KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act, 1956)

Coimbatore - 641 021, India

FACULTY OF ARTS, SCIENCE AND HUMANITIES (FASH)

Department of CS,CA & IT

II B.Sc CS **III SEMESTER** **BATCH : 2016 - 2019**

16CSU303	**COMPUTER NETWORKS**	**4H – 4C**

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Int : **40** Ext : **60** Total: **100**

SCOPE

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

OBJECTIVES

- Build an understanding of the fundamental concepts of computer networking.
- Various transmission media, their comparative study, fiber optics and wireless media
- Categories and topologies of networks (LAN and WAN) Layered architecture (OSI and TCP/IP) and protocol suites.
- Channel error detection and correction, MAC protocols, Ethernet and WLAN.
- Details of IP operations in the INTERNET and associated routing principles

LEARNING OUTCOMES

After completing this course the student must demonstrate the knowledge and ability to:

- Independently understand basic computer network technology.
- Understand and explain Data Communications System and its components.
- Identify the different types of network topologies and protocols.
- Enumerate the layers of the OSI model and TCP/IP. Explain the function(s) of each layer.
- Identify the different types of network devices and their functions within a network
- Understand and building the skills of subnetting and routing mechanisms.

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 ACSUess mechanisms: Circuit switching; packetswitching - 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 ACSUess 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.(2012). Data Communications and Networking(5th ed.). New Delhi: THM.
2. Tanenbaum, A. S. (2011). Computer Networks (5th 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

Department of CS,CA & IT

II B.Sc CS - III Semester

COMPUTER NETWORKS - 16CSU303

UNIT I

S.NO	Lecture Duration (Hours)	Topics To Be Covered	Support Materials/ Pg.No
		Introduction to Computer Networks	
1	1	Network definition	W1
2	1	network topologies	
3	1	network classifications	
4	1	network protocol	T1: 19
5	1	layered network architecture	T1: 30
6	1	overview of OSI reference model	T1: 33-42
7	1	overview of TCP/IP protocol suite	T1: 43-45
		Data Communication Fundamentals and Techniques	
8	1	Analog and digital signal	T1: 57-58
9	1	data-ratelimits	T1: 85-88
10	1	digital to digital line encoding schemes	T1: 101-116
11	1	pulse code modulation	T1: 121
12	1	parallel and serial transmission	T1: 131-132
13	1	Discussion of Important Questions	
		Total No of Hours Planned for Unit I	**13**

UNIT II

S.NO	Lecture Duration (Hours)	Topics To Be Covered	Support Materials/ Pg.No
1	1	digital to analog modulation	T1: 14-148
		multiplexing techniques	T1: 161-179
2	1	FDM	
3	1	TDM	
4	1	transmission media	T1: 191-207
		Networks Switching Techniques and ACSUess mechanisms	
5	1	Circuit switching	T1: 214-218
6	1	packetswitching	T1: 232
7	1	connectionless datagram switching	

8	1	connection-oriented virtual circuit switching	W2
9	1	dial-up modems	T1: 248-249
10	1	digital subscriber line	T1: 251-255
11	1	cable TV for data transfer	T1: 257-259
12	1	Recapitulation of Important Questions	
		Total No of Hours Planned for Unit II	**12**

UNIT III

S.NO	Lecture Duration (Hours)	Topics To Be Covered	Support Materials/ Pg.No
		Data Link Layer Functions and Protocol	
1	1	Error detection techniques	T1: 267-299
2	1	error correction techniques	
3	1	data-link control	W1
4	1	framing control	T1: 307-311
5	1	flow control	
6	1	error recovery protocols	W1
7	1	stop and wait ARQ,	T1: 318-324
8	1	go-back-n ARQ	
9	1	Point to Point Protocol on Internet	T1: 346-355
10	1	Point to Point Protocol on Internet	
11	1	Recapitulation of Important Questions	
		Total No of Hours Planned for Unit III	**11**

UNIT IV

S.NO	Lecture Duration (Hours)	Topics To Be Covered	Support Materials/ Pg.No
		Multiple ACSUess Protocol and Networks	
1	1	CSMA/CD protocols	T1: 370-373
2	1	Ethernet LANS	T2: 271-286
3	1	connecting LAN and back-bone networks	W3
4	1	repeaters, hubs	T2: 2326
5	1	switches, bridges	
6	1	router and gateways	
		Networks Layer Functions and Protocols	
7	1	Routing; routing algorithms	T2: 350-373
8	1	routing algorithms	
		network layer protocol of Internet	T2: 431-449
9	1	IP protocol,	
10	1	Internet control protocols	
11	1	Discussion of Important Questions	
		Total No of Hours Planned for Unit IV	**11**

UNIT V

S.NO	Lecture Duration (Hours)	Topics To Be Covered	Support Materials/ Pg.No
		Transport Layer Functions and Protocols	
1	1	Transport services	T2: 481-482
2	1	error control	T2: 506
3	1	flow control	
4	1	Connection establishment and release	T2: 496-502
5	1	three way handshake	W1
		Overview of Application layer protocol	
6	1	Overview of DNS protocol	T2: 576-586
7	1	DNS	
8	1	Overview of WWW	T2: 611-651
9	1	Overview of HTTP protocol	
10	1	Recapitulation and Discussuin of Important Questions	
11	1	Discussion of previous ESE question papers	
12	1	Discussion of previous ESE question papers	
13	1	Discussion of previous ESE question papers	
		Total No of Hours Planned for Unit V	**13**

Total Hours	**60**

S.NO	TEXT BOOKS
T1	Forouzan, B. A.(2012). Data Communications and Networking(5th ed.). New Delhi: THM.
T2	Tanenbaum, A. S. (2011). Computer Networks (5th ed.). New Delhi: PHI.

.

S.NO	WEB SITES
W1	www.tutorialspoint.com
W2	http://www.studytonight.com/computer-networks
W3	http://www.cs.ccsu.edu/

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;

INTRODUCTION TO COMPUTER NETWORKS

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

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 through which we can share our data. It is also called data network. The best example of computer network is Internet. Computer network does not mean a system with control unit and other systems as its slave. It is called a distributed system

A network must be able to meet certain criteria, these are mentioned below:

1. Performance
2. Reliability
3. Scalability

Performance
It can be measured in following ways :

- **Transit time :** It is the time taken to travel a message from one device to another.

- **Response time :** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :
1. Efficiency of software

2. Number of users
3. Capability of connected hardware

Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Security

It refers to the protection of data from the unauthorised user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of Good Network

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

Basic Communication Model

Communication model is used to exchange data between two parties. For example communication between a computer, server and telephone (through modem).

Source

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Transmitter

The data generated by the source system are not directly transmitted in the form they are generated. The transmitter transforms and encodes the information in such a form to produce electromagnetic waves or signals.

Transmission System

A transmission system can be a single transmission line or a complex network connecting source and destination.

Receiver

Receiver accepts the signal from the transmission system and converts it to a form which is easily managed by the destination device.

Destination
Destination receives the incoming data from the receiver.

Data Communication
The exchange of data between two devices through a transmission medium is Data Communication. The data is exchanged in the form of 0's and 1's. The transmission medium used is wire cable. For data communication to occur, the communication device must be part of a communication system. Data Communication has two types Local and Remote which are discussed below :

Local :
Local communication takes place when the communicating devices are in the same geographical area, same building, face-to-face between individuals etc.

Remote :
Remote communication takes place over a distance i.e. the devices are farther. Effectiveness of a Data Communication can be measured through the following features :

1. Delivery : Delivery should be done to the correct destination.
2. Timeliness : Delivery should be on time.
3. Accuracy : Data delivered should be accurate.

Components of Data Communication

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

NETWORK DEFINITION

- A network can be defined as two or more computers connected together in such a way that they can share resources.
- The purpose of a network is to share resources.

A resource may be:

- A file
- A folder
- A printer

- A disk drive
- Or just about anything else that exists on a computer.

Definition

A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Advantages of networking

- Connectivity and Communication
- Data Sharing
- Hardware Sharing
- Internet Access
- Internet Access Sharing
- Data Security and Management
- Performance Enhancement and Balancing
- Entertainment

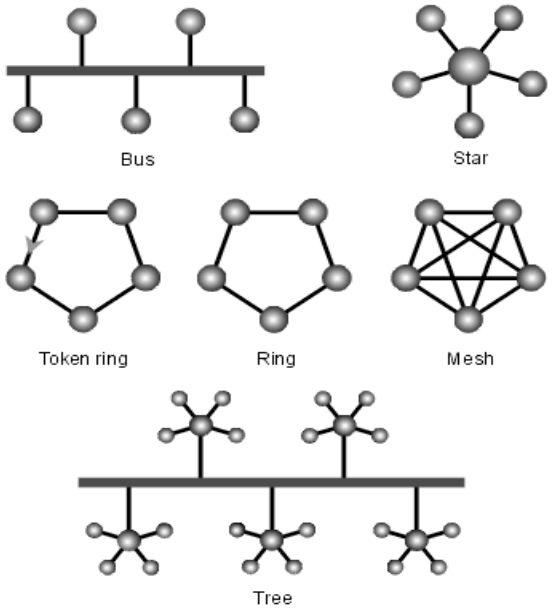
The Disadvantages (Costs) of Networking

- Network Hardware, Software and Setup Costs
- Hardware and Software Management and Administration Costs
- Undesirable Sharing
- Illegal or Undesirable Behavior
- Data Security Concerns

NETWORK TOPOLOGIES

- A *topology* is a way of "laying out" the network. Topologies can be either physical or logical.
- *Physical topologies* describe how the cables are run.
- *Logical topologies* describe how the network messages travel

- Bus (can be both logical and physical)
- Star (physical only)
- Ring (can be both logical and physical)
- Mesh (can be both logical and physical)



Types of Network Topology

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

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 and 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

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.

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.

Advantages and Disadvantages of Network Topologies

Topology	Advantages	Disadvantages
Bus	Cheap. Easy to install.	Difficult to reconfigure. Break in bus disables entire network.
Star	Cheap. Easy to install. Easy to reconfigure. Fault tolerant.	More expensive than bus.
Ring	Efficient. Easy to install.	Reconfiguration difficult. Very expensive.
Mesh	Simplest. Most fault tolerant.	Reconfiguration extremely difficult. Extremely expensive. Very complex.

NETWORK CLASSIFICATIONS

Classification of Networks by Scale

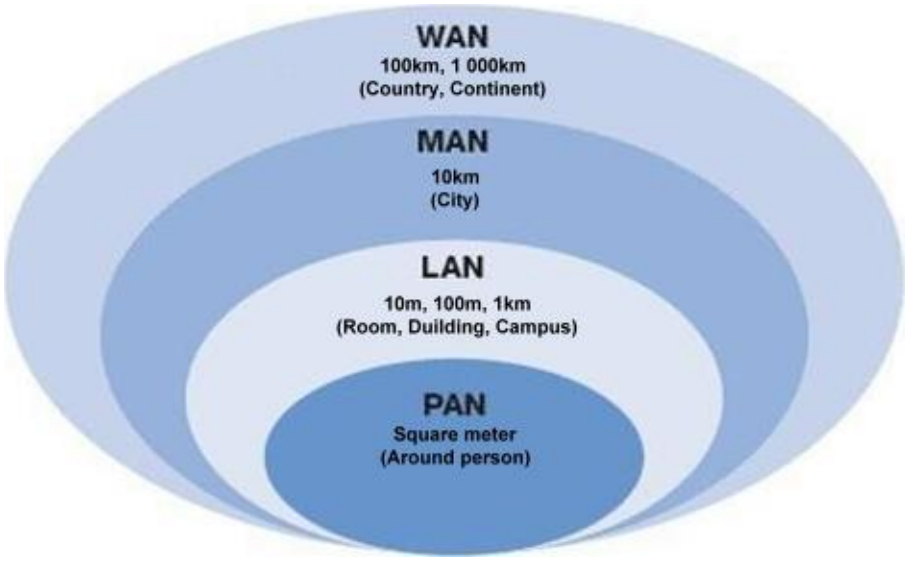
- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Networks (WAN)

Personal Area Network (PAN) - The interconnection of devices within the range of an individual person, typically within a range of 10 meters. For example, a wireless network connecting a computer with its keyboard, mouse or printer is a PAN. Also, a PDA that controls the user's hearing aid or pacemaker fits in this category. Another example of PAN is a Bluetooth. Typically, this kind of network could also be interconnected without wires to the Internet or other networks.

Local Area Network (LAN) - Privately-owned networks covering a small geographic area, like a home, office, building or group of buildings (e.g. campus). They are widely used to connect computers in company offices and factories to share resources (e.g., printers) and exchange information. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps.

Metropolitan Area Network (MAN) - Covers a larger geographical area than is a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of LANs. Metropolitan Area Networks can span up to 50km, devices used are modem and wire/cable.

Wide Area Networks (WAN) - Computer network that covers a large geographical area, often a country or continent. (any network whose communications links cross metropolitan, regional, or national boundaries). Less formally, a network that uses routers and public communications links.



Networks by Scale

NETWORK PROTOCOL - TYPES OF NETWORK PROTOCOLS

Network Protocol is a set of rules that governs the communications between computers on a network.

What is a Network Protocol

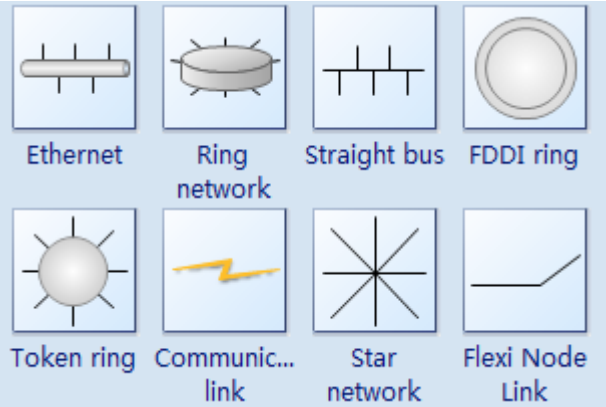
Rules of Network Protocol include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

Types of Network Protocols

The most common network protocols are:

- Ethernet
- Local Talk
- Token Ring
- FDDI
- ATM

The followings are some commonly used network symbols to draw different kinds of network protocols.



Different Types of Computer Protocols

In today's world, there are number of people communicating the number of different languages they use, the number of different machines they use, the number of ways in which they transmit data and the different software they use.

We would never be able to communicate worldwide if there were no 'standards' governing the way we communicate and the way our machines treat data. These standards are sets of rules.

There are rules governing how data is transferred over networks, how they are compressed, how they are presented on the screen and so on. These set of rules are called protocols. There are many protocols, each one governing the way a certain technology works. For example, the IP protocol defines a set of rules governing the way computers use IP packets to send data over the Internet or any other IP-based network. It also defines addressing in IP. Likewise, we have other protocols like:

TCP: Transmission Control Protocol, used for the reliable transmission of data over a network.
HTTP: Hypertext Transfer Protocol, used for transmitting and displaying information in the form of web pages on browsers.

FTP: File Transfer Protocol, used for file transfer (uploading and downloading) over the Internet.

POP: The most common protocol for receiving mail is Post Office Protocol (POP). It is now in version 3 so it is called POP3. Email clients such as Outlook Express require an address for a POP3 server before they can read mail. The SMTP and POP3 servers may or may not be the same address

SMTP: Simple Mail Transfer Protocol, used for email
Both SMTP and POP3 use TCP for managing the transmission and delivery of mail across the Internet.

Ethernet: Used for data transmission over a LAN.

