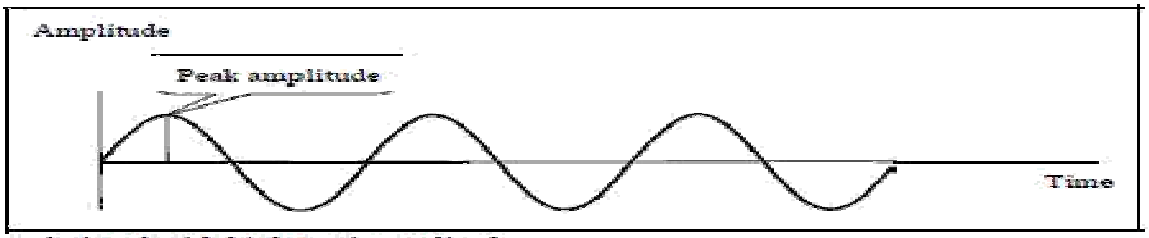


Characteristics of Signals:

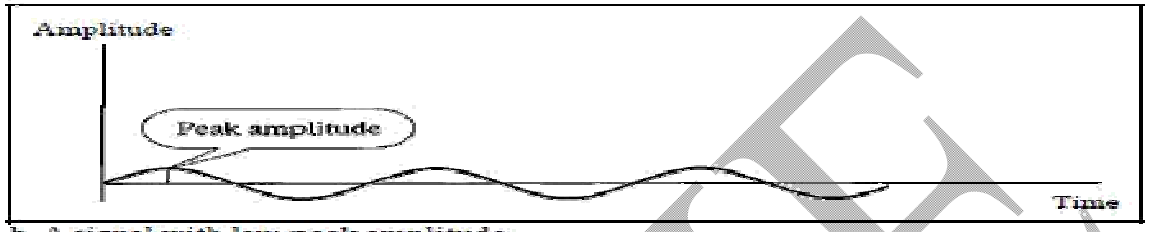
1. ***Peak Amplitude***

The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in *volts*. Figure below shows two signals and their peak amplitudes.

Two signals with the same phase and frequency, but different amplitudes



a. A signal with high peak amplitude



b. A signal with low peak amplitude

2. ***Period and Frequency***

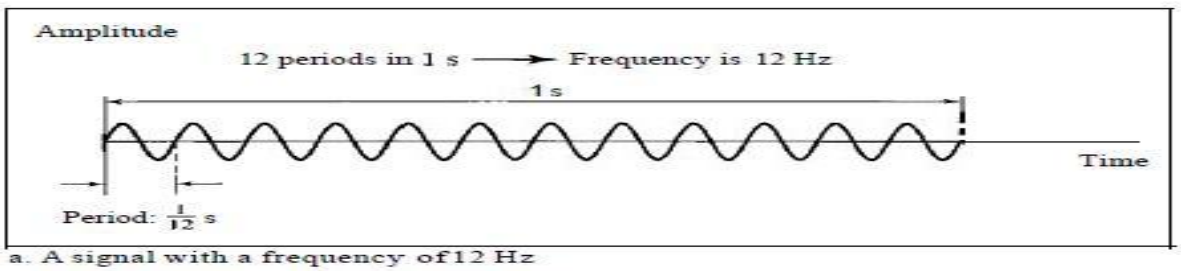
Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.

Frequency refers to the number of periods in I s. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show.

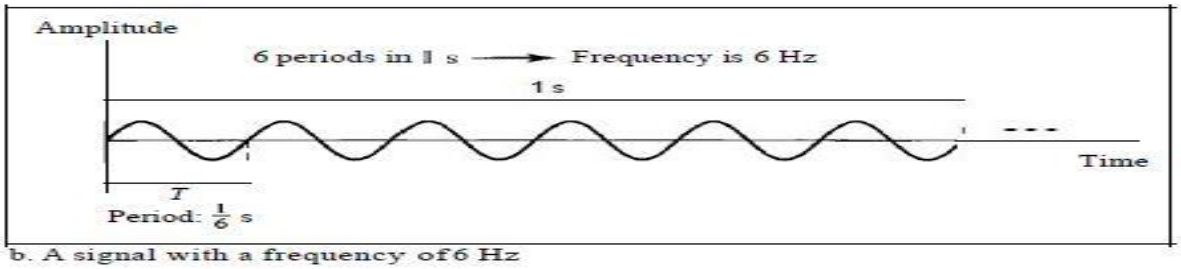
$f=1/T$ and $T=1/f$

Period is formally expressed in seconds. Frequency is formally expressed in Hertz (Hz), which is cycle per second.

Two signals with the same amplitude and phase, but different frequencies



a. A signal with a frequency of 12 Hz

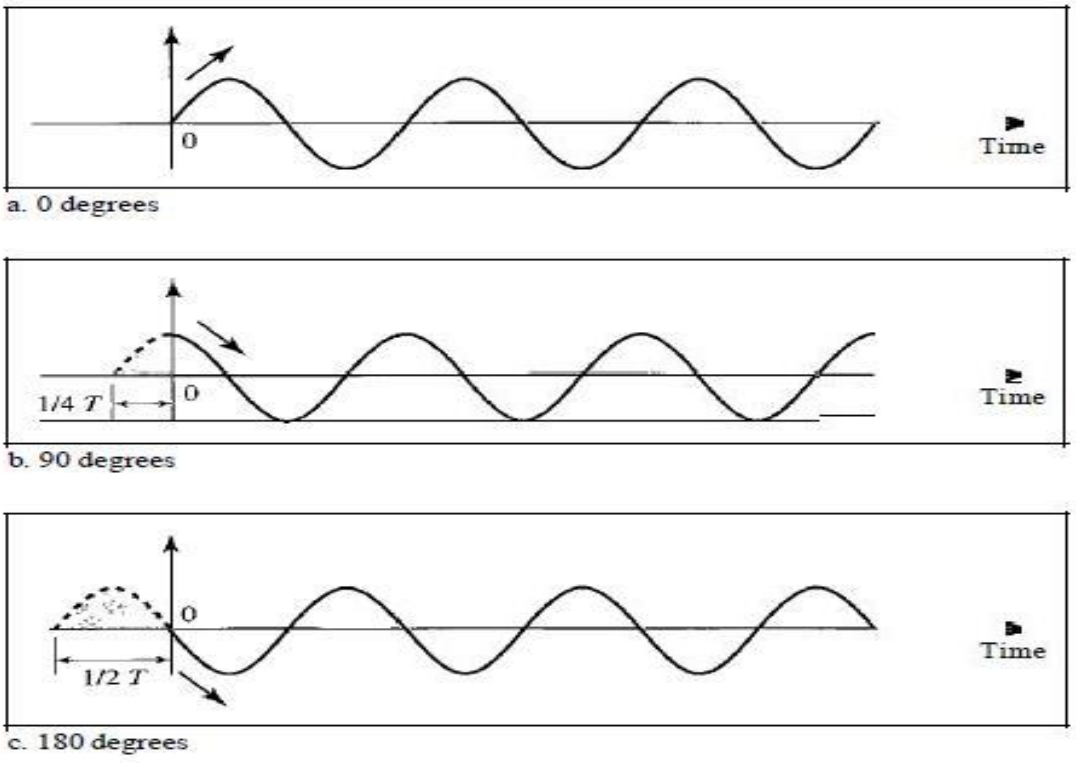


b. A signal with a frequency of 6 Hz

3. ***Phase***

The term phase describes the position of the waveform relative to time O. If we think of the wave as something that can be shifted backward or forward along the time axis, phase describes the amount of that shift. It indicates the status of the first cycle. Phase is measured in degrees or radians [360° is *2n* rad; 1° is *2n/360* rad, and 1 rad is *360/(2n)]*. A phase shift of 360° corresponds to a shift of a complete period; a phase shift of 180° corresponds to a shift of one-half of a period; and a phase shift of 90° corresponds to a shift of one-quarter of a period.

Three sine waves with the same amplitude andfrequency, but different phases



I. A sine wave with a phase of 0° starts at time 0 with a zero amplitude. The amplitude is increasing.
II. A sine wave with a phase of 90° starts at time 0 with a peak amplitude. The amplitude is decreasing.

III. A sine wave with a phase of 180° starts at time 0 with a zero amplitude. The amplitude is decreasing.

4. ***Wavelength***

Wavelength is another characteristic of a signal traveling through a transmission medium. Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium. While the frequency of a signal is independent of the medium, the wavelength depends on both the frequency and the medium. Wavelength is a property of any type of signal. In data communications, we often use wavelength to describe the transmission of light in an optical fiber. The wavelength is the distance a simple signal can travel in one period. Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. However, since period and frequency are related to each other, if we represent wavelength by λ, propagation speed by c (speed of light), and frequency by *f,* we get Wavelength=Propagation speed * Period = propagation speed/frequency

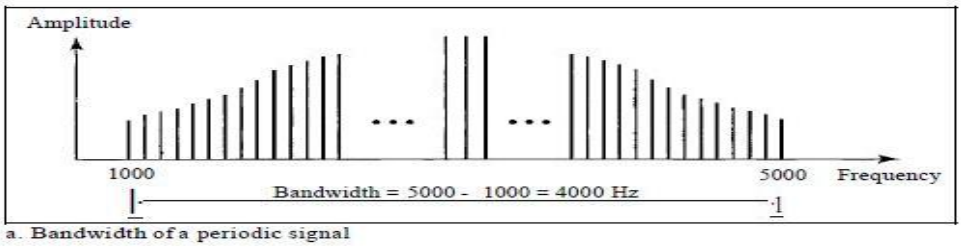
$$\lambda = c/f$$

The wavelength is normally measured in micrometers (microns) instead of meters.

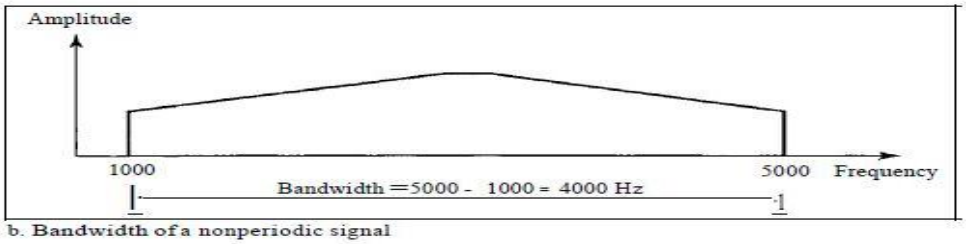
Bandwidth

The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000. Figure 3.12 shows the concept of bandwidth. The figure depicts two composite signals, one periodic and the other nonperiodic. The bandwidth of the periodic signal contains all integer frequencies between 1000 and 5000 (1000, 100 I, 1002, ...). The bandwidth of the nonperiodic signals has the same range, but the frequencies are continuous.

Figure 3.12 *The bandwidth ofperiodic and nonperiodic composite signals*



a. Bandwidth of a periodic signal

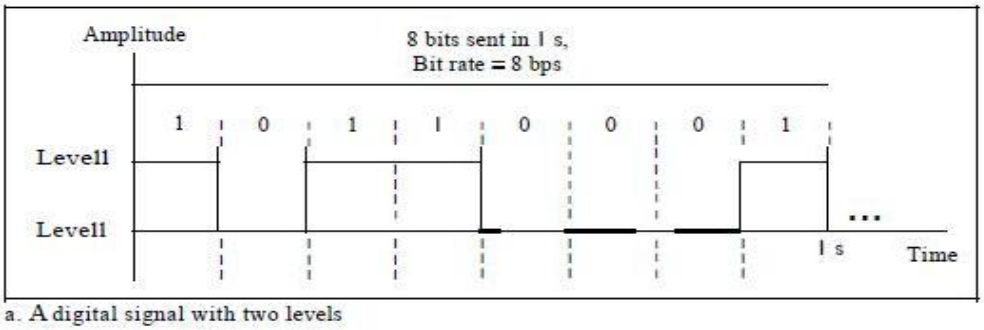


b. Bandwidth of a nonperiodic signal

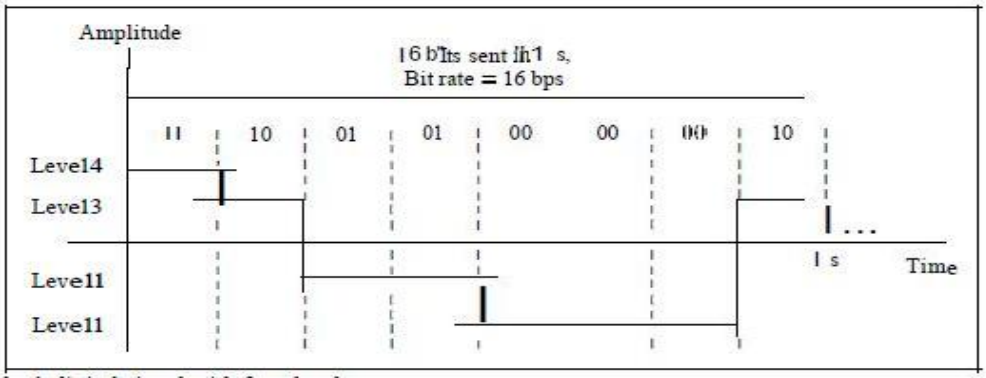
DIGITAL SIGNALS

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level. Figure 3.16 shows two signals, one with two levels and the other with four.

Figure 3.16 *Two digital signals: one with two signal levels and the other with four signal levels*



a. A digital signal with two levels



b. A digital signal with four levels

We send 1 bit per level in part a of the figure and 2 bits per level in part b of the figure. In general, if a signal has *L* levels, each level needs *log2L* bits.

Bit Rate

Most digital signals are nonperiodic, and thus period and frequency are not appropriate characteristics. Another *term-bit rate is* used to describe digital signals. The bit rate is the number of bits sent in 1s, expressed in bits per second (bps). Figure 3.16 shows the bit rate for two signals.

Bit Length

We discussed the concept of the wavelength for an analog signal: the distance one cycle occupies on the transmission medium. We can define something similar for a digital signal: the bit length. The bit length is the distance one bit occupies on the transmission medium.

Bit length =propagation speed x bit duration

DATA RATE LIMITS

A very important consideration in data communications is how fast we can send data, in bits per second. over a channel. Data rate depends on three factors:

1. The bandwidth available

2. The level of the signals we use

3. The quality of the channel (the level of noise)

Two theoretical formulas were developed to calculate the data rate: one by **Nyquist** for a noiseless channel. another by **Shannon** for a noisy channel.

Noiseless Channel: Nyquist Bit Rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

BitRate = 2 x bandwidth x 10g2 *L*

In this formula, bandwidth is the bandwidth of the channel, *L* is the number of signal levels used to represent data, and BitRate is the bit rate in bits per second. According to the formula, we might think that, given a specific bandwidth, we can have any bit rate we want by increasing the number of signa11eve1s. Although the idea is theoretically correct, practically there is a limit. When we increase the number of signal1eve1s, we impose a burden on the receiver. If the number of levels in a signal is just 2, the receiver can easily distinguish between a 0 and a 1. If the level of a signal is 64, the receiver must be very sophisticated to distinguish between 64 different levels. In other words, increasing the levels of a signal reduces the reliability of the system.

Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

Capacity =bandwidth X log2 (1 +SNR)

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal-to-noise ratio, and capacity is the capacity of the channel in bits per second. Note that in the Shannon formula there is no indication of the signal level, which means that no matter how many levels we have, we cannot achieve a data rate higher than the capacity of the channel. In other words, the formula defines a characteristic of the channel, not the method of transmission.

Bandwidth in Bits per Seconds

The term *bandwidth* can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

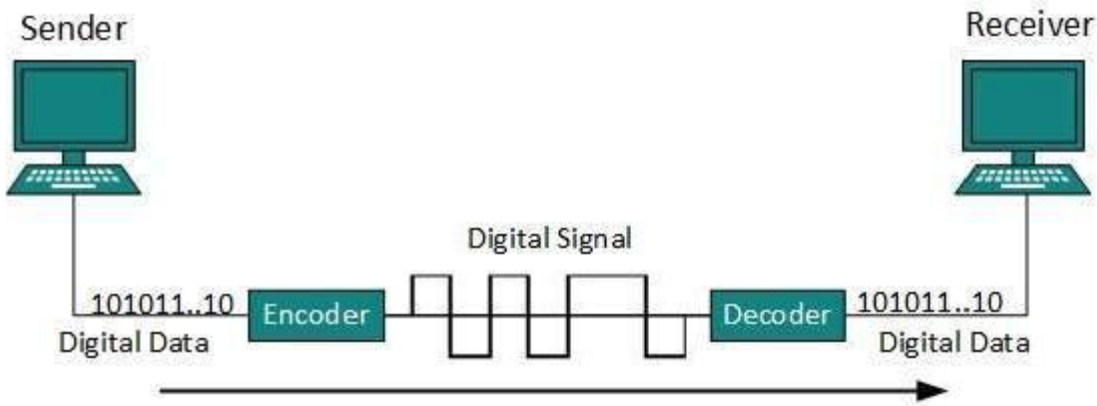
DIGITAL TO DIGITAL LINE ENCODING SCHEMES

Data or information can be stored in two ways, analog and digital. For a computer to use that data is must

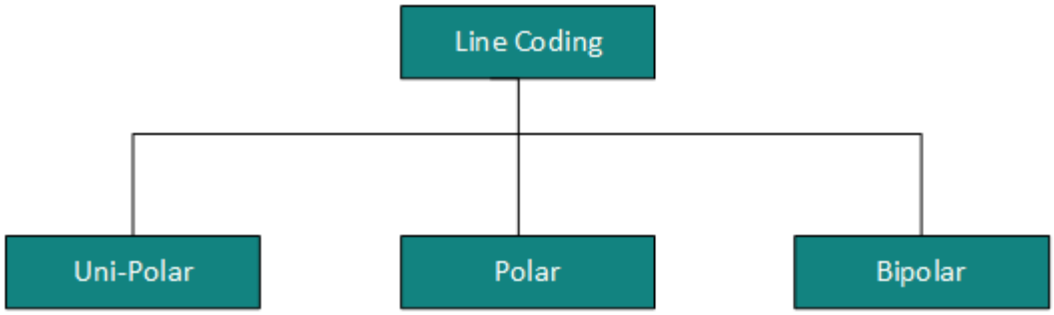
be in discrete digital form. Like data, signals can also be in analog and digital form. To transmit data digitally it needs to be first converted to digital form.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format.It is represented (stored) internally as series of 1s and 0s.

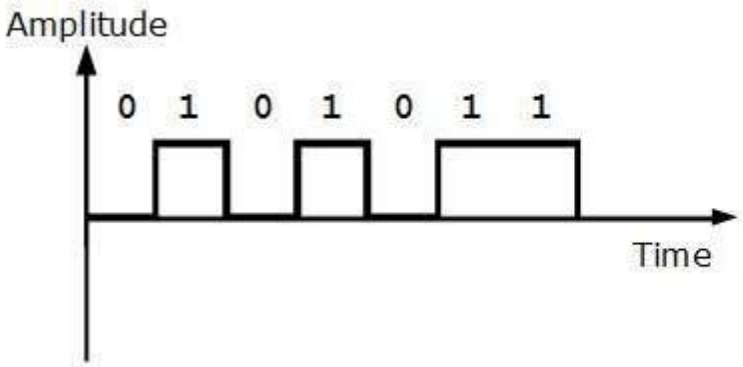


Digital signal is denoted by discreet signal, which represents digital data.There are three types of line coding schemes available:



Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.

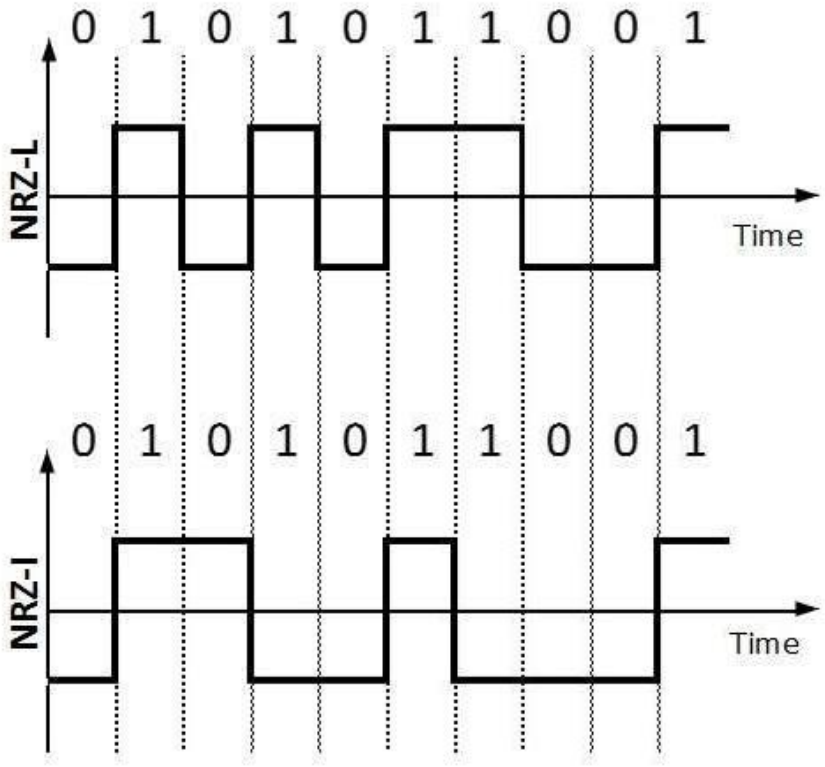


Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- **Polar Non-Return to Zero (Polar NRZ)**

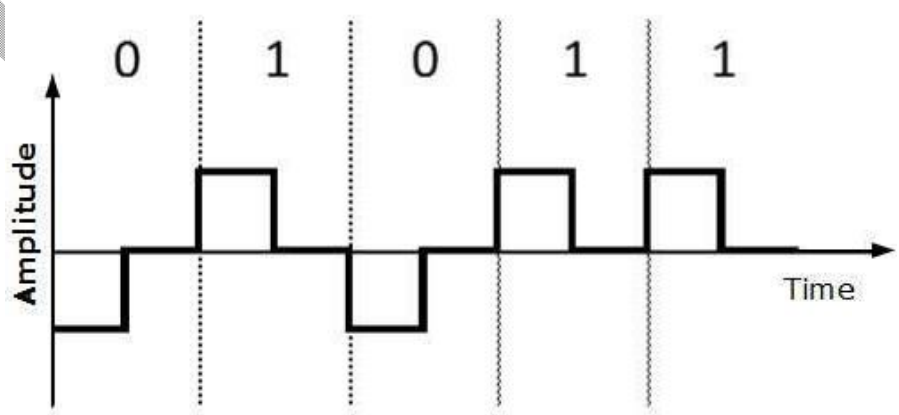
It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.
NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

- **Return to Zero (RZ)**

Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

- **Manchester**

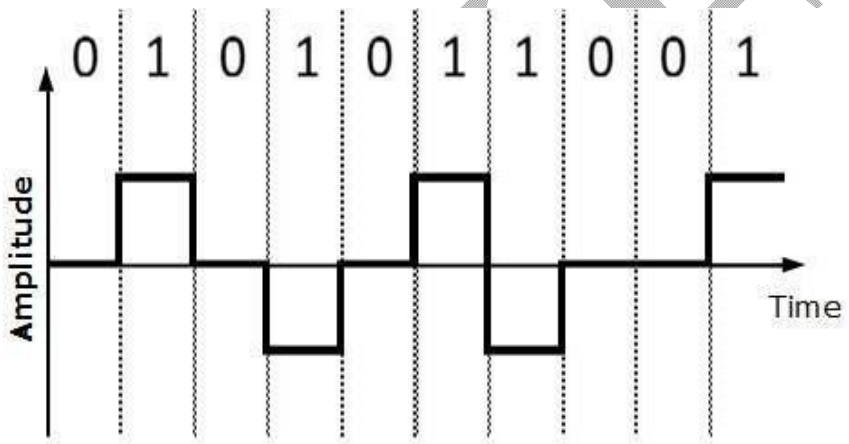
This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

- **Differential Manchester**

This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding

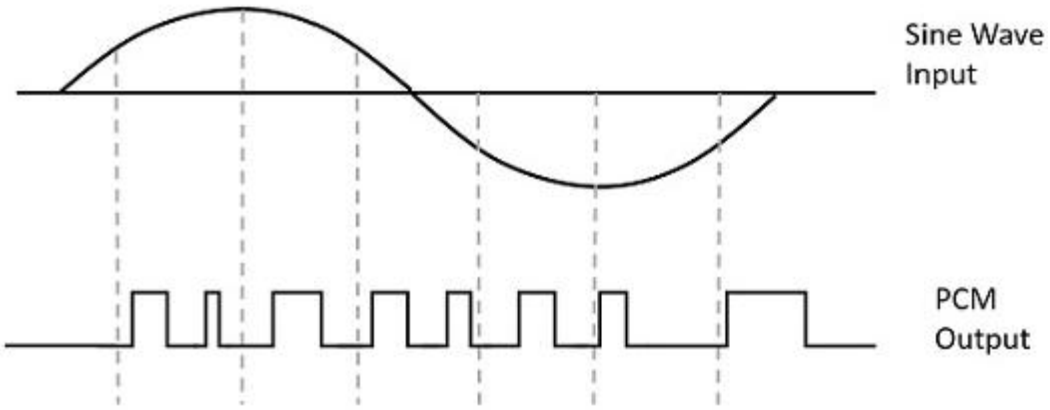
To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.

PULSE CODE MODULATION

Modulation is the process of varying one or more parameters of a carrier signal in accordance with the instantaneous values of the message signal.

The message signal is the signal which is being transmitted for communication and the carrier signal is a high frequency signal which has no data, but is used for long distance transmission.
There are many modulation techniques, which are classified according to the type of modulation employed. Of them all, the digital modulation technique used is **Pulse Code Modulation (PCM)**.

A signal is pulse code modulated to convert its analog information into a binary sequence, i.e., **1s** and **0s**. The output of a PCM will resemble a binary sequence. The following figure shows an example of PCM output with respect to instantaneous values of a given sine wave.



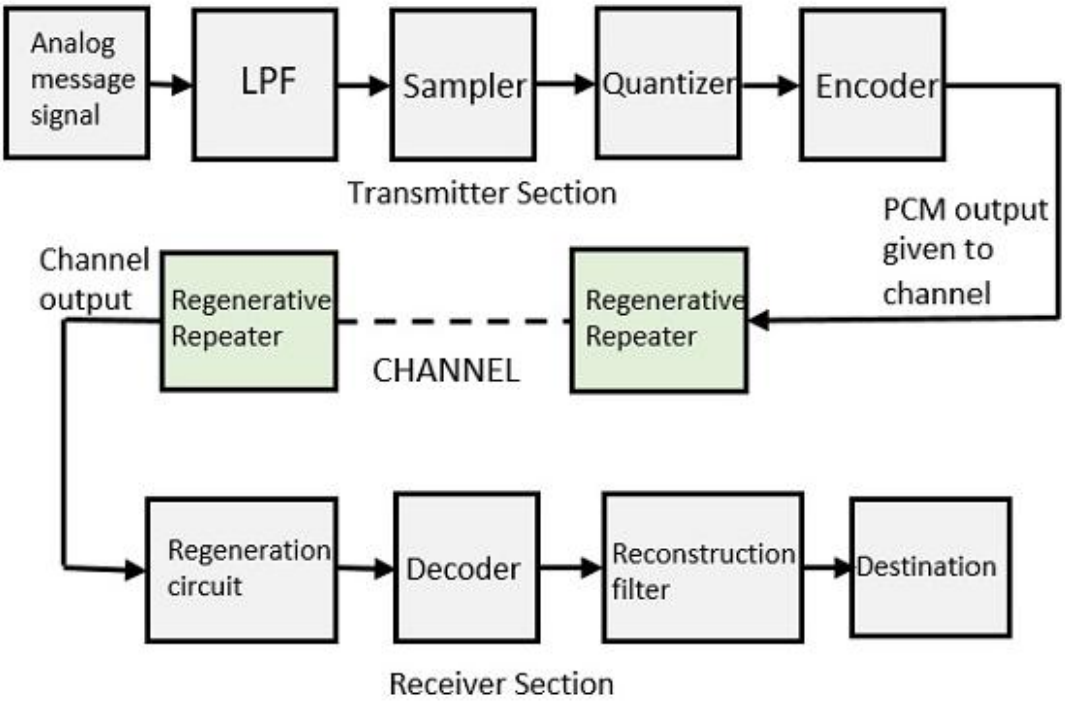
Instead of a pulse train, PCM produces a series of numbers or digits, and hence this process is called as **digital**. Each one of these digits, though in binary code, represent the approximate amplitude of the signal sample at that instant.

In Pulse Code Modulation, the message signal is represented by a sequence of coded pulses. This message signal is achieved by representing the signal in discrete form in both time and amplitude.

Basic Elements of PCM

The transmitter section of a Pulse Code Modulator circuit consists of **Sampling, Quantizing** and **Encoding**, which are performed in the analog-to-digital converter section. The low pass filter prior to sampling prevents aliasing of the message signal.

The basic operations in the receiver section are **regeneration of impaired signals, decoding,** and **reconstruction** of the quantized pulse train. Following is the block diagram of PCM which represents the basic elements of both the transmitter and the receiver sections.



Low Pass Filter

This filter eliminates the high frequency components present in the input analog signal which is greater than the highest frequency of the message signal, to avoid aliasing of the message signal.

Sampler

This is the technique which helps to collect the sample data at instantaneous values of message signal, so as to reconstruct the original signal. The sampling rate must be greater than twice the highest frequency component **W**of the message signal, in accordance with the sampling theorem.

Quantizer

Quantizing is a process of reducing the excessive bits and confining the data. The sampled output when given to Quantizer, reduces the redundant bits and compresses the value.

Encoder

The digitization of analog signal is done by the encoder. It designates each quantized level by a binary code. The sampling done here is the sample-and-hold process. These three sections (LPF, Sampler, and Quantizer) will act as an analog to digital converter. Encoding minimizes the bandwidth used.

Regenerative Repeater

This section increases the signal strength. The output of the channel also has one regenerative repeater circuit, to compensate the signal loss and reconstruct the signal, and also to increase its strength.

Decoder

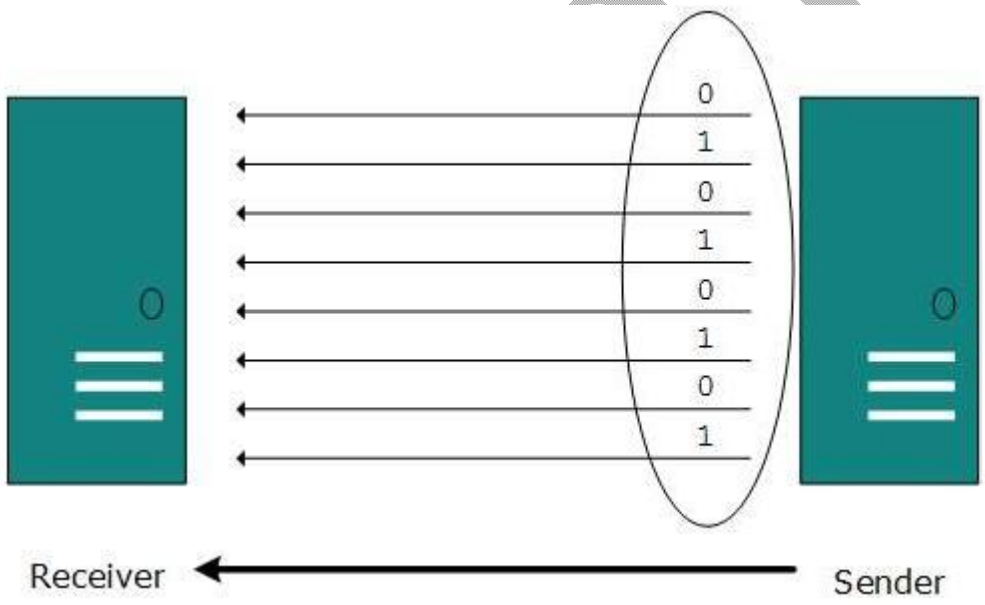
The decoder circuit decodes the pulse coded waveform to reproduce the original signal. This circuit acts as the demodulator.