Wi-Fi: One of the wireless protocols.

IP: Internet Protocol is the primary network protocol used on the Internet, developed in the 1970s. On the Internet and many other networks, IP is often used together with the Transport Control Protocol (TCP) and referred to interchangeably as

TCP/IP: IP supports unique addressing for computers on a network. Most networks use the Internet Protocol version 4 (IPv4) standards that features IP addresses four bytes (32 bits) in length. The newer Internet Protocol version 6 (IPv6) standard features addresses 16 bytes (128 bits) in length.

Data on an Internet Protocol network is organized into packets. Each IP packet includes both a header (that specifies source, destination, and other information about the data) and the message data itself.IP functions at layer 3 of the OSI model. It can therefore run on top of different data link interfaces including Ethernet and Wi-Fi.

FTP: File Transfer Protocol (FTP) lives up to its name and provides a method for copying files over a network from one computer to another. More generally, it provides for some simple file management on the contents of a remote computer. It is an old protocol and is used less than it was before the Word Wide Web came along. Today, its primary use is uploading files to a Web site. It can also be used for downloading from the Web but, more often than not, downloading is done via HTTP.

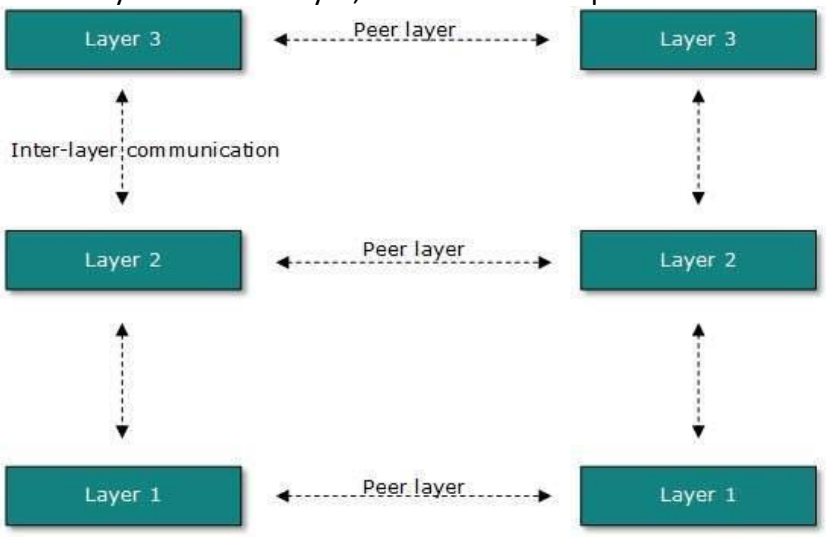
LAYERED NETWORK ARCHITECTURE

Layered Tasks

In layered architecture of Network Model, 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

the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.



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

Definition

An **architecture** in which data moves from one defined level of processing to another. Communications protocols are a primary example.

- **Layers:** grouping the common functions
- **Benefits of layers**:
  - Simplicity: easy to design once layers and their interaction are defined clearly
  - Flexibility: easy to modify and develop networks by separate layers modifications
  - Incremental changes: add new layers, add new functions to a layer

Three obvious tasks (layers)

- Transport of data across the network from one end to the other
- Routing/forwarding of packets across multiple hops
- Transfer of a frame from one interface to another (i.e., one hop).

Big picture of layered architectures

- Web browsing and e-mail examples
- OSI reference model (Seven layers)
- TCP/IP architecture
- Detailed end-to-end examples to complete big picture of layered architectures
- Socket API and other utilities

OVERVIEW OF OSI REFERENCE MODEL

THE NEED FOR STANDARDS

- Over the past couple of decades many of the networks that were built used different hardware and software implementations, as a result they were incompatible and it became difficult for networks using different specifications to communicate with each other.
- To address the problem of networks being incompatible and unable to communicate with each other, the International Organisation for Standardisation (ISO) researched various network schemes.
- The ISO recognised there was a need to create a NETWORK MODEL that would help vendors create interoperable network implementations.

ISO - ORGANISATION FOR STANDARDISATION

- The International Organisation for Standardisation (ISO) is an International standards organisation responsible for a wide range of standards, including many that are relevant to networking.
- In 1984 in order to aid network interconnection without necessarily requiring complete redesign, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.

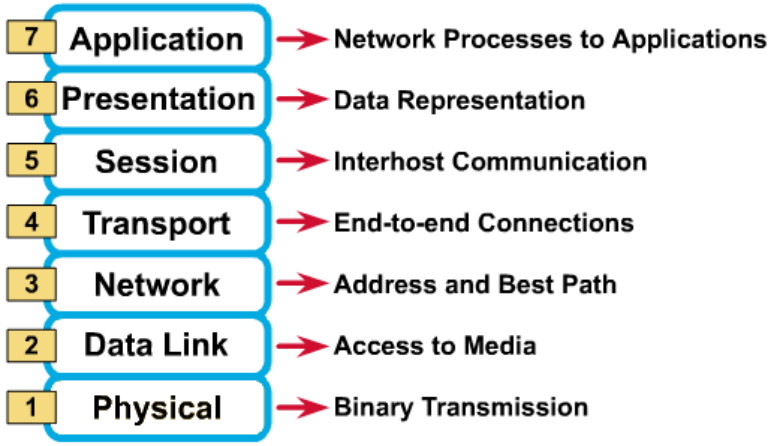
THE OSI REFERENCE MODEL

- The model was developed by the International Organisation for Standardisation (ISO) in 1984. It is now considered the primary Architectural model for inter-computer communications.
- The Open Systems Interconnection (OSI) reference model is a descriptive network scheme. It ensures greater compatibility and interoperability between various types of network technologies.
- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .
- This separation into smaller more manageable functions is known as layering.

A LAYERED NETWORK MODEL

- The OSI Reference Model is composed of seven layers, each specifying particular network functions.
- The process of breaking up the functions or tasks of networking into layers reduces complexity.
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer's software or hardware on other computers.
- The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- The upper four layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.
- Data is Encapsulated with the necessary protocol information as it moves down the layers before network transit.

THE SEVEN OSI REFERENCE MODEL LAYERS



LAYER 7: APPLICATION

- The application layer is the OSI layer that is closest to the user.
- It provides network services to the user's applications.
- It differs from the other layers in that it does not provide services to any other OSI layer, but rather, only to applications outside the OSI model.
- Examples of such applications are spreadsheet programs, word processing programs, and bank terminal programs.
- The application layer establishes the availability of intended communication partners, synchronizes and establishes agreement on procedures for error recovery and control of data integrity.

LAYER 6: PRESENTATION

- The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system.
- If necessary, the presentation layer translates between multiple data formats by using a common format.
- Provides encryption and compression of data.
- Examples :- JPEG, MPEG, ASCII, EBCDIC, HTML.

LAYER 5: SESSION

- The session layer defines how to start, control and end conversations (called sessions) between applications.
- This includes the control and management of multiple bi-directional messages using dialogue control.
- It also synchronizes dialogue between two hosts' presentation layers and manages their data exchange.
- The session layer offers provisions for efficient data transfer.
- Examples :- SQL, ASP(AppleTalk Session Protocol).

LAYER 4: TRANSPORT

- The transport layer regulates information flow to ensure end-to-end connectivity between host applications reliably and accurately.
- The transport layer segments data from the sending host's system and reassembles the data into a data stream on the receiving host's system.
- The boundary between the transport layer and the session layer can be thought of as the boundary between application protocols and data-flow protocols. Whereas the application, presentation, and session layers are concerned with application issues, the lower four layers are concerned with data transport issues.
- Layer 4 protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

LAYER 3: NETWORK

- Defines end-to-end delivery of packets.
- Defines logical addressing so that any endpoint can be identified.
- Defines how routing works and how routes are learned so that the packets can be delivered.
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.
- Routers operate at Layer 3.
- Examples :- IP, IPX, AppleTalk.

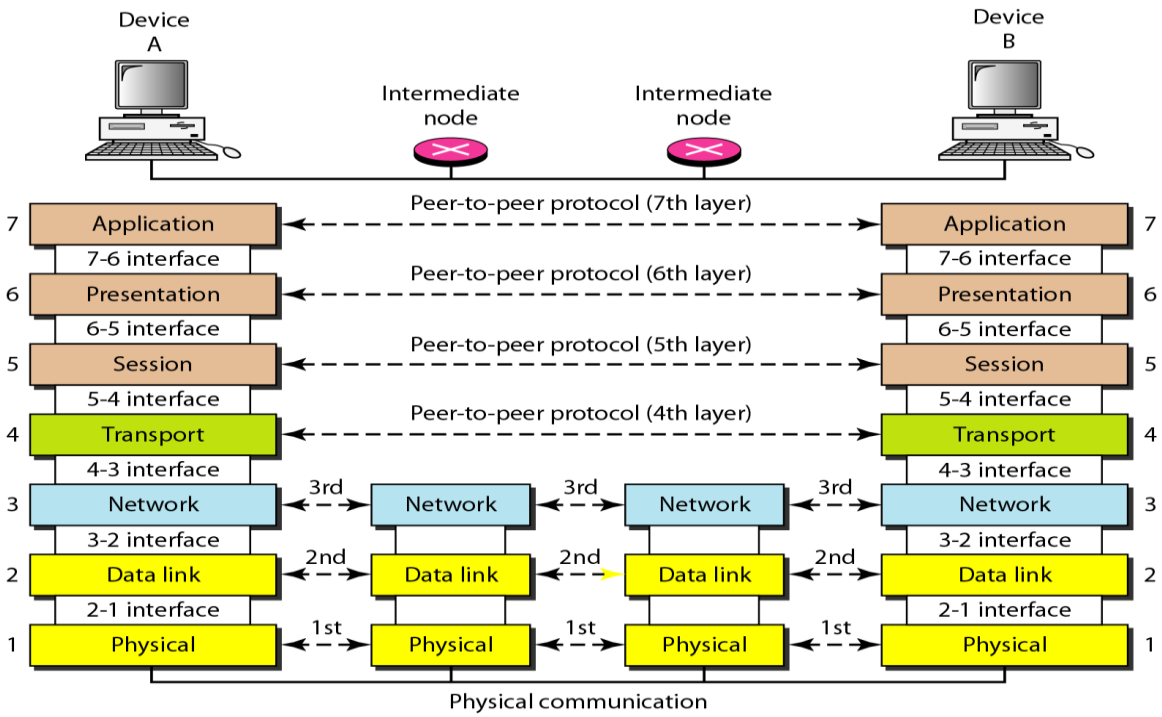
LAYER 2: DATA LINK

- The data link layer provides access to the networking media and physical transmission across the media and this enables the data to locate its intended destination on a network.
- The data link layer provides reliable transit of data across a physical link by using the Media Access Control (MAC) addresses.
- The data link layer uses the MAC address to define a hardware or data link address in order for multiple stations to share the same medium and still uniquely identify each other.
- Concerned with network topology, network access, error notification, ordered delivery of frames, and flow control.
- Examples :- Ethernet, Frame Relay, FDDI.

LAYER 1: PHYSICAL

- The physical layer deals with the physical characteristics of the transmission medium.
- It defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.
- Examples :- EIA/TIA-232, RJ45, NRZ.

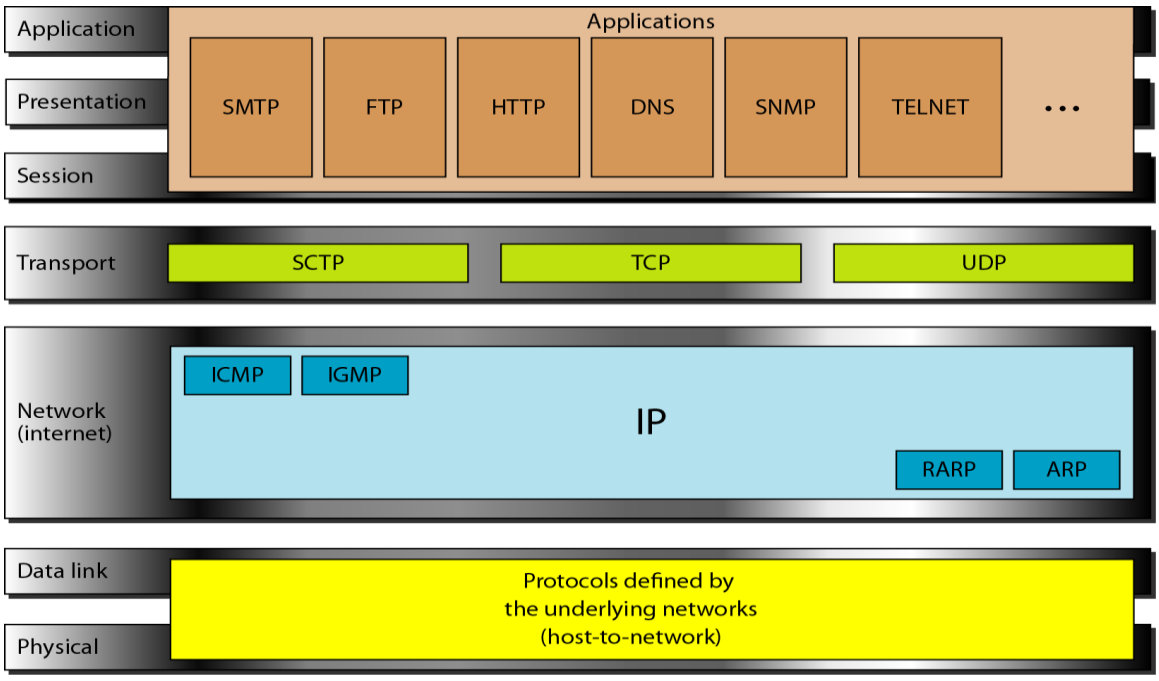
The interaction between layers in the OSI model



OVERVIEW OF TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

TCP/IP and OSI model



DATA COMMUNICATION FUNDAMENTALS AND TECHNIQUES:

Analog and digital signal

To send the digital data over an analog media, it needs to be converted into analog signal.There can be two cases according to data formatting.

Bandpass: The filters are used to filter and pass frequencies of interest. A bandpass is a band of frequencies which can pass the filter.

Low-pass: Low-pass is a filter that passes low frequencies signals.
When digital data is converted into a bandpass analog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into bandpass analog signal, it is called analog-to-analog conversion.

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)

Capacity of a System

- The bit rate of a system increases with an increase in the number of signal levels we use to denote a symbol.
- A symbol can consist of a single bit or "n" bits.
- The number of signal levels = 2n.
- As the number of levels goes up, the spacing between level decreases -> increasing the probability of an error occurring in the presence of transmission impairments.

Nyquist Theorem

- Nyquist gives the upper bound for the bit rate of a transmission system by calculating the bit rate directly from the number of bits in a symbol (or signal levels) and the bandwidth of the system (assuming 2 symbols/per cycle and first harmonic).
- Nyquist theorem states that for a noiseless channel:

  C = 2 B log22n

  C= capacity in bps

  B = bandwidth in Hz

Noiseless Channel: Nyquist Bit Rate

Defines theoretical maximum bit rate for Noiseless Channel:
Bit Rate=2 X Bandwidth X log2L

Example:

Does the Nyquist theorem bit rate agree with the intuitive bit rate described in baseband transmission?

Solution

They match when we have only two levels. We said, in baseband transmission, the bit rate is 2 times the bandwidth if we use only the first harmonic in the worst case. However, the Nyquist formula is more general than what we derived intuitively; it can

be applied to baseband transmission and modulation. Also, it can be applied when we have two or more levels of signals.