Reconstruction Filter
After the digital-to-analog conversion is done by the regenerative circuit and the decoder, a low-pass filter is employed, called as the reconstruction filter to get back the original signal.

Hence, the Pulse Code Modulator circuit digitizes the given analog signal, codes it and samples it, and then transmits it in an analog form. This whole process is repeated in a reverse pattern to obtain the original signal.

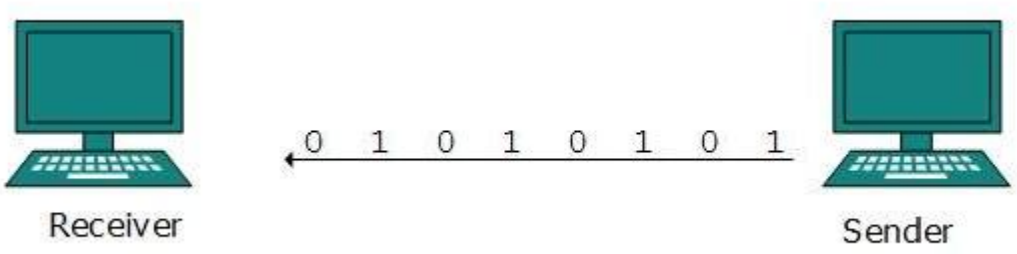
PARALLEL AND SERIAL TRANSMISSION

Transmission Modes
The transmission mode decides how data is transmitted between two computers.The binary data in the form of 1s and 0s can be sent in two different modes: Parallel and Serial.
Parallel Transmission



The binary bits are organized in-to groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines.Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go. Advantage of Parallel transmission is high speed and disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.

Serial Transmission
In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel.



Serial transmission can be either asynchronous or synchronous.

Asynchronous Serial Transmission
It is named so because there is no importance of timing. Data-bits have specific pattern and they help receiver recognize the start and end data bits. For example, a 0 is prefixed on every data byte and one or more 1s are added at the end.

Two continuous data-frames (bytes) may have a gap between them.

Synchronous Serial Transmission
Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits. There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes. Therefore, timing becomes very important.

It is up to the receiver to recognize and separate bits into bytes. The advantage of synchronous transmission is high speed, and it has no overhead of extra header and footer bits as in asynchronous transmission.

POSSIBLE QUESTIONS

UNIT-I

PART-A (20 MARKS)

(Q.NO 1 TO 20 Online Examination)

PART-B (2 MARKS)

1. Define Network and Internet.
2. What are the elements of data communication?
3. Define data communication.
4. What is protocol?
5. Define Simplex and Duplex Communication.
6. List out the network topologies.
7. What is UDP and SMTP?
8. Define analog and digital signal.
9. What is Modulation?
10. Mention the basic elements of PCM.
11. Define parallel and serial transmission.

PART-C (6 MARKS)

1. Explain about the network topologies with neat diagram.
2. Give a detailed description about the Network Classifications
3. Draw a neat sketch of OSI Reference Model and explain in detail.
4. Describe about TCP/IP protocol suite with neat diagram.
5. Explain Date Rate limits.
6. Discuss about Digital to Digital Line Encoding Schemes with neat sketch.
7. Explain in detail on Analog to digital conversion with neat sketch.
8. Illustrate PCM with neat diagram.
9. Explain about Parallel and Serial Transmission.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CS Batch:2017

Subject: COMPUTER NETWORKS

SubCode: 17CSU303

UNIT I

S.NO	QUESTION	CHOICE1	CHOICE2	CHOICE3	CHOICE4	ANSWER
1	Data communication means exchange of data between devices.	one	two	six	four	two
2	The combination of two or more networks are called	Internetwork	LAN	WAN	MAN	Internetwork
3	A_____ is the set of rules.	protocols	transmission medium	networks	ip	protocols
4	In_____, the communication is unidirection.	duplex mode	full duplex mode	half duplex mode	simplex mode	simplex mode
5	A_____is a set of devices connected by communication links.	protocols	networks	computer	printer	networks
6	A_____connection provides a dedicated link between two devices.	point-to-point	multi-point	mesh	physical	point-to-point
7	One long cable acts as a _____to link all the devices in a network.	bus	mesh	hub	backbone	backbone
8	MAN stands for _____	metropolitician area network	metropolitan area network	metropolitical area network	macro area network	metropolitan area network
9	A _____ can be a device which is capable of sending or receiving data	node	data	bit	link	node
10	The multipoint topology is _____	Bus	Star	Mesh	Ring	Bus
11	In physical layer we can transfer data into	frame	packet	bit	sp du	bit
12	A communication path way that transfers data from one point to another is called	Link	Node	Medium	Topology	Link

13	The _____layer is responsible for process to process delivery.	physical	presentation	networks	transport	transport
14	The _____layer is responsible for dialog control and synchronization.	transport	session	application	presentation	session
15	Tcp/Ip is a _____protocol.	hyper text	transfer	internet	hierarchical	internet
16	Ip is a_____protocol.	hop to hop	node to node	process to process	host to host	host to host
17	A set of devices connected by a _____links	data	networks	communicatio n	application	communication
18	In _____ topology every device is connected to a single cable	Bus	Star	Ring	Mesh	Bus
19	Periodic analog signals can be classified into	simple	composite	simple or composite	simple and composite	simple or composite
20	Period and frequency has the following formula.	f=1/t and t=1/f	t=1/f or f=1/t	c=t/f	t=c/f	f=1/t and t=1/f
21	Wavelength is_____	propagation speed	propagation speed *	propagation speed/period	propagation speed/frequency	propagation speed/frequenc
22	ISP stands for _____	Internet Service Provider	Internet System Provider	International Service	International System Program	Internet Service Provider
23	The range of frequency contained in a _____ signal is its bandwidth.	simple	composite	periodic	non periodic	composite
24	The bandwidth of the composite signal is the difference between the	highest	highest or lowest	highest and lowest	lowest	highest and lowest
25	The _____is the number of bits sent in a second.	bit length	bandpass	bandwidth	bit rate	bit rate
26	Bit length is _____	propagation speed/period	propagation speed *	bit	propagation speed*bit	propagation speed*bit
27	A_____signal is a composite analog signal with an infinite bandwidth	simple	composite	digital	analog	digital
28	Bus topology is also called as_____	Linear Bus Topology	Hybrid Bus Topology	Dual Ring topology	Non Linear Bus Topology	Linear Bus Topology
29	Transmission time=_____	message size/birate	distance/bandw idth	message size/distance	message size/bandwidth	message size/bandwidth

30	_____and star is a point to point device.	bus	ring	mesh	physical	mesh
31	_____ **and** _____ is an example of simplex communication	Keyboard and Monitor	Printer and fax	Mobile and Tab	Bus and ring	Keyboard and Monitor
32	_____is a basic key element.	protocols	standards	topology	protocols and standards	protocols and standards
33	Bit rate=_____	4*BW*log2L	2*BW*log2L	4*BW/L	2*BW*log 4L	2*BW*log2L
34	OSI stands for_____	open systems interconnection	open system internetworkin	open symantic interconnectio	open system internet	open systems interconnection
35	Net work layer delivers data in the form of_____	frame	bits	data	packet	packet
36	Session layer provides_____ services.	one	two	three	four	two
37	UDP stands for _____	user data protocol	user datagram protocol	user defined protocol	user dataframe protocol	user datagram protocol
38	FTP stands for _____	file transmit protocol	file transmission	file transfer protocol	flip transfer protocol	file transfer protocol
39	SMTP stands for _____	single mail transfer protocol	simple mail transfer	simple mail transmission	single mail transmit	simple mail transfer
40	Complete a cycle is called as _____	period	frequency	non periodic	periodic	period
41	_____ generally expands throughout a city such as cable TV network	LAN	WAN	MAN	PAN	MAN
42	_____is reliable and **connection oriented protocol.**	TCP	UDP	FTP	SMTP	TCP
43	Full duplex also called as_____	simple duplex	single duplex	multiple duplex	duplex	duplex
44	_____can be measured in transmit time and response time.	performance	frequency	period	non period	performance
45	A multipoint is also called as_____	multi line	multi drop	multi level	single level	multi drop
46	Mesh has _____ physical channels to link n devices	n(n-1)	n(n+1)	n(n+1)/2	n(n-1)/2	n(n-1)/2

47	A_____topology on the other hand is multipoint.	star	ring	bus	mesh	bus
48	Combination of two or more network topology is called	Mesh	Star	Ring	Hybrid	Hybrid
49	A MAN is a network with a size between a and .	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
50	_____ refers to information that has discrete states.	Digital data	Analog data	bits	bytes	Digital data
51	The_____layer is responsible for providing services to the user.	presentation	datalink	application	network	application
52	The _____ layer is responsible for translation, compression encryption.	transport	data link	presentation	application	presentation
53	The_____layer is responsible for the delivery of a message from one process to another.	data link	transport	presentation	network	transport
54	A _____layer is responsible for the delivery of packets from the source to destination.	physical	data link	network	session	network
55	The _____layer is responsible for moving frames from one hop to the next.	data link	physical	network	presentation	data link
56	The _____layer is responsible for movements of bits from one hop to next.	data link	physical	transport	session	physical
57	RARP stands for _____	reverse address resolution	reverse address result protocol	reverse addess revolutinized	reverse addess research	reverse address resolution
58	In multicast communication, the relationship is	One to one	One to many	Many to one	many to many	One to many
59	The TCP/IP protocol suite was developed prior to the model.	OSI	ISO	TCP	IP	OSI
60	The _____layer is responsible for flow control.	session	presentation	application	transport	transport
61	The term _____ data refers to information continous	analog	digital	physical	analog and digital	analog
62	The sine wave is the most fundamental form of a analog signal.	composite	single	periodic	non periodic	periodic

UNIT – II

SYLLABUS

(cont..)digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media.

Networks Switching Techniques and Access mechanisms: Circuit switching; packet switching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

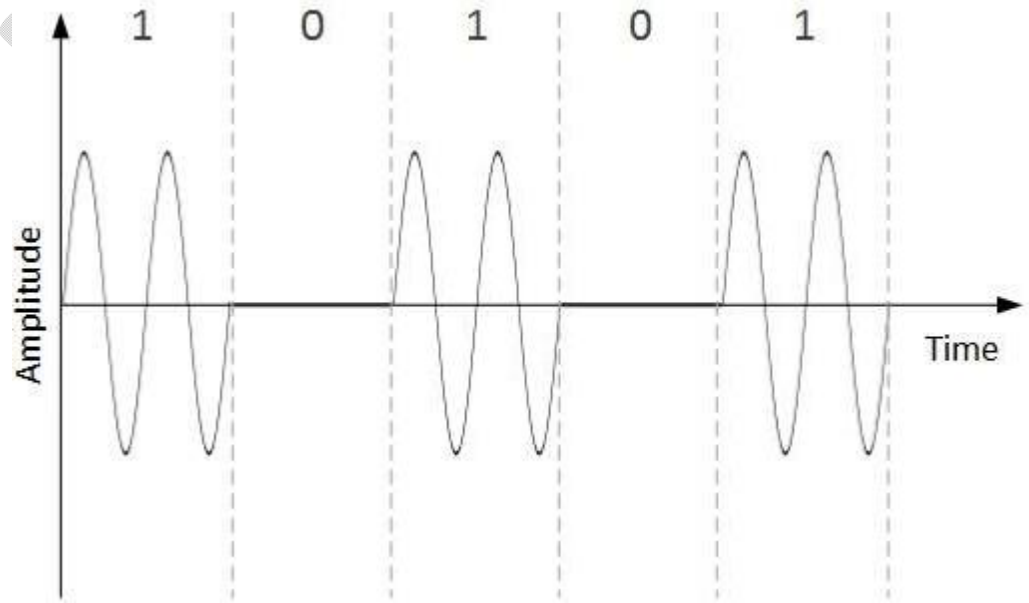
DIGITAL-TO-ANALOG CONVERSION

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

- **Amplitude Shift Keying**

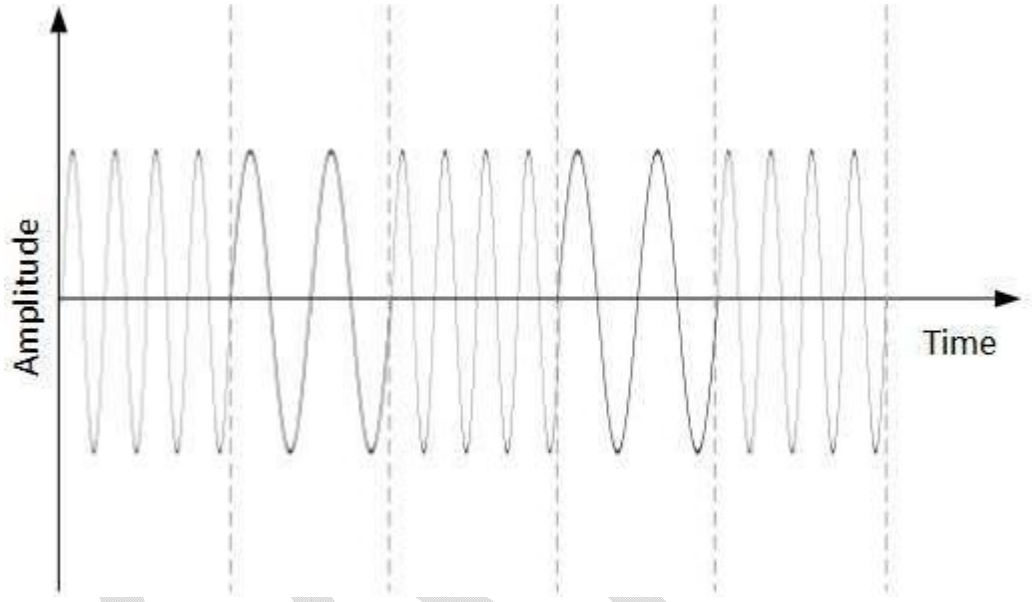
In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

- **Frequency Shift Keying**

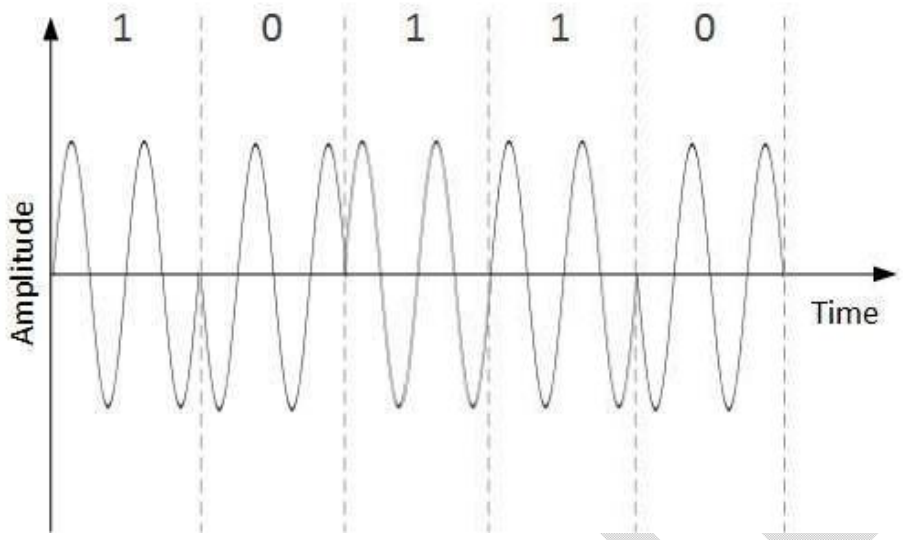
In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

- **Phase Shift Keying**

In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

- **Quadrature Phase Shift Keying**

QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique.

MULTIPLEXING

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

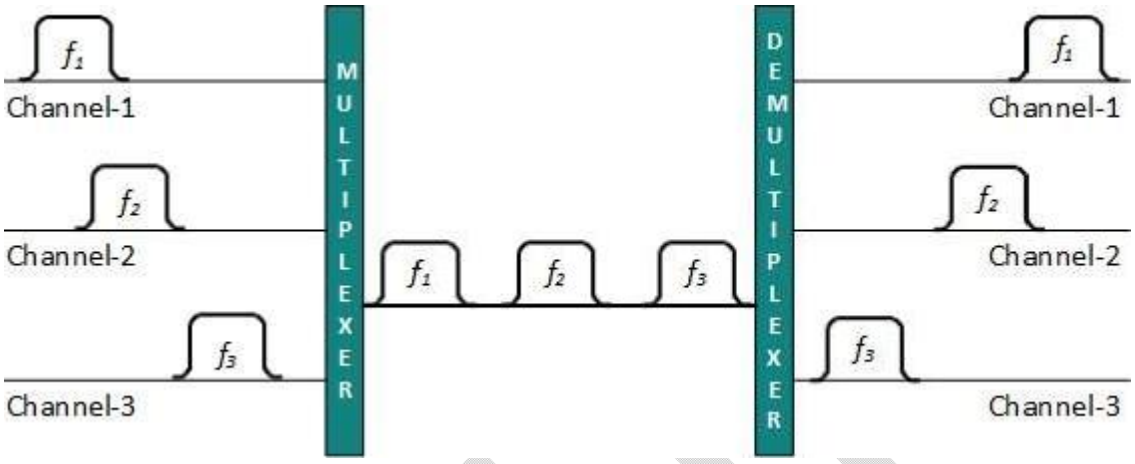
Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

FREQUENCY DIVISION MULTIPLEXING

When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each

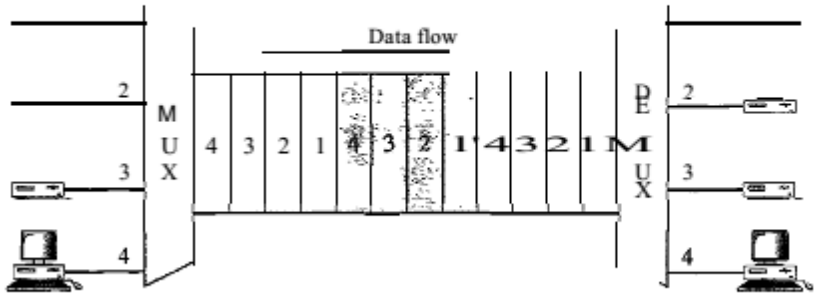
user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



TIME DIVISION MULTIPLEXING

Time-division multiplexing (TDM) is a digital process that allows several connectionsto share the high bandwidth of a linle Instead of sharing a portion of the bandwidth as inFDM, time is shared. Each connection occupies a portion of time in the link. Figure 6.12gives a conceptual view of TDM. Note that the same link is used as in FDM; here, however, the link is shown sectioned by time rather than by frequency. In the figure, portionsof signals 1,2,3, and 4 occupy the link sequentially.

Figure 6.12 *TDM*



Note that in Figure 6.12 we are concerned with only multiplexing, not switching.This means that all the data in a message from source 1 always go to one specific destination, be it 1, 2, 3, or 4. The delivery is fixed and unvarying, unlike switching.

We also need to remember that TDM is, in principle, a digital multiplexing technique.Digital data from different sources are combined into one timeshared link. However, thisdoes not mean that the sources cannot produce analog data; analog data can be sampled,changed to digital data, and then multiplexed by using TDM.

TDM is a digital multiplexing technique for combiningseveral low-rate channels into one high-rate one.

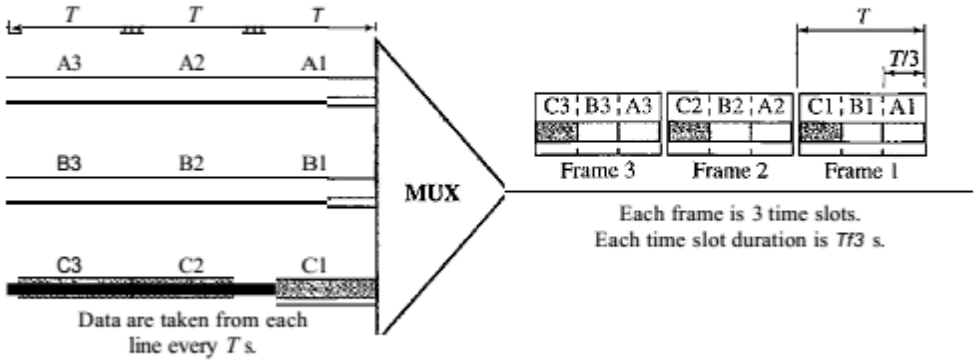
We can divide TDM into two different schemes: **synchronous and statistical.** We firstdiscuss synchronous TDM and then show how statistical TDM differs.

Synchronous Time-Division Multiplexing

In synchronousTDM, each input connection has an allotment in the output even if it is not sending data.

*Time Slots and Frames*In synchronous TDM, the data flow of each input connection is divided into units, whereeach input occupies one input time slot. A unit can be 1 bit, one character, or one block ofdata. Each input unit becomes one output unit and occupies one output time slot. However, the duration of an output time slot is *n* times shorter than the duration of an inputtime slot. If an input time slot is *T* s, the output time slot is *Tin* s, where *n* is the numberof connections. In other words, a unit in the output connection has a shorter duration; ittravels faster. Figure 6.13 shows an example of synchronous TDM where *n* is 3.

Figure 6.13 *Synchronous time-division multiplexing*



In synchronous TDM, a round of data units from each input connection is collected into a frame (we will see the reason for this shortly). If we have *n* connections, a frame is divided into *n* time slots and one slot is allocated for each unit, one for each input line. If the duration of the input unit is *T,* the duration of each slot is *Tin* and the duration of each frame is *T* (unless a frame carries some other information, as we will see shortly).

The data rate of the output link must be *n* times the data rate of a connection to guarantee the flow of data. In Figure 6.13, the data rate of the link is 3 times the data rate of a connection; likewise, the duration of a unit on a connection is 3 times that of the time slot (duration of a unit on the link). In the figure we represent the data prior to multiplexing as 3 times the size of the data after multiplexing. This is just to convey the idea that each unit is 3 times longer in duration before multiplexing than after.

In synchronous TDM, the data rate of the link is *n* times faster,and the unit duration is *n* times shorter.

Time slots are grouped into frames. A frame consists of one complete cycle of time slots, with one slot dedicated to each sending device. In a system with *n* input lines, each frame has *n* slots, with each slot allocated to carrying data from a specific input line.

Statistical Time-Division Multiplexing

in synchronous TDM, each input has a reserved slotin the output frame. This can be inefficient if some input lines have no data to send. Instatistical time-division multiplexing, slots are dynamically allocated to improve bandwidth efficiency. Only when an input line has a slot's worth of data to send is it given aslot in the output frame. In statistical multiplexing, the number of slots in each frame isless than the number of input lines. The multiplexer checks each input line in roundrobin fashion; it allocates a slot for an input line if the line has data to send; otherwise,it skips the line and checks the next line.

Wavelength Division Multiplexing

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.

Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

TRANSMISSION MEDIA

The transmission media is nothing but the physical media over which communication takes place in computer networks.

The medium over which the information between two computer systems is sent, called Transmission Media.

Transmission media comes in two forms.

Guided Media

All communication wires/cables comes into this type of media, such as UTP, Coaxial and Fiber Optics. In thismedia the sender and receiver are directly connected and the information is send (guided) through it.

- **Twisted Pair Cable**
- **Coaxial Cable**
- **Fiber Optics**

Unguided Media

Wireless or open air space is said to be unguided media, because there is no connectivity between the senderand receiver. Information is spread over the air, and anyone including the actual recipient may collect theinformation.

- **Radio waves**
- **Micro waves**
- **Infrared waves**

Twisted Pair Cable

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference. The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk.

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

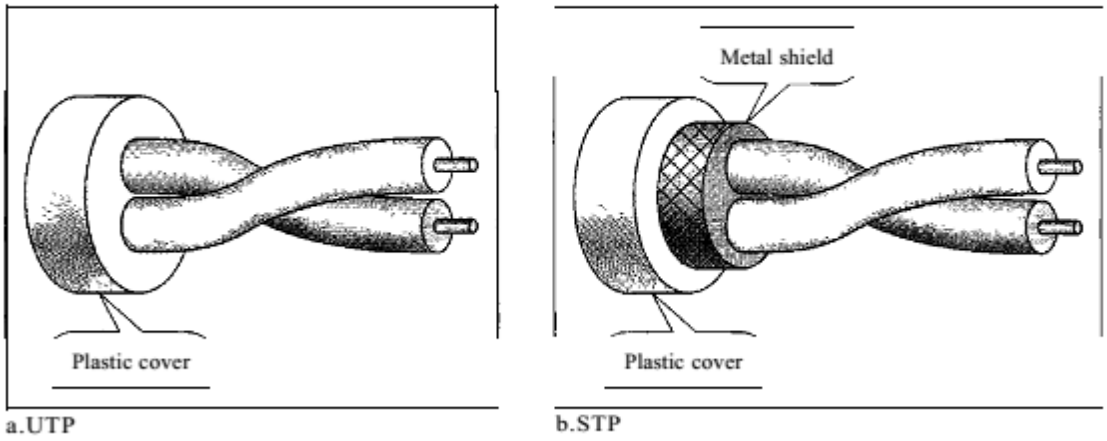
Figure 7.3 *Twisted-pair cable*

Applications Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office---commonly consists of unshielded twisted-pair cables

There are two types of twisted pair cables:

- Shielded Twisted Pair (STP) Cable
- Unshielded Twisted Pair (UTP) Cable

Figure 7.4 *UTP and STP cables*



STP cables comes with twisted wire pair covered in metal foil. This makes it more indifferent to noise and crosstalk.

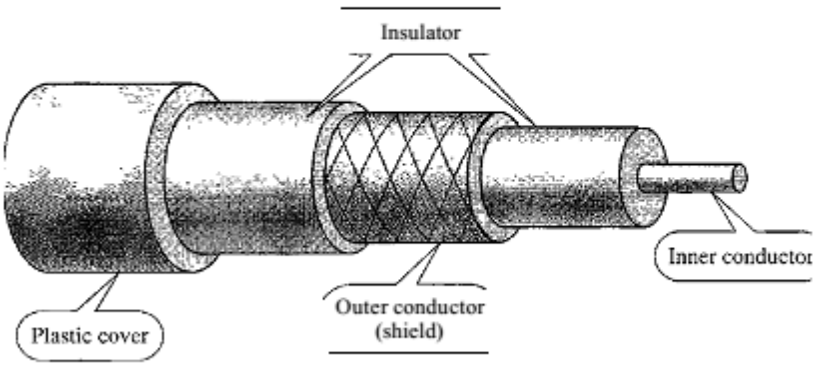
UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

Coaxial Cable

Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor.The core is enclosed in an insulating sheath.The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath.This all is covered by plastic cover.

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twistedpair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable isprotected by a plastic cover (see Figure 7.7).

Figure 7.7 *Coaxial cable*



Because of its structure,the coax cable is capable of carrying high frequency signals than that of twisted pair cable.The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

There are three categories of coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG stands for Radio Government.

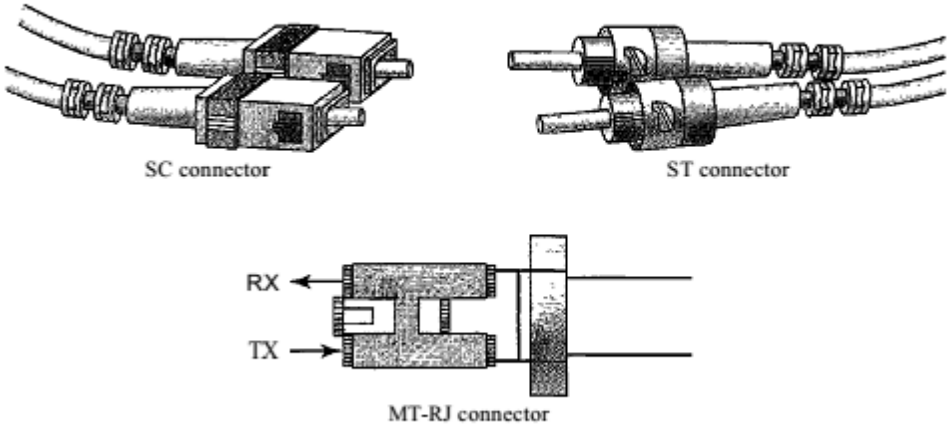
Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.

Fiber Optics

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.

Fiber Optic provides the highest mode of speed. It comes in two modes; one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.

Figure 7.15 *Fiber-optic cable connectors*



The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.

MT-RJ is a connector that is the same size as RJ45.

Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.

UnGuided Transmission Media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

Radio Waves

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.

Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna send waves that can be received by any receiving antenna. The omnidirectional property has disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.

Radio waves, particularly with those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Omnidirectional Antenna for Radio Waves

Radio waves use omnidirectional antennas that send out signals in all directions.

Applications of Radio Waves

- The omnidirectional characteristics of radio waves make them useful for multicasting in which there is one sender but many receivers.
- AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Micro Waves

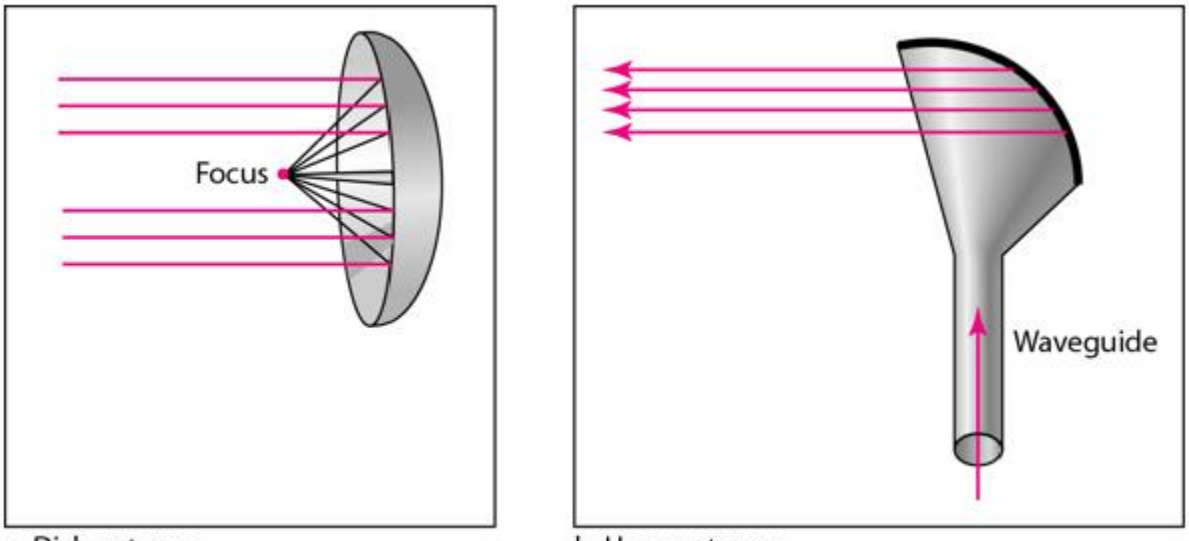
Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

The following describes some characteristics of microwaves propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside the buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned and a high date rate is possible.
- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna for Micro Waves

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: **Parabolic Dish** and **Horn**.



a. Dish antenna

b. Horn antenna

A parabolic antenna works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received

transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications of Micro Waves

Microwaves, due to their unidirectional properties, are very useful when unicast(one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks and wireless LANs.

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

When we use infrared remote control, we do not interfere with the use of the remote by our neighbours. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

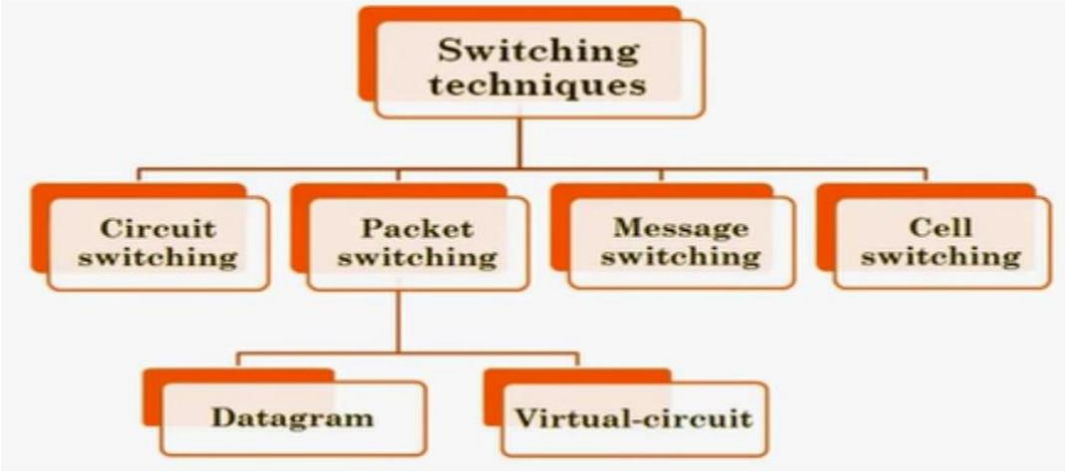
Applications of Infrared Waves

- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association(IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mouse, PCs and printers.
- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

NETWORKS SWITCHING TECHNIQUES AND ACCESSES MECHANISMS:

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

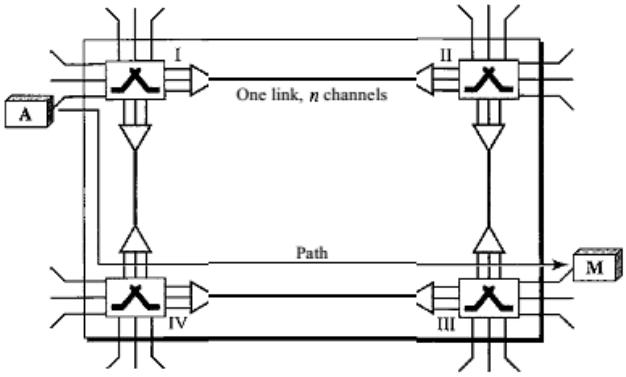


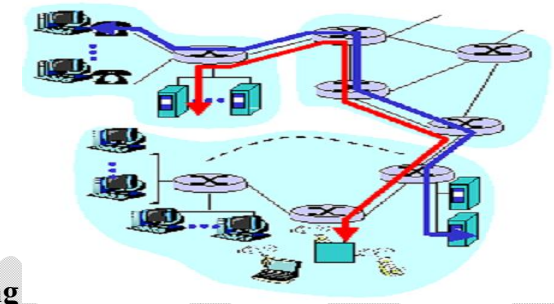
Circuit Switching

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

Circuit switching is a methodology of implementinga telecommunications network inwhich two networknodes establish a dedicated communicationschannel (circuit) through the network before the nodesmay communicate. The circuit guarantees the fullbandwidth of the channel and remains connected forthe duration of the communication session. The circuitfunctions as if the nodes were physically connected as with an electrical circuit.The defining example of a circuit-switched network isthe early analog telephone network. When a call is made from one telephone to another, switches withinthe telephone exchanges create a continuous wirecircuit between the two telephones, for as long as thecall lasts.

Figure 8.3 *A trivial circuit-switched network*





Packet Switching

Packet switching features deliveryof variable bit rate data streams(sequences of packets) over a computernetwork which allocates transmissionresources as needed using statisticalmultiplexing or dynamic bandwidthallocation techniques. When traversingnetwork adapters, switches, routers, andother network nodes, packets are bufferedand queued, resulting in variable delayand throughput depending on thenetwork's capacity and the traffic load on the network.Packet switching is used to optimize the use of the channel capacity available in digitaltelecommunication networks such as computer networks.

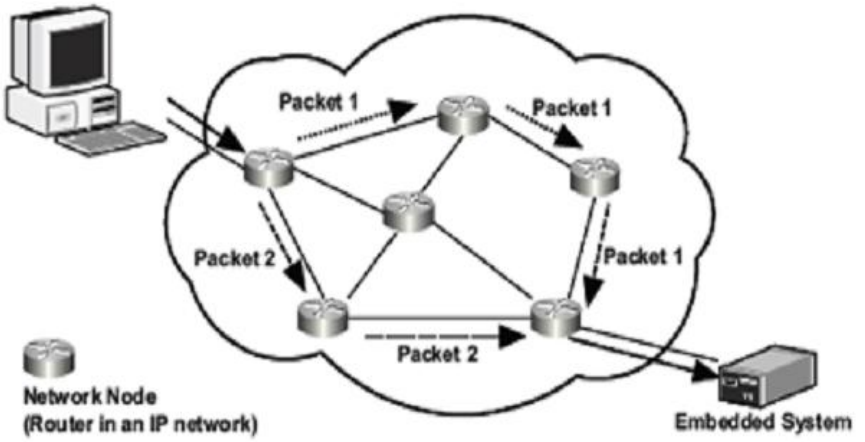


Figure 2-2 Packet Switched Network

	CIRCUIT SWITCHING	PACKET SWITCHING
Call Setup	Required	Optional
Overhead during call	Minimal	Per Packet
State	Stateful	No state
Resource Reservation	Easy	Difficult
QoS (Quality of Service)	Easy	Difficult
Sharing	By overbooking	Easy

Connectionless and connection-oriented packet switching

Two major packet switching modes exist:

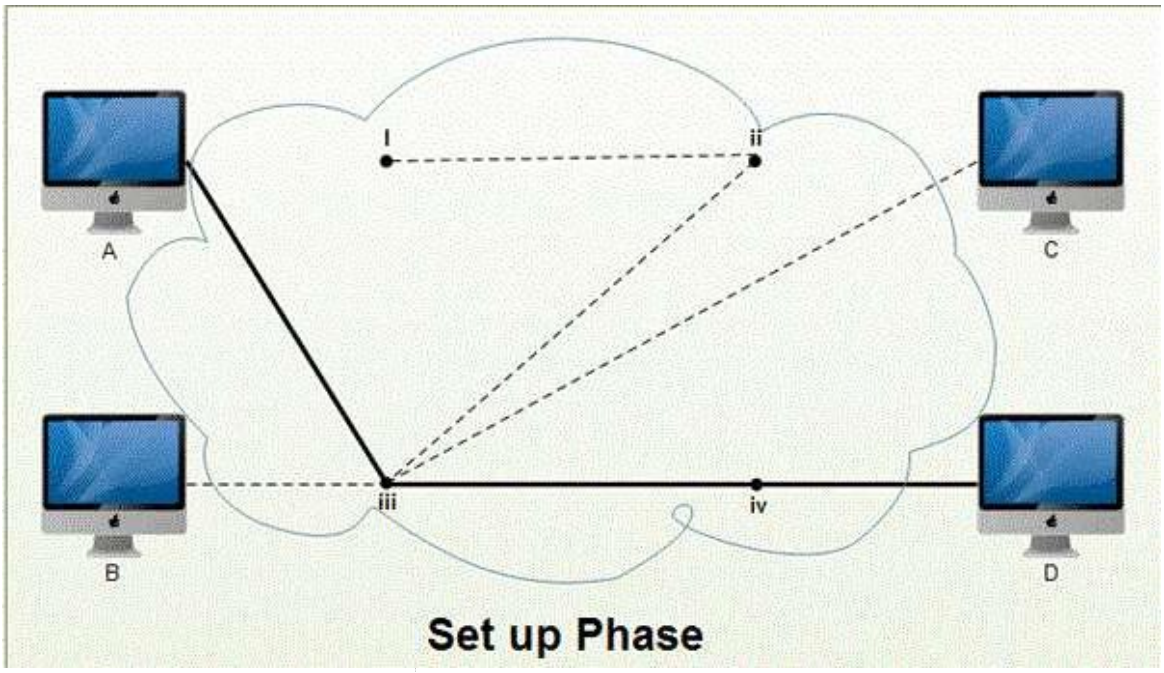
1. connectionless packet switching, also known as datagram switching; and
2. connection-oriented packet switching, also known as virtual circuit switching.

Types of Packet Switching

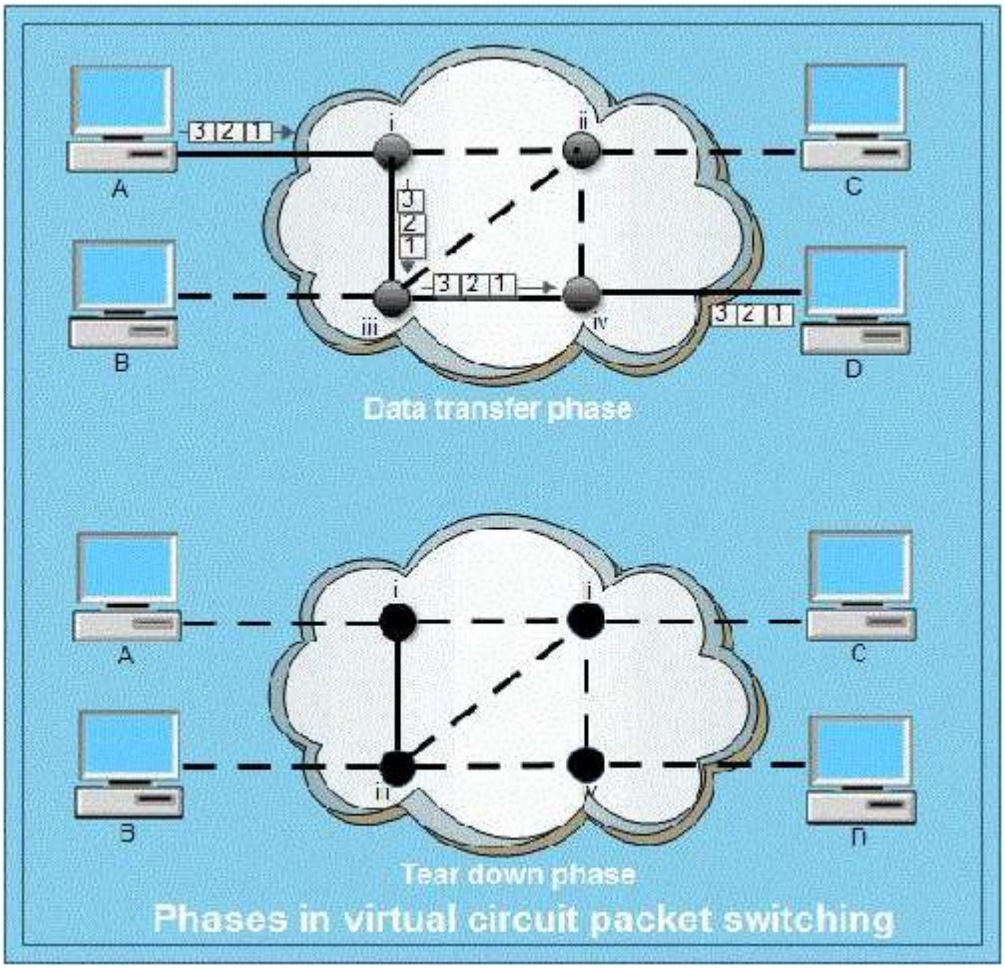
The packet switching has two approaches: Virtual Circuit approach and Datagram approach. WAN, ATM, frame relay and telephone networks use connection oriented virtual circuit approach; whereas internet relies on connectionless datagram based packet switching.

(i) **Virtual Circuit Packet Switching:**

In virtual circuit packet switching, a single route is chosen between the sender and receiver and all the packets are sent through this route. Every packet contains the virtual circuit number. As in circuit switching, virtual circuit needs call setup before actual transmission can be started. He routing is based on the virtual circuit number.

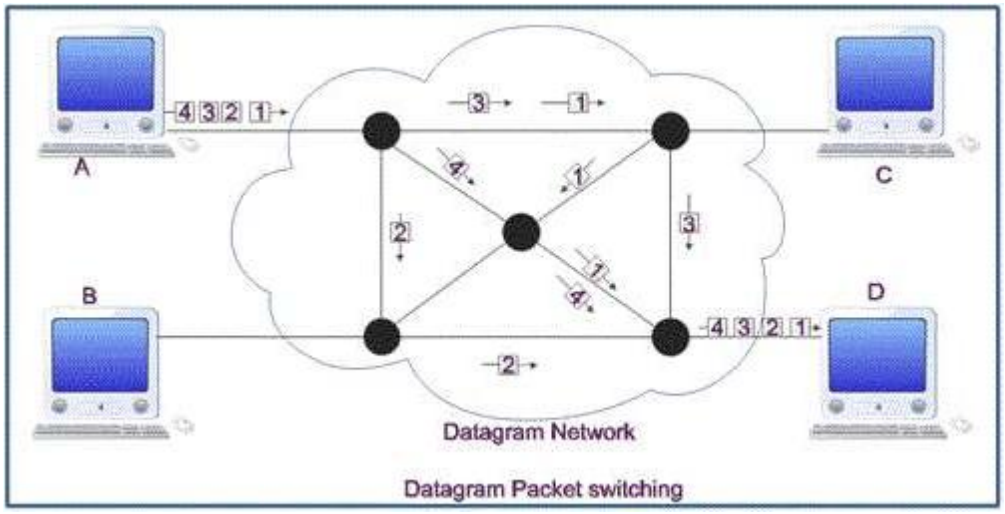


This approach preserves the relationship between all the packets belonging to a message.Just like circuit switching, virtual circuit approach has a set up, data transfer and tear down phases. Resources can be allocated during the set up phase, as in circuit switched networks or on demand, as in a datagram network. All the packets of a message follow the same path established during the connection. A virtual circuit network is normally implemented in the data link layer, while a circuit switched network is implemented in the physical layer and a datagram network in the network layer.



(ii) **Datagram Packet Switching:** In datagram packet switching each packet is transmitted without any regard to other packets. Every packet contain full packet of source and destination. Every packet is treated as individual, independent transmission.

Even if a packet is a part of multi-packet transmission the network treats it as though it existed alone. Packets in this approach are called **datagrams.** Datagram switching is done at the network layer. Figure show how a datagram approach is used to deliver four packets from station A to station D. All the four packets belong to same message but they may travel via different paths to reach the destination *i.e.* station D.



Datagram Packet switching

Datagram approach can cause the datagrams to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of lack of resources. The datagram networks are also referred as connectionless networks. Here connectionless means that the switch does not keep information about connection state. There are no connection establishment or tear down phases.

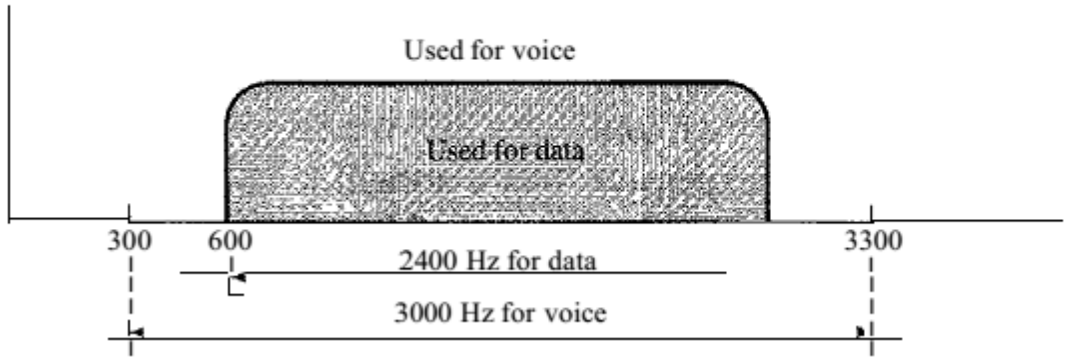
The datagram can arrive at the destination with a different order from the order in which they where sent. The source and destination address are used by the routers to decide the route for packets. Internet use datagram approach at the network layer.

In the first case, each packet includes complete addressing or routing information. The packets arerouted individually,sometimes resulting in different paths and out-of-order delivery. In the secondcase, a connection is defined and pre-allocated in each involved node during a connection setupphase before any packet is transferred. The packets include a connection identifier rather thanaddress information. Some connectionless protocols are Ethernet, IP, and UDP; connection oriented packet-switching protocols include X.25, Frame relay, Multiprotocol Label Switching (MPLS), and TCP.

Dial-Up Modems

Traditional telephone lines can carry frequencies between 300 and 3300 Hz, giving them a bandwidth of 3000 Hz. All this range is used for transmitting voice, where a great deal of interference and distortion can be accepted without loss of intelligibility. As we have seen, however, data signals require a higher degree of accuracy to ensure integrity. For safety's sake, therefore, the edges of this range are not used for data communications. In general, we can say that the signal bandwidth must be smaller than the cable bandwidth. The effective bandwidth of a telephone line being used for data transmission is 2400 Hz, covering the range from 600 to 3000 Hz. Note that today some telephone lines are capable of handling greater bandwidth than traditional lines. However, modem design is still based on traditional capability

Telephone line bandwidth



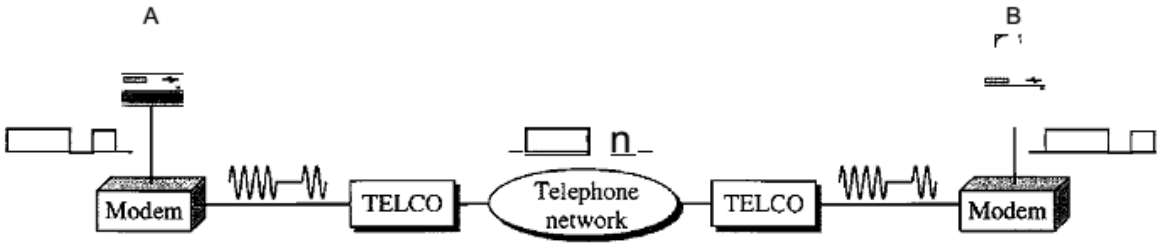
The term modem is a composite word that refers to the two functional entities that make up the device: a signal modulator and a signal demodulator. A modulator creates a band pass analog signal from binary data. A demodulator recovers the binary data from the modulated signal.

Modem stands for modulator/demodulator.

The computer on the left sends a digital signal to the modulator portion of the modem; the data are sent as an analog signal on the telephone lines. The modem on the right receives the analog signal,
demodulates it through its demodulator, and delivers data to the computer on the right. The communication can be bidirectional, which means the computer on the right can simultaneously send data to the computer on the left, using the same modulation/demodulation processes.

Modulation/demodulation

TELCO: Telephone company



Modem Standards

Today, many of the most popular modems available are based on the V-series standards published by the ITU-T.

V.32 and V.32bis

The V.32 modem uses a combined modulation and encoding technique called trelliscoded modulation.

V:90

b. Constellation and bandwidth for V.32bis Traditional modems have a data rate limitation of 33.6 kbps, as determined by the Shannon capacity (see Chapter 3). However, V.90 modems with a bit rate of 56,000 bps are available; these are called 56K modems.

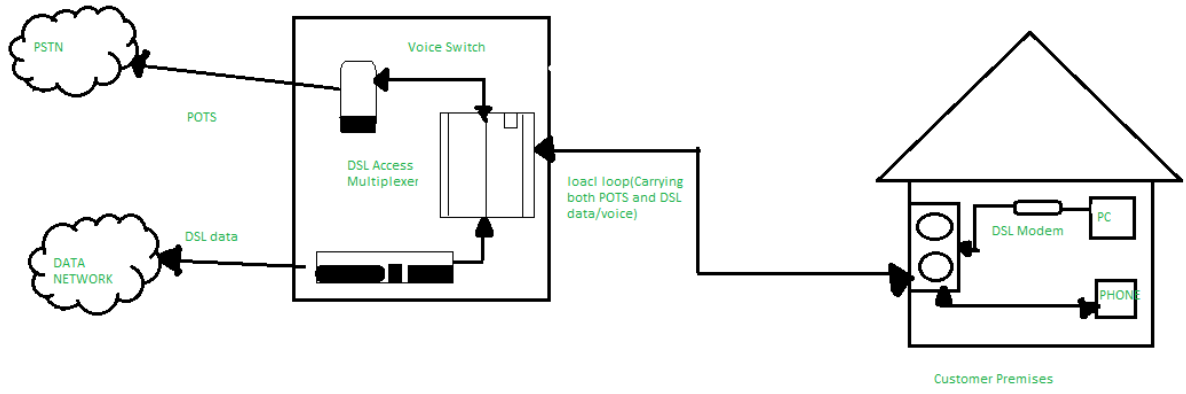
V:92

The standard above V90 is called ~92. These modems can adjust their speed, and if the noise allows, they can upload data at the rate of 48 kbps. The downloading rate is still 56 kbps. The modem has additional features. For example, the modem can interrupt the Internet connection when there is an incoming call if the line has call-waiting service.

DIGITAL SUBSCRIBER LINE:

Digital Subscriber Line (DSL, *originally*, **digital subscriber loop**) is a communication medium, which is used to transfer internet through copper wire telecommunication line.Along with cable internet, DSL is one of the most popular ways *ISPs* provide broadband internet access.

- Its aim is to maintain the high speed of the internet being transfered.
- If we ask that how we gonna achieve such thing i.e., both telephone and internet facility, then the answer is by using *splitters or DSL filters*(shown in below diagram).Basically, the use *splitter* is to splits the frequency and make sure that they can't get interrupted.



Types of DSL –

1. **Symmetric DSL –** SDSL, *splits* the upstream and downstream frequencies evenly, providing equal speeds to both uploading and downloading data transfer.This connection may provide *2 Mbps*upstream and downstream.it is mostly preferred by small organizations.

2. **Asymmetric DSL –** ADSL, provides a wider frequency range for downstream transfers, which offers several times faster downstream speeds.an ADSL connection may offer *20 Mbps downstream and 1.5 Mbps upstream*, it is because most users download more data than they upload.

Benefits –

- **No Additional Wiring –** A DSL connection makes use of your existing telephone wiring, so you will not have to pay for expensive upgrades to your phone system.
- **Cost Effective –** DSL internet is a very cost-effective method and is best in connectivity
- Availability of DSL modems by the service providers.
- User can use the both telephone line and internet at a same time.And it is because the voice is transferred on other frequency and digital signals are transferred on others.
- User can choose between different connection *speeds* and *pricing* from various providers.

DSL Internet service only works over a limited physical distance and remains unavailable in many areas where the local telephone infrastructure does not support DSL technology. The service is not available everywhere. The connection is faster for receiving data than it is for sending data over the Internet.

CABLE TV FOR DATA TRANSFER:

Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer. DSL technology provides high-data-rate connections for residential subscribers over the local loop.

1. Bandwidth

Even in an HFC system, the last part of the network, from the fiber node to the subscriber premises, is still a coaxial cable. This coaxial cable has a bandwidth that ranges from 5 to 750 MHz (approximately). To provide Internet access, the cable company has divided this bandwidth into three bands: video, downstream data, and upstream data.

Figure 1.61 Division of coaxial cable band by CATV

Downstream Video Band

The downstream video band occupies frequencies from 54 to 550 MHz. Since each TV channel occupies 6 MHz, this can accommodate more than 80 channels.

Downstream Data Band

The downstream data (from the Internet to the subscriber premises) occupies the upper band, from 550 to 750 MHz. This band is also divided into 6-MHz channels. Modulation Downstream data band uses the 64-QAM (or possibly 256-QAM) modulation technique. Downstream data are modulated using the 64-QAM modulation technique.

Upstream Data Band

The upstream data (from the subscriber premises to the Internet) occupies the lower band, from 5 to 42 MHz. This band is also divided into 6-MHz channels. Modulation The upstream data band uses lower frequencies that are more susceptible to noise and interference. For this reason, the QAM technique is not suitable for this band.

2. CM and CMTS

To use a cable network for data transmission, we need two key devices: a cable modem (CM) and a cable modem transmission system (CMTS).

CM

The cable modem (CM) is installed on the subscriber premises. It is similar to an ADSL.

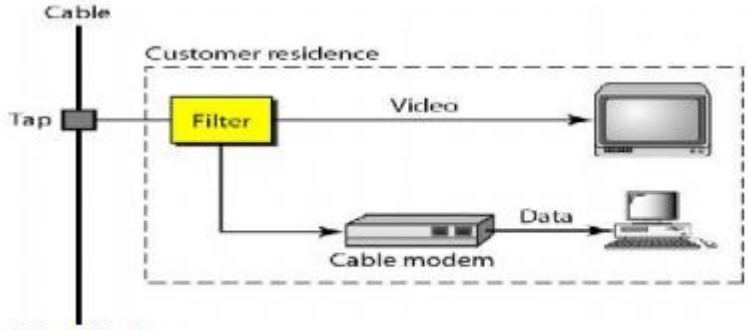


Figure 1.61 Cable Modem

CMTS

The cable modem transmission system (CMTS) is installed inside the distribution hub by the cable company. It receives data from the Internet and passes them to the combiner, which sends them to the subscriber. The CMTS also receives data from the subscriber and passes them to the Internet. Figure 1.77 shows the location of the CMTS.

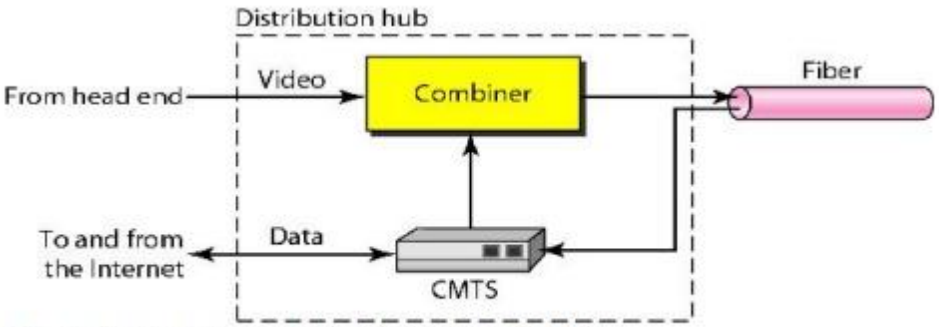


Figure 1.77 Cable modem transmission system (CMTS)

3. Data Transmission Schemes: DOCSIS

Several schemes have been designed for data transmission over an HFC network.

Upstream Communication

The following describes the steps that must be followed by a CM:

· The CM checks the downstream channels for a specific packet periodically sent by the CMTS. The packet asks any new CM to announce itself on a specific upstream channel.

·The CMTS sends a packet to the CM, defining its allocated downstream and upstreamChannels.

·The CM then starts a process, called ranging, which determines the distance between the CM and CMTS. This process is required for synchronization between all CMs and CMTSs for the minislots used for timesharing of the upstream channels.

·The CM sends a packet to the ISP, asking for the Internet address.

·The CM and CMTS then exchange some packets to establish security parameters, which are needed for a public network such as cable TV.

·The CM sends its unique identifier to the CMTS.

·Upstream communication can start in the allocated upstream channel; the CM can contend for the minislots to send data.

Downstream Communication

In the downstream direction, the communication is much simpler. There is no contention because there is only one sender. The CMTS sends the packet with the address of the receiving CM, using the allocated downstream channel.

POSSIBLE QUESTIONS

UNIT-II

PART-A (20 MARKS)

(Q.NO 1 TO 20 Online Examination)

PART-B (2 MARKS)

1. List out the type of digital to analog conversions.
2. Name the three multiplexing techniques.
3. What are the transmission media used for computer networks?
4. What are the three protocols used for noisy channels?
5. What are the classifications of packet switching?
6. Define Switching. List the types of switching?
7. What is Dial-up modem.
8. Define DSL and list its types.