Example:

Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as

Bit Rate = $2 \times 3000 \times \log_2 2 = 6000$ bps

Consider the same noiseless channel, transmitting a signal with four signal levels (for each level, we send two bits). The maximum bit rate can be calculated as:

Bit Rate = 2 x 3000 x log2 4 = 12,000 bps

Note: Increasing the levels of a signal may reduce the reliability of the system.

Noisy Channel: Shannon Capacity

Defines theoretical maximum bit rate for Noisy Channel:

Capacity=Bandwidth X log2(1+SNR)

Example:

Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity is calculated as

C = B log2 (1 + SNR) = B log2 (1 + 0)

= B log2 (1) = B $\times$ 0 = 0

This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

Note: The Shannon capacity gives us the upper limit; the Nyquist formula tells us how many signal levels we need

Digital To Digital Line Encoding Schemes

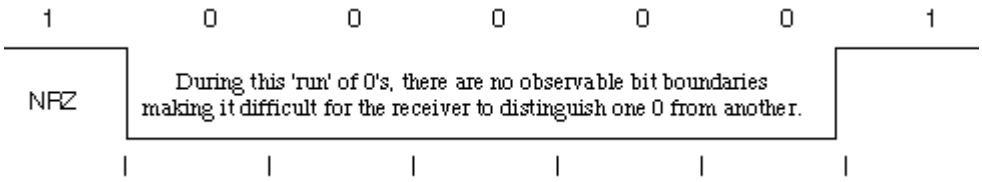
Digital data to digital signals

A digital signal is sequence of discrete , discontinuous voltage pulses. Each pulses a signal element. Encoding scheme is an important factor in how successfully the receiver interprets the incoming signal.

Encoding Techniques

Following are several ways to map data bits to signal elements.

- **Non return to zero(NRZ)** NRZ codes share the property that voltage level is constant during a bit interval. High level voltage = bit 1 and Low level voltage = bit 0. A problem arises when there is a long sequence of 0s or 1s and the volatage level is maintained at the same value for a long time. This creates a problem on the recieving end because now, the clock synchronization is lost due to lack of any transitions and hence, it is difficult to determine the exact number of 0s or 1s in this sequence.



The two variations are as follows:

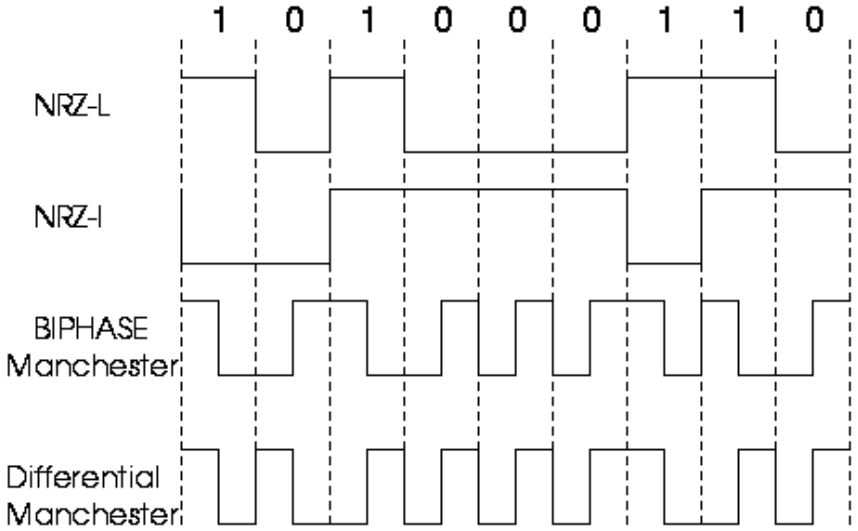
1. **NRZ-Level:** In NRZ-L encoding, the polarity of the signal changes only when the incoming signal changes from a 1 to a 0 or from a 0 to a 1. NRZ-L method looks just like the NRZ method, except for the first input one data bit. This is because NRZ does not consider the first data bit to be a polarity change, where NRZ-L does.
2. **NRZ-Inverted:** Transition at the beginning of bit interval = bit 1 and No Transition at beginning of bit interval = bit 0 or vicecersa. This technique is known as differential encoding.

NRZ-I has an advantage over NRZ-L. Consider the situation when two data wires are wrongly connected in each other's place.In NRZ-L all bit sequences will get reversed (B'coz voltage levels get swapped).Whereas in NAZ-I since bits are recognized by transition the bits will be correctly interpreted. A disadvantage in NRZ codes is that a string of 0's or 1's will prevent synchronization of transmitter clock with receiver clock and a separate clock line need to be provided.

- **Biphase encoding:** It has following characteristics:
  1. Modulation rate twice that of NRZ and bandwidth correspondingly greater. (Modulation is the rate at which signal level is changed).
  2. Because there is predictable transition during each bit time,the receiver can synchronize on that transition i.e. clock is extracted from the signal itself.
  3. Since there can be transition at the beginning as well as in the middle of the bit interval the clock operates at twice the data transfer rate.

  Types of Encoding -->

  - **Biphase-manchester:** Transition from high to low in middle of interval = 1 and Transition from low to high in middle of interval = 0
  - **Differential-manchester:** Always a transition in middle of interval. No transition at beginning of interval=1 and Transition at beginning of interval = 0



  - **4B/5B Encoding:** In Manchester encoding scheme , there is a transition after every bit. It means that we must have clocks with double the speed to send same amount of data as in NRZ encodings. In other words, we may say that only 50% of the data is sent. This performance factor can be significantly improved if we use a better encoding scheme. This scheme may have a transition after fixed number of bits instead of every other bit. Like if we have a transition after every four bits, then we will be

sending 80% data of actual capacity. This is a significant improvement in the performance.

This scheme is known as **4B/5B**. So here we convert 4-bits to 5-bits, ensuring at least one transition in them. The basic idea here is that 5-bit code selected must have :

- one leading 0
- no more than two trailing 0s

Thus it is ensured that we can never have more than three consecutive 0s. Now these 5-bit codes are transmitted using NRZI coding thus problem of consecutive 1s is solved.

The exact transformation is as follows :

4-bit Data	5-bit code	4-bit Data	5-bit code
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Of the remaining 16 codes, 7 are invalid and others are used to send some control information like line idle(11111), line dead(00000), Halt(00100) etc.

There are other variants for this scheme viz. 5B/6B, 8B/10B etc. These have self suggesting names.

- **8B/6T Encoding:** In the above schemes, we have used two/three voltage levels for a signal. But we may altogether use more than three voltage levels so that more than one-bit could be send over a single signal. Like if we use six voltage levels and we use 8-bits then the scheme is

called **8B/6T**. Clearly here we have 729(3^6) combinations for signal and 256(2^8) combinations for bits.

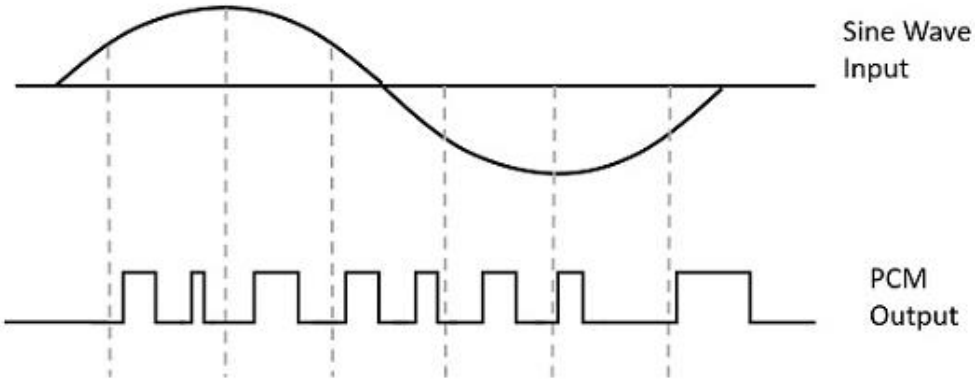
- **Bipolar AIM:** Here we have 3 voltage levels: middle,upper,lower
  - Representation 1: Middle level =0 Upper,Lower level =1 such that successive 1's will be represented alternately on upper and lower levels.
  - Representation 2 (pseudoternary): Middle level =1 Upper,Lower level=0

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.



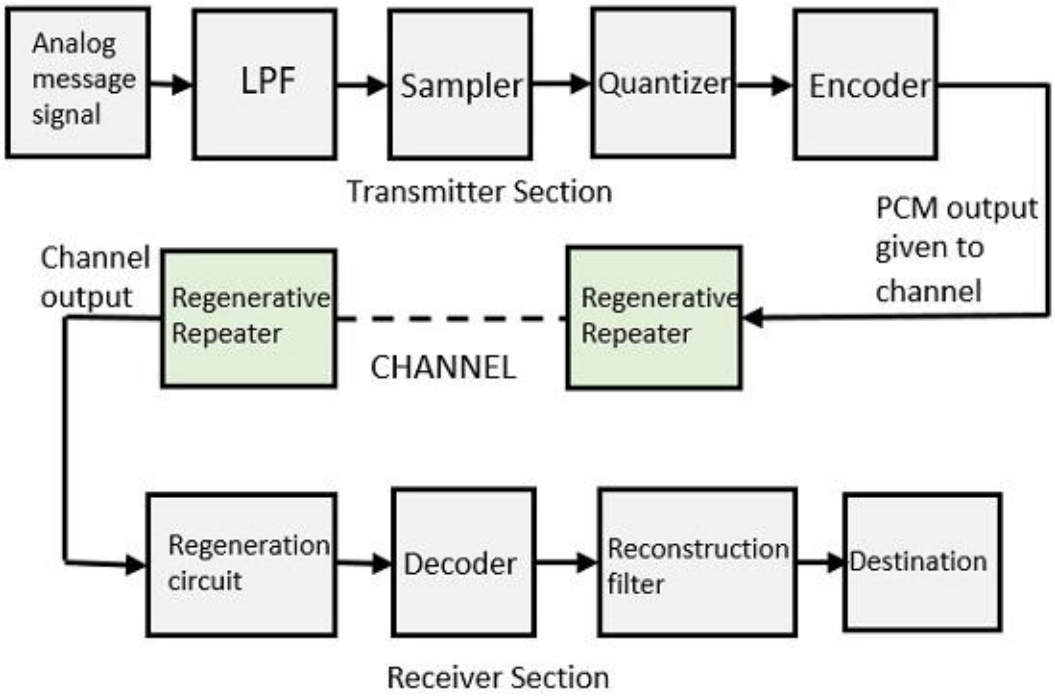
Instead of a pulse train, PCM produces a series of numbers or digits, and hence this process is called as **digital**. Each one of these digits, though in binary code, represent the approximate amplitude of the signal sample at that instant.

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

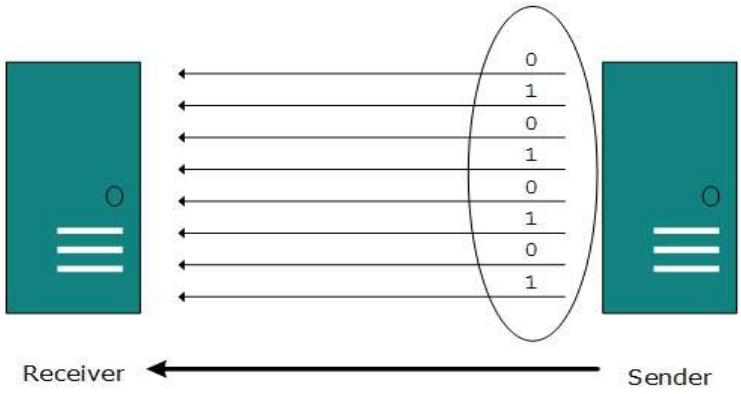
After the digital-to-analog conversion is done by the regenerative circuit and the decoder, a low-pass filter is employed, called as the reconstruction filter to get back the original signal.

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

Transmission Mode

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.

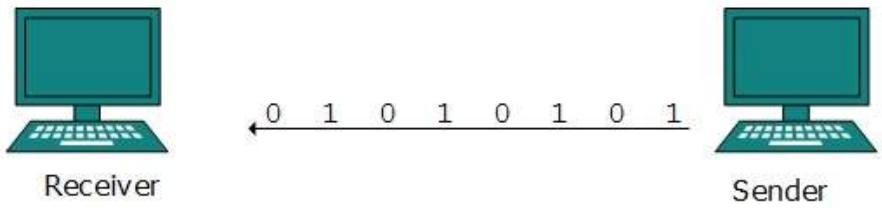
Parallel Transmission



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

PART A – Multiple Choice Questions

1. MAN stands for _____
   a. Metropolitician area network b. Metropolitan area network
   c. Metropolitical area network d. Macro area network
2. In physical layer we can transfer data into _____
   a. Frame b. packet c. bit d. byte
3. FTP_____
   a. file transmit protocol b. file transmission protocol
   c. file transfer protocol d. flip transfer protocol
4. A_____ is the set of rules.
   a. Protocols b. transmission mode c. networks d. ip
5. The _____is the number of bits sent in a second.
   a. Bit length b. bandpass c. bandwidth d. bit rate

PART B – 2 Mark Questions

1. Define networks
2. Differentiate analog and digital signals.
3. What are the elements of data communication?
4. Define data communication
5. Define distributed processing

PART C – 8 Mark Questions

1. Discuss the layered architecture of OSI reference model with a neat diagram.
2. Write note on pulse code modulation with suitable diagram
3. Describe in detail about classifications of networks with neat sketch.
4. Explain the various network topologies with a neat diagram
5. Explain serial and parallel transmission

Prepared by : A.Jeevarathinam,Dept of CS,CA & IT,KAHE

KARPAGAM ACADEMY OF HIGHER EDUCATION

DEPARTMENT OF CS,CA & IT

II B.Sc CS

COMPUTER NETWORKS (16CSU303)

UNIT I

S.NO	QUESTION	CHOICE 1	CHOICE 2	CHOICE 3	CHOICE 4	ANSWER
1	Data communication means exchange of data between _____devices.	one	two	six	four	two
2	The system must deliver data to the correct destination is called_____	accuracy	jitter	delivery	timeliness	delivery
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	The term timing refers to _____ characteristics.	two	three	four	six	two
10	_____standards are often established originally by manufactures.	de jure	de facto	de fact	semantics	de facto
11	In physical layer we can transfer data into _____	frame	packet	bit	sp du	bit
12	Hob to hob delivery is done by the _____	session layer	datalink layer	network layer	transport layer	datalink layer
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	hierarchical
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	Bus topology has a long link called_____	backbone	hub	host	hop	backbone
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/frequenc	propagation speed/frequency
22	Composite signal can be classified into _____types	five	three	four	two	two
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 duration
27	A_____signal is a composite analog signal with an infinite bandwidth	simple	composite	digital	analog	digital
28	Decibel (dB) =_____	10 log10 p2/p1	p1/p2	10 log10 p1/p2	2log10 p1/p2	10 log10 p2/p1
29	Transmission time=_____	message size/birate	distance/bandwid th	message size/distance	message size/bandwidth	message size/bandwidth
30	_____and star is a point to point device.	bus	ring	mesh	physical	mesh

31	Protocols can be classified into _____ key elements	one	three	four	two	three
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 interconnectio	open system internetworking	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 _____	user data protocol	user datagram protocol	user defined protocol	user dataframe protocol	user datagram protocol
38	FTP_____	file transmit protocol	file transmission protocol	file transfer protocol	flip transfer protocol	file transfer protocol
39	SMTP_____	single mail transfer	simple mail transfer protocol	simple mail transmission	single mail transmit	simple mail transfer protocol
40	Complete a cycle is called as _____	period	frequency	non periodic	periodic	period
41	Jitter is a form of_____	frames	bits	packets	dp tu	packets
42	Each set is called a _____	node	code	unicode	polar	node
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 topology we need _____	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	A_____can be hybrid	physical	networks	data	link	networks
49	A MAN is a network with a size between a _____ and _____.	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
50	When Two or more networks are connected they become an _____	network	inter network	internet connection	interconnection	inter network
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 _____	reverse address	reverse address result protocol	reverse addess	reverse addess research	reverse address resolution protocol
58	_____does not define any specific protocol.	TCP	HTTP	TCP/IP	SMTP	TCP/IP
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

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

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

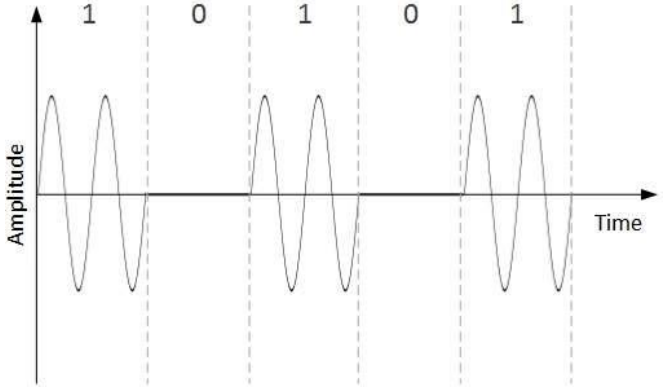
Data Communication Fundamentals and Techniques:

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.