PART-C (6 MARKS)

1. Discuss in detail Digital to analog conversion.
2. Explain in detail multiplexing techniques with proper diagram.
3. Differentiate between guided and unguided media. Briefly explain virtual circuit switching.
4. Discuss in detail about virtual- circuit network with diagrams.
5. Elaborate the working of message switching networks with neat diagrams.
6. Discuss the working of packet switched networks with neat diagrams.
7. Elaborate the working of Datagram networks with neat diagrams.
8. Write in detail about Dial-Up modems.
9. Explain in detail about digital subscriber line.
10. Discuss about cable TV for data transfer.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CS Batch:2017

Subject: COMPUTER NETWORKS

SubCode: 17CSU303

UNIT - II

S.No	Questions	CHOICE 1	CHOICE 2	CHOICE 3	CHOICE 4	ANSWER
1	Before data can be transmitted, they must be transformed to_____	periodic signals	electromagnetic signals	Aperiodic signals	low frequency sine waves	electromagnetic signals
2	Which of the following can be determined from a frequency_domain graph of a signal?	frequency	phase	power	all the above	frequency
3	Which of the following can be determined from a frequency_domain graph of a signal?	bandwidth	phase	power	all the above	bandwidth
4	In a frequency_domain plot, the vertical axis measures the_____	peak amplitude	frequency	phase	slope	peak amplitude
5	In a frequency_domain plot, the horizontal axis measures the_____	peak amplitude	frequency	phase	slope	frequency
6	As frequency increases, the period_____	dereases	increases	remains the same	doubles	increases
7	The last step in Pulse Code Modulation (PCM) is____	Quantization	Sampling	Encoding	Modulation	Encoding
8	A sine wave is_____	periodic and continuous	aperiodic and continuous	periodic and discrete	aperiodic and discrete	periodic and continuous
9	the signal loses strength due to the resistance of the transmission medium	attenuation	distortion	noise	decibel	attenuation
10	the signal loses strength due to different propogation speeds of each frequency that makes up the signal	attenuation	distortion	noise	decibel	distortion
11	_____is a type of transmission impairment in which an outside source such as crosstalk corrupts a signal	attenuation	distortion	noise	decibel	noise

12	Propogation time is_____ proportional to distance and_____ proportional to propogation speed	inversely; directly	directly; inversely	inversely; inversely	directly; directly	directly; inversely
13	The wavelength of a signal depend on the_____	frequency of the signal	medium	phase of signal	(a) and (b)	(a) and (b)
14	Unipolar, bipolar and polar encoding are types of_____ encoding	line	block	NRZ	manchester	line
15	Guided media provides a conduit from one device to another, includes _____	twisted pair cable	fiber optic cable	coaxial cable	All of the above	All of the above
16	_____ encoding has a transition at the middle of each bit	RZ	manchester	differential manchester	all the above	RZ
17	Optical fibers use reflection to guide light through a _____	channel	metal wire	light	plastic	channel
18	PCM is an example of_____conversion	digital-to-digital	digital-to-anolog	anolog-to-analog	analog-to-digital	analog-to-digital
19	The nyquist theorem specifies the minimum sampling rate to be_____	equal to the lowest frequency of signal	highest frequency of a	bandwidth of a signal	highest frequency of	frequency of signal
20	Which encoding type always has a nonzero average amplitude?	unipolar	polar	bipolar	all the above	unipolar
21	Which of the following encoding methods does not provide for synchronization?	NRZ-L	RZ	NRZ-I	manchester	NRZ-L
22	Which encoding method uses altering positive and negative voltage for bit 1?	NRZ-I	RZ	manchester	Biploar encoding	Biploar encoding
23	RZ encoding involves_____ signal levels	two	three	four	five	three
24	Unguided medium is _____	twisted pair cable	coaxial cable	fiber optic cable	free space	free space
25	Block coding can help is_____ at the receiver	synchronization	error detection	attenuation	(a) and (b)	synchronization
26	_____ transmission, bits are transmitted simultaneously, each across the own wire	asynchronous serial	synchronous serial	parallel	(a) and (b)	parallel

27	In_____ transmission, bits are transmitted over a single wire, one at a time	asynchronous serial	synchronous serial	parallel	(a) and (b)	(a) and (b)
28	In_____ transmission, a start bit and a stop bit frame a character byte	asynchronous serial	synchronous serial	parallel	(a) and (b)	synchronous serial
29	In asynchronous transmission, the gap tim between bytes is_____	fixed	variable	a function of the data rate	zero	fixed
30	synchronous transmission does not have_____	a start bit	a stop bit	gaps between bytes	all the above	all the above
31	ASK, PSK, FSK and QAM are examples of_____ modulation	digital-to-digital	digital-to-anolog	analog-to-analog	analog-to-digital	digital-to-anolog
32	AM and FM are examples of modulation	digital-to-digital	digital-to-anolog	analog-to-analog	analog-to-digital	anolog-to-analog
33	In QAM, both phase and_____ of a carrier frequency are varied	amplitude	frequency	bit rate	baud rate	amplitude
34	Telephone companies implement _____ multiplexing	TDM	FDM	WDM	DWDM	TDM
35	The applications of Frequency-Division Multiplexing (FDM) are_____	broadcasting	AM and FM radio stations	cellular telephones	All of the mentioned	All of the mentioned
36	The Time-Division multiplexing (TDM) is a digital technique of _____	Encoding	Decoding	Multiplexing	Demultiplexing	Multiplexing
37	Wavelength division multiplexing is same as_____	FDM	TDM	DWDM	SDM	FDM
38	The types of multiplexing techniques are _____	one	two	three	four	three
39	Switching in the Internet is done by using the datagram approach to packet switching at the _____	Network Layer	Application Layer	Data link Layer	physical Layer	Network Layer
40	A Circuit-Switched Network is made of a set of switches connected by physical ____	Links	media	nodes	limes	Links
41	A switch in a datagram network uses a ____	destination address	sender address	routing table	header	routing table

42	Time Division Multiplexing inside a switch, is used by _____	Space division switch	crossbar switch	packet switch	switch	switch
43	The identifier that is actually used for data transfer is called the _____	virtual-circuit identifier	global address	local address	header	virtual-circuit identifier
44	Global and local addressing are types of _____	WAN network	local area circuit network	virtual-circuit network	MAN network	virtual-circuit network
45	A modulator converts _____ signal to _____ signal	digital ; analog	analog; digital	PSK; FSK	FSK; PSK	analog; digital
46	analog carrier signal is modified to reflect binary data?	FSK	ASK	PSK	TSK	ASK
47	The sharing of medium and its link by two or more devices is called_____	decoding	encoding	line discipline	multiplexing	multiplexing
48	Which multiplexing technique transmits analog signals	FDM	TDM	WDM	(a) and ©	(a) and ©
49	Which multiplexing technique transmits digital signals?	FDM	TDM	WDM	none of the above	TDM
50	Which multi plexing technique shifts each signal to a different carrier frequency?	FDM	TDM	both(a) and (b)	none of the above	FDM
51	In TDM, for n signal sources of the same data rate, each frame contains_____ slots	n	n+1	n-1	0 to n	n
52	Guard bands increases the bandwidth for_____	FDM	TDM	both(a) and (b)	none of the above	FDM
53	Which multiplexing technique involves signals composed of light beams?	FDM	TDM	WDM	none of the above	WDM
54	Transmission media are usually categorized as_____	fixed or unfixed	guided of unguided	determinate or indeterminate	metallic or non-metallic	guided of unguided
55	Transmission media are usually categorized as_____	physical	network	transport	application	physical
56	Category 1 UTP cable is most often used in_____ networks	fast ethernet	traditional ethernet	infrared	telephone	telephone

57	BNC connectors are used by_____ cables	UTP	STP	coaxial	fiber-optic	coaxial
58	In fiber optics, the signal source is_____ waves	light	radio	infrared	very low frequency	light
59	A parabolic dish Antenna is a(n)_____ antenna	omni directional	bi directional	uni directional	horn	uni directional
60	A telephone network is an example of a_____ network	packet switching	circuit switched	message switched	none of the above	circuit switched
61	Radio waves are _____.	omnidirectional	unidirectional	bidirectional	multidirectional	omnidirectional
62	Microwaves are _____.	omnidirectional	unidirectional	bidirectional	multidirectional	unidirectional
63	_____ are used for short-range communications such as those between a PC and a peripheral device.	Radio waves	Microwaves	Miniwaves	Infrared waves	Infrared waves

UNIT – III

SYLLABUS

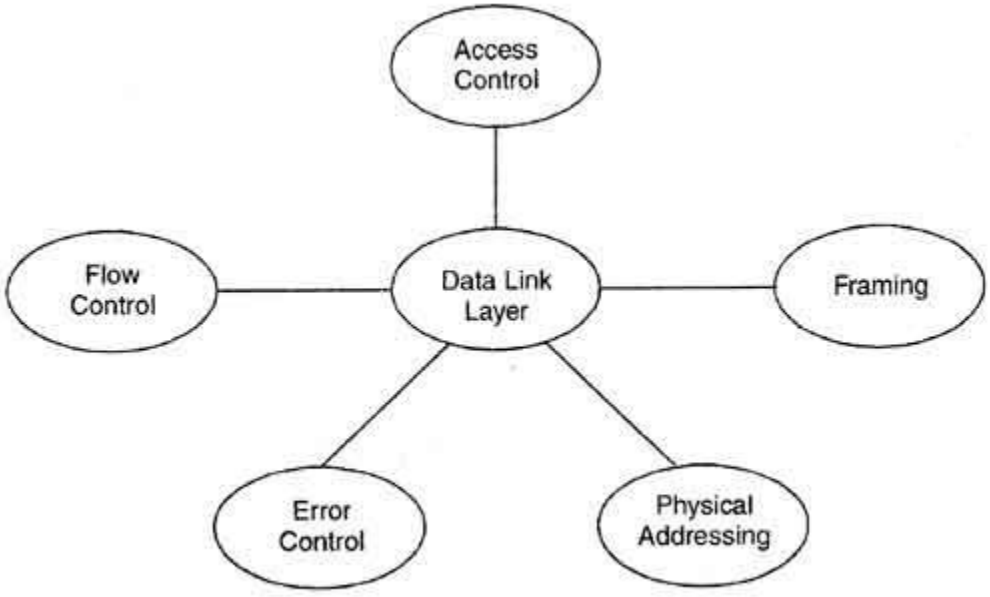
Data Link Layer Functions and Protocol: Error detection and error correction techniques; data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

DATA LINK LAYER FUNCTIONS AND PROTOCOL:

Data link layer is the second layer in OSI reference model and lies above the physical layer.

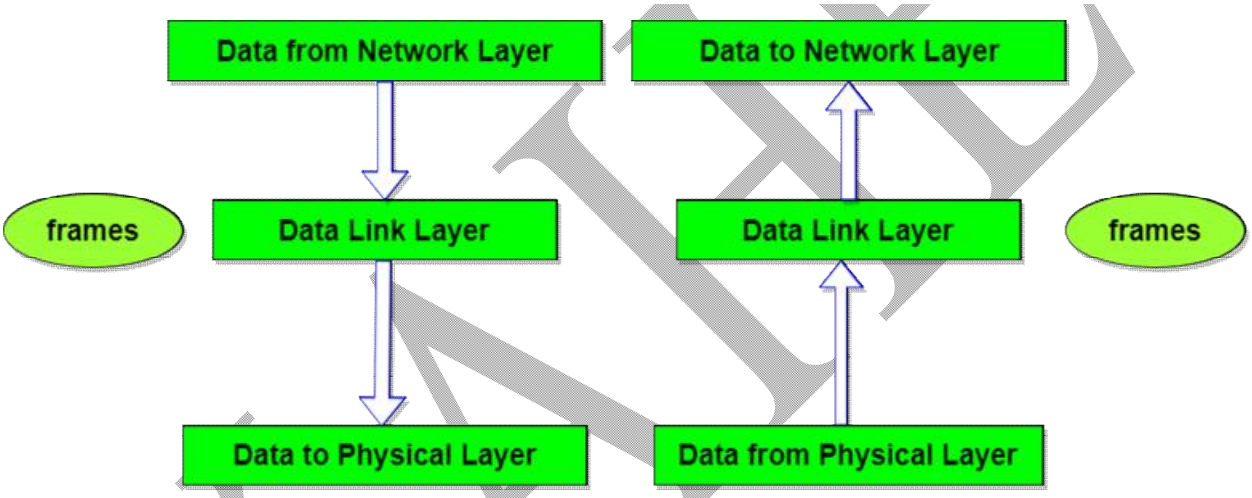
The data link layer performs the following functions.

1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.



Functions of data link layer

3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames is also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



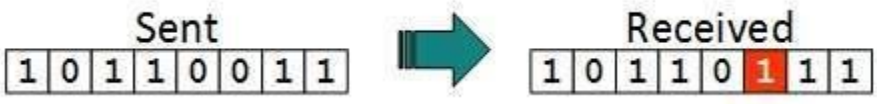
ERROR DETECTION AND ERROR CORRECTION TECHNIQUES:

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

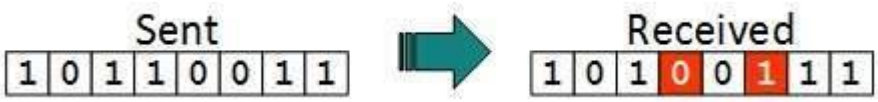
There may be three types of errors:

- **Single bit error**



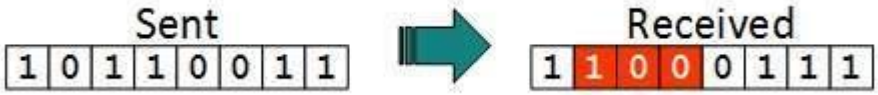
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



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

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

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

Parity Check

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

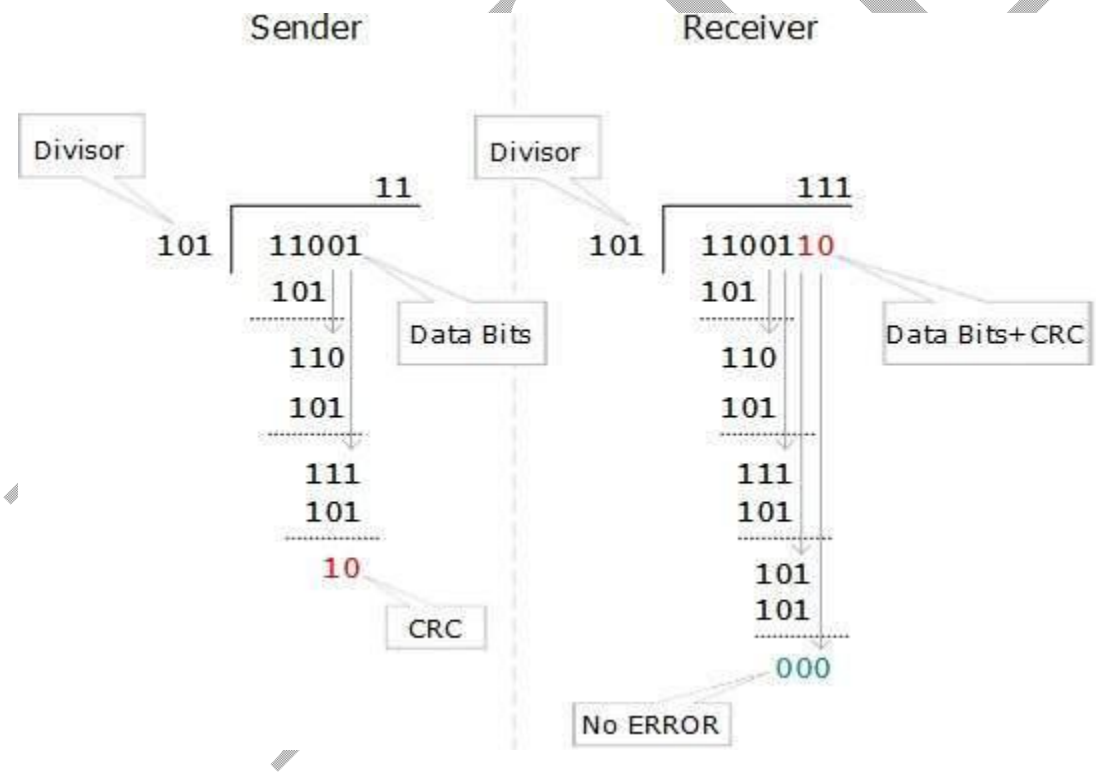
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

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

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

Cyclic Redundancy Check (CRC)

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



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

Error Correction

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

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

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

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

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

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

DATA-LINK CONTROL- FRAMING AND FLOW CONTROL:

Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

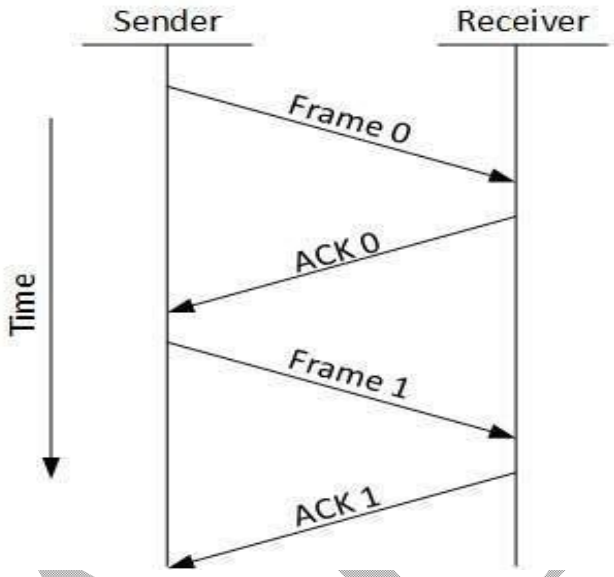
Flow Control

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

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

- **Stop and Wait**

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



- **Sliding Window**

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

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which help them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

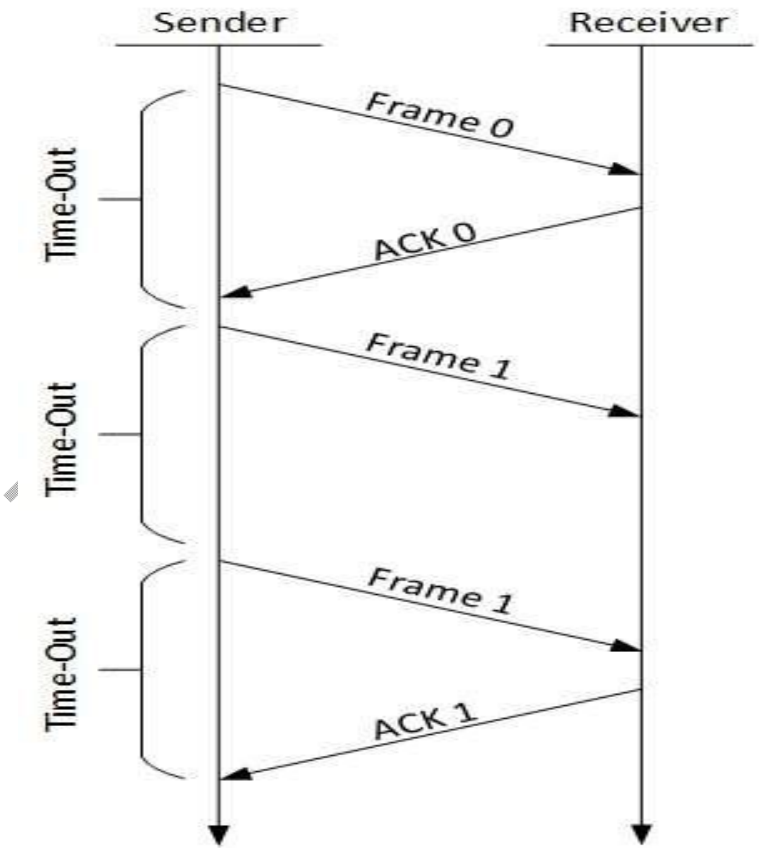
Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.

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

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

- **Stop-and-wait ARQ**



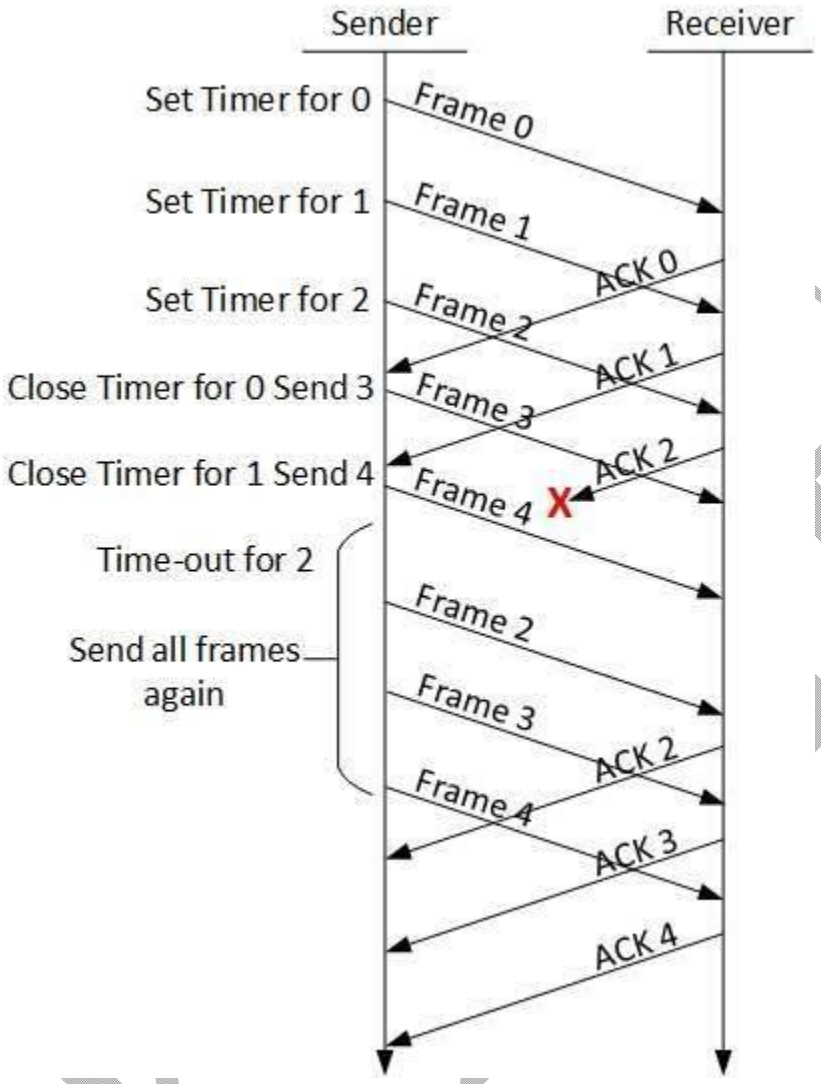
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.

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

- **Go-Back-N ARQ**

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

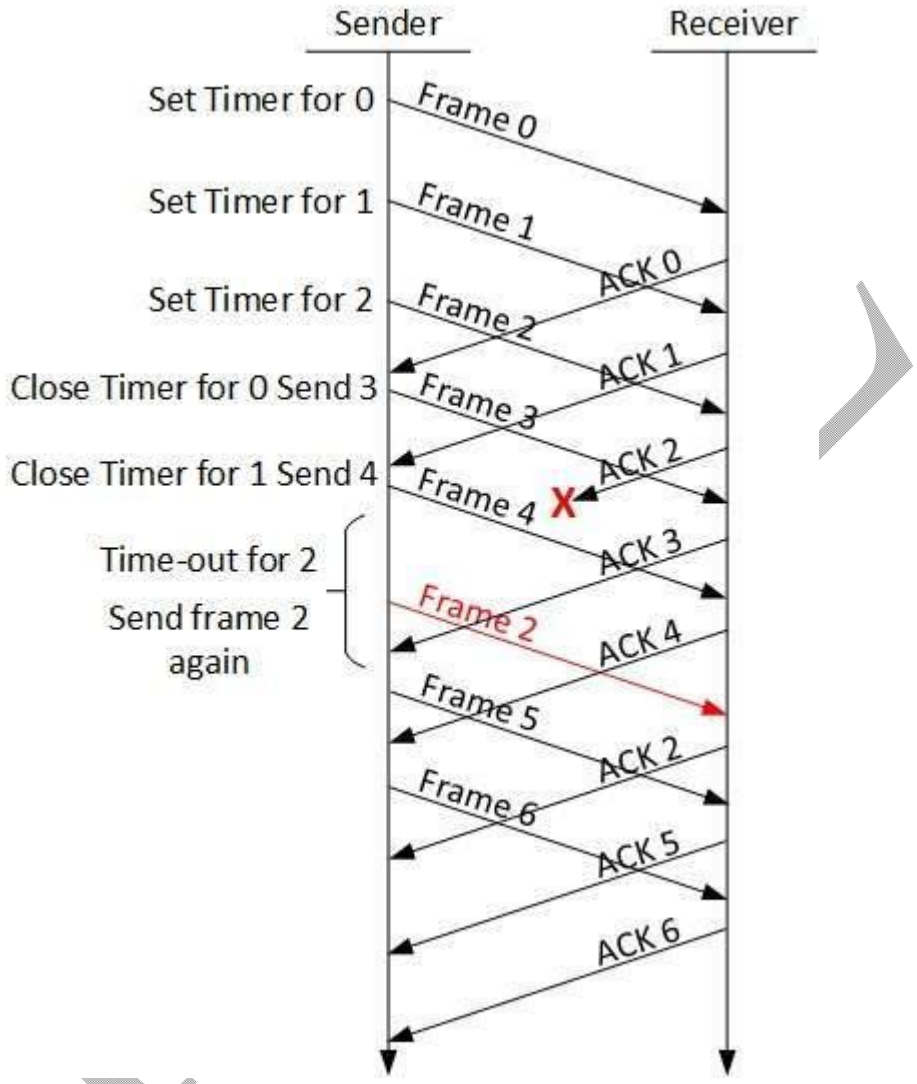


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

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

- **Selective Repeat ARQ**

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



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

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

Error Recovery Protocols:

It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender. Error control in the data link layer is based on automatic repeat request (ARQ). Whenever an error is detected, specified frames are retransmitted.

STOP AND WAIT ARQ:

Characteristics

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1

Useful Terms:

1. **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.
   Propagation Delay = (Distance between routers) / (Velocity of propagation)
2. RoundTripTime (**RTT**) = 2* Propagation Delay
3. TimeOut (**TO**) = 2* RTT
4. Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 180 seconds)

Simple Stop and Wait

Sender:

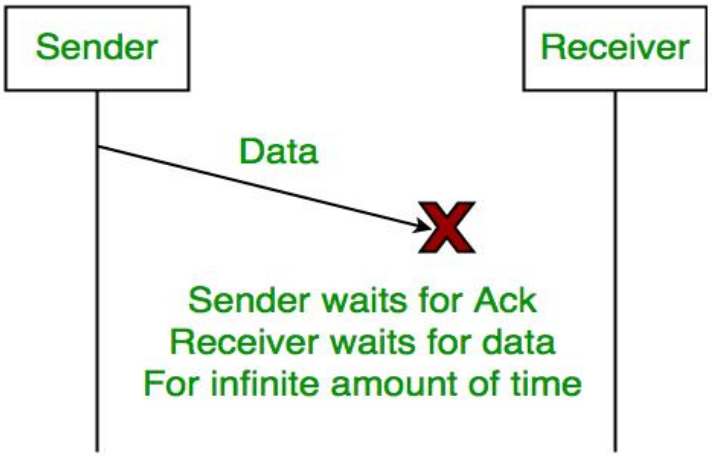
Rule 1) Send one data packet at a time.
Rule 2) send next packet only after receiving acknowledgement for previous.

Receiver:

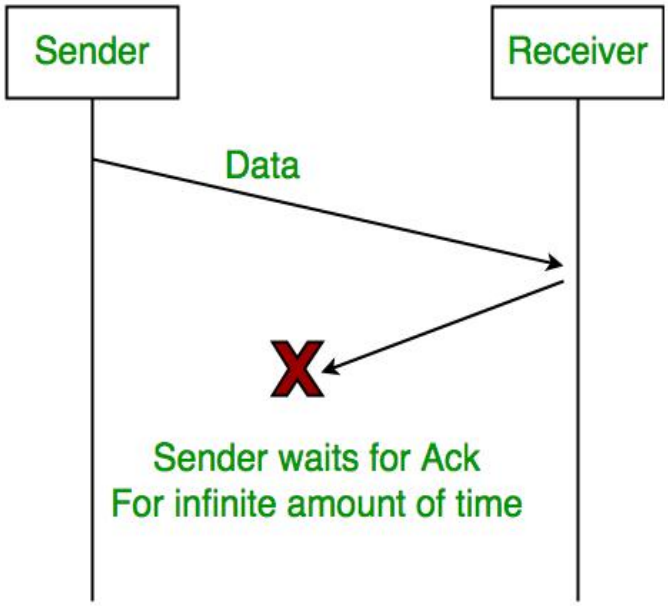
Rule 1) Send acknowledgement after receiving and consuming of data packet.
Rule 2) After consuming packet acknowledgement need to be sent (Flow Control)

Problems:

1. Lost Data



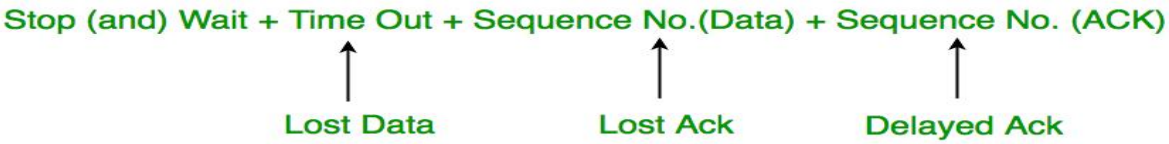
2. Lost Acknowledgement:



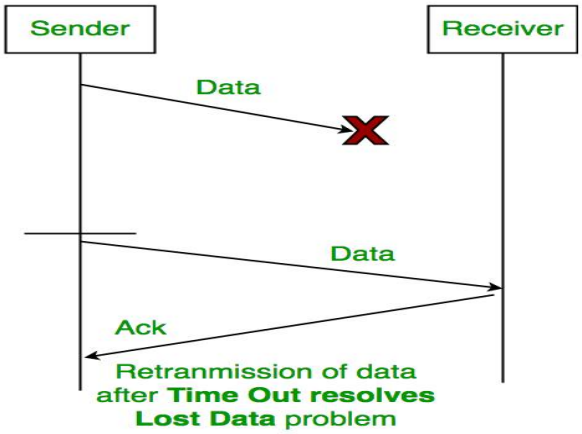
3. Delayed Acknowledgement/Data: After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait ARQ (Automatic Repeat Request)

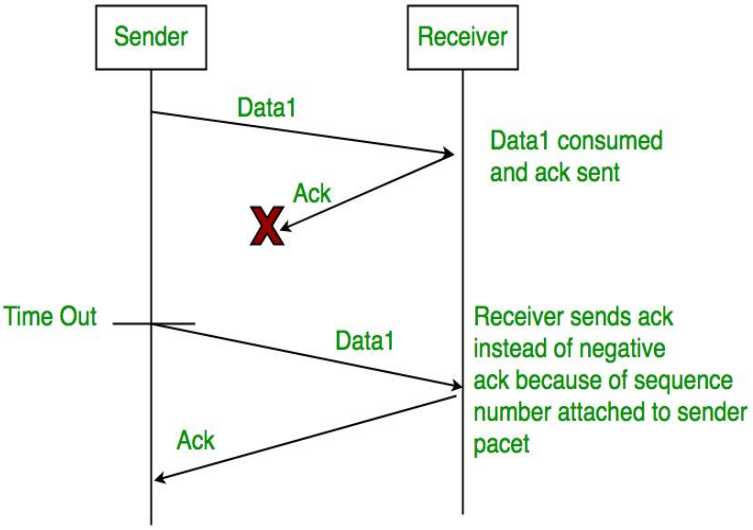
Above 3 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.



1. Time Out:



2. Sequence Number (Data)

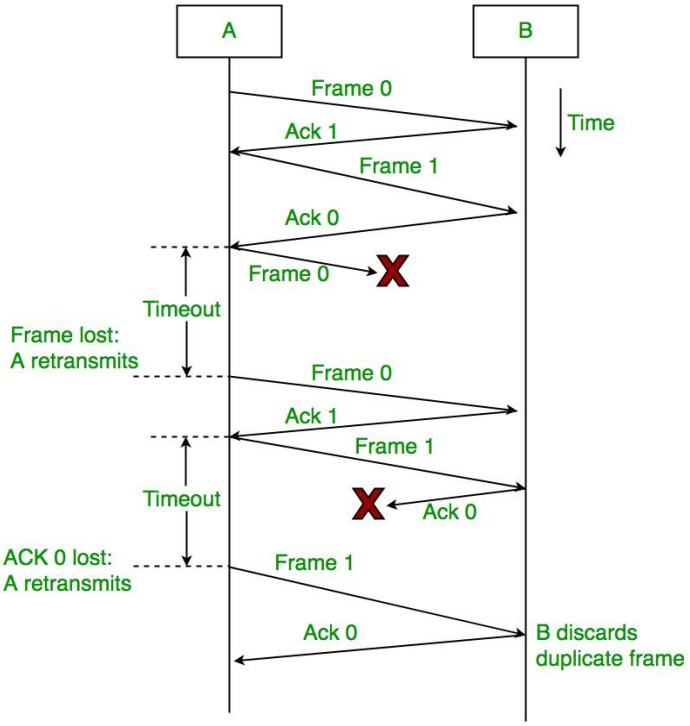


3. Delayed Acknowledgement:

This is resolved by introducing sequence number for acknowledgement also.

Working of Stop and Wait ARQ:

1) Sender A sends a data frame or packet with sequence number 0.
2) Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)
There is only one bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.



Characteristics of Stop and Wait ARQ:

- It uses link between sender and receiver as half duplex link
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example for "**Closed Loop OR connection oriented** " protocols
- It is an special category of SWP where its window size is 1
- Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequence numbers 0 and 1

The Stop and Wait ARQ solves main three problems, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you

are connected to some server in some other country though a high speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence numbers. So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections, but performs badly for distant connections like satellite connection.

Sliding Window Protocol | Set 1 (Sender Side)

The Stop and Wait ARQ offers error and flow control, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high speed connection); you can't use this full speed due to limitations of stop and wait.

Sliding Window protocol handles this efficiency issue by sending more than one packet at a time with a larger sequence numbers. The idea is same as pipelining in architectures.

Few Terminologies:

Transmission Delay (Tt) – Time to transmit the packet from host to the outgoing link. If B is the Bandwidth of the link and D is the Data Size to transmit

$$Tt = D/B$$

Propagation Delay (Tp) – It is the time taken by the first bit transferred by the host onto the outgoing link to reach the destination. It depends on the distance d and the wave propagation speed s (depends on the characteristics of the medium).

$$Tp = d/s$$

Efficiency – It is defined as the ratio of total useful time to the total cycle time of a packet. For stop and wait protocol,

Total cycle time = Tt(data) + Tp(data) +

Tt(acknowledgement) + Tp(acknowledgement)

= Tt(data) + Tp(data) + Tp(acknowledgement)

= Tt + 2*Tp

Since acknowledgements are very less in size, their transmission delay can be neglected.

Efficiency = Useful Time / Total Cycle Time

= Tt/(Tt + 2*Tp) (For Stop and Wait)

= 1/(1+2a) [Using a = Tp/Tt]

Effective Bandwidth(EB) or Throughput – Number of bits sent per second.

EB = Data Size(L) / Total Cycle time(Tt + 2*Tp)

Multiplying and dividing by Bandwidth (B),

= (1/(1+2a)) * B [Using a = Tp/Tt]

= Efficiency * Bandwidth

Capacity of link – If a channel is Full Duplex, then bits can be transferred in both the directions and without any collisions. Number of bits a channel/Link can hold at maximum is its capacity.

Capacity = Bandwidth(B) * Propagation(Tp)

For Full Duplex channels,

Capacity = 2*Bandwidth(B) * Propagation(Tp)

Concept of Pipelining

In Stop and Wait protocol, only 1 packet is transmitted onto the link and then sender waits for acknowledgement from the receiver. The problem in this setup is that efficiency is very less as we are not filling the channel with more packets after 1st packet has been put onto the link. Within the total cycle time of Tt + 2*Tp units, we will now calculate the maximum number of packets that sender can transmit on the link before getting an acknowledgement.

In Tt units ----> 1 packet is Transmitted.

In 1 units ----> 1/Tt packet can be Transmitted.

In Tt + 2*Tp units -----> (Tt + 2*Tp)/Tt

packets can be Transmitted

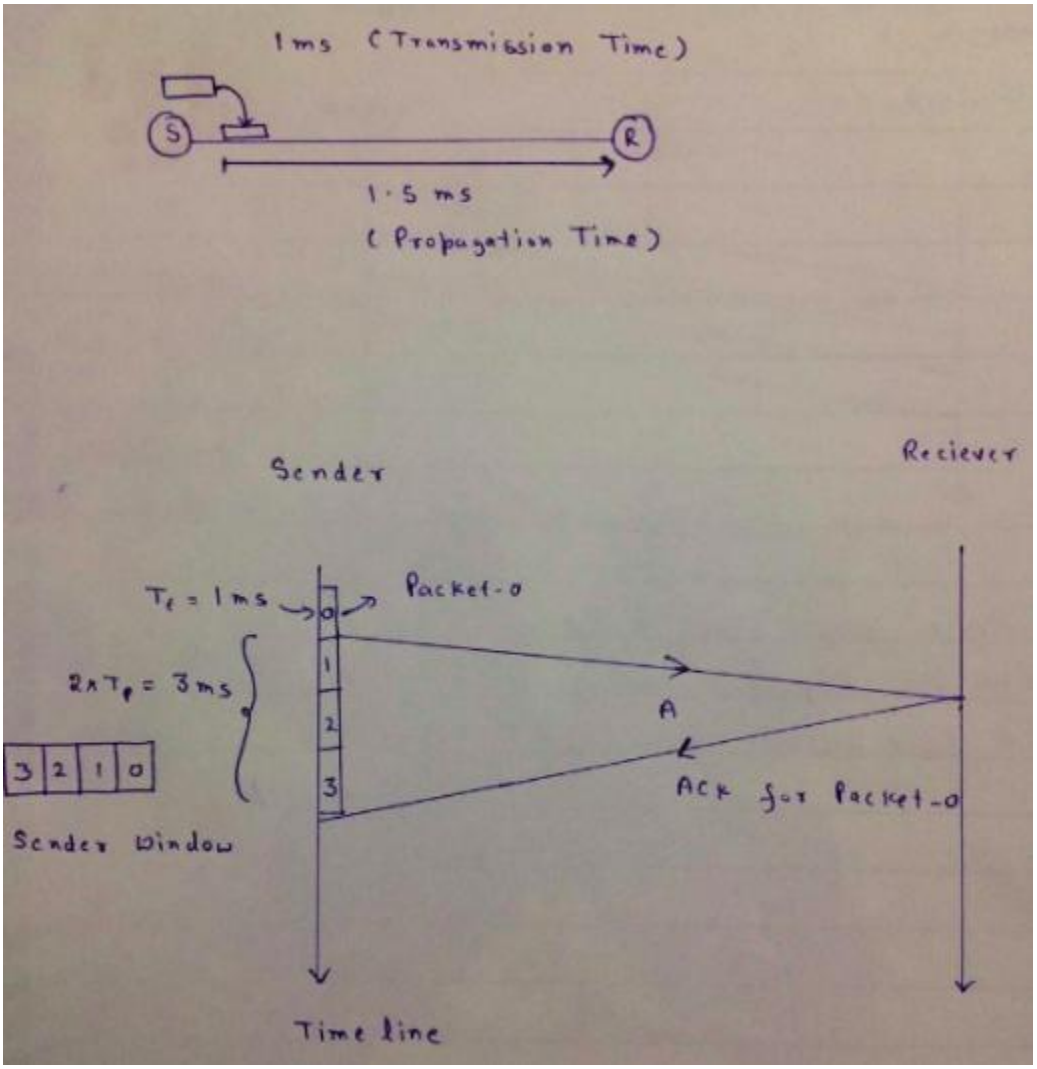
------> 1 + 2a [Using a = Tp/Tt]

Maximum packets That can be Transmitted in total cycle time = 1+2*a

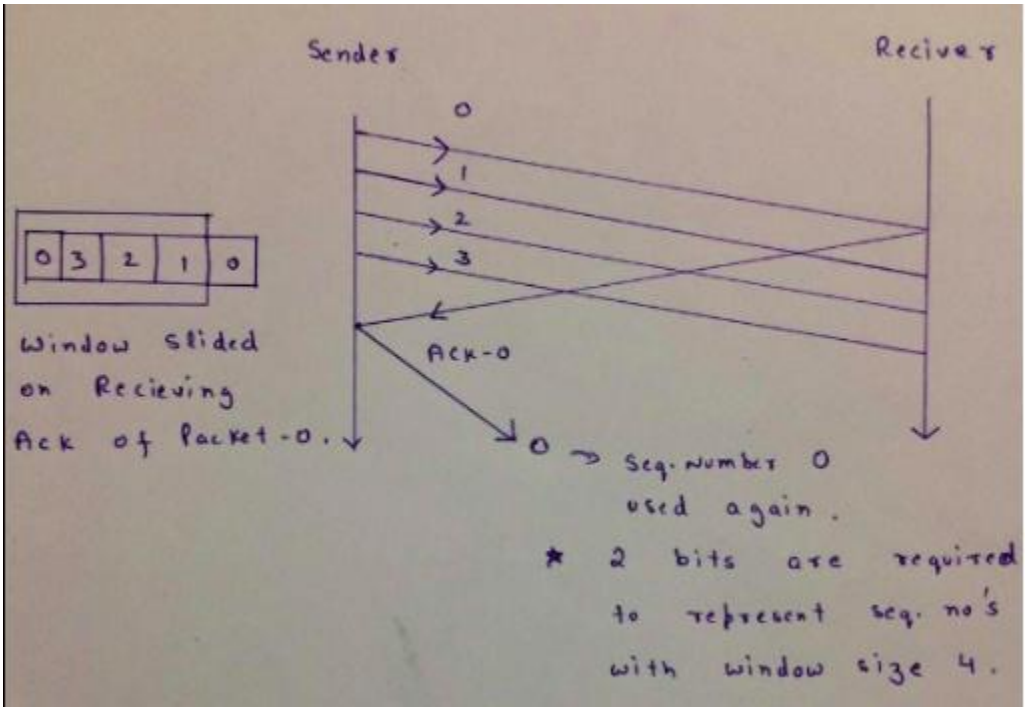
Let me explain now with the help of an example.

Consider Tt = 1ms, Tp = 1.5ms.

In the picture given below, after sender has transmitted packet 0, it will immediately transmit packets 1, 2, 3. Acknowledgement for 0 will arrive after 2*1.5 = 3ms. In Stop and Wait, in time 1 + 2*1.5 = 4ms, we were transferring one packet only. Here we keep a **window of packets which we have transmitted but not yet acknowledged**.



After we have received the Ack for packet 0, window slides and the next packet can be assigned sequence number 0. We reuse the sequence numbers which we have acknowledged so that header size can be kept minimum as shown in the diagram given below.



Minimum Number of Bits for Sender window (Very Important For GATE)

As we have seen above,

Maximum window size = 1 + 2*a where a = Tp/Tt

Minimum sequence numbers required = 1 + 2*a.

All the packets in the current window will be given a sequence number. Number of bits required to represent the sender window = ceil(log2(1+2*a)).

But sometimes number of bits in the protocol headers is pre-defined. Size of sequence number field in header will also determine the maximum number of packets that we can send in total cycle time. If N is the size of sequence number field in the header in bits, then we can have 2^N sequence numbers.

Window Size ws = min(1+2*a, 2^N)

If you want to calculate minimum bits required to represent sequence numbers/sender window, it will be **ceil(log2(ws))**.

SLIDING WINDOW PROTOCOL | SET 2 (RECEIVER SIDE):

Sliding Window Protocol is actually a theoretical concept in which we have only talked about what should be the sender window size (1+2a) in order to increase the efficiency of stop and wait arq. Now we will talk about the practical implementations in which we take care of

what should be the size of receiver window. Practically it is implemented in two protocols namely :

1. Go Back N (GBN)
2. Selective Repeat (SR)

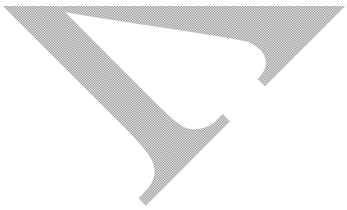
In this article, we will explain you about the first protocol which is GBN in terms of three main characteristic features and in the last part we will be discussing SR as well as comparison of both these protocols

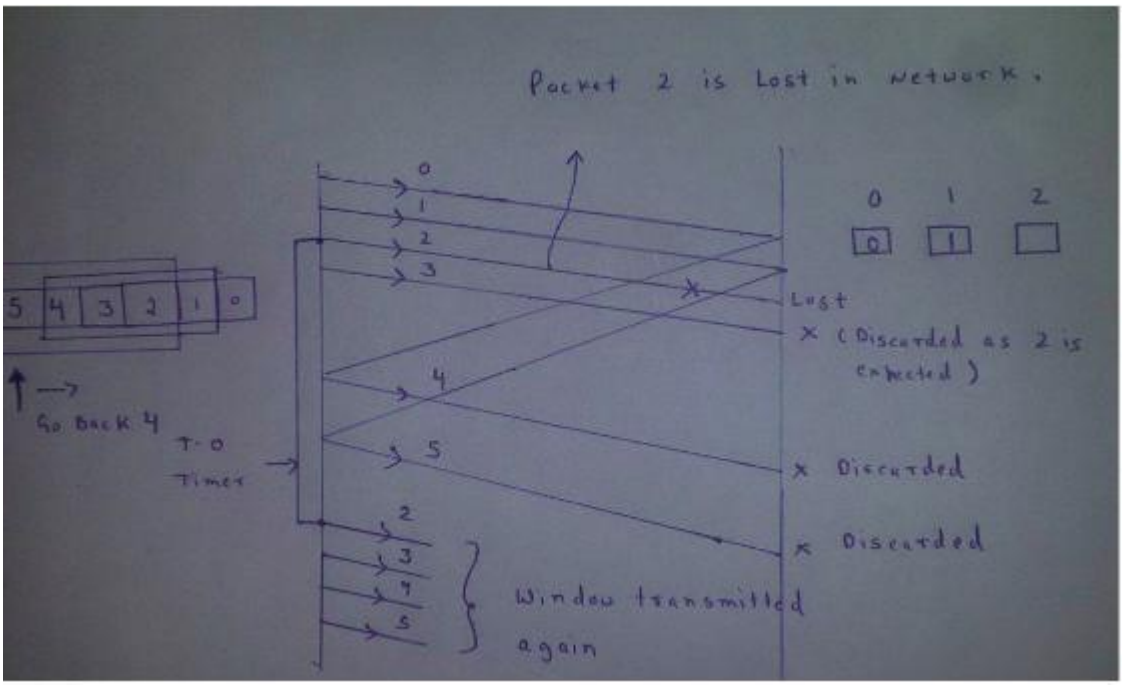
Sender Window Size (WS)
It is N itself. If we say protocol is GB10, then Ws = 10. N should be always greater than 1 in order to implement pipelining. For N = 1, it reduces to Stop and Wait protocol.

Efficiency Of GBN = N/(1+2a) Where a = Tp/Tt

If B is the bandwidth of the channel, then Effective Bandwidth or Throughput = Efficiency * Bandwidth = (N/(1+2a)) * B.

Receiver Window Size (WR)
WR is always 1 in GBN.
Now what exactly happens in GBN, we will explain with a help of example. Consider the diagram given below. We have sender window size of 4. Assume that we have lots of sequence numbers just for the sake of explanation. Now the sender has sent the packets 0, 1, 2 and 3. After acknowledging the packets 0 and 1, receiver is now expecting packet 2 and sender window has also slided to further transmit the packets 4 and 5. Now suppose the packet 2 is lost in the network, Receiver will discard all the packets which sender has transmitted after packet 2 as it is expecting sequence number of 2. On the sender side for every packet send there is a time out timer which will expire for packet number 2. Now from the last transmitted packet 5 senders will go back to the packet number 2 in the current window and transmit all the packets till packet number 5. That's why it is called Go Back N. Go back means sender has to go back N places from the last transmitted packet in the unacknowledged window and not from the point where the packet is lost.

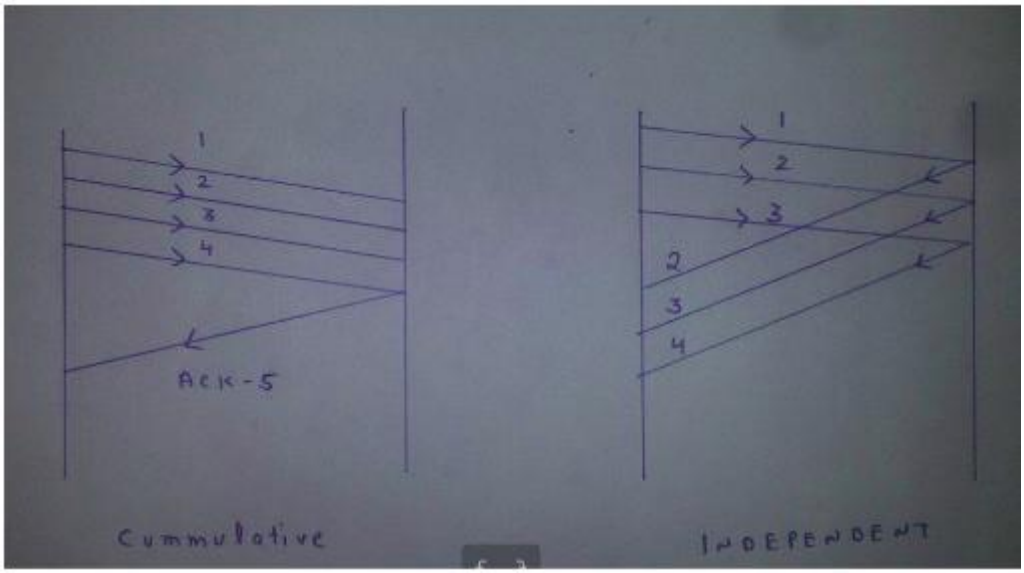




Acknowledgements

There are 2 kinds of acknowledgements namely:

- **Cumulative Ack** – One acknowledgement is used for many packets. Main advantage is traffic is less. Disadvantage is less reliability as if one ack is loss that would mean that all the packets sent are lost.
- **Independent Ack** – If every packet is going to get acknowledgement independently. Reliability is high here but disadvantage is that traffic is also high since for every packet we are receiving independent ack.



GBN uses Cumulative Acknowledgement. At the receiver side, it starts a acknowledgement timer whenever receiver receives any packet which is fixed and when it expires, it is going to send a cumulative Ack for the number of packets received in that interval of timer. If receiver has received N packets, then the Acknowledgement number will be N+1. Important point is Acknowledgement timer will not start after the expiry of first timer but after receiver has received a packet.
Time out timer at the sender side should be greater than Acknowledgement timer.

POINT TO POINT PROTOCOL ON INTERNET:

PPP is most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem.

• This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

1. PPP defines the format of the frame to be exchanged between the devices.

2. It defines link control protocol (LCP) for:-

(a) Establishing the link between two devices.

(b) Maintaining this established link.

(c) Configuring this link.

(d) Terminating this link after the transfer.

3. It defines how network layer data are encapsulated in data link frame.

4. PPP provides error detection.

5. Unlike SLIP that supports only IP, PPP supports multiple protocols.

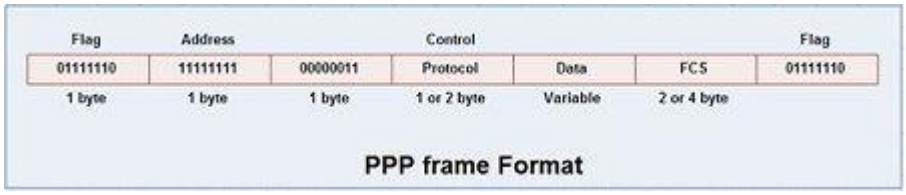
6. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

7. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

8. It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:



PPP frame Format

1. **Flag field**: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

2. **Address field**: This field is of 1 byte and is always 11111111. This address is the broadcast address *i.e.* all the stations accept this frame.

3. **Control field**: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.

4. **Protocol field**: This field specifies the kind of packet in the data field *i.e.* what is being carried in data field.

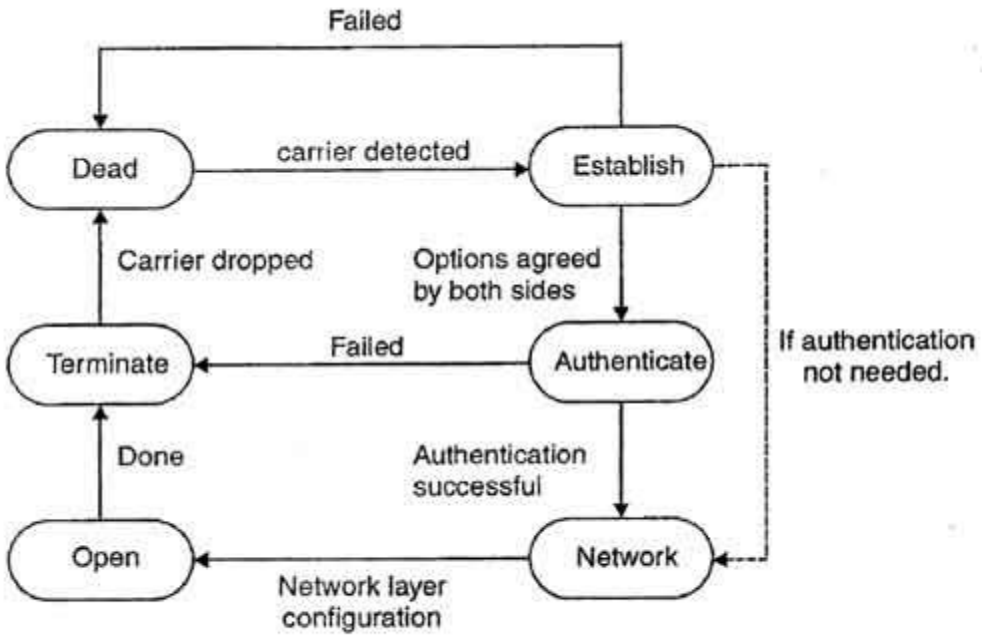
5. **Data field**: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

6. **FCS field**: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

Transition Phases in PPP

The PPP connection goes through different states as shown in fig.

1. **Dead**: In dead phase the link is not used. There is no active carrier and the line is quiet.



Transition phases

2. **Establish**: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase. LCP packets are used for this purpose.

3. **Authenticate**: This phase is optional. The two nodes may decide during the establishment phase, not to skip this phase. However if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

4. **Network**: In network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. This is because PPP supports several protocols at network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.

5. **Open**: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.

6. **Terminate**: In this phase connection is terminated.

Point-to-point protocol Stack

PPP uses several other protocols to establish link, authenticate users and to carry the network layer data.

The various protocols used are:

1. Link Control Protocol

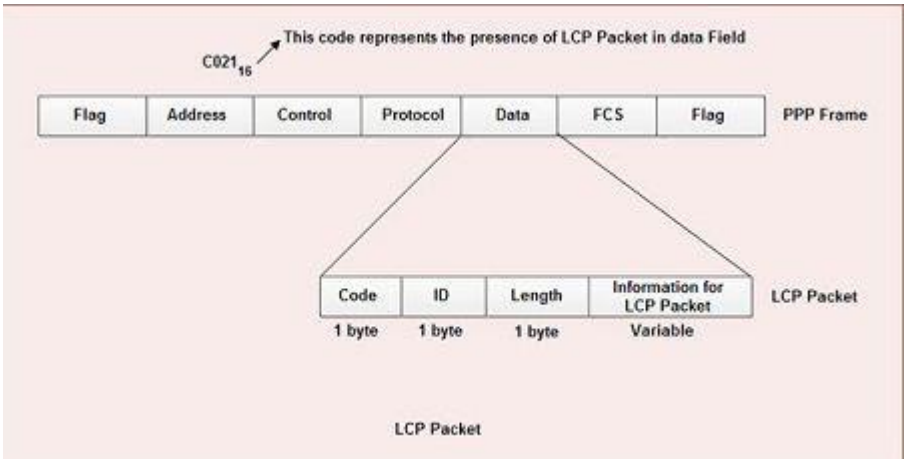
2. Authentication Protocol

3. Network Control Protocol

1. Link Control Protocol

• It is responsible for establishing, maintaining, configuring and terminating the link.

• It provides negotiation mechanism to set options between two endpoints.



• All LCP packets are carried in the data field of the PPP frame.

• The presence of a value $C021_{16}$ in the protocol field of PPP frame indicates that LCP packet is present in the data field.

• The various fields present in LCP packet are:

1. **Code**: 1 byte-specifies the type of LCP packet.

2. I**D**: 1 byte-holds a value used to match a request with the reply.

3. **Length**: 2 byte-specifies the length of entire LCP packet.

4. **Information**: Contains extra information required for some LCP packet.

• There are eleven different type of LCP packets. These are categorized in three groups:

1. **Configuration packet**: These are used to negotiate options between the two ends. For example: configure-request, configure-ack, configure-nak, configure-reject are some configuration packets.

2. **Link termination packets**: These are used to disconnect the link between two end points. For example: terminate-request, terminate-ack, are some link termination packets.

3. **Link monitoring and debugging packets**: These are used to monitor and debug the links. For example: code-reject, protocol-reject, echo-request, echo-reply and discard-request are some link monitoring and debugging packets.

2. Authentication Protocol

Authentication protocols help to validate the identity of a user who needs to access the resources.

There are two authentication protocols:

1. Password Authentication Protocols (PAP)

2. Challenge Handshake Authentication Protocol (CHAP)

1. PAP (Password Authentication Protocol)

This protocol provides two step authentication procedures:

Step 1: User name and password is provided by the user who wants to access a system.

Step 2: The system checks the validity of user name and password and either accepts or denies the connection.

• PAP packets are also carried in the data field of PPP frames.

• The presence of PAP packet is identified by the value $C023_{16}$ in the protocol field of PPP frame.

• There are three PAP packets.

1. **Authenticate-request**: used to send user name & password.

2. **Authenticate-ack**: used by system to allow the access.

3. **Authenticate-nak**: used by system to deny the access.

2. CHAP (Challenge Handshake Authentication Protocol)

• It provides more security than PAP.

• In this method, password is kept secret, it is never sent on-line.

• It is a three-way handshaking authentication protocol:

1. System sends. a challenge packet to the user. This packet contains a value, usually a few bytes.

2. Using a predefined function, a user combines this challenge value with the user password and sends the resultant packet back to the system.

3. System then applies the same function to the password of the user and challenge value and creates a result. If result is same as the result sent in the response packet, access is granted, otherwise, it is denied.

• There are 4 types of CHAP packets:

1. Challenge-used by system to send challenge value.

2. Response-used by the user to return the result of the calculation.

3. Success-used by system to allow access to the system.

4. Failure-used by the system to deny access to the system.

3. Network Control Protocol (NCP)

• After establishing the link and authenticating the user, PPP connects to the network layer. This connection is established by NCP.

• Therefore NCP is a set of control protocols that allow the encapsulation of the data coming from network layer.

• After the network layer configuration is done by one of the NCP protocols, the users can exchange data from the network layer.

• PPP can carry a network layer data packet from protocols defined by the Internet, DECNET, Apple Talk, Novell, OSI, Xerox and so on.

• None of the NCP packets carry networks layer data. They just configure the link at the network layer for the incoming data.

POSSIBLE QUESTIONS

UNIT-III

PART-A (20 MARKS)

(Q.NO 1 TO 20 Online Examination)

PART-B (2 MARKS)

1. What are the responsibilities of Data Link Layer?
2. Define error detection and error correction.
3. What are the error recovery protocols?
4. Define Stop and Wait Protocol.
5. Define Go back and N protocol.
6. What is selective repeat protocol?

PART-C (6 MARKS)

1. Give an account of Error correction and Detections in detail.
2. Explain the concept of cyclic codes error detection and correction.
3. Explain cyclic redundancy check with the help of an example.
4. Elaborate the working of flow control protocols with neat sketches.
5. Illustrate data-link control with proper diagram.
6. Describe the stop and wait ARQ with proper diagram
7. Explain go back n ARQ with neat sketch.
8. Explain Point to Point Protocol on Internet.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CS Batch:2017

Subject: COMPUTER NETWORKS

SubCode: 17CSU303

UNIT III

SL NO	QUESTIONS	OPTION A	OPTION B	OPTION C	OPTION D	ANSWER
1	Transmission errors are usually detected at the……..layer of OSI model	physical	datalink	network	transport	physical
2	Transmission errors are usually corrected at the……..layer of OSI model	network	transport	datalink	physical	transport
3	Datalink layer imposes a ……mechanism to avoid	flow control	error control	access control	none of the above	flow control
4	Error control mechanism of datalink layer is achieved through a ……..added to the end	header	trailer	adress	frames	trailer
5	The datalink layer is responsible for moving……from one hop to next	packets	frames	signals	message	frames
6	In a single_bit error,how many bits in a data unit are changed	one	two	four	five	one
7	In a burst error,how many bits in a data unit are changed	less than 2	2 or more than 2	2	3	2 or more than 2
8	The length of the burst error is measured from ……	first bit to last bit	first corrupted bit to last corrupted	two	three	first corrupted bit to last corrupted
9	Single bit error will least occur in……data transmissions	serial	parallel	synchronous	asynchronous	serial
10	To detect errors or correct errors,we need to send …… with data	address	frames	extra bits	packets	extra bits
11	Which of the following best describes a single bit error	a single bit is inverted	a single bit is inverted per data	a single bit is inverted per	any of the above	a single bit is inverted per data
12	In block coding,we divide our message intp blocks,each of k bits,called	dataword	codeword	integers	none of the above	dataword
13	In block coding,the length of the block is …….	k	r	k+r	k-r	k+r
14	Block coding can detect only ……error	single	burst	multiple	none of the above	single

15	We need ……..redundant bits for error correction than for error detection	less	more	equal	less than or equal to	more
16	The corresponding codeword for the dataword 01 is…..	011	000	101	110	011
17	The hamming distance can easily be found if we apply the …… operation	XOR	OR	AND	NAND	XOR
18	The …… hamming distance is the smallest hamming distance between all	minimum	maximum	equal	none of the above	minimum
19	The hamming distance d(000,111) is …….	1	0	2	3	2
20	To guarantee correction of upto t errors in all cases,the minimum hamming distance in a	d(min)=2t+1	d(min)=2t-1	d(min)=2t	d(min)=t+1	d(min)=2t+1
21	To guarantee correction of upto s errors in all cases,the minimum hamming distance in	d(min)=s-1	d(min)=s+1	d(min)=s	none of the above	d(min)=s+1
22	A simple_parity check code is a single bit error detecting code in which n=…… with	K	K*1	K-1	K+1	K+1
23	The codeword corresponding to the dataword 1111 is	11110	11111	11101	11011	11110
24	A simple_parity check code can detect an ……. Number of errors	odd	even	prime	none of the above	odd
25	The hamming code is a method of ……..	error detection	error correcton	error encapsulation	A and B	error correcton
26	To make the hamming code respond to a burst error of size N,we neeed to make ……	N+1	N-1	N	0	N
27	CRC is used in network such as …….	WAN	LAN and WAN	LAN	MAN	LAN and WAN
28	In CRC there is no error if the remainder at the receiver is……..	equal to the remainder at the	all 0's	non zero	the quotient at the sender	all 0's
29	At the CRC checker,…….means that the dataunit is damaged.	string of 0's	string of 1's	a string of alternating 1's	a non-zero remainder	a non-zero remainder
30	……. Is a regulation of data transmission so that the receiver buffer do not become	flow control	error control	access control	none of the above	flow control
31	……..in the datalink layer separates a message from one source ti a destination or	packets	address	framing	none of the above	framing
32	…….is the process of adding 1 extra byte whenever there is a flag or escape character	byte stuffing	redundancy	bit_stuffing	none of the above	byte stuffing
33	…….is the process of adding 1 extra 0 whenever five consecutive 1's follows a 0 in	byte stuffing	redundancy	bit_stuffing	none of the above	bit_stuffing

34	……in the data link layer is based on automatic repeat request,which is the	error control	flow control	access control	none of the above	error control
35	At any time an error is detected in an exchange specified frames are retransmitted	ARQ	ACK	NAK	SEL	ARQ
36	The datalink layer at the sender side gets data from its……..layer	network	physical	application	transport	network
37	ARQ stands for ……..	acknowledge repeat request	automatic repeat request	automatic repeat	automatic retransmission	automatic repeat request
38	Which of the following is a data link layer function	line discipline	error control	flow control	all the above	all the above
39	In protocols the flow and error control information such as ACK and NAK is	stop and wait	go_back	A and B	piggybacking	piggybacking
40	In stop and wait ARQ ,the sequence of numbers is based on…….	modulo-2-arithmetic	modulo-12-arithmetic	modulo-N-arithmetic	all the above	modulo-2-arithmetic
41	Error correction in …….is done by keeping a copy of the send frames and	stop and wait ARQ	ARQ	ACK	NAQ	stop and wait ARQ
42	In the Go_Back N protocol,the sequence numbers are modulo……..	2^m	2^{m-1}	2^{m+1}	2	2m
43	In sliding window ,the range which is the concern of the sender is called……..	send sliding window	receive sliding window	piggybacking	none of the above	send sliding window
44	Piggypacking is used to improve the efficiency of the ……..protocols.	bidirectional	unidirectional	multidirectional	none of the above	bidirectional
45	The send window can slide …….slots when a valid acknowledgment arrive	one or more	one	two	two or more	one or more
46	The upper sublayer that is responsible for flow and error control is	logical	media access	A and B	all the above	logical
47	The MAC(media access control)sublayer co-ordinates the datalink task within a	LAN	MAN	WAN	LAN and MAN	LAN
48	The lower sublayer that is responsible for multiple access resolution is called	Logical	media access	A and B	all the above	media access
49	In the sliding window method or flow control several frame can be be ……..at a	transit	received	A and B	none of the above	transit
50	The sliding window of the sender expands to the ……..when acknowledgement are	left	middle	right	B and C	right
51	Error detecting codes require ……..nuber of redundant bits.	less	equal	more	less than or equal to	more
52	The datalink layer transforms the ……,a raw transmission facility to a	datalink	physical	network	transport	physical

53	Datalink layer divided into …… functionality oriented sublayer.	one	zero	two	three	two
54	The send window in Go_Back N maximum size can be ……	2^m	2^{m+1}	2	2^{m-1}	2m-1
55	In stop and wait ARQ and Go_Back_N ARQ,the size of the send window	0	3	1	2	1
56	The relationship between m and n in hamming code is ……	n=2m-1	n=m	n=m-1	n=2m+1	n=2m-1
57	A simple parity_check code is a single_bit error detecting code in which n=k+1 with	3	1	0	2	2
58	……..mechanism of datalink layer is achieved through added to the trailer added	ARQ	ARC	Error control	Flow control	Error control
59	In ……,we divide our message into blocks	convolution coding	block coding	linear coding	A and C	block coding
60	The …….layer at the sender site gets data from its network layer.	physical	datalink	application	transport	datalink
61	In the …….protocol,the sequence numbers are modulo 2^m	Go_Back N	Simplest	Stop and wait	all the above	Go_Back N
62	_____ and encapsulates them into frames for transmission.	network layer	physical layer	transport layer	application layer	network layer
63	Which one of the following task is not done by data link layer?	framing	error control	flow control	channel coding	channel coding
64	CRC stands for_____	cyclic redundancy check	code repeat check	redundancy check	cyclic repeat check	cyclic redundancy check

UNIT IV

SYLLABUS

Multiple Access Protocol and Networks: CSMA/CD protocols; Ethernet LANS; connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router and gateways; **Networks Layer Functions and Protocols**: Routing; routing algorithms; network layer protocol of Internet- IP protocol, Internet control protocols.