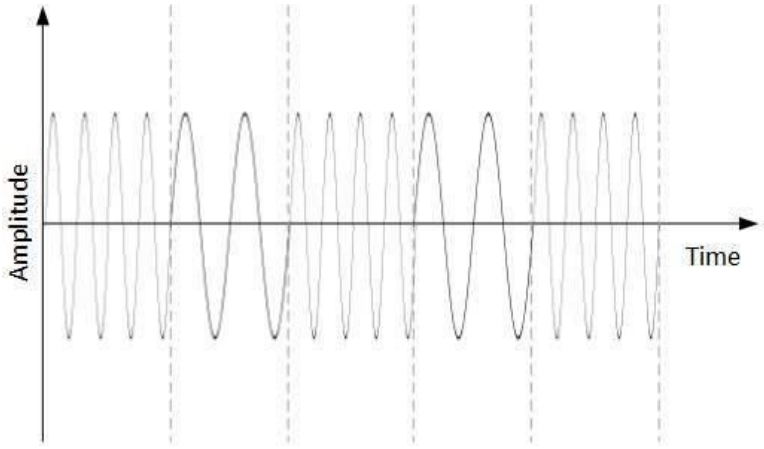
An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

- **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.

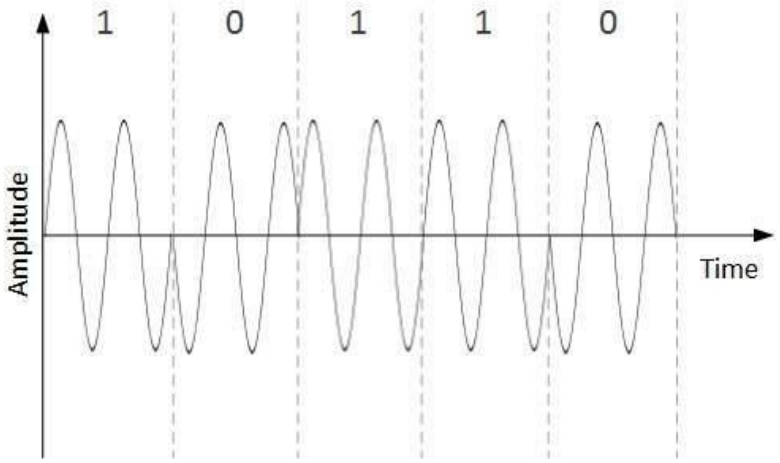
- **Frequency Shift Keying**
  In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



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.

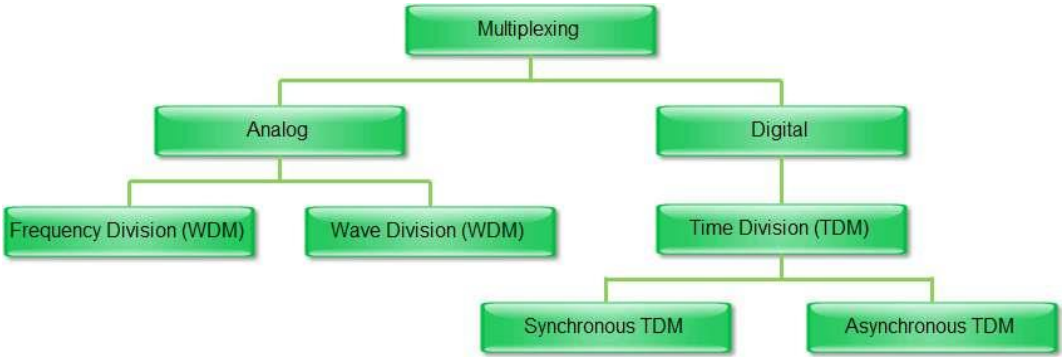
- **Quadrature Phase Shift Keying**

  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. Later, both the digital signals are merged together.

MULTIPLEXING TECHNIQUES

A communications device that multiplexes (combines) several signals for transmission over a single medium. A demultiplexer completes the process by separating multiplexed signals from a transmission line. Frequently a multiplexer and demultiplexer are combined into a single device capable of processing both outgoing and incoming signals. **A multiplexer is sometimes called a mux**.

.

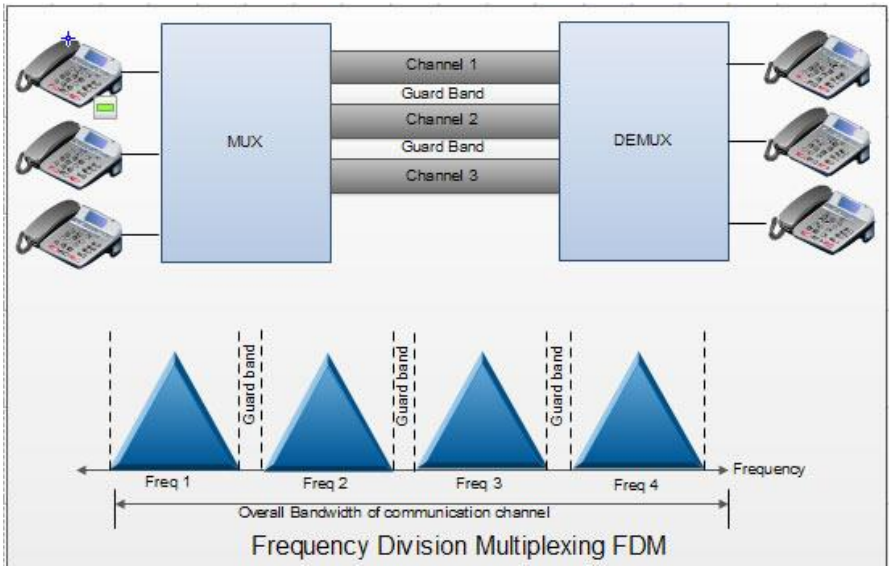


FDM:

Frequency-Division Multiplexing (FDM) is a scheme in which **numerous signals are combined for transmission on a single communications line or channel.** It is analog technique. Each signal is assigned a different frequency (sub channel) within the main channel.

FDM requires that the bandwidth of a link should be greater than the combined bandwidths of the various signals to be transmitted. Thus each signal having different frequency forms a particular logical channel on the link and follows this channel only. These channels are then separated by the strips of unused bandwidth called guard bands. These guard bands prevent the signals from overlapping as shown in Fig.

In FDM, signals to be transmitted must be analog signals. Thus digital signals need to be converted to analog form, if they are to use FDM.



A typical analog Internet connection via a twisted pair telephone line requires approximately three kilohertz (3 kHz) of bandwidth for accurate and reliable data transfer.

Twisted-pair lines are common in households and small businesses. But major telephone cables, operating between large businesses, government agencies, and municipalities, are capable of much larger bandwidths.

Advantages of FDM:

1. A large number of signals (channels) can be transmitted simultaneously.

2. FDM does not need synchronization between its transmitter and receiver for proper operation.

3. Demodulation of FDM is easy.

4. Due to slow narrow band fading only a single channel gets affected.

Disadvantages of FDM:

1. The communication channel must have a very large bandwidth.

2. Intermodulation distortion takes place.

3. Large number of modulators and filters are required.

4. FDM suffers from the problem of crosstalk.

5. All the FDM channels get affected due to wideband fading.

Applications of FDM

1. FDM is used for FM & AM radio broadcasting. Each AM and FM radio station uses a different carrier frequency. In AM broadcasting, these frequencies use a special band from 530 to 1700 KHz. All these signals/frequencies are multiplexed and are transmitted in air. A receiver receives all these signals but tunes only one which is required. Similarly FM broadcasting uses a bandwidth of 88 to 108 MHz

2. FDM is used in television broadcasting.

3. First generation cellular telephone also uses FDM.

Time Division Multiplexer

Short for Time Division Multiplexing, a type of multiplexing that combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel. Within T-Carrier systems, such as T-1 and T-3, TDM combines Pulse Code Modulated (PCM) streams created for each conversation or data stream.

TDM is the digital multiplexing technique.

2. In TDM, the channel/link is not divided on the basis of frequency but on the basis of time.

3. Total time available in the channel is divided between several users.

4. Each user is allotted a particular a time interval called time slot or time slice during which the data is transmitted by that user.

5. Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time.

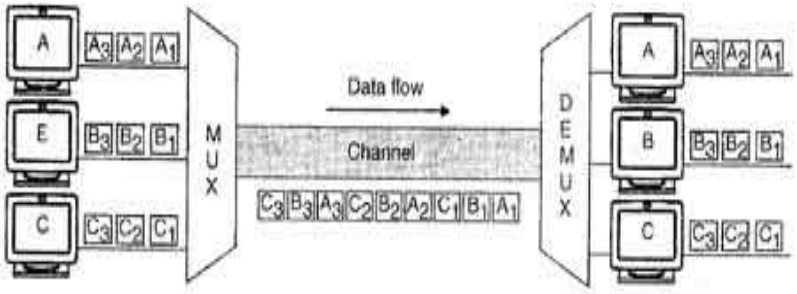
6. In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices.

7. In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one.

8. Thus each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel.

9. The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing.

10. The TDM signal in the form of frames is transmitted on the common communication medium.



Time Division Multiplexing (TDM)

Advantages of TDM :

1. Full available channel bandwidth can be utilized for each channel.
2. lntermodulation distortion is absent.
3. TDM circuitry is not very complex.
4. The problem of crosstalk is not severe.

Disadvantages of TDM :

1. Synchronization is essential for proper operation.
2. Due to slow narrowband fading, all the TDM channels may get wiped out.

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.

Code Division Multiplexing

Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals.

Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth.The receiver knows in advance the chip code signal it has to receive.

TRANSMISSION MEDIA.

Transmission media is a pathway that carries theinformation from sender to receiver. We use different types of cables or waves to transmit data.Data is transmitted normally through electrical or electromagnetic signals.

An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called **Communicationchannel.**

Types of Transmission Media

Transmission media is broadly classified into two groups.

1. Wired or Guided Media or Bound Transmission Media

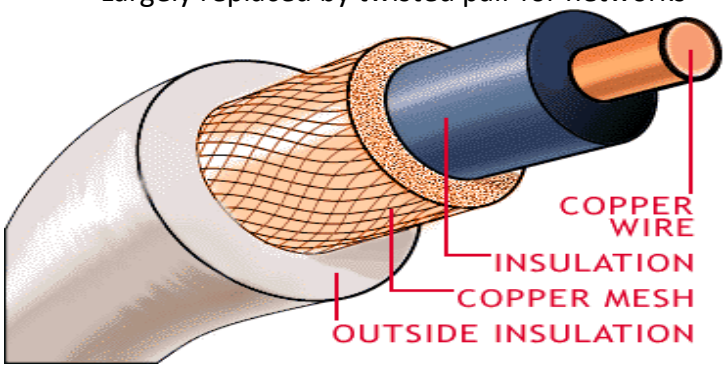
2. Wireless or Unguided Media or Unbound Transmission Media

How transmissions flow over media

- Simplex – only in one direction
- Half-Duplex – Travels in either direction, but not both directions at the same time
- Full-Duplex – can travel in either direction simultaneously

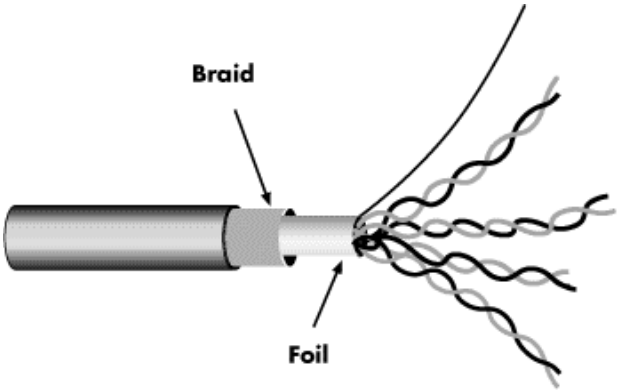
Coaxial Cable

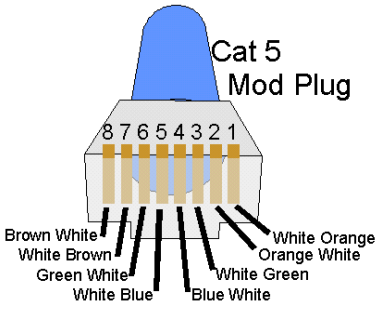
- First type of networking media used
- Available in different types (RG-6 – Cable TV, RG58/U – Thin Ethernet, RG8 – Thick Ethernet
- Largely replaced by twisted pair for networks



Unshielded Twisted Pair

- **Advantages**
  - Inexpensive
  - Easy to terminate
  - Widely used, tested
  - Supports many network types
- **Disadvantages**
  - Susceptible to interference
  - Prone to damage during installation
  - Distance limitations not understood or followed





Networks Switching Techniques and Access 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:

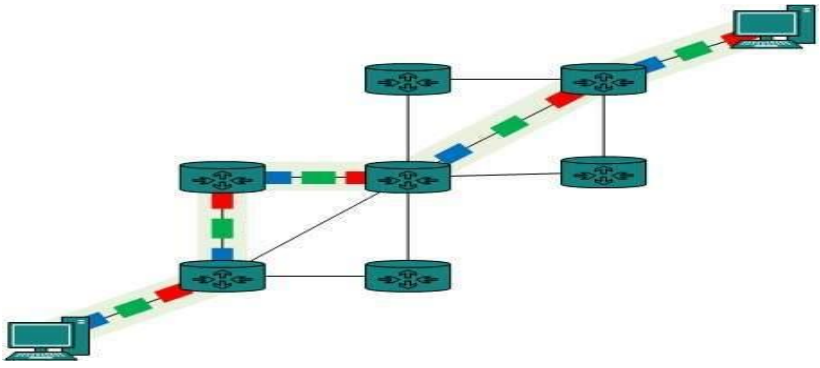
- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. 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

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.There 'is a need of pre-specified route from which data will travels and no other data is permitted.In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

- Establish a circuit
- Transfer the data
- Disconnect the circuit

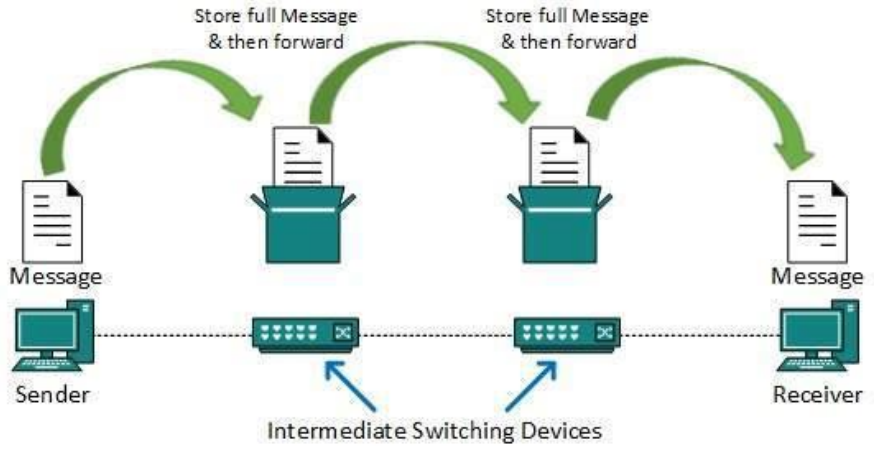


Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.



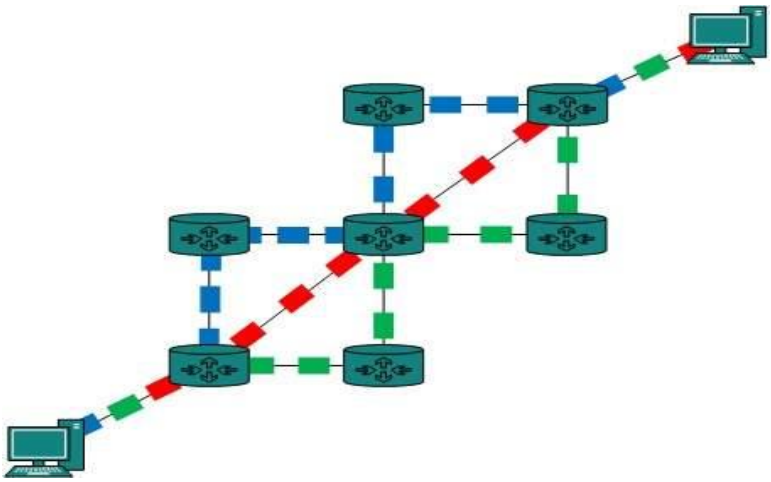
This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.



Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

Internet Connectivity

Here in this tutorial, we will discuss how to connect to internet i.e. internet service providers, software and hardware requirements, configuring internet connection etc.

Internet Service Providers (ISP)

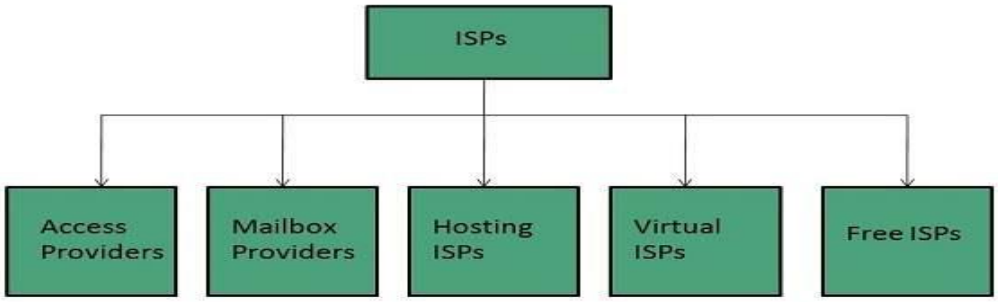
Internet Service Provider (ISP) is a company offering access to internet. They offer various services:

- Internet Access
- Domain name registration
- Dial-up access

- Leased line access

ISP Types

ISPs can broadly be classified into six categories as shown in the following diagram:



ACCESS PROVIDERS

They provide access to internet through telephone lines, cable wi-fi or fiber optics.

MAILBOX PROVIDER

Such providers offer mailbox hosting services.

HOSTING ISPS

Hosting ISPs offers e-mail, and other web hosting services such as virtual machines, clouds etc.

VIRTUAL ISPS

Such ISPs offer internet access via other ISP services.

FREE ISPS

Free ISPs do not charge for internet services.

Connection Types

There exist several ways to connect to the internet. Following are these connection types available:

1. Dial-up Connection
2. ISDN
3. DSL
4. Cable TV Internet connections

5. Satellite Internet connections
6. Wireless Internet Connections

Dial-up Connection

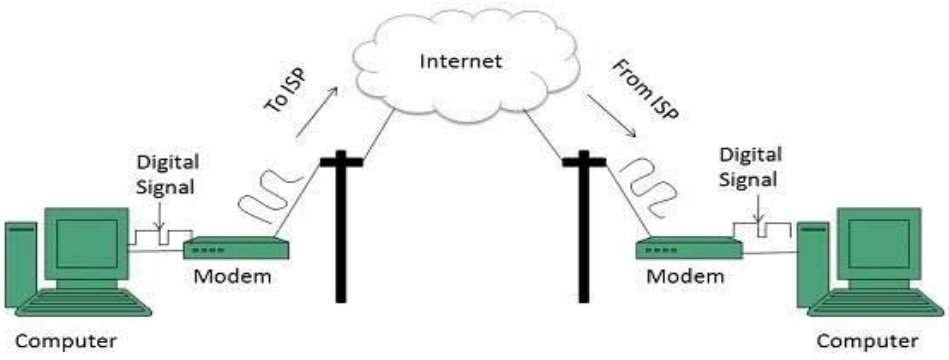
Dial-up connection uses telephone line to connect PC to the internet. It requires a modem to setup dial-up connection. This modem works as an interface between PC and the telephone line.

There is also a communication program that instructs the modem to make a call to specific number provided by an ISP.

Dial-up connection uses either of the following protocols:

1. Serial Line Internet Protocol (SLIP)
2. Point to Point Protocol (PPP)

The following diagram shows the accessing internet using modem:



ISDN

ISDN is acronym of **Integrated Services Digital Network.** It establishes the connection using the phone lines which carry digital signals instead of analog signals.

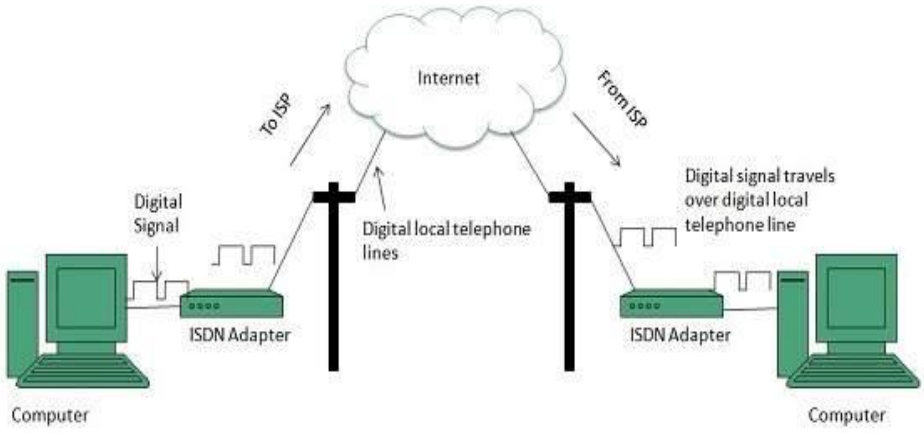
There are two techniques to deliver ISDN services:

1. Basic Rate Interface (BRI)
2. Primary Rate Interface (PRI)

Key points:

- The BRI ISDN consists of three distinct channels on a single ISDN line: t1o 64kbps B (Bearer) channel and one 16kbps D (Delta or Data) channels.
- The PRI ISDN consists of 23 B channels and one D channels with both have operating capacity of 64kbps individually making a total transmission rate of 1.54Mbps.

The following diagram shows accessing internet using ISDN connection:



DSL

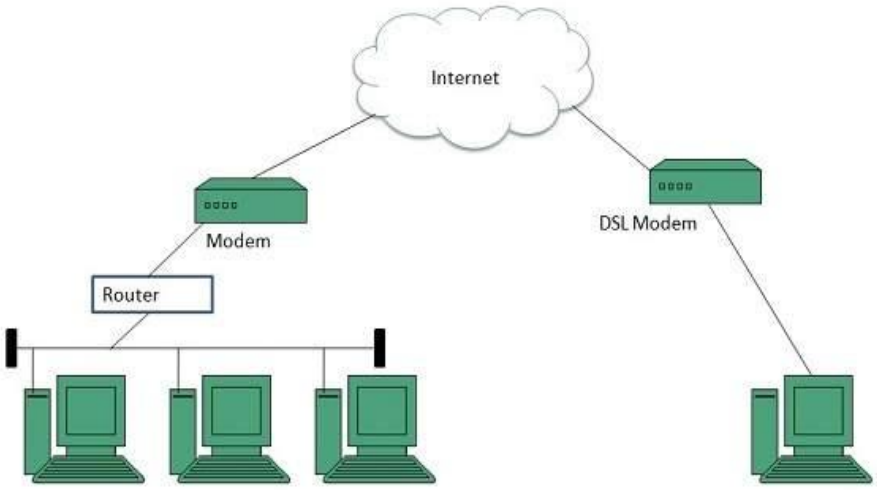
DSL is acronym of **Digital Subscriber Line.** It is a form of broadband connection as it provides connection over ordinary telephone lines.

Following are the several versions of DSL technique available today:

1. Asymmetric DSL (ADSL)
2. Symmetric DSL (SDSL)
3. High bit-rate DSL (HDSL)
4. Rate adaptive DSL (RDSL)
5. Very high bit-rate DSL (VDSL)
6. ISDN DSL (IDSL)

All of the above mentioned technologies differ in their upload and download speed, bit transfer rate and level of service.

The following diagram shows that how we can connect to internet using DSL technology:



Internet Access Using DSL Modem

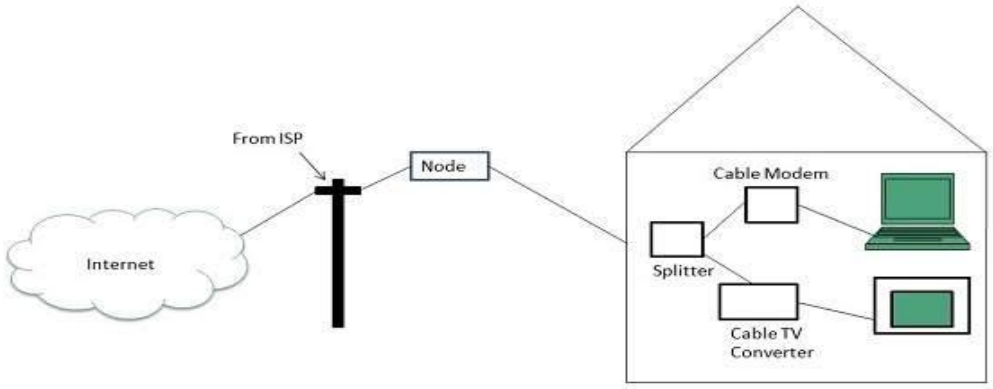
Cable TV Internet Connection

Cable TV Internet connection is provided through Cable TV lines. It uses coaxial cable which is capable of transferring data at much higher speed than common telephone line.

Key Points:

- A cable modem is used to access this service, provided by the cable operator.
- The Cable modem comprises of two connections: one for internet service and other for Cable TV signals.
- Since Cable TV internet connections share a set amount of bandwidth with a group of customers, therefore, data transfer rate also depends on number of customers using the internet at the same time.

The following diagram shows that how internet is accessed using Cable TV connection:



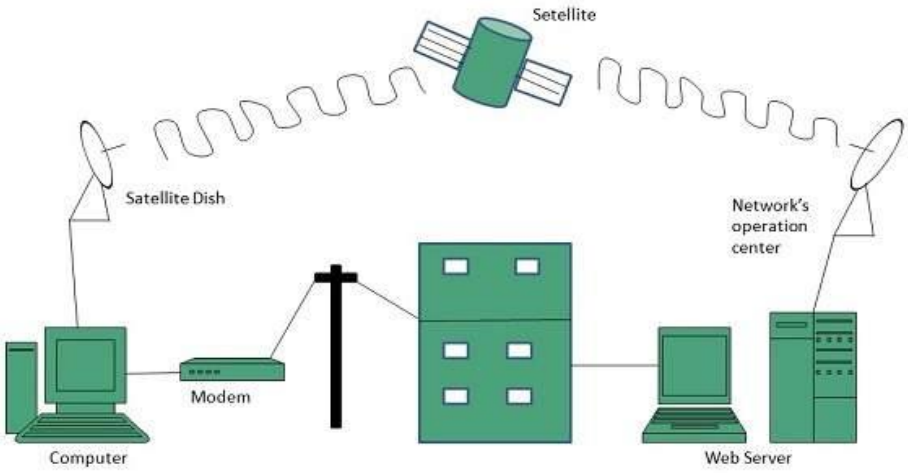
Satellite Internet Connection

Satellite Internet connection offers high speed connection to the internet. There are two types of satellite internet connection: one way connection or two way connection.

In one way connection, we can only download data but if we want to upload, we need a dialup access through ISP over telephone line.

In two way connection, we can download and upload the data by the satellite. It does not require any dialup connection.

The following diagram shows how internet is accessed using satellite internet connection:



Wireless Internet Connection

Wireless Internet Connection makes use of radio frequency bands to connect to the internet and offers a very high speed. The wireless internet connection can be obtained by either WiFi or Bluetooth.

Key Points:

- Wi Fi wireless technology is based on IEEE 802.11 standards which allow the electronic device to connect to the internet.
- Bluetooth wireless technology makes use of short-wavelength radio waves and helps to create personal area network (PAN).

POSSIBLE QUESTIONS

PART A – Multiple Choice Questions

1.In a frequency_domain plot, the vertical axis measures the_____
A)peak amplitude B)frequency C)phase D)slope

2. _____is a type of transmission impairment in which the signal loses strength due to different propogation speeds of each frequency that makes up the signal.
A) attenuation B) distortion C) distortion D) decibel

3. _____is a type of transmission impairment in which an outside source such as crosstalk corrupts a signal.
A) attenuation B)distortion C)noise D)decibel

4.The datalink layer is responsible for moving……from one hop to next
A)packets B)frames C)signals D)message

5.In a single_bit error,how many bits in a data unit are changed
A)one B)two C)four D)five

PART B – 2 Mark Questions

1. What are the approaches of packet switching?
2. What are the classes of transmission media?
3. What is a Link?
4. What is point-point link?
5. What are the types of switching
6. What is the purpose of Physical layer?

PART C – 8 Mark Questions

1. Elaborate the working of packet it switched networks with neat diagrams.
2. What is the transmission media used for computer networks?
3. Discuss in detail about virtual- circuit network with diagrams.
4. Explain in detail multiplexing techniques with proper diagram.
5. Describe in detail the characteristics of periodic analog signals.
6. Discuss in detail Digital to analog conversion.