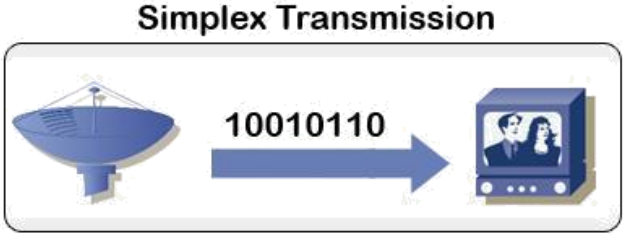
Multiple Access Protocol and Networks

CSMA/CD protocols

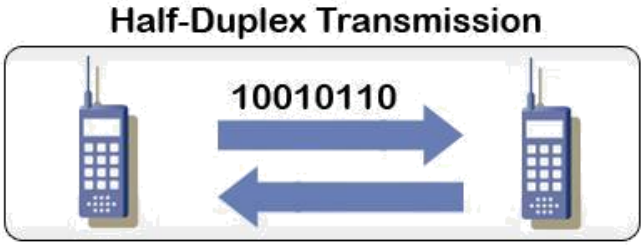
Carrier Sense Multiple Access/Collision Detect (CSMA/CD) is the protocol for carrier transmission access in Ethernet networks. On Ethernet, any device can try to send a frame at any time. Each device senses whether the line is idle and therefore available to be used. If it is, the device begins to transmit its first frame. If another device has tried to send at the same time, a collision is said to occur and the frames are discarded. Each device then waits a random amount of time and retries until successful in getting its transmission sent.

Simplex, Half-Duplex, and Full-Duplex Operation

Before we get into CSMA/CD in particular, we need to review who is vulnerable to collisions. Some types of data transmission are virtually invulnerable to collisions- while others are somewhat lacking in this defense.

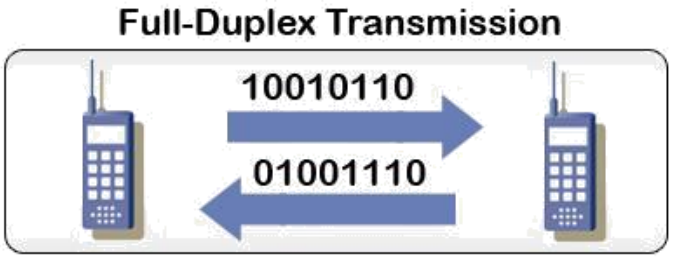


Simplex transmission is, well- simple. It is a connection in which data will always flow in one direction, and will not suffer collisions as a result. Since data flows in one direction, this is poor for mutual communication- so we likely won't see simplex operation in everyday networks. You do, however, come into contact with simplex transmissions more than you think. Your cable company sends video in a one-way data transmission to your television set.



Half-duplex transmission allows both devices to communicate. However, note that in the above diagram that data is only being sent from one device at a time. Half-Duplex operation is where almost all collisions will take place: since each device may not know the other is transmitting. If this occurs, the data collides over the line and the data is corrupted.

For a practical example, we could make reference to phones. If you try to call someone who is using the phone line, you will more than likely get a busy tone and not get a connection to the person. This is the same principle; although with computers we will get a destructive loss in data, as compared to a busy tone the phone would provide.



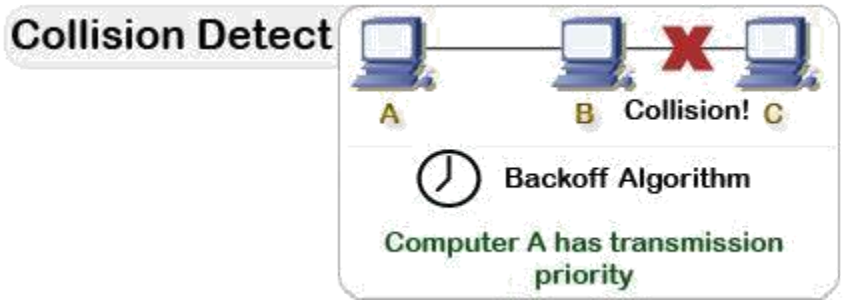
Full-duplex operation is much like half-duplex, only devices can send and receive data at the same time. Virtually no collisions take place on a full-duplex transmission. Perhaps a bigger benefit is the increase in overall throughput- since we are sending and receiving on two different channels, we just theoretically doubled our data transfer rate.

CSMA/CD: What's in a Name?

First let's take a look at what CS (carrier sense) is in CSMA/CD. Carrier sense is the ability of a network interface card (NIC) to check the network for any communication. Obviously if there is data being transmitted over the network, the NIC should not attempt to transmit data. If there is no traffic on the network, the NIC will then attempt to transmit the data. However, we can't be sure that data isn't in the process of being sent by other computers- so this is one possible beginning of a collision.

The MA (multiple access) part of CSMA/CD tells us that there will be multiple devices using the same network. This, of course, means collisions are more than possible. It also tells us that in the ring topology, no collision will ever occur since only one computer uses the media at a given time. Lastly, you can bet that even if you are using wireless, you'll be victim to collisions since multiple computers are using the same medium.

The CD (collision detect) part of CSMA/CD states that we need a method for detecting a collision. After all, we need to tell other computers to hold off on transmissions until the problem is sorted. Collisions can be spotted since they are generally higher in signal amplitude than normal signals. If we do indeed spot a collision, a jamming signal is sent to all computers and a back-off algorithm is observed. This algorithm simply tells computers not to transmit new data for a random amount of time. When transmission is again ready, the devices involved in the collision do not have priority.



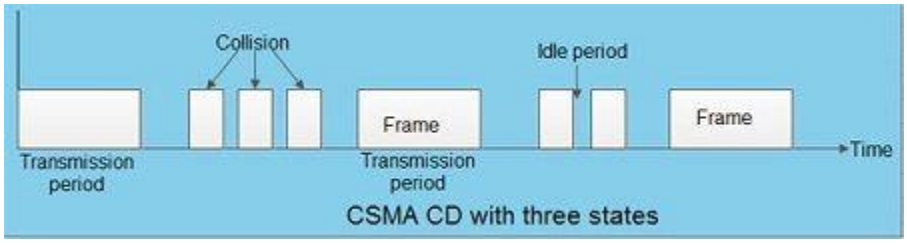
From the above information, we can deduce two things about CSMA/CD. First, it is a nondeterministic approach- meaning first come first served. It's an all out brawl for who gets to transmit data- as compared to the deterministic approach of the ring topology.

The Collision Detection and Solution Process

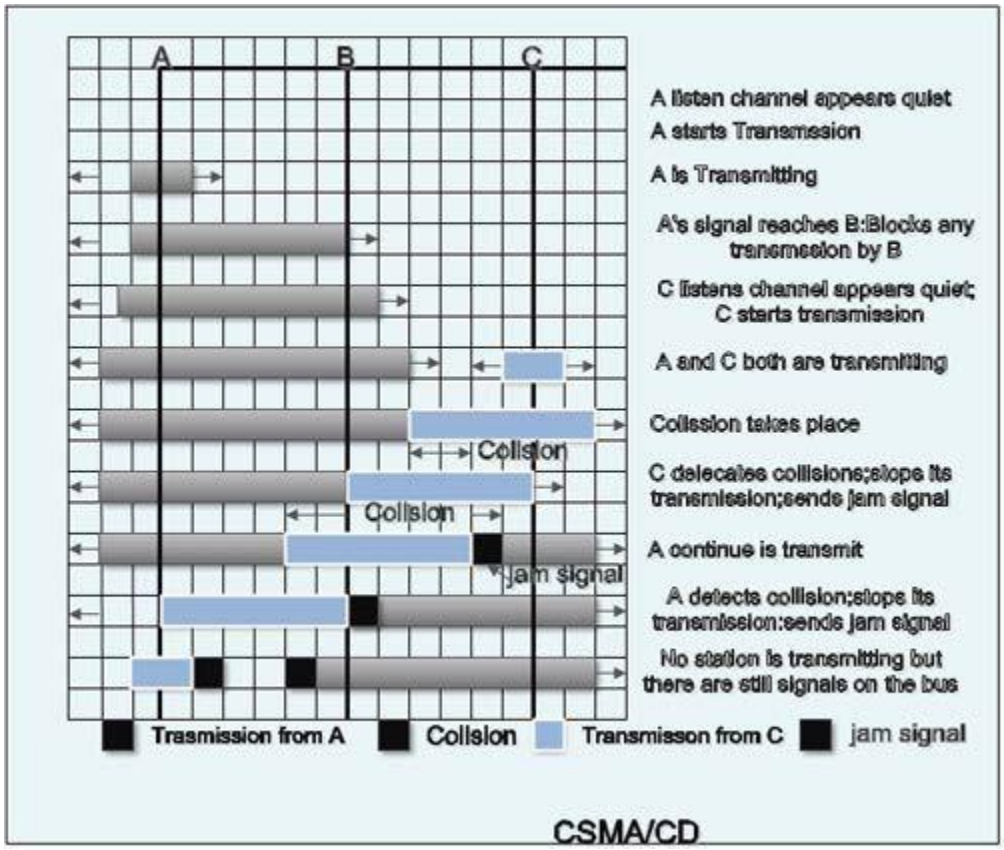
- **1 –** A collision is detected.
- **2 –** Devices involved in the collision keep transmitting for a short period of time, to make sure all devices on the network see the collision (also referred to as the jamming signal)
- **3 –** Each device sees the jamming signal, and invokes the back-off algorithm. Each device will have a random timer that determines when it can transmit again.
- **4 –** When the back-off timer expires, devices are free to transmit data again. Devices involved in the collision earlier do not have priority to transmit data.

To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA / CD): CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA. If the channel is busy, the station waits. it listens at the same time on communication media to ensure that there is no collision with a packet sent by another station. In a collision, the issuer immediately cancel the sending of the package. This allows to limit the duration of collisions: we do not waste time to send a packet complete if it detects a collision. After a collision, the transmitter waits again silence and again, he continued his hold for a random number; but this time the random number is nearly double the previous one: it is this called back-off (that is to say, the "decline") exponential. In fact, the window collision is simply doubled (unless it has already reached a maximum). From a packet is transmitted successfully, the window will return to its original size.

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

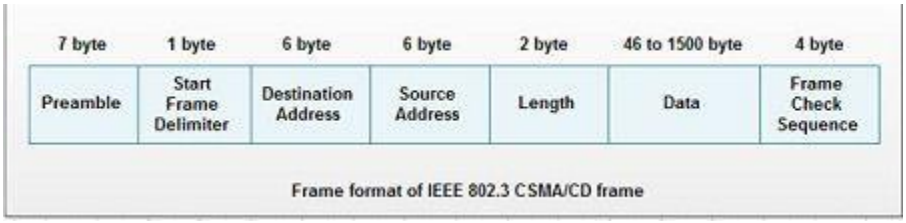


The entire scheme of CSMA/CD is depicted in the fig.



Frame format of CSMA/CD

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



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

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

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

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

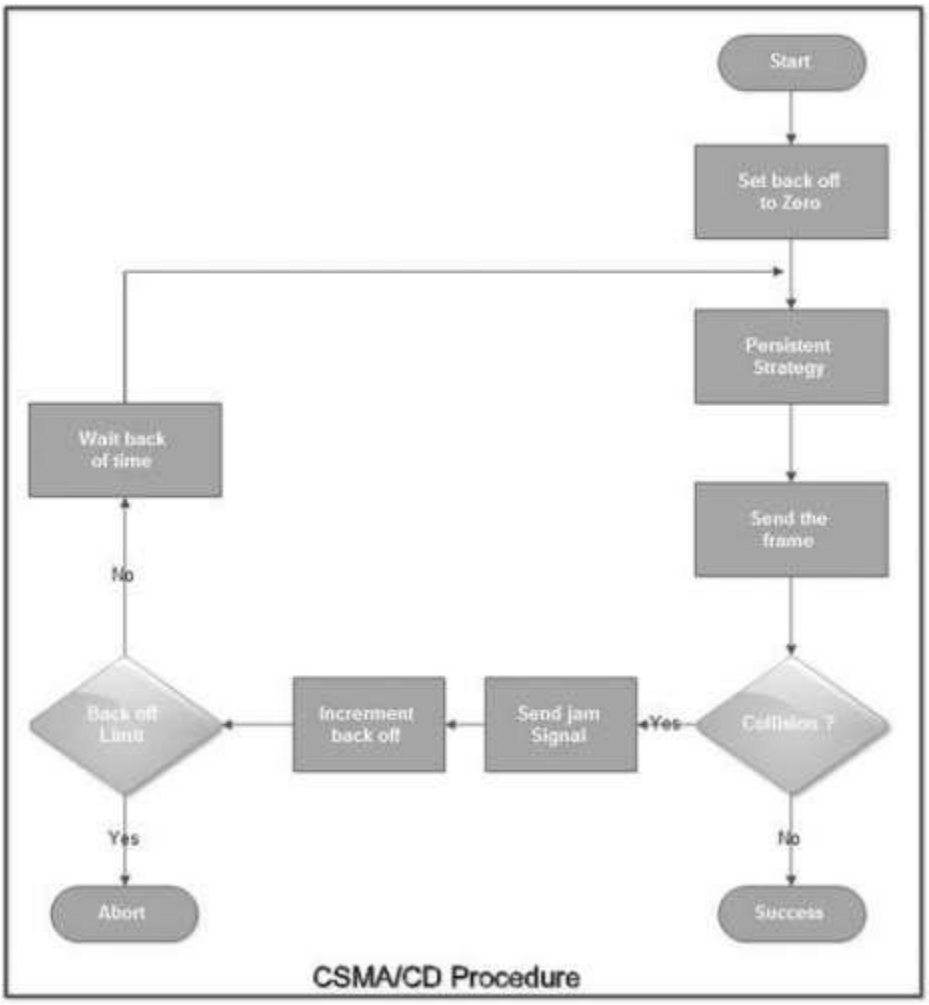
5. **Length**: This two byte field specifies the length or number of bytes in data field.

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

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

CSMA/CD Procedure:

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



CSMA/CD Procedure

Explanation:

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

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

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

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

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

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

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

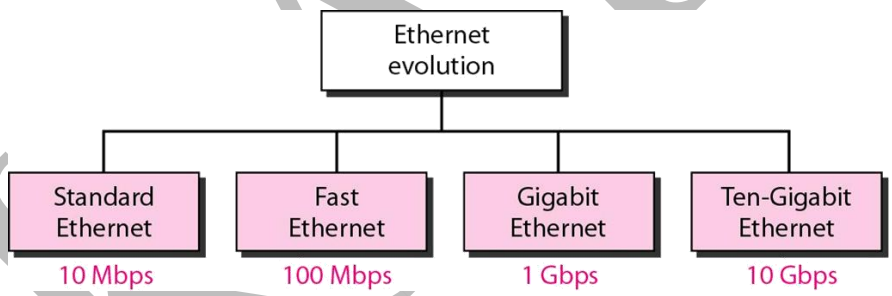
• *CSMA/CD* is an important protocol. IEEE 802.3 (Ethernet) is an example of *CSMNCD*. It is an international standard.

• The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision the receiver may not have copied the frame correctly.

Ethernet LANS

Ethernet

It is a way of connecting computers together in a local area network or LAN. It has been the most widely used method of linking computers together in LANs since the 1990s. The basic idea of its design is that multiple computers have access to it and can send data at any time.



Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit

Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Fast Ethernet

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks will support even higher data transfer speeds.

Gigabit Ethernet

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as “gigabit-Ethernet-over-copper” or 1000Base-T, GigE is a version of Ethernet that runs at speeds

10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

From the data link layer of the OSI model upward, the look and implementation of Gigabit Ethernet is identical to that of Ethernet. The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

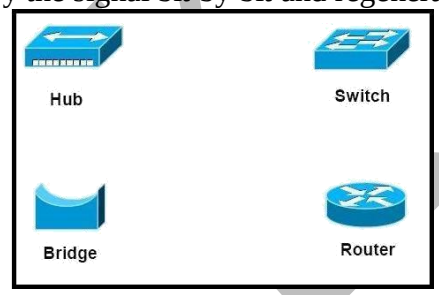
10 Gigabit Ethernet

10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined

Connecting Lan And Back-Bone Networks

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.



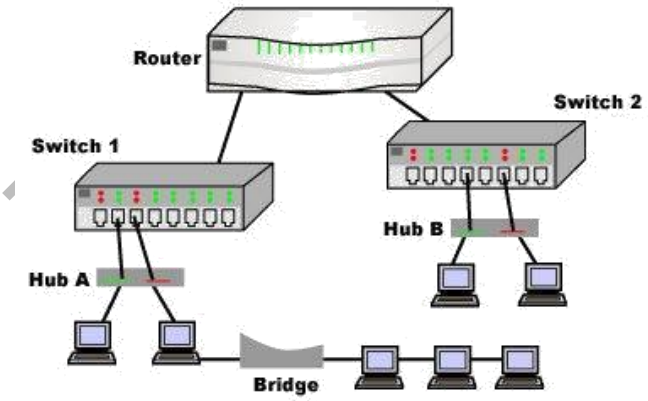
2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected

devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

4. **Switch** – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domainremains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

NETWORKS LAYER FUNCTIONS AND PROTOCOLS

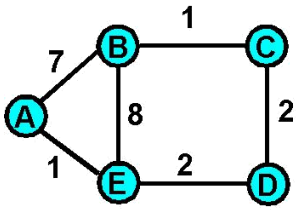
Routing information is obtained in the two following ways:

- Static routing
- Dynamic routing

Static routing: This is a function of IP and it requires routing tables to be manually built and manually updated. Because the routing tables are static; static routers do not inform each other in the event of a route change, nor do they exchange routing information with dynamic routers.

Dynamic Routing

•Distributed Routing:
Dynamic routing
Changing topology of the network
Need to recomputed route continuously



E

D ( )		cost to destination via A	B	D
destinat.	A	1	14	5
	B	7	8	5
	C	6	9	4
	D	4	11	2

A **Routing Algorithm** is a method for determining the routing of packets in a node. For each node of a network, the algorithm determines a routing table, which in each destination, matches an output line. The algorithm should lead to a consistent routing, that is to say without loop. This means that you should not route a packet a node to another node that could send back the package.

There are three main types of routing algorithms:

• Distance Vector (distance-vector routing);

• To link state (link state routing);

• Path to vector (path-vector routing).

Distance vector routing algorithms require that each node exchanges information between neighbors, that is to say between nodes directly connected. Therefore, each node can keep updated a table by adding information on all its neighbors. This table shows the distance is each node and each network to be reached. First to be implemented in the Arpanet, this technique quickly becomes cumbersome when the number of nodes increases since we must carry a lot of information node to node. RIP (Routing Information Protocol) is the best example of a protocol using distance vector.

In this type of algorithm, each router broadcasts to its neighbors a vector that lists each network it can reach the metric associated with, that is to say the number of hops. Each router can therefore build a routing table with information received from its neighbors but has no idea of the identity of routers that are on the selected route. Therefore, the use of this solution poses numerous problems for external routing protocols. Indeed, it is assumed that all routers use the same metric, which may not be the case between autonomous systems. Furthermore, an autonomous system can have special reasons to behave differently from another autonomous system. In particular, if an autonomous system needs to determine how else autonomous system will pass its messages, e.g. for security reasons, he can not know.

The algorithms link state had initially intended to overcome the shortcomings of distance vector routing. When a router is initialized, it must define the cost of each of its links connected to another node. The node then broadcasts the information to all nodes in the autonomous system, and therefore not only to its neighbors. From all this information, the nodes can perform their calculation for obtaining a routing table indicating the cost of achieving each destination. When a router receives information that alters its routing table, it notifies all intervening routers in its configuration. As each node has the network topology and costs of each link, routing can be seen as central in each node. OSPF (Open Shortest Path First) implements this technique, which is the second generation of Internet protocols.

The algorithms link state solves the problems mentioned above for external routing but raise other. The various autonomous systems may have different metrics and specific restrictions, so it is not possible to achieve a coherent route. The dissemination of all information necessary for all the autonomous systems can also quickly become unmanageable.

The purpose of the path-vector algorithms is to overcome the shortcomings of the first two categories by providing metrics and seeking to know which network can be reached by any node and autonomous systems which must be crossed for it. This approach is very different from that distance-vector because the paths vectors do not take into account the distances or costs. In addition, the fact that each list routing information all autonomous systems that must be traversed to reach the destination router, the path vector approach is much more directed towards the external routing systems. BGP (Border Gateway Protocol) belongs to this category.

RIP (Routing Information Protocol)

RIP is the most widely used protocol in the TCP / IP environment to route packets between the gateways of the Internet. It is a protocol IGP (Interior Gateway Protocol), which uses an algorithm to find the shortest path.

By the way, refers to the number of nodes crossed, which must be between 1 and 15. The value 16 indicates impossibility. In other words, if the path to get from one point to another of the Internet is above 15, the connection can not be established. RIP messages to establish the routing tables are sent approximately every 30 seconds. If a RIP message does not reach its neighbor after three minutes, the latter considers that the link is no longer valid; the number of links is greater than 15. RIP is based on a periodic distribution of states network from a router to its neighbors. The release includes a RIP2 routing subnet, message authentication, multipoint transmission, etc.

OSPF (Open Shortest Path First)

OSPF is part of the second generation of routing protocols. Much more complex than RIP, but at higher performance rates, it uses a distributed database that keeps track of the link state. This

information forms a description of the network topology and the status of nodes, which defines the routing algorithm by calculating the shortest paths.

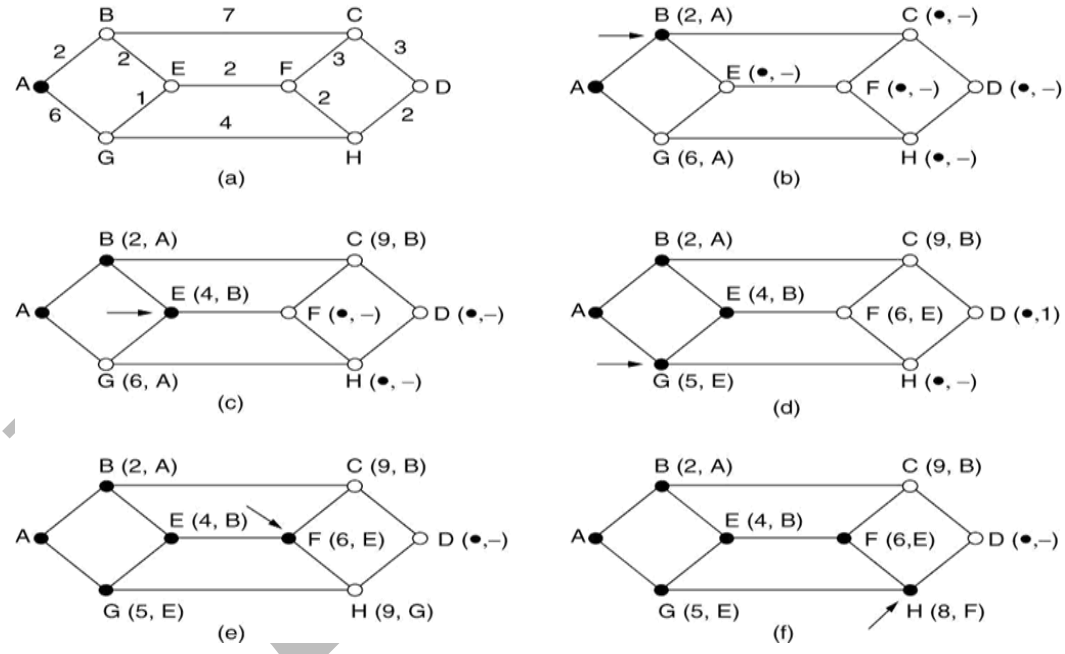
The algorithm allows OSPF, from a node, to calculate the shortest path, with the constraints specified in the content associated with each link. OSPF routers communicate with each other via the OSPF protocol, placed on top of IP. Now look at this protocol a bit more detail.

Dijkstra's Algorithm Background

The algorithm proceeds by assigning to all nodes a *label* which is either *temporary or permanent.* A temporary label represents an upper bound on the shortest distance from the home node to that node; while a permanent label is the actual shortest distance from the home node to that node.

We also record information about predecessor nodes so that we may find our way along the path from the home node to the final node of the network.

The paths traced out by the shortest route algorithm forms what is known as a tree structure and this is a very important concept in communications and transportation theory.



Distance Vector Routing Algorithms

•Distance Vector Routing:
•(Distributed Bellman Ford, Fulkerson)
Each router maintain a table:

destination, estimated cost, link, hop count, time delay in ms, queue length, … Updated by exchanging information between router -ICMP

Distance Vector Routing Protocol (DVRP) is one of two major routing protocols for communications methods that use data packets sent over Internet Protocol (IP). DVRP requires routing hardware to report the distances of various nodes within a network or IP topology in order to determine the best and most efficient routes for data packets.

In contrast to DVRP and the other predominant type of routing protocol, which is called Link State Routing Protocol, the DVRP method tends to contemplate only two factors: distance and vector. Distance is commonly defined as the number of steps, or hosts, a message must go through to get to its destination. The vector describes the trajectory of the message over a given set of network nodes. Link state protocols use a slightly more sophisticated method to look at how fast or efficient a given point in the vector is in order to run messages through faster network points instead of slower ones.

DVRP and link state protocols are useful in Voice over IP and other types of communications that use routed data packets. As the IP infrastructure becomes more valuable to telecom and global markets in general, it's likely that future advances will continue to boost the capacity of IP traffic with improved methods and hardware.

INTERNET PROTOCOL

- IP stands for Internet Protocol
- IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
- IP by itself is something like the postal system.
- It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient.
- TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

IP services

Delivery service of IP is minimal.

IP provides an unreliable connectionless best effort service

- Unreliable : IP doesn't make an attempt to recover lost packets
- Connectionless : Each packet is handled independently
- Best Effort : IP doesn't make guarantees on the service (No through output , No delay guarantee…)

- IP supports the following services
  - One-to-one (unicast)
  - One-to-all (broadcast)
  - One-to-several (multicast)

IP Address

- What is an IP address…?
  - An IP address is a unique global address for a network interface

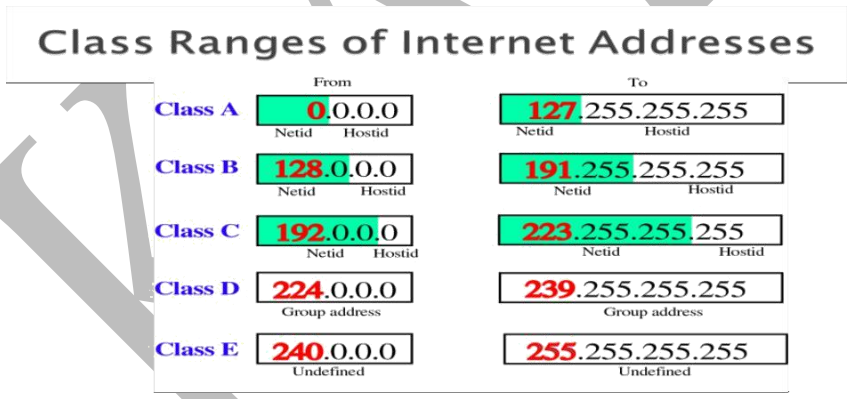
- is a **32 bit long** identifier

10000000 **10001111** **10001001** **10010000**

1st Byte 2nd Byte 3rd Byte 4th Byte

= 128 **= 143** **= 137** **= 144**

128.143.137.144



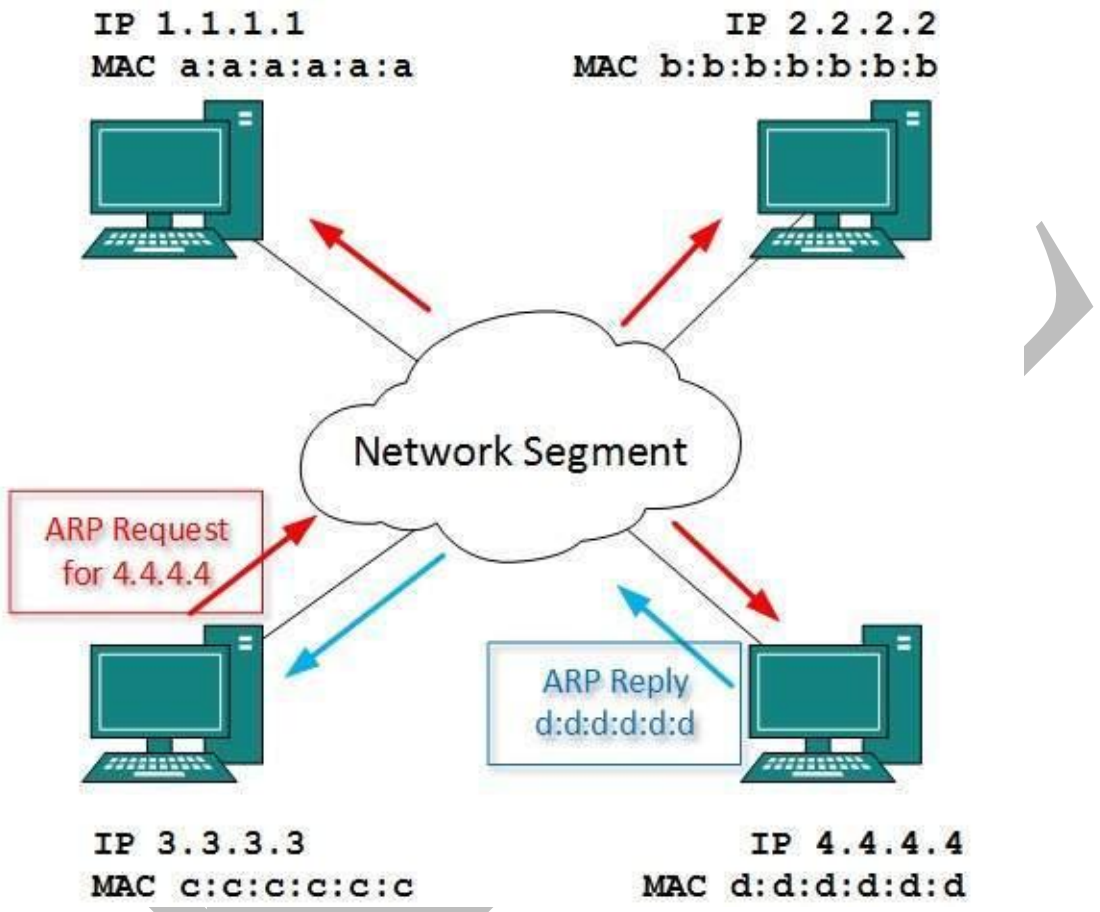
NETWORK LAYER PROTOCOL

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

Address Resolution Protocol(ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.