UNIT V				
S.NO	**QUESTION**	**OPTION 1**	**OPTION 2**	**OPTION 3**
1	---------- are qualitative values that represent a flow data	data traffic	data descriptor	data traffic and data descriptor
2	the----- define the maximum data rate of the traffic	peak data rate	maximum burst size	bandwith
3	the----- define the maximum length of time the traffic is generated in the peak	effective bandwith	constant rate	peak data rate
4	the------- is the bandwith that the network needs to allocate for the flow of traffic	effective bandwith	peak data rate	maximum burst size
5	a constant-bit-rate is also called as -------	fixed_rate	nonfixed rate	both a & b
6	in ----------the rate of data flow changes in time, whith the change smooth	constant-bit-rate	variable-bit-rate	both a & b
7	in the ----------the data rate changes suddenly in a very short times	variable-bit-rate	constant-bit-rate	bursty data
8	congestion control is divided into-------- types	1	2	3
9	a ----------is mechanism that can prevent before and after it happens	open-loop	closed-loop	congestion control
10	in---------- control ,policies are applied to prevent congestion before it happens	open-loop congestion	closed-loop congestion	both a & b
11	if the sender feels that a sent packets is lost ,the packet needs to ----------	transmission	delete	retransmission
12	the type of ---------- at the sender may also affect congestion	closed-loop	window	control
13	the -------- policy imposed by the receiver may also effect	acknowledgment	discarding	admission
14	a good ------- policy by the routers may prevent congestion and the same time may	admission	window	discarding
15	an---------- policy , which is a quality of service mechanism	acknowledgment	window	daiscarding
16	a ----------is mechanism try to alleviate congestion after it happens	open-loop	closed-loop	congestion control
17	the technique od--------- refer to congestion control mechanism in which a congestion	choke packet	control	window
18	in---------- is anodeto node congestion control that start with a node and	backpressure	choke packet	none
19	a---------- is apacket sent by anode to the source to inform it of congestion	control	choke packet	admission
20	in ----------there is no communication between the congested nodes and source	explict signaling	left side	implicit signaling
21	lack of reliablity means losing a ----------	packet	control	data flow
22	a ---------- in a file transfer or E-mail is less important	jitter	delay	reliablity
23	a ---------- in the variation in delay for packets belonging to the same flow	jitter	reliablity	delay
24	different application need different ----------	maximum burst size	effective bandwith	bandwith

25	packets from different flows arrive at ----------	scheduling	fifo	bandwith
26	a good ---------- technique treats the different flows in apair in appropriate	bandwith	scheduling	admission
27	several scheduling are designed to improve ----------	quality of service	quality of data	quality of control
28	in -------- queuing , packets wait in a buffer(queue) until the node is ready to	lifo	linked	fifo
29	in --------- queuing , packets are first assigned to a priorety class	fifo	lifo	circular
30	in priority the packets in a---------- priority queue are processed first	lowest	highest	medium
31	a better scheduling method is---------- queuing, in this ,the packets are still	weighted fair	priority	both a & b
32	the-------- is amechanism to control the amount and rate of traffic sent to the	priority	data descriptor	traffic shaping
33	the ---------- does not credit an idle host	token bucket	leak bucket	both a & b
34	a---------- algorithm shapes bursty traffic into fixed-rete traffic by averaging	leak bucket	token bucket	empty bucket
35	the ------- bucket allows the bursty traffic at aregulated maximum rate	empty bucket	leak bucket	token bucket
36	the---------- can be combained to credit an idle host and at the same time regulate	leak bucket	token bucket	empty bucket
37	_____allows us to send message include text,auido and video .	mail	internet	E-mail
38	the_____client established a connection with MTA server on the system	MTA	alice	UA
39	the first component of an electrionic mail system is the_____	alice	server	user agent
40	_____is the example of user agents are mail,pine,and elm	user agent	command driven	GUI-based
41	_____ define the names of aspecial files	local part	domain name	mime
42	the second part of address is_____	system server	internet	domain name
43	MIME is_____	multiple internet mail extensions	multipurpose interface mail	multipurpose internet mail
44	_____ has delete and keep mode	pop	pop2	pop3
45	_____is the mechanism provided by TCP/IP for copying a file from one host	FTP	MIME	UA
46	_____ is the default formate for transferring text files	image	ASCII	data structure
47	_____ is the default formate for transferring binary files	image	data structure	record structure
48	in the _____ formate, the file is a continuous stream of byte	file structure	record structure	data structure
49	the service provider is distrubuted over many location called _____	internet	sites	www
50	theweb page store at the _____	hard disk	disk	client

51	the _____ is the computer on which the information is located	path	sites	host
52	_____is the pathname of the file where the information is located	host	path	server
53	_____ is language for creating web pages	HTML	C	C++
54	a_____ is created by a web server whenever a browser request the	common gate way	dynamic document	script
55	_____ is the protocol used mainly to access data on the world wide web	communicatio	network	WWW
56	a_____ replaces one symbol with another	substitution cipher	monoalphabetic ciphet	traditional cipher
57	a_____ reorders (permutes) symbols in a block of symbols	traditional cipher	substitution cipher	transposition cipher
58	the _____ is sometimes referred to as the caesar cipher	monoalphabetic ciphet	shift cipher	traditional cipher
59	a _____ is a techique that emplys the morden block ciphers such as	modes	modes of operation	operating server
60	the most common public key algorithm is _____	RSA	RSSA	RSS
61	_____means that the data can must arrive at the receiver exactly as they	integrity	message integrity	authentication
62	_____ is the service beyond message integrity	message authentication	message integrity	integrity
63	a digital signature needs a _____ system	private-key	primary-key	public-key
64	a digital signature today provides _____	message authentication	integrity	message integrity
65	a_____ keys between two parties is used only once	session	primary-key	private-key

OPTION 4	ANS
traffic data	data descriptor
effective bandwith	peak data rate
maximum burst size	maximum burst size
data descriptor	effective bandwith
none	fixed_rate
bit rate	variable-bit-rate
constant-bit-rate	bursty data
4	2
none	congestion control
congestion control	open-loop congestio
none	retransmission
discarding	window
window	acknowledgment
acknowledgment	discarding
admission	admission
none	closed-loop
backpressure	backpressure
window	backpressure
backpressure	choke packet
both a&c	implicit signaling
admission	packet
none	delay
none	jitter
peak data rate	bandwith

switch	switch
window	scheduling
quality of data flow	quality of service
none	fifo
priority	priority
none	highest
fair queuing	weighted fair
weighted fair	traffic shaping
empty bucket	leak bucket
both a & b	leak bucket
none	token bucket
both a & b	both a & b
all the above	E-mail
system server	MTA
services provider	user agent
E-mail	command
both a & b	local part
local part	domain name
multipurpose internet mail	multipurpose
none	pop3
pop3	FTP
record structure	ASCII
ASCII	image
image	file structure
http	sites
server	server

cookies	host
sites	path
java	HTML
all the above	dynamic document
HTTP	HTTP
none	substitution cipher
monoalphabetic ciphet	transposition cipher
transposition cipher	shift cipher
none	modes of operation
none	RSA
message authentication	message integrity
authentication	message authentica
none	public-key
authentication	message integrity
public-key	session

UNIT IV

Q.no	Question	Choice1	Choice2	Choice3
1	Internetwork is made of_____networks.	3 LANs and 2 WANs	2 LANs and 3	.4 LANs and 1
2	Internet at the network layer is a_____network.	packet-switched	.LAN	connection
3	Internet has chosen the datagram approach to_____in network layer	routers	packets	switching
4	Internet is made of so many_____networks.	homogenous	hetrogeneous	MAN
5	Communication at network layer in the internet is_____.	connectionless	point-to-point	connection oriented
6	What is the abbrevation for IPV4_____.	Inter Protocol Versus 4	Inter Position	Internet protocol
7	IPV4 provides the term 'best-effort' means that_____.	no error control	error control	error detection
8	Packets in the IPV4 layer are called_____.	frames	datagroup	switching
9	A datagram is a variable length packet consisting of_____parts.	one	six	two
10	The total length field defines the total length of the datagram including_____.	footer	header	flags
11	Abbravation for MTU_____.	Minimum Transfer Unit	Maximum Transfer	Maximum Travel
12	_____in the IPV4 packet covers only header,not the data.	Check subtract	Check sum	options
13	Options can be used for network testings and_____.	checking	packets	types
14	A no-operation option is a _____ byte used as a filler between option.	three	six	one
15	_____can only used as the last option.	end-of-option	first-of-option	options
16	Record route can list up to_____router address.	fifteen	sixty	nine
17	_____route has less rigid.	loose source	strict source	no route
18	_____is expressed in millisecond,from midnight.	time stand	time stamp	time shot
19	IPv4 also known as_____.	IPNg	IPNG	ipNG
20	The adoption of IPv6 has been_____.	fast	slow	neuter
21	An IPv6 address is_____bits long.	128	126	125
22	IPv6 has_____options to allow for additional functionalities.	old	first	new
23	In packet format,the extension headers and data from the upper layer conains upto_____bytes of	65.033	65.535	65.536
24	Base header with_____fields.	eight	ten	five

25	The 4bit field defines the_____number of the IP.	versus	header	.footer
26	Delivery has_____types.	3	4	5
27	Source and destination of the packet are located on the same physical network called_____.	Indirect delivery	Inward delivery	Direct delivery
28	One technique to reduce the content of a routing table is_____.	before-hop	next-hop	first hop
29	The Routing table holds only the address of the next hop_____.	next hop	route method	network method
30	A second technique to reduce the routing table_____.	next hop	default	forward
31	All hosts connected to the same network as one single entity_____.	route	next-hop	host specific
32	In classless addressing,atleast_____columns in a routing table.	5	6	3
33	In an address aggregation,the network for each organization is_____.	independent	dependent	department
34	The routing table can be either_____.	static	static and dynamic	static or dynamic
35	A static routing table can be used in a_____internet.	big	small	multi
36	Dynamic routing protocols such as_____.	RIP	OSPF	BGP
37	The flags are_____.	U,G,H,D,M	G,H,S,S,D	U,G,H
38	The one of the flag is not present,the router is down_____.	G	U	H
39	D means_____.	added by direction	added	added by redirectio
40	Routing inside an autonomous system____	Intra	Inter	Inside
41	Abbrevation for BGP_____.	Border Gateway Process	Bit Gateway	Border Gateway
42	A node sends its routing table,at every_____in a periodic update.	33s	30s	31s
43	_____algorithm creates a shortest path tree from a graph.	data	dakstra	define
44	An area is a collection of_____.	networks	hosts	route
45	_____link is a network and is connected to only one router.	stub	point-to-point	transient
46	Multicasting of the relationship is_____.	one-to-one	many-to-one	one-to-many
47	_____layer is responsible for process-to-process delivery.	transport	physical	application
48	Internet has decided to use universal port numbers for severs called_____.	well-unknown port	well-known	well-known
49	IANA has divided the port numbers into_____ranges.	six	four	five
50	_____a connection,is first established between the sender and receiver.	connection-oriented	connectionless	token

51	UDP is called_____.	connection-oriented	check point	token
52	UDP length = IP length - _____.	IP length	IP breadth	IP header's
53	UDP is a suitable transport protocol for_____.	unicasting	multicasting	nocasting
54	TCP groups a number of bytes together into a packet called_____.	segment	encapsulation	datagram
55	The acknowledgement number is _____.	natural	whole	integers
56	_____ flag is used to terminate the connection.	TER	FIN	URG
57	_____ protocol is used to remote procedure call.	DNS	PRC	RPC
58	An ACK segment,if carrying _____data consumes no sequence number.	no	2	3
59	In TCP,one end can stop sending data while still receiving data is_____.	full-close	full-open	half-close
60	The value of RTO is dynamic in TCP and is updated based on _____segment.	RTO	RTT	ACK

Choice4	ANS
1 LAN and 4	.4 LANs and 1
connetionless	packet-switched
protocol	protocol
multipoint	hetrogeneous
packet-switched	connectionless
Internet Position	Internet protocol
datagram	no error control
datagrams	datagrams
three	two
frames	header
Minimum Travel	Maximum Transfer
Check product	Check sum
debugging	debugging
four	one
no options	end-of-option
ten	nine
record	loose source
all the above	time stamp
lpng	lpng
quick	slow
127	128
last	new
65.035	65.535
none of these	eight

version	version
2	2
Outward delivery	Direct delivery
last hop	next-hop
host method	route method
network specific	network specific
d.network specific	host specific
4	4
none of these	independent
all the above	static or dynamic
LAN	small
all the above	all the above
none of these	U,G,H,D, M
D	U
none	added by redirectio
all the above	Inside
Byte Gateway	Border Gateway
35s	30s
dijkstra	dijkstra
all the above	all the above
none of these	stub
many-to-many	one-to-many
network	transport
well-unknown	well-known
three	three
dialog	connection-oriented

connetionless	connetionless
IP header's	IP header's
none of these	multicasting
data binding	segment
cumulative	cumulative
PSH	FIN
RPCC	RPC
5	no
none	half-close
none	RTT

UNIT III			
SL NO	**QUESTIONS**	**OPTION A**	**OPTION B**
1	Transmission errors are usually detected at the……..layer of OSI model	physical	datalink
2	Transmission errors are usually corrected at the……..layer of OSI model	network	transport
3	Datalink layer imposes a ……mechanism to avoid	flow control	error control
4	Error control mechanism of datalink layer is achieved through a ……..added to the	header	trailer
5	The datalink layer is responsible for moving……from one hop to next	packets	frames
6	In a single_bit error,how many bits in a data unit are changed	one	two
7	In a burst error,how many bits in a data unit are changed	less than 2	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 bit
9	Single bit error will least occur in……data transmissions	serial	parallel
10	To detect errors or correct errors,we need to send …… with data	address	frames
11	Which of the following best describes a single bit error	a single bit is inverted	a single bit is inverted per data
12	In block coding,we divide our message intp blocks,each of k bits,called	dataword	codeword
13	In block coding,the length of the block is …….	k	r
14	Block coding can detect only ……error	single	burst
15	We need ……..redundant bits for error correction than for error detection	less	more
16	The corresponding codeword for the dataword 01 is…..	011	000
17	The hamming distance can easily be found if we apply the …… operation	XOR	OR
18	The …… hamming distance is the smallest hamming distance between all	minimum	maximum
19	The hamming distance d(000,111) is …….	1	0
20	To guarantee correction of upto t errors in all cases,the minimum hamming distance	d(min)=2t+1	d(min)=2t-1
21	To guarantee correction of upto s errors in all cases,the minimum hamming distance	d(min)=s-1	d(min)=s+1
22	A simple_parity check code is a single bit error detecting code in which n=……	K	K*1
23	The codeword corresponding to the dataword 1111 is	11110	11111