To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, "Who has this IP address?" Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol (ICMP)

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for host addressing
- **Class B** - it uses first two octets for network addresses and last two for host addressing
- **Class C** - it uses first three octets for network addresses and last one for host addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6.

INTERNET PROTOCOL (IP):

Internet Protocol (IP) is the principal set (or communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to as TCP/IP). Messages are exchanged as datagrams, also known as data packets or just packets.

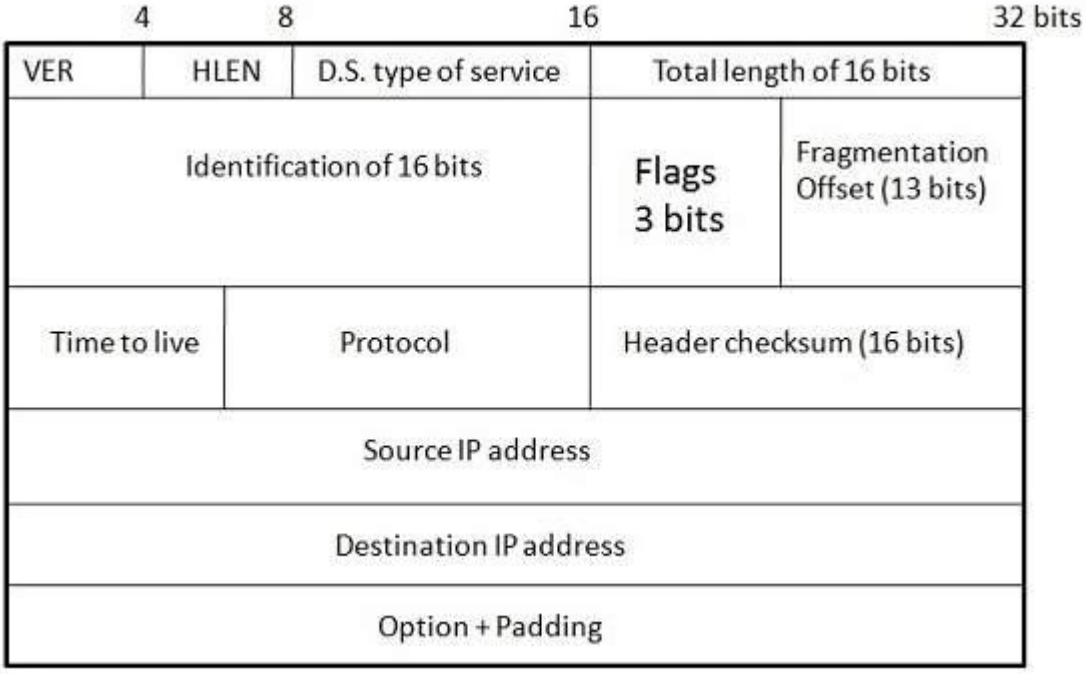
IP is the primary protocol in the Internet Layer of the Internet Protocol Suite, which is a set of communications protocols consisting of four abstraction layers: link layer (lowest), Internet layer, transport layer and application layer (highest).

The main purpose and task of IP is the delivery of datagrams from the source host (source computer) to the destination host (receiving computer) based on their addresses. To achieve this, IP includes methods and structures for putting tags (address information, which is part of metadata) within datagrams. The process of putting these tags on datagrams is called encapsulation.

Internet Protocol is **connectionless** and **unreliable** protocol. It ensures no guarantee of successfully transmission of data.

In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Internet protocol transmits the data in form of a datagram as shown in the following diagram:



Points to remember:

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

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

ICMPv4

- There are some occasions when IP cannot deliver the packet to the destination host. This happens if TTL gets expired and route to the specified destination address is missing from the routing table due to insufficient buffer space of gateway for passing a specific packet.
- If router is unable to forward a packet for some reasons, the router sends an error message back to the source to report the problem.
- The ICMP handles the error and other control messages.
- The ICMP messages are encapsulated by IP packets.

- The value of the protocol field in the IP datagram is '1' to indicate that the IP data is an ICMP message.

There are two types of Messages:

1. Error- reporting messages
The error -reporting message reports a problems that a router or a host (destination) may encounter, while processing an IP packet.

2. Query messages
The query messages which occur in pairs, help a host or a network manager to get specific information from a router or another host.

For example: Nodes can discover their neighbors. Also, a host can discover and learn about routers on their network. Routers can help a node to redirect its messages.

ICMPv6

- It is an integral part of IPv6 and very useful in error reporting, diagnostic functions, neighbour discovery and a framework for extensions to implement future Internet Protocol aspects.
- ICMPv6 is defined in RFC 44443.

Messages are classified in two types:
1. Error messages
2. Information messages.

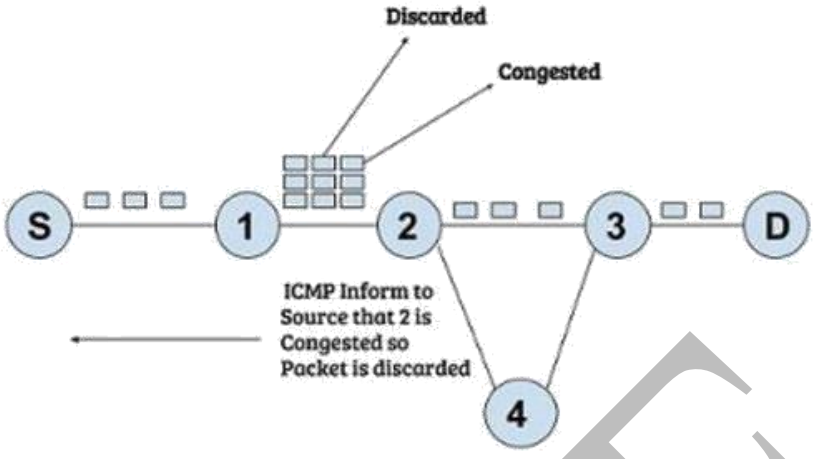
- ICMPv6 messages are transported by IPv6 packets in which the IPv6 Next header value for ICMPv6 is set to 58.

ICMP
Since IP does not have a inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.

e.g. the requested service is not available or that a host or router could not be reached.

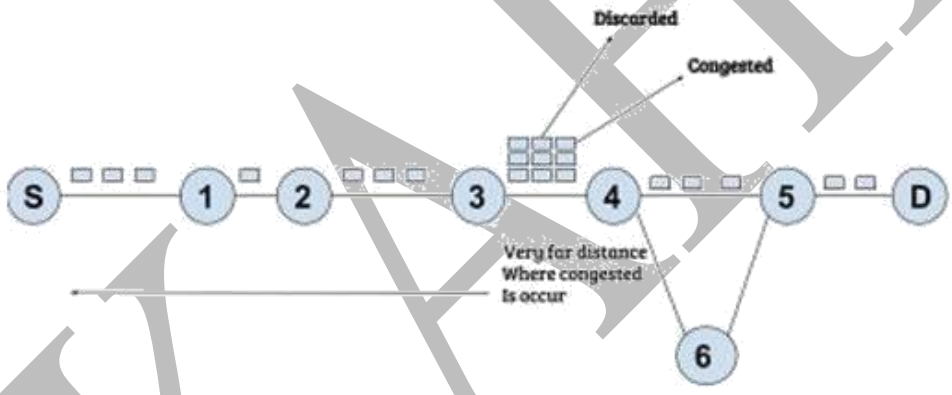
Source quench message :

Source quench message is request to decrease traffic rate for messages sending to the host(destination). Or we can say, when receiving host detects that rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.



ICMP will take source IP from the discarded packet and informs to source by sending source quench message.

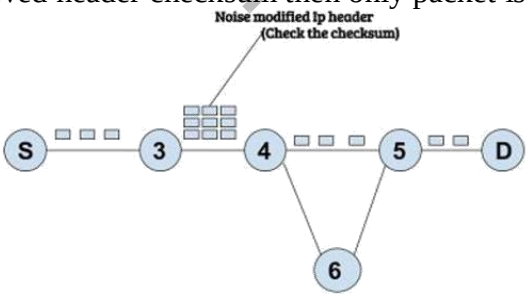
Then source will reduce the speed of transmission so that router will free for congestion.



When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.

Parameter problem :

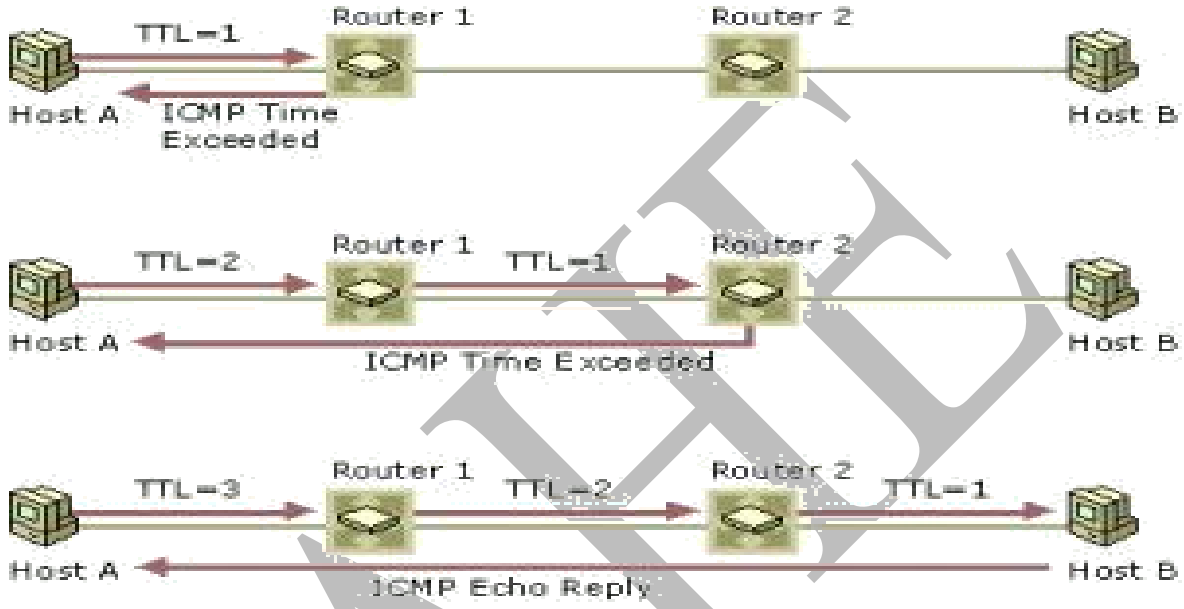
Whenever packets come to the router then calculated header checksum should be equal to recieved header checksum then only packet is accepted by the router.



If there is mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and informs to source by sending parameter problem message.

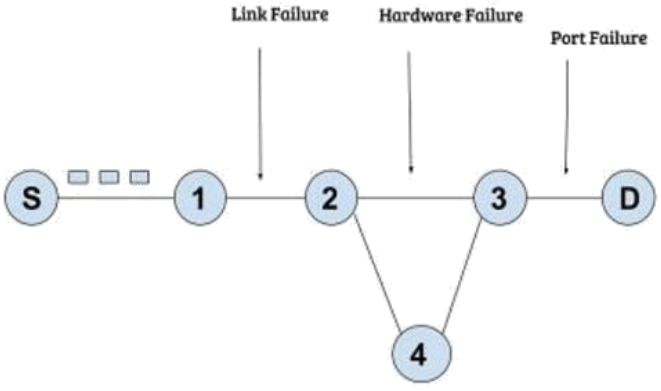
Time exceeded message :



When some fragments are lost in a network then the holding fragment by the router will be droped then ICMP will take source IP from discarded packet and informs to the source, of discarded datagram due to time to live field reaches to zero, by sending time exceeded message.

Destination un-reachable :

Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



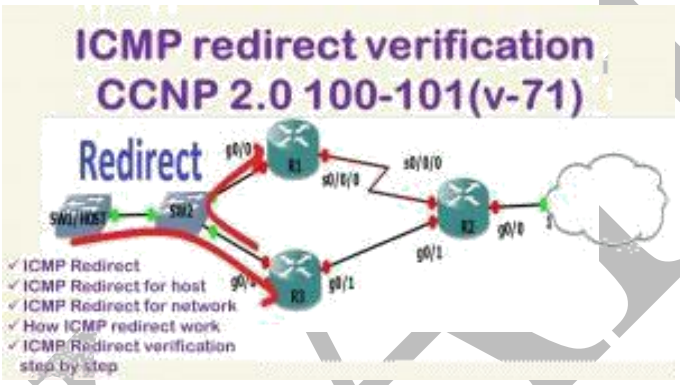
There is no necessary condition that only router give the ICMP error message some time destination host send ICMP error message when any type of failure (link failure, hardware failure, port failure etc) happen in the network.

Redirection message :

Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route).

Ex. If host tries to send data through a router R1 and R1 sends data on a router R2 and there is a direct way from host to R2. Then R1 will send a redirect message to inform the host that there is a best way to the destination directly through R2 available. The host then sends data packets for the destination directly to R2.

The router R2 will send the original datagram to the intended destination. But if datagram contains routing information then this message will not be sent even if a better route is available as redirects should only be sent by gateways and should not be sent by Internet hosts.



Whenever a packet is forwarded in a wrong direction later it is re-directed in a current direction then ICMP will send re-directed message.

POSSIBLE QUESTIONS

PART A – Online Multiple Choice Questions

PART B – 2 Mark Questions

1. Define ICMP?
2. What are the various types of connecting devices?
3. What do you mean by Backbone networks?
4. What do you mean by ARP?
5. What is Unicast & Multicast communication?
6. Define Routing.

PART C – 8 Mark Questions

1. Describe CSMA/CD protocols.
2. What is Routing? List and explain routing algorithms in network layer.
3. Explain: repeaters, hubs, switches with appropriate diagram.
4. Discuss in detail about error and flow control
5. Discuss IP Protocol in detail.
6. Write in detail about Network layer protocols with neat diagram.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Class: II BSC CS Batch:2017
Subject: COMPUTER NETWORKS
SubCode: 17CSU303
UNIT IV

S.NO	QUESTION	CHOICE1	CHOICE2	CHOICE3	CHOICE4	ANSWER
1	CSMA/CD stands for _____	Carrier Sense Multiple Access/Collision Detect	Carrier Sense Mono Access/Collision Detect	Control State Multiple Access/Collision Detect	Carrier Sense Multiple Access/Control Data	Carrier Sense Multiple Access/Collision Detect
2	_____ is the protocol for carrier transmission access in Ethernet networks	CSMA/CD	TCP	IP	FTP	CSMA/CD
3	Internet at the network layer is a_____network.	packet-switched	LAN	connection	connetionless	packet-switched
4	Internet has chosen the datagram approach to_____in network layer	routers	packets	switching	protocol	protocol
5	Internet is made of so many_____networks.	homogenous	hetrogeneous	MAN	multipoint	hetrogeneous
6	Communication at network layer in the internet is_____.	connectionless	point-to-point	connection oriented	packet-switched	connectionless
7	What is the abbrevation for IPV4_____.	Inter Protocol Versus 4	Inter Position Version 4	Internet protocol version 4	Internet Position Versus 4	Internet protocol version 4
8	IPV4 provides the term 'best-effort' means that_____.	no error control	error control	error detection	datagram	no error control
9	Packets in the IPV4 layer are called_____.	frames	datagroup	switching	datagrams	datagrams
10	A datagram is a variable length packet consisting of_____parts.	one	six	two	three	two
11	The total length field defines the total length of the datagram including_____.	footer	header	flags	frames	header
12	Abbravation for MTU_____.	Minimum Transfer Unit	Maximum Transfer Unit	Maximum Travel Unit	Minimum Travel Unit	Maximum Transfer Unit
13	_____in the IPV4 packet covers only header,not the data	Check subtract	Check sum	options	Check product	Check sum

14	Options can be used for network testings and_____.	checking	packets	types	debugging	debugging
15	_____can only used as the last option.	end-of-option	first-of-option	options	no options	end-of-option
16	Record route can list up to_____router address.	fifteen	sixty	nine	ten	nine
17	_____route has less rigid.	loose source	strict source	no route	record	loose source
18	_____is expressed in millisecond,from midnight.	time stand	time stamp	time shot	all the above	time stamp
19	IPv4 also known as_____.	IPNg	IPNG	ipNG	Ipng	Ipng
20	The adoption of IPv6 has been_____.	fast	slow	neuter	quick	slow
21	An IPv6 address is_____bits long.	128	126	125	127	128
22	IPv6 has_____options to allow for additional functionalities.	old	first	new	last	new
23	A_____ is basically a multiport repeater	hub	Repeater	gateway	router	hub
24	Base header with_____fields.	eight	ten	five	none of these	eight
25	The 4bit field defines the_____number of the IP.	versus	header	.footer	version	version
26	A repeater operates at the _____ layer	physical	datalink	application	transport	physical
27	Source and destination of the packet are located on the same physical network called_____.	Indirect delivery	Inward delivery	Direct delivery	Outward delivery	Direct delivery
28	One technique to reduce the content of a routing table is_____.	before-hop	next-hop	first hop	last hop	next-hop
29	The Routing table holds only the address of the next hop_____.	next hop	route method	network method	host method	route method
30	A second technique to reduce the routing table_____.	next hop	default	forward	network specific	network specific
31	All hosts connected to the same network as one single entity_____.	route	next-hop	host specific	d.network specific	host specific
32	In classless addressing,atleast_____columns in a routing table.	5	6	3	4	4
33	In an address aggregation,the network for each organization is_____.	independent	dependent	department	none of these	independent

34	The routing table can be either_____.	static	static and dynamic	static or dynamic	all the above	static or dynamic
35	A static routing table can be used in a_____internet.	big	small	multi	LAN	small
36	Dynamic routing protocols such as_____.	RIP	OSPF	BGP	all the above	all the above
37	A bridge operates at _____layer	data link	physical	application	network	data link
38	_____ is network diagnostic and error reporting protocol	ICMP	FTP	UDP	HTTP	ICMP
39	_____is a device like a switch that routes data packets based on their IP addresses.	router	hub	repeater	bridge	router
40	Routing inside an autonomous system____	Intra	Inter	Inside	all the above	Inside
41	Abbrevation for BGP_____.	Border Gateway Process	Bit Gateway Process	Border Gateway Protocol	Byte Gateway Protocol	Border Gateway Protocol
42	A node sends its routing table,at every_____in a periodic update.	33s	30s	31s	35s	30s
43	_____algorithm creates a shortest path tree from a graph.	data	dakstra	define	dijkstra	dijkstra
44	An area is a collection of_____.	networks	hosts	route	all the above	all the above
45	_____link is a network and is connected to only one router.	stub	point-to-point	transient	none of these	stub
46	Multicasting of the relationship is_____.	one-to-one	many-to-one	one-to-many	many-to-many	one-to-many
47	_____layer is responsible for process-to-process delivery.	transport	physical	application	network	transport
48	Internet has decided to use universal port numbers for severs called_____.	well-unknown port	well-known port	well-known protocol	well-unknown process	well-known port
49	IANA has divided the port numbers into_____ranges.	six	four	five	three	three
50	_____a connection,is first established between the sender and receiver.	connection-oriented	connectionless	token	dialog	connection-oriented
51	UDP is called_____.	connection-oriented	check point	token	connetionless	connetionless
52	UDP length = IP length - _____.	IP length	IP breadth	IP header's length	IP header's breadth	IP header's length

53	UDP is a suitable transport protocol for_____.	unicasting	multicasting	nocasting	none of these	multicasting
54	TCP groups a number of bytes together into a packet called_____.	segment	encapsulation	datagram	data binding	segment
55	The acknowledgement number is _____.	natural	whole	integers	cumulative	cumulative
56	_____ flag is used to terminate the connection.	TER	FIN	URG	PSH	FIN
57	_____ protocol is used to remote procedure call.	DNS	PRC	RPC	RPCC	RPC
58	An ACK segment,if carrying _____data consumes no sequence number.	no	2	3	5	no
59	_____, as the name suggests, is a passage to connect two networks together that may work upon different networking models.	gateway	router	repeater	hub	gateway
60	In _____ routing, the routing table need to recompute the route continuously	static	dynamic	state	none of these	dynamic

UNIT V

SYLLABUS

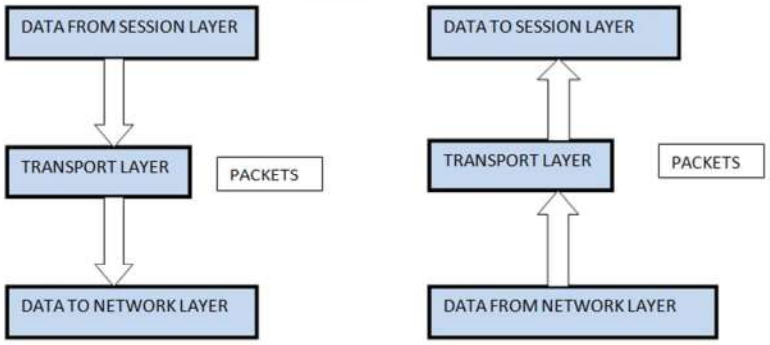
Transport Layer Functions and Protocols: Transport services- error and flow control, Connection establishment and release- three way handshake; **Overview of Application layer protocol**: Overview of DNS protocol; overview of WWW &HTTP protocol.

Transport Layer Functions and Protocols

TRANSPORT LAYER - OSI MODEL

The main aim of transport layer is to be delivered the entire message from source to destination. Transport layer ensures whole message arrives intact and in order, ensuring both error control and flow control at the source to destination level. It decides if data transmission should be on parallel path or single path

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer and ensures that message arrives in order by checking error and flow control.



FUNCTIONS OF TRANSPORT LAYER:

1. **Service Point Addressing :** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling :** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.

3. **Connection Control :** It includes 2 types :
4. **Connectionless Transport Layer :** Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
5. **Connection Oriented Transport Layer :** Before delivering packets, connection is made with transport layer at the destination machine.
6. **Flow Control :** In this layer, flow control is performed end to end.
7. **Error Control :** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

DCN - Transport Layer Introduction

Next Layer in OSI Model is recognized as Transport Layer (Layer-4). All modules and procedures pertaining to transportation of data or data stream are categorized into this layer. As all other layers, this layer communicates with its peer Transport layer of the remote host.

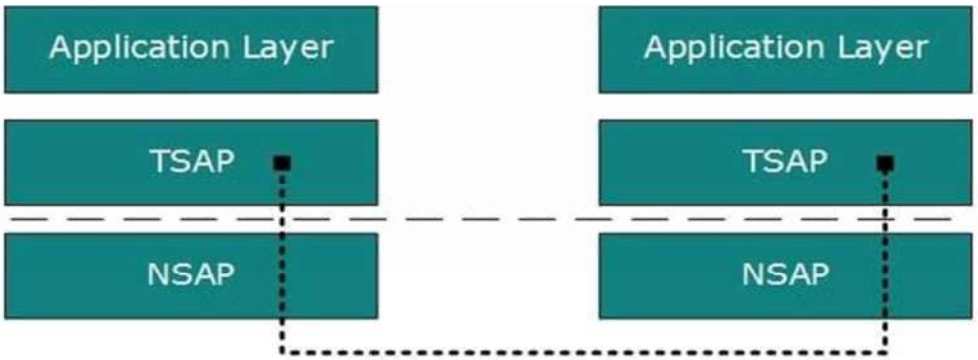
Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.

Functions

- This Layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments. It numbers every byte in the segment and maintains their accounting.
- This layer ensures that data must be received in the same sequence in which it was sent.
- This layer provides end-to-end delivery of data between hosts which may or may not belong to the same subnet.
- All server processes intend to communicate over the network are equipped with well-known Transport Service Access Points (TSAPs) also known as port numbers.

End-to-End Communication

A process on one host identifies its peer host on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.



For example, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number 67. When a DNS client wants to communicate with remote DNS server, it always requests on port number 53 (UDP).

The two main Transport layer protocols are:

- **Transmission Control Protocol**

  It provides reliable communication between two hosts.

- **User Datagram Protocol**

  It provides unreliable communication between two hosts.

DCN - Transmission Control Protocol

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.

- TCP ensures that the data reaches intended destination in the same order it was sent.

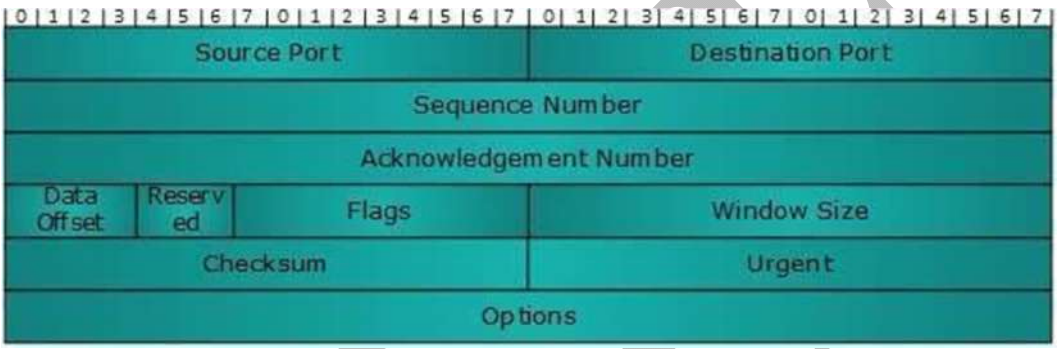
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.

- TCP provides error-checking and recovery mechanism.

- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**

- **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.

- **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.

- **ECE** -It has two meanings:

  - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
  - If SYN bit is set to 1, ECE means that the device is ECT capable.

- **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
- **ACK** - It indicates that Acknowledgement has significance. If ACK is field cleared to 0, it indicates that packet does not contain any acknowledgement.

- **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.

- **RST** - Reset flag has the following features:

  - It is used to refuse an incoming connection.
  - It is used to reject a segment.
  - It is used to restart a connection.

- **SYN** - This flag is used to set up a connection between hosts.

- **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.

- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.

- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.

- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Addressing

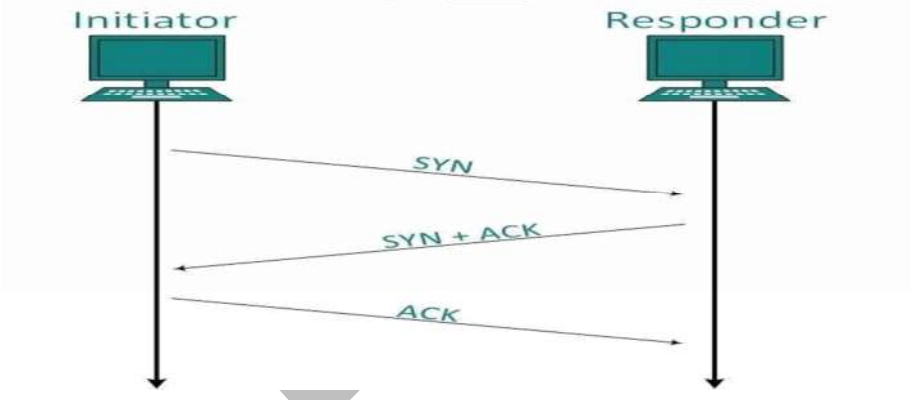
TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 –65535)

CONNECTION ESTABLISHMENT AND RELEASE

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

Bandwidth Management

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

Error Control & and Flow Control

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

Multiplexing

The technique to combine two or more data streams in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

Congestion Control

When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

Timer Management

TCP uses different types of timer to control and management various tasks:

Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

Persist timer:

- TCP session can be paused by either host by sending Window Size 0.

- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds (4 minutes).

Crash Recovery

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

When a TCP Server crashes mid-way communication and re-starts its process it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

DCN - User Datagram Protocol

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Requirement of UDP

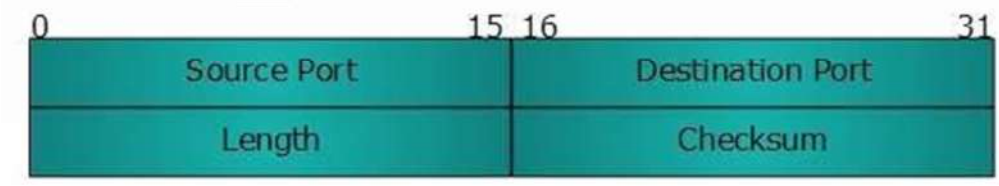
A question may arise, why do we need an unreliable protocol to transport the data? We deploy UDP where the acknowledgement packets share significant amount of bandwidth along with the actual data. For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain huge amount of bandwidth wastage. The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not calamitous and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP Header

UDP header is as simple as its function.



UDP header contains four main parameters:

- **Source Port** - This 16 bits information is used to identify the source port of the packet.

- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.

- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.

- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.

UDP application

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

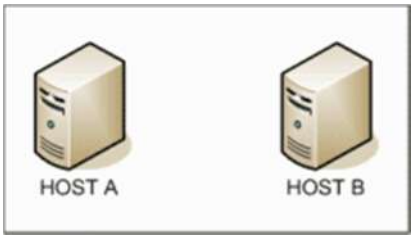
THREE WAY HANDSHAKE

The TCP three-way handshake in Transmission Control Protocol (also called the TCP-handshake; three message handshake and/or SYN-SYN-ACK) is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network. TCP's three way handshaking technique is often referred to as "SYN-SYN-ACK" (or more accurately SYN, SYN-ACK, ACK) because there are three messages transmitted by TCP to negotiate and start a TCP session between two computers. The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network TCP socket connection before transmitting data such as SSH and HTTP web browser requests.

This 3-way handshake process is also designed so that both ends can initiate and negotiate separate TCP socket connections at the same time. Being able to negotiate multiple TCP socket connections in both directions at the same time allows a single physical network interface, such as ethernet, to be multiplexed to transfer multiple streams of TCP data simultaneously.