24	A simple_parity check code can detect an ……. Number of errors	odd	even
25	The hamming code is a method of ……..	error detection	error correcton
26	To make the hamming code respond to a burst error of size N,we neeed to make	N+1	N-1
27	CRC is used in network such as …….	WAN	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
29	At the CRC checker,…….means that the dataunit is damaged.	string of 0's	string of 1's
30	……. Is a regulation of data transmission so that the receiver buffer do	flow control	error control
31	……..in the datalink layer separates a message from one source ti a destination or	packets	address
32	…….is the process of adding 1 extra byte whenever there is a flag or escape	byte stuffing	redundancy
33	…….is the process of adding 1 extra 0 whenever five consecutive 1's follows a 0	byte stuffing	redundancy
34	……in the data link layer is based on automatic repeat request,which is the	error control	flow control
35	At any time an error is detected in an exchange specified frames are	ARQ	ACK
36	The datalink layer at the sender side gets data from its……..layer	network	physical
37	ARQ stands for ……..	acknowledge repeat request	automatic repeat request
38	Which of the following is a data link layer function	line discipline	error control
39	In protocols the flow and error control information such as ACK and NAK is	stop and wait	go_back
40	In stop and wait ARQ ,the sequence of numbers is based on…….	modulo-2-arithmetic	modulo-12-arithmetic
41	Error correction in …….is done by keeping a copy of the send frames and	stop and wait ARQ	ARQ
42	In the Go_Back N protocol,the sequence numbers are modulo……..	2^m	2^{m-1}
43	In sliding window ,the range which is the concern of the sender is called……..	send sliding window	receive sliding window
44	Piggypacking is used to improve the efficiency of the …….protocols.	bidirectional	unidirectional
45	The send window can slide …….slots when a valid acknowledgment arrive	one or more	one
46	The upper sublayer that is responsible for flow and error control is	logical	media access
47	The MAC(media access control)sublayer co-ordinates the datalink task within a	LAN	MAN
48	The lower sublayer that is responsible for multiple access resolution is called	Logical	media access
49	In the sliding window method or flow control several frame can be be ……..at	transit	received

50	The sliding window of the sender expands to the ……..when acknowledgement are	left	middle
51	Error detecting codes require …….nuber of redundant bits.	less	equal
52	The datalink layer transforms the ……,a raw transmission facility to a	datalink	physical
53	Datalink layer divided into …… functionality oriented sublayer.	one	zero
54	The send window in Go_Back N maximum size can be ……	2^m	2^{m+1}
55	In stop and wait ARQ and Go_Back_N ARQ,the size of the send window	0	3
56	The relationship between m and n in hamming code is ……	n=2m-1	n=m
57	A simple parity_check code is a single_bit error detecting code in which n=k+1 with	3	1
58	……..mechanism of datalink layer is achieved through added to the trailer added	ARQ	ARC
59	In ……,we divide our message into blocks	convolution coding	block coding
60	The …….layer at the sender site gets data from its network layer.	physical	datalink
61	In the …….protocol,the sequence numbers are modulo 2^m	Go_Back N	Simplest

OPTION C	OPTION D	
network	transport	physical
datalink	physical	transport
access control	none of the above	flow control
adress	frames	trailer
signals	message	frames
four	five	one
2	3	2 or more than 2
two	three	first corrupted bit to last corrupted
synchronous	asynchronous	serial
extra bits	packets	extra bits
a single bit is inverted per	any of the above	a single bit is inverted per data
integers	none of the above	dataword
k+r	k-r	k+r
multiple	none of the above	single
equal	less than or equal to	more
101	110	011
AND	NAND	XOR
equal	none of the above	minimum
2	3	2
d(min)=2t	d(min)=t+1	d(min)=2t+1
d(min)=s	none of the above	d(min)=s+1
K-1	K+1	K+1
11101	11011	11110

prime	none of the above	odd
error encapsulation	A and B	error correcton
N	0	N
LAN	MAN	LAN and WAN
non zero	the quotient at the sender	all 0's
a string of alternating 1's and	a non-zero remainder	a non-zero remainder
access control	none of the above	flow control
framing	none of the above	framing
bit_stuffing	none of the above	byte stuffing
bit_stuffing	none of the above	bit_stuffing
access control	none of the above	error control
NAK	SEL	ARQ
application	transport	network
automatic repeat quantisation	automatic retransmission	automatic repeat quantisation
flow control	all the above	all the above
A and B	piggybacking	piggybacking
modulo-N-arithmetic	all the above	modulo-2-arithmetic
ACK	NAQ	stop and wait ARQ
2^{m+1}	2	2m
piggybacking	none of the above	send sliding window
multidirectional	none of the above	bidirectional
two	two or more	one or more
A and B	all the above	logical
WAN	LAN and MAN	LAN
A and B	all the above	media access
A and B	none of the above	transit

right	B and C	right
more	less than or equal to	more
network	transport	physical
two	three	two
2	2^{m-1}	2m-1
1	2	1
n=m-1	n=2m+1	n=2m-1
0	2	2
Error control	Flow control	Error control
linear coding	A and C	block coding
application	transport	datalink
Stop and wait	all the above	Go_Back N

KARPAGAM ACADEMY OF HIGHER EDUCATION

DEPARTMENT OF CS,CA & IT

II B.Sc CS

COMPUTER NETWORKS (16CSU303)

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	Given two sine waves A and B, if frequency of A is twice that of B, then the period of B is_____ that of A	one_half	twice	the same as	indetermine from	one_half
8	A sine wave is_____	periodic and continuous	aperiodic and continuous	periodic and discrete	aperiodic and discrete	periodic and continuous

9	_____is a type of transmission impairment in which the signal loses strength due to the resistance of the transmission medium	attenuation	distortion	noise	decibel	attenuation
10	_____is a type of transmission impairment in which 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 destance 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	If a symbol is composed of 3bits ther are_____ data levels	2	4	8	16	8
16	_____ encoding has a transition at the middle of each bit	RZ	manchester	differential manchester	all the above	manchester
17	_____ encoding has a transition at the begining of each 0 bit	RZ	manchester	differential manchester	all the above	RZ
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	equal to the highest frequency of a signal	twice the bandwidth of a signal	twice the highest frequency of	twice the highest 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 alternating positive and negative values for 1's?	NRZ-I	RZ	manchester	AMI	AMI
23	RZ encoding involves_____ signal levels	two	three	four	five	three
24	Which encoding technique attempts to solve loss of synchronization due to long string of 0's?	BNZS	NRZ	AMI	(a) and (b)	BNZS
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	anolog-to-analog	analog-to-digital	digital-to-anolog
32	AM and FM are examples of modulation	digital-to-digital	digital-to-anolog	anolog-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	Which of the following is most affected by noise?	PSK	ASK	FSK	QAM	ASK

35	If the baud rate is 400 for a 4-PSK signal, the baud rate is_____ bps	100	400	800	1600	800
36	If the bit rate for an ASK signal is 1200bps, the baud rate is	300	400	600	1200	1200
37	If the bit rate for an FSK signal is 1200bps, the baud rate is_____	300	400	600	1200	1200
38	If the baud rate for a QAM signal is 3000 and a signal unit is represented by a tribit, what is the bit rate?	300	400	1000	9000	9000
39	In if-QAM there are 16_____	combintion of phase & amplitude	amplitude	phases	bps	combintion of phase & amplitude
40	What modulation technique involves tribits, eight different phase shifts and one amplitude?	FSK	8-PSK	ASK	4-PSK	8-PSK
41	The bandwidth of an FM signalrequires 10 times the bandwidth of the_____ signal	carrier	modulating	bipolar	sampling	modulating
42	Modulation of an analog signal can be accomplished through changing the_____ of the carrier signal	amplitude	frequency	phase	any of the above	frequency
43	As the bit rate of an FSK signal increases, the bandwidth_____	dereases	increases	remains the same	doubles	increases
44	The bit rate always equals the baud rate in which type of signal?	FSK	QAM	4-PSK	all the above	FSK
45	A modulator converts a(n)_____ signal to a(n)_____ signal	digital; analog	analog; digital	PSK; FSK	FSK; PSK	analog; digital
46	A 56K modern can download at a rate of_____ kbps and upload at a rate of_____kbps	33.6; 33.6	33.6; 56.6	56.6; 33.6	56.6; 56.6	56.6; 33.6
47	The sharing of medium and its link by two or more devices is called_____	modulation	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 contenna is a(n)_____ antenna	omni directional	bi directional	uni directional	horn	omni directional
60	A telephone network is an example of a_____ network	packet switching	circuit switched	message switched	none of the above	circuit switched

KARPAGAM ACADEMY OF HIGHER EDUCATION

DEPARTMENT OF CS,CA & IT

II B.Sc CS

COMPUTER NETWORKS (16CSU303)

UNIT I

S.NO	QUESTION	CHOICE1	CHOICE2	CHOICE3	CHOICE4	ANS
1	Data communication means exchange of data between _____devices.	one	two	six	four	two
2	The system must deliver data to the correct destination is called_____	accuracy	jitter	delivery	timeliness	delivery
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	The term timing refers to _____ characteristics.	two	three	four	six	two
10	_____standards are often established originally by manufactures.	de jure	de facto	de fact	semantics	de facto
11	In physical layer we can transfer data into _____	frame	packet	bit	sp du	bit
12	Hob to hob delivery is done by the _____	session layer	datalink layer	network layer	transport layer	datalink layer
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	hierarchical
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	Bus topology has a long link called_____	backbone	hub	host	hop	backbone
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/frequenc	propagation speed/frequency
22	Composite signal can be classified into _____types	five	three	four	two	two
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 duration
27	A_____signal is a composite analog signal with an infinite bandwidth	simple	composite	digital	analog	digital
28	Decibel (dB) =_____	10 log10 p2/p1	p1/p2	10 log10 p1/p2	2log10 p1/p2	10 log10 p2/p1
29	Transmission time=_____	message size/birate	distance/bandwid th	message size/distance	message size/bandwidth	message size/bandwidth
30	_____and star is a point to point device.	bus	ring	mesh	physical	mesh

31	Protocols can be classified into _____ key elements	one	three	four	two	three
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 interconnectio	open system internetworking	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 _____	user data protocol	user datagram protocol	user defined protocol	user dataframe protocol	user datagram protocol
38	FTP_____	file transmit protocol	file transmission protocol	file transfer protocol	flip transfer protocol	file transfer protocol
39	SMTP_____	single mail transfer	simple mail transfer protocol	simple mail transmission	single mail transmit	simple mail transfer protocol
40	Complete a cycle is called as _____	period	frequency	non periodic	periodic	period
41	Jitter is a form of_____	frames	bits	packets	dp tu	packets
42	Each set is called a _____	node	code	unicode	polar	node
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 topology we need _____	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	A_____can be hybrid	physical	networks	data	link	networks
49	A MAN is a network with a size between a _____ and _____.	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
50	When Two or more networks are connected they become an _____	network	inter network	internet connection	interconnection	inter network
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 _____	reverse address resolution	reverse address result protocol	reverse addess revolutinized	reverse addess research	reverse address resolution protocol
58	_____does not define any specific protocol.	TCP	HTTP	TCP/IP	SMTP	TCP/IP
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 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.

Data Link Layer Functions and Protocol

DCN - Error Detection & Correction

Error

A condition when the receiver's information does not matches with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

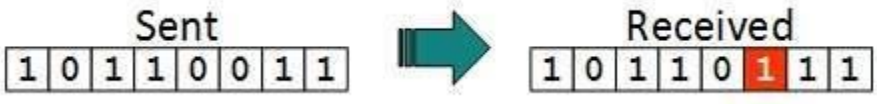
There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing.Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

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

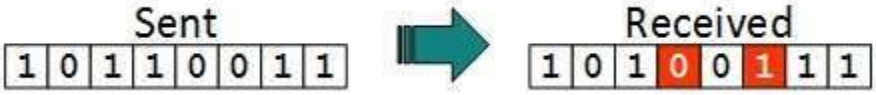
There may be three types of errors:

- **Single bit error**



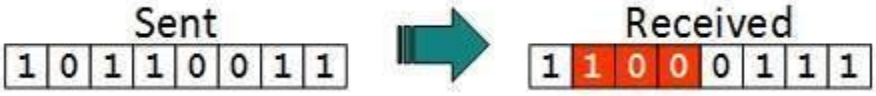
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



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

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

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

Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

Some popular techniques for error detection are:
1. Simple Parity check
2. Two-dimensional Parity check

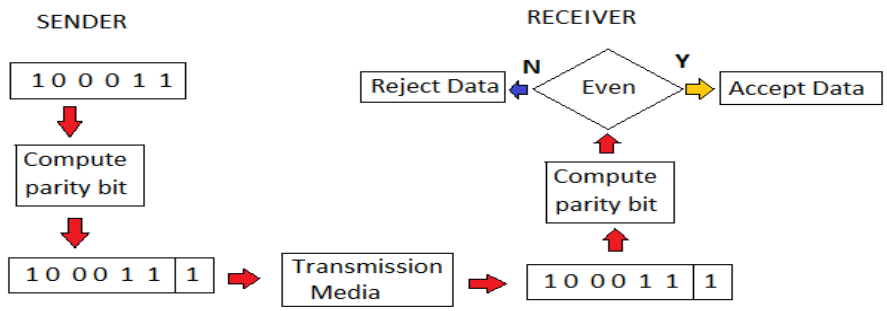
3. Checksum
4. Cyclic redundancy check

1. Simple Parity check

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

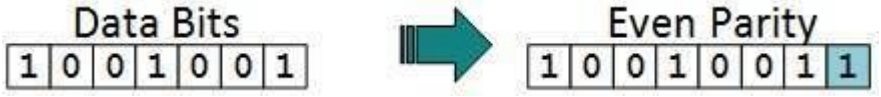
This scheme makes the total number of 1's even, that is why it is called even parity checking.



Parity Check

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

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

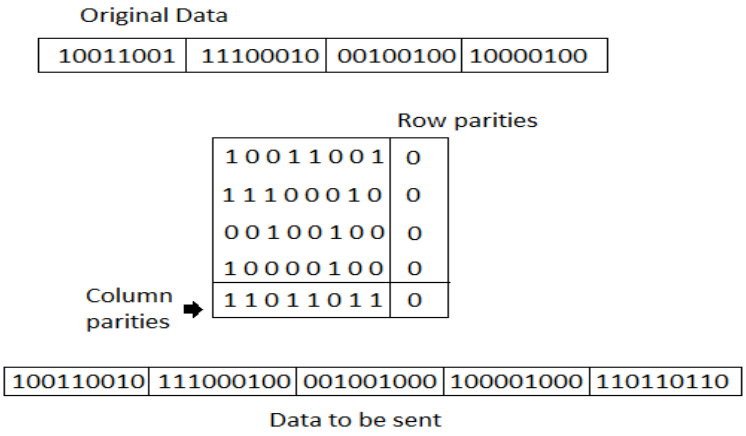


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

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

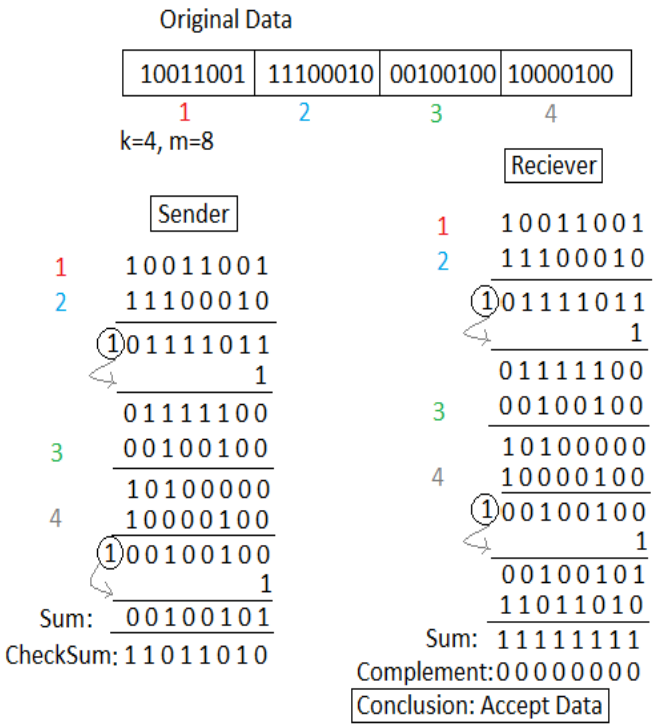
2. Two-dimensional Parity check

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.