TCP 3-Way Handshake Diagram
Below is a (very) simplified diagram of the TCP 3-way handshake process. Have a look at the diagram on the right as you examine the list of events on the left.

EVENT DIAGRAM



Host A sends a TCP SYNchronize packet to Host B
Host B receives A's SYN
Host B sends a SYNchronize-ACKnowledgement
Host A receives B's SYN-ACK
Host A sends ACKnowledge
Host B receives ACK.
TCP socket connection is ESTABLISHED.

Tcp three-way handshake,syn,syn-ack,ack
TCP Three Way Handshake
(SYN,SYN-ACK,ACK)
SYNchronize and ACKnowledge messages are indicated by a either the SYN bit, or the ACK bit inside the TCP header, and the SYN-ACK message has both the SYN and the ACK bits turned on (set to 1) in the TCP header.
TCP knows whether the network TCP socket connection is opening, synchronizing, established by using the SYNchronize and ACKnowledge messages when establishing a network TCP socket connection.

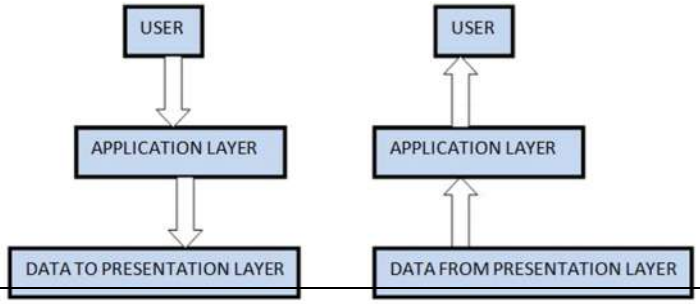
When the communication between two computers ends, another 3-way communication is performed to tear down the TCP socket connection. This setup and teardown of a TCP socket connection is part of what qualifies TCP a reliable protocol. TCP also acknowledges that data is successfully received and guarantees the data is reassembled in the correct order.

Note that UDP is connectionless. That means UDP doesn't establish connections as TCP does, so UDP does not perform this 3-way handshake and for this reason, it is referred to as an unreliable protocol. That doesn't mean UDP can't transfer data, it just doesn't negotiate how the connection will work, UDP just transmits and hopes for the best.

Overview of Application layer protocol:

Application Layer - OSI Model

It is the top most layer of OSI Model. Manipulation of data (information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring of files, distributing the results to user, directory services, network resource etc.



FUNCTIONS OF APPLICATION LAYER:

1. **Mail Services :** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal :** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services :** This layer provides access for global information about various services.
4. **File Transfer, Access and Management (FTAM) :** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

DCN - Application Protocols

There are several protocols which work for users in Application Layer. Application layer protocols can be broadly divided into two categories:

- Protocols which are used by users.For email for example, eMail.
- Protocols which help and support protocols used by users.For example DNS.

Few of Application layer protocols are described below:

Domain Name System

The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme. The DNS server is configured with Fully Qualified Domain Names (FQDN) and email addresses mapped with their respective Internet Protocol addresses.

A DNS server is requested with FQDN and it responds back with the IP address mapped with it. DNS uses UDP port 53.

Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.

Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. SMTP uses TCP port number 25 and 587.

Client software uses Internet Message Access Protocol (IMAP) or POP protocols to receive emails.

File Transfer Protocol

The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client.

FTP uses out-of-band controlling i.e. FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21.

The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

Post Office Protocol (POP)

The Post Office Protocol version 3 (POP 3) is a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server.

When a client needs to retrieve mails from server, it opens a connection with the server on TCP port 110. User can then access his mails and download them to the local computer. POP3 works in two modes. The most common mode the delete mode, is to delete the emails from remote server after they are downloaded to local machines. The second mode, the keep mode, does not delete the email from mail server and gives the user an option to access mails later on mail server.

Hyper Text Transfer Protocol (HTTP)

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

HTTP versions

- HTTP 1.0 uses non persistent HTTP. At most one object can be sent over a single TCP connection.
- HTTP 1.1 uses persistent HTTP. In this version, multiple objects can be sent over a single TCP connection.

INTERNET DOMAIN NAME SYSTEM (DNS)

Overview

When **DNS** was not into existence, one had to download a **Host file** containing host names and their corresponding IP address. But with increase in number of hosts of internet, the size of host file also increased. This resulted in increased traffic on downloading this file. To solve this problem the DNS system was introduced.

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

IP Address

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

- IP address is the unique address assigned to each host present on Internet.
- IP address is 32 bits (4 bytes) long.
- IP address consists of two components: **network component** and **host component**.

- Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example 137.170.4.124

IP address is 32-bit number while on the other hand domain names are easy to remember names. For example, when we enter an email address we always enter a symbolic string such as webmaster@tutorialspoint.com.

Uniform Resource Locator (URL)

Uniform Resource Locator (URL) refers to a web address which uniquely identifies a document over the internet.

This document can be a web page, image, audio, video or anything else present on the web.

For example, **www.tutorialspoint.com/internet_technology/index.html** is an URL to the index.html which is stored on tutorialspoint web server under internet_technology directory.

URL Types

There are two forms of URL as listed below:

1. Absolute URL
2. Relative URL

ABSOLUTE URL

Absolute URL is a complete address of a resource on the web. This completed address comprises of protocol used, server name, path name and file name.

For example http:// www.tutorialspoint.com / internet_technology /index.htm. where:

- **http** is the protocol.
- **tutorialspoint.com** is the server name.
- **index.htm** is the file name.

The protocol part tells the web browser how to handle the file. Similarly we have some other protocols also that can be used to create URL are:

- FTP
- https
- Gopher
- mailto
- news

RELATIVE URL

Relative URL is a partial address of a webpage. Unlike absolute URL, the protocol and server part are omitted from relative URL.

Relative URLs are used for internal links i.e. to create links to file that are part of same website as the WebPages on which you are placing the link.

For example, to link an image on tutorialspoint.com/internet_technology/internet_referemce_models, we can use the relative URL which can take the form like **/internet_technologies/internet-osi_model.jpg.**

Difference between Absolute and Relative URL

Absolute URL	**Relative URL**
Used to link web pages on different websites	Used to link web pages within the same website.
Difficult to manage.	Easy to Manage
Changes when the server name or directory name changes	Remains same even of we change the server name or directory name.
Take time to access	Comparatively faster to access.

Domain Name System Architecture

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

Domain Names

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

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

Domain Name	**Meaning**
Com	Commercial business
Edu	Education
Gov	U.S. government agency
Int	International entity
Mil	U.S. military
Net	Networking organization
Org	Non profit organization

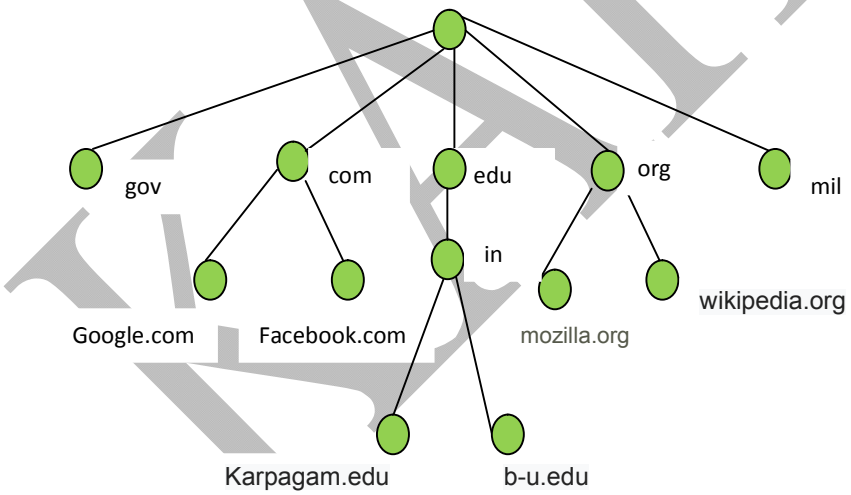
The following table shows the **Country top-level** domain names:

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

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

Domain Name Space

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



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

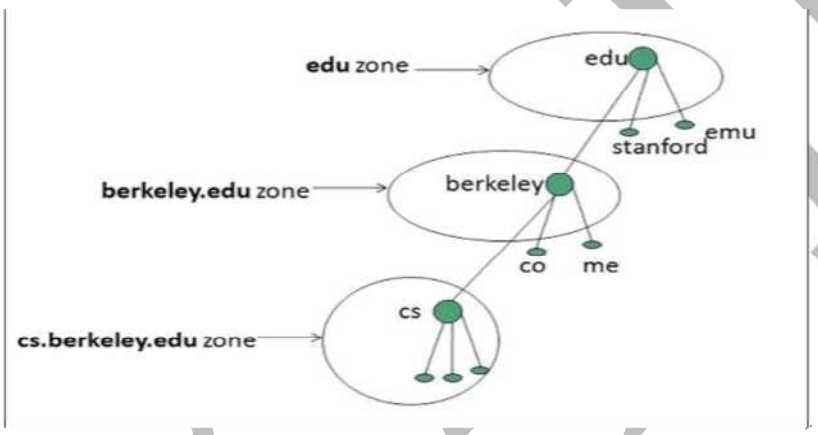
Name Server

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

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

Zones

Zone is collection of nodes (sub domains) under the main domain. The server maintains a database called zone file for every zone.



If the domain is not further divided into sub domains then domain and zone refers to the same thing.

The information about the nodes in the sub domain is stored in the servers at the lower levels however; the original server keeps reference to these lower levels of servers.

TYPES OF NAME SERVERS

Following are the three categories of Name Servers that manages the entire Domain Name System:

1. Root Server
2. Primary Server
3. Secondary Server

ROOT SERVER

Root Server is the top level server which consists of the entire DNS tree. It does not contain the information about domains but delegates the authority to the other server

PRIMARY SERVERS

Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file.

SECONDARY SERVER

Secondary Server transfers complete information about a zone from another server which may be primary or secondary server. The secondary server does not have authority to create or update a zone file.

DNS Working

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

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

  Here the local DNS is at ISP end.

- When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.

- The root DNS server replies with delegation that **I do not know the IP address of www.tutorialspoint.com but know the IP address of DNS Server.**

- The local DNS server then asks the com DNS Server the same question.

- The **com** DNS Server replies the same that it does not know the IP address of www.tutorialspont.com but knows the address of tutorialspoint.com.

- Then the local DNS asks the tutorialspoint.com DNS server the same question.

- Then tutorialspoint.com DNS server replies with IP address of www.tutorialspoint.com.

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

WWW Overview

Tim Berners-Lee, a British scientist at CERN (the European Organization for Nuclear Research, is one of the world's largest and most respected centers for scientific research), invented the **World Wide Web** (WWW) in 1989. The **web** was originally conceived and developed to meet the demand for automatic information-sharing between scientists in universities and institutes around the **world**.

The internet is a series of huge computer networks that allows many computers to connect and communicate with each other globally. Upon the internet reside a series of languages which allow information to travel between computers. These are known as protocols. For instance, some common protocols for transferring emails are IMAP, POP3 and SMTP. Just as email is a layer on the internet, the World Wide Web is *another* layer which uses different protocols.

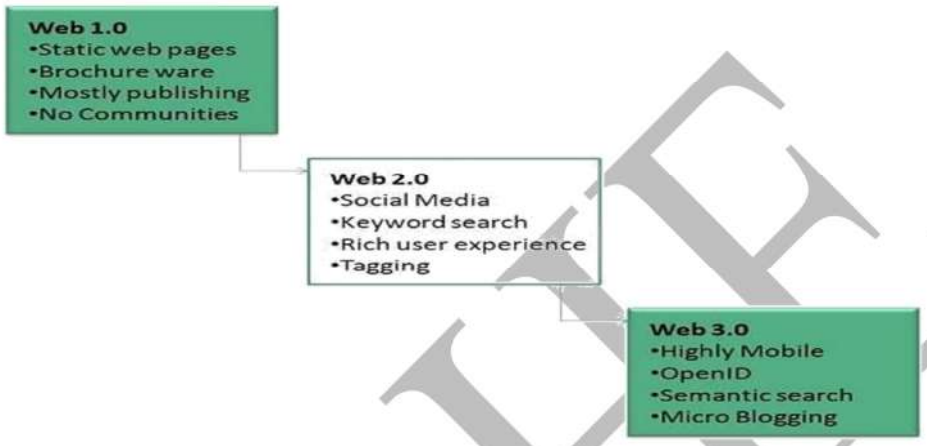
The World Wide Web uses three protocols:

- **HTML (Hypertext markup language)** - The language that we write our web pages in.
- **HTTP (Hypertext Transfer Protocol)** - Although other protocols can be used such as FTP, this is the most common protocol. It was developed specifically for the World Wide Web and favored for its simplicity and speed. This protocol requests the 'HTML' document from the server and serves it to the browser.
- **URLS** (Uniform resource locator) - The last part of the puzzle required to allow the web to work is a URL. This is the address which indicates where any given document lives on the web. It can be defined as <protocol>://<node>/<location>

In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

Internet and **Web** is not the same thing: Web uses internet to pass over the information.

The following diagram briefly defines evolution of World Wide Web:



WWW Architecture

The Internet World-Wide Web (WWW) architecture provides a very flexible and powerful programming model. Applications and content are presented in standard data formats, and are *browsed* by application known as *web browsers* (Figure 1). The web browser sends requests for named data objects to a web server and the server responds with the data encoded using the standard formats.

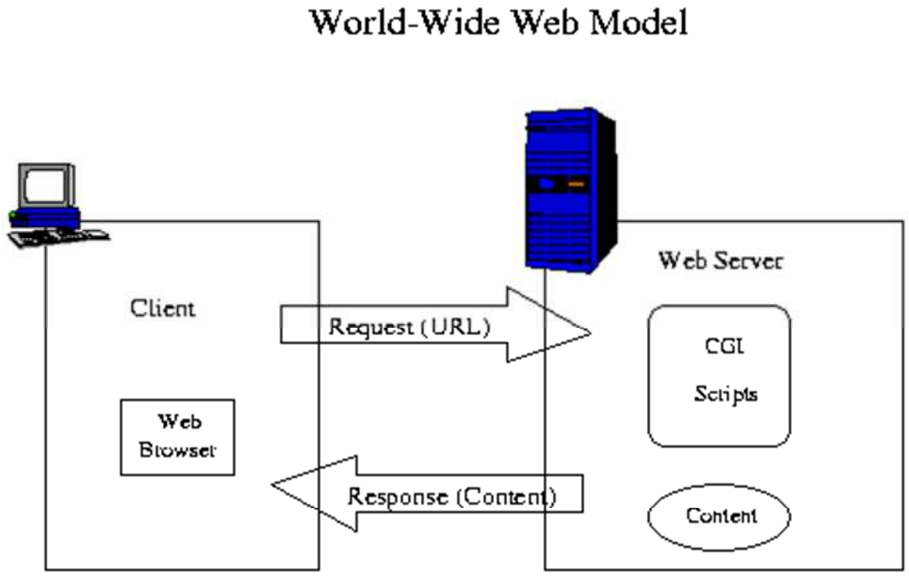


Figure 1. WWW Programming Model

The WWW standards for building a an application environment includes:

- Standard naming model - All servers and content on the WWW are named with an Internet-standard *Uniform Resource Locator* (URL).
- Content typing - All servers and content on the WWW is given a specific type thereby allowing web browsers to correctly process the content based on its type.
- Standard content formats - All web browsers support a set of standard content formats, including HTML and JavaScript.
- Standard Protocols - Standard networking protocols allow any web browser to communicate with any web server. The most commonly used protocol on the WWW is HTTP.

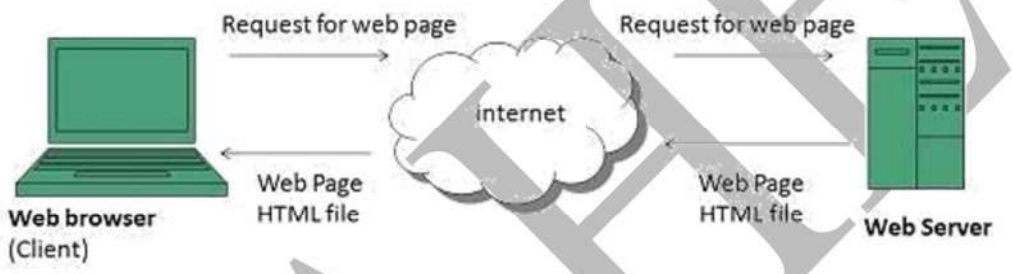
The WWW protocols define three classes of servers:

- Origin Server - The server on which a given resource (content) resides or is to be created.
- Proxy - An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. The proxy typically resides between clients and servers that have not means of direct communications, eg across a firewall.

Requests are either serviced by the proxy program or passed on, with possible transactions, to other servers. A proxy must implement both the client and server requirements of the WWW specifications.

- Gateway - A server which acts as an intermediary for some other server. Unlike a proxy, a gateway receives requests as if it were the origin server for the requested resource. The requesting client may not be aware that it is communicating with a gateway

WWW Operation



WWW works on client- server approach. Following steps explains how the web works:

1. User enters the URL (say, **http://www.tutorialspoint.com**) of the web page in the address bar of web browser.

2. Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.

3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.

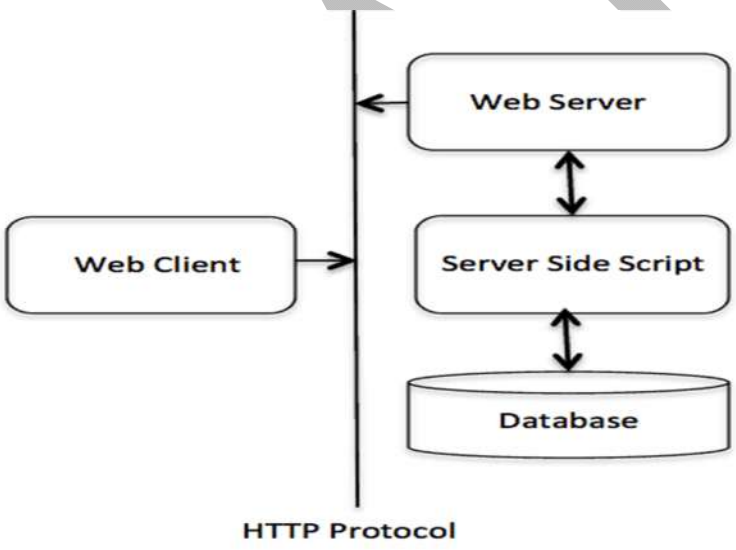
4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.

5. Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.

AN OVERVIEW OF HTTP

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990.

HTTP is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and a client-server protocol, which means requests are initiated by the recipient, usually the Web browser. A complete document is reconstructed from the different sub-documents fetched, for instance text, layout description, images, videos, scripts, and more.



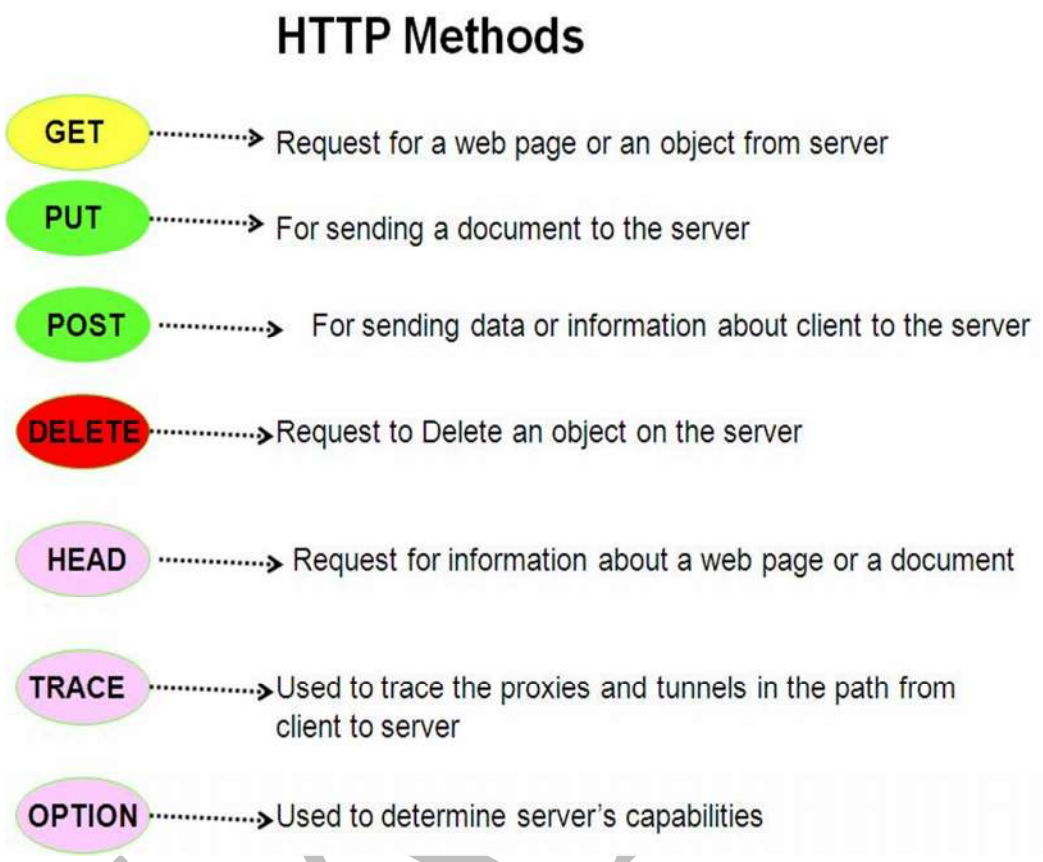
HTTP (Hyper Text Transfer Protocol) is the most popular protocol used for web browsing. It is basically a computer networking application layer protocol provided to the applications for accessing data on the world wide web (www).

A sample HTTP request and response

HTTP Basic Theory of Operation

- HTTP is a standard text based, application layer protocol, used by all browsers to access millions and millions of web pages, stored across the entire globe.
- It is similar to FTP in some aspects as it uses TCP as the underlying transport layer protocol to transfer files and supports methods like get and put for data transfer. However, HTTP uses just a single TCP connection compared to two TCP connections used by FTP (one control and one data). HTTP is also similar to SMTP in the structure of protocol messages.
- HTTP is a reliable protocol, making sure that all data transferred through it reaches the peer machine without any loss. Due to this reliability requirement, HTTP uses TCP as the transport layer protocol.
- It is a simple **Client-Server REQUEST-REPLY protocol**, where clients send HTTP requests and servers respond with HTTP replies.
- HTTP is a **stateless protocol** as each HTTP Requests and Replies are treated independently by the client and server. So server does not maintain any specific state about each HTTP transaction.
- HTTP supports multiple basic operations in the form of different HTTP methods like GET/PUT/POST/HEAD etc. The functions of some of the basic HTTP methods are

given in the diagram below:



Different Types of HTTP Methods

- HTTPS is a secured version of the protocol. It uses SSL protocol to send encrypted data.

Communication between a host and a client occurs, via a **request/response pair**. The client initiates an HTTP request message, which is serviced through a HTTP response message in return. We will look at this fundamental message-pair in the next section.

The current version of the protocol is **HTTP/1.1**, which adds a few extra features to the previous 1.0 version.

A later version, the successor HTTP/2, was standardized in 2015, and is now supported by major web servers and browsers.

Security on the Internet has been playing an ever-increasing role of importance in the past few years. Cyber crimes, such as credit card theft and other types of theft through the Internet has been on the rise. The Secure Sockets Layer (SSL) is a solution to battle these types of problems. SSL is a security layer that exists between TCP/IP and application protocols, such as HTTP, LDAP, FTP, and Telnet.

The Secure Sockets Layer (SSL) protocol, originally developed by Netscape, has been universally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers.

Features of SSL

Data Privacy

SSL also can detect tampering of the data transmitted, so that users on both sides of the connection know if anything was changed during the transit.

Ease of Use

SSL networking is just as easy as regular networking in Java. This is made possible by using JSSE.

Authentication

SSL also includes Server Authentication and Client Authentication Capability. This is accomplished through the use of cryptographically signed certificates between the two sides, namely the Server and the Client.

POSSIBLE QUESTIONS

PART A – Online Multiple Choice Questions

PART B – 2 Mark Questions

1. What are the responsibilities of Transport Layer?
2. What is meant by quality of service?
3. What are the responsibilities of Application Layer?
4. What is User Agent?
5. What are the types of messages in HTTP transaction?
6. What is DNS?

PART C – 8 Mark Questions

1. Describe in detail about Transport services in transport layer.
2. Discuss about Connection establishment and release.
3. Give a detail note on - three way handshake.
4. Elaborate HTTP protocol in detail.
5. Describe about WWW protocol in detail.
6. Explain in detail about DNS protocol.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Class: II BSC CS Batch:2017
Subject: COMPUTER NETWORKS
SubCode: 17CSU303
UNIT V

S.NO	QUESTION	CHOICE1	CHOICE2	CHOICE3	CHOICE4	ANSWER
1	In the transport layer, a message is normally divided into transmittable _____	Segments	Signals	Networks	Frames	Segments
2	The transport layer may be responsible for flow and error Control, like the _____	Physical Layer	Data Link Layer	Subnet Layer	Application Layer	Data Link Layer
3	The transport layer is responsible for process-to-process delivery of the _____	Message	Address of Message	Few Packets of Message	Partial Message	Address of Message
4	applications into a single stream before passing it to _____	network layer	data link layer	application layer	physical layer	network layer
5	Which one of the following is a transport layer protocol used in networking?	TCP	UDP	Both TCP and UDP	None of the mentioned	Both TCP and UDP
6	Which one of the following is a transport layer protocol?	stream control transmission protocol	internet control message protocol	neighbor discovery protocol	dynamic host configuration protocol	stream control transmission protocol
7	Transmission control protocol is _____	connection oriented protocol	handshake to establish a connection	recievs data from application as a single stream	all of the mentioned	all of the mentioned
8	flow across a computer network is called _____	socket	pipe	port	none of the mentioned	socket
9	Transport layer protocols deals with _____	application to application communication	process to process communication	node to node communication	none of the mentioned	process to process communication
10	Congestion control is divided into--------types	1	2	3	4	2
11	A ----------is mechanism that can prevent before and after it happens	open-loop	closed-loop	congestion control	none	congestion control
12	In---------- control ,policies are applied to prevent congestion before it happens	open-loop congestion	closed-loop congestion	both a & b	congestion control	open-loop congestion

13	If the sender feels that a sent packets is lost ,the packet needs to ----------	transmission	delete	retransmission	none	retransmission
14	The name of the domain is the domain name of the node at the top of the _____	Sub Tree	Main Tree	Leaf Node	Bottom Tree	Sub Tree
15	The domain, which is used to map an address to a name is called _____	Generic Domains	Inverse Domain	Main Domains	Sub-Domains	Inverse Domain
16	to their generic behavior, is called _____	Generic Domains	Main Domains	Super-Domains	Sub-Domains	Generic Domains
17	The DNS client adds the suffix atc.jhda.edu. before passing the address to the _____	DNS Client	DNS Server	DNS Label	DNS Recipient	DNS Server
18	New domains can be added to DNS through a _____	Query	Registrar	Domain	Response	Registrar
19	The country domains section uses two-character country _____	Generations	Abbreviations	Notations	Zones	Abbreviations
20	Hyper Text Transfer Protocol (HTTP) support	Proxy Domain	Proxy Documents	Proxy Server	Proxy IP	Proxy Server
21	or graphic images is not a physical part of an _____	WebPage	WebData	HTML	Web-document	HTML
22	The documents in the WWW can be grouped into three broad categories _____	Static, double, active	Stateless, dynamic, archive	Static, domain, architecture	Static, dynamic, active	Static, dynamic, active
23	configured to access the proxy instead of the _____	Proxy Server	Target Server	Domain Server	Original Server	Target Server
24	In WWW and HTTP. a technology that creates and handles dynamic documents is called _____	Common Gateway Interface	Common Gateway Integrate	Common Gateway IP	Common Gateway Internet	Common Gateway Interface
25	HTTP is _____ protocol.	application layer	transport layer	network layer	mentioned	application layer
26	. In the network HTTP resources are located by	uniform resource identifier	unique resource locator	unique resource identifier	none of the mentioned	uniform resource identifier
27	The default connection type used by HTTP is _____	Persistent	Non-persistent	persistent or non-persistent depending on connection request	None of the mentioned	Persistent
28	The HTTP request message is sent in _____ part of three-way handshake.	First	Second	Third	None of the mentioned	Third

29	The values GET, POST, HEAD etc are specified in _____ of HTTP message	Request line	Header line	Status line	Entity body	Request line
30	Find the oddly matched HTTP status codes	200 OK	400 Bad Request	301 Moved permanently	304 Not Found	400 Bad Request
31	the service provider is distrubuted over many location called _____	internet	sites	www	http	sites
32	The web page is stored at the _____	hard disk	disk	client	server	server
33	The _____ is the computer on which the information is located	path	sites	host	cookies	host
34	_____is the pathname of the file where the information is located	host	path	server	sites	path
35	pages	HTML	C	C++	java	HTML
36	A_____ is created by a web server whenever a browser request the document	common gate way	dynamic document	script	all the above	dynamic document
37	_____ is the protocol used mainly to access data on the world wide web	communicatio	network	WWW	HTTP	HTTP
38	In _____each segment is considered as an i	Connectionless	Connection Oriente	static	dynamic	Connectionless
39	In _____ before delivering packets, connecti	Connectionless	Connection Oriente	static	dynamic	Connectionless
40	_____ provides reliable communication between two hosts.	TCP	UDP	FTP	SMTP	TCP
41	_____ provides unreliable comm	TCP	UDP	FTP	SMTP	UDP
42	Three way handshake is referred by _____	SYN, SYN-ACK, A	SYN, ACK	SYN-ACK, ACK	ACK	SYN, SYN-ACK,
43	Websites	Absolute URL	Relative URL	dynamic URL	static URL	Absolute URL
44	_____ is used to link web pages within the s	Absolute URL	Relative URL	dynamic URL	static URL	Relative URL
45	database	Name	Web	Mail	Data	Name
46	The HTTP uses a TCP connection to	Establishment of se	Transfer whole data	Client server conne	Transfer files	Transfer files
47	In Hyper Text Transfer Protocol (HTTP), a client	Web-based connect	Domain	TELNET	Linear Connection	TELNET
48	The Uniform Resource Locator (URL), is a standa	Server-End	Client-End	WebPage	Internet	Internet
49	_____allows us to send message include text,auido and video .	mail	internet	E-mail	all the above	E-mail
50	The_____client established a connection with MTA server on the system	MTA	alice	UA	system server	MTA

51	The first component of an electrionic mail system is the_____	alice	server	user agent	services provider	user agent
52	_____is the example of user agents are mail,pine,and elm	user agent	command driven	GUI-based	E-mail	command driven
53	files	local part	domain name	mime	both a & b	local part
54	The second part of address is_____	system server	internet	domain name	local part	domain name
55	MIME is_____	multiple internet mail extensions	multipurpose interface mail extensions	multipurpose internet mail exchange	multipurpose internet mail extensions	multipurpose internet mail extensions
56	_____ has delete and keep mode	pop	pop2	pop3	none	pop3
57	TCP/IP for copying a file from one host to another	FTP	MIME	UA	pop3	FTP
58	transferring text files	image	ASCII	data structure	record structure	ASCII
59	transferring binary files	image	data structure	record structure	ASCII	image
60	In the _____ format, the file is a continuous stream of byte	file structure	record structure	data structure	image	file structure

ACK