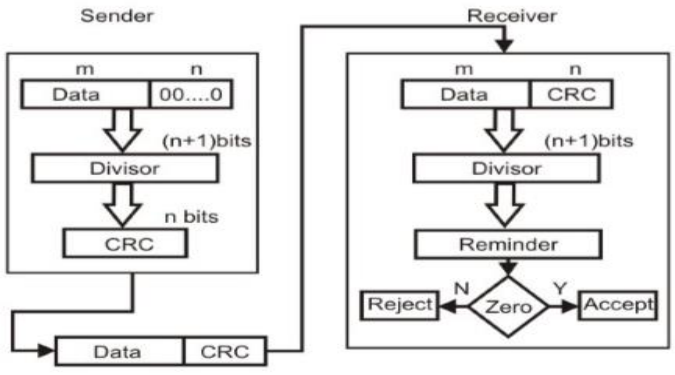
3. Checksum

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.



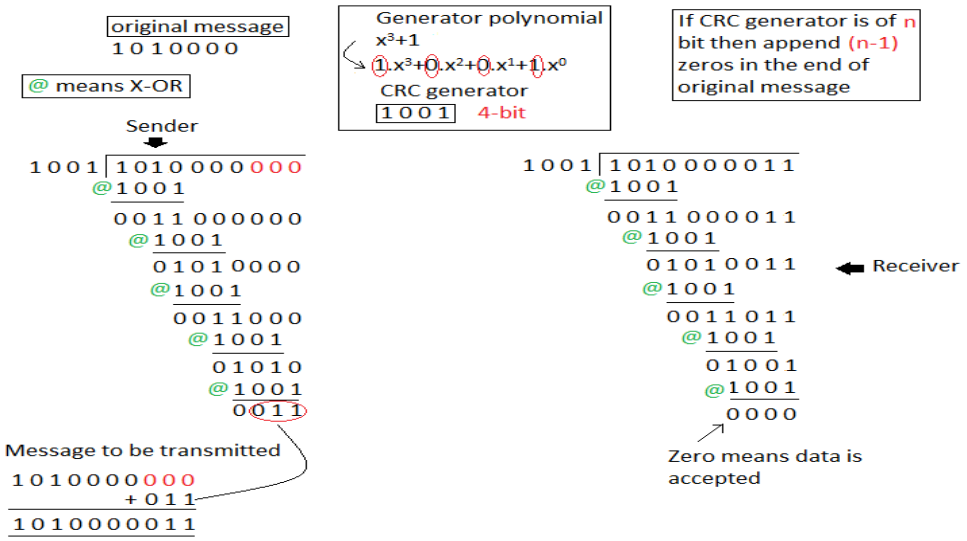
4. Cyclic redundancy check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



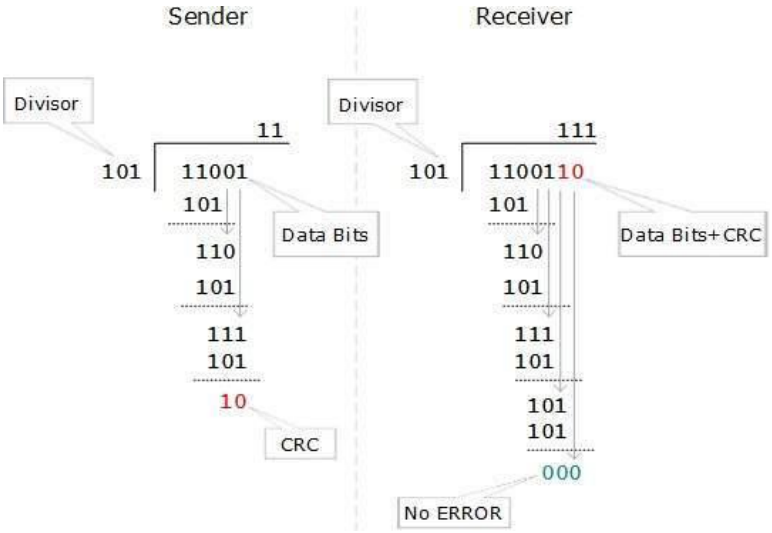
.

Example :



Cyclic Redundancy Check (CRC) EXAMLE 2

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.

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

DCN - Data-link Control & Protocols

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

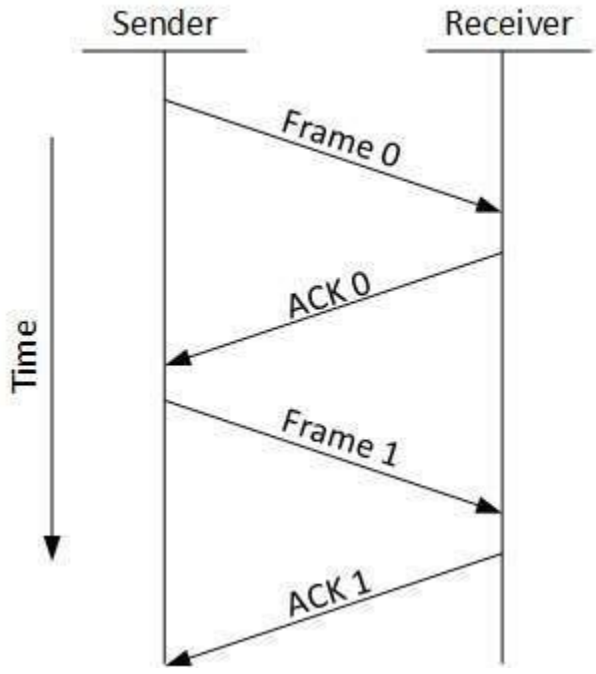
Flow Control

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

Requirements for error control mechanism:

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

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

Stop and Wait ARQ

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:

- **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)

- RoundTripTime (**RTT**) = 2* Propagation Delay
- TimeOut (**TO**) = 2* RTT
- Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 180 seconds)

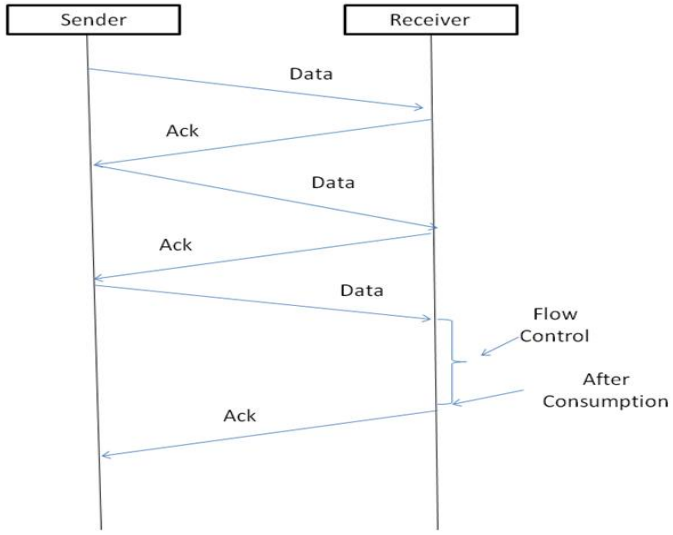
Simple Stop and Wait

Sender:

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

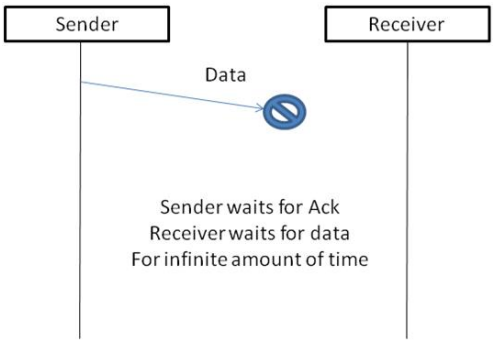
Receiver:

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

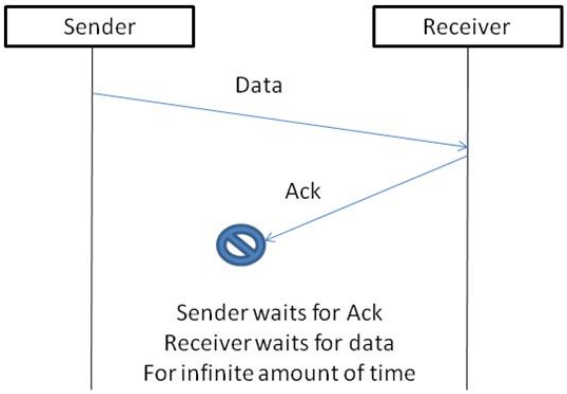


Problems :

1. Lost Data



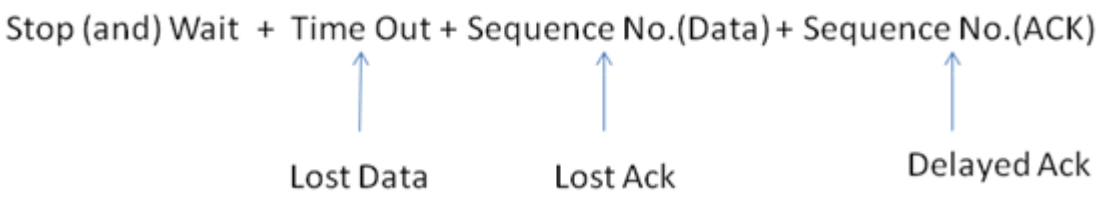
2. Lost Acknowledgement:



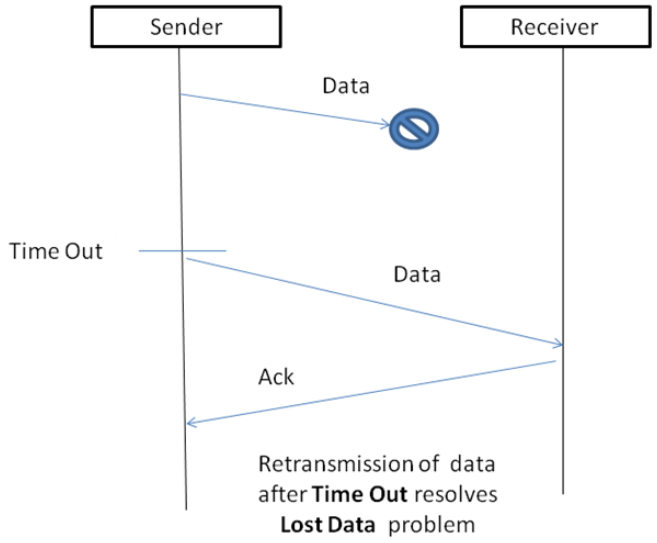
3. Delayed Acknowledgement/Data: After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait ARQ (Automatic Repeat Request)

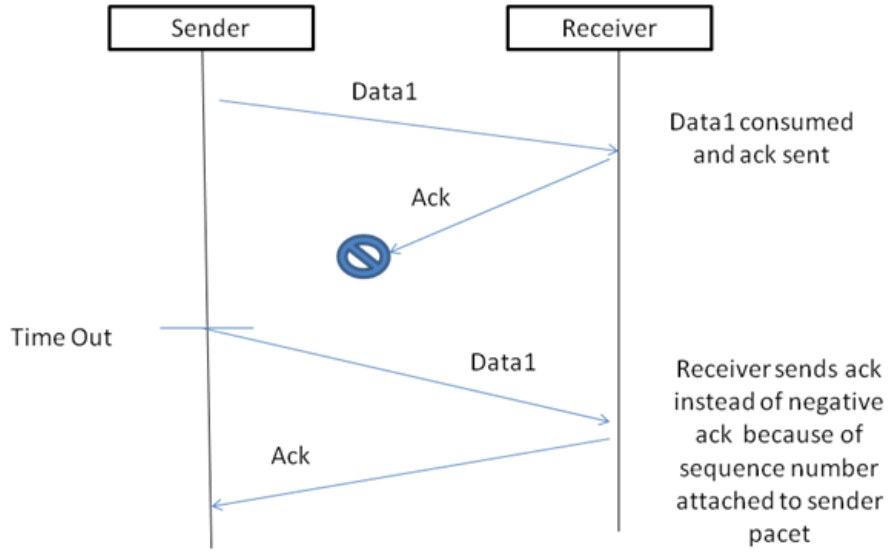
Above 3 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.



1. Time Out:



2. Sequence Number (Data)

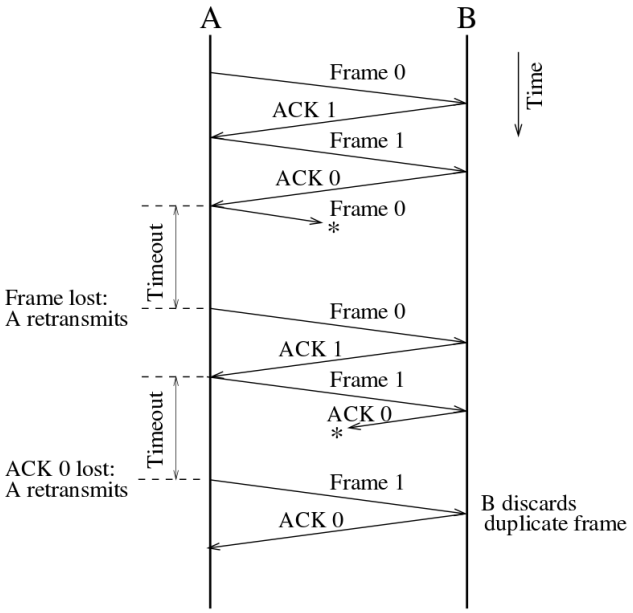


3. Delayed Acknowledgement:

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.



Above image is taken from here.

Characteristics of Stop and Wait ARQ:

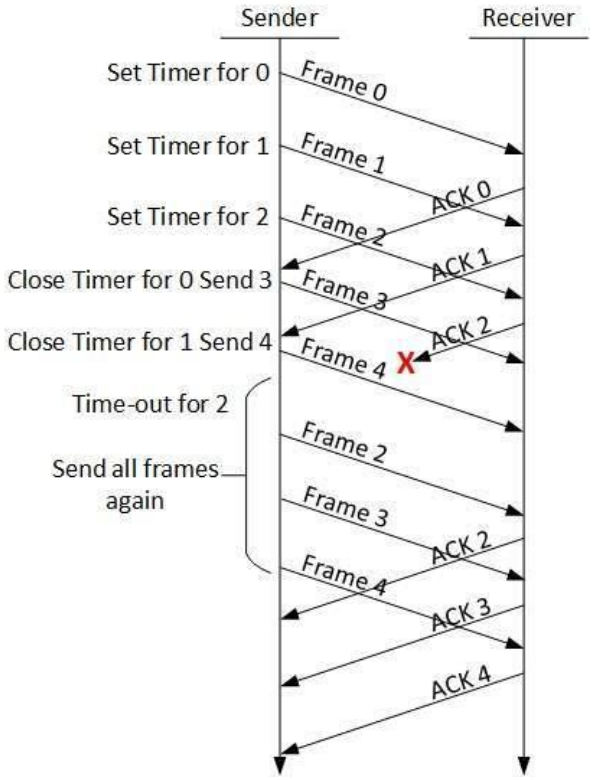
- It uses link between sender and receiver as half duplex link
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example 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. We will be discussing these protocols in next articles.

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.

- **Go-Back-N ARQ**

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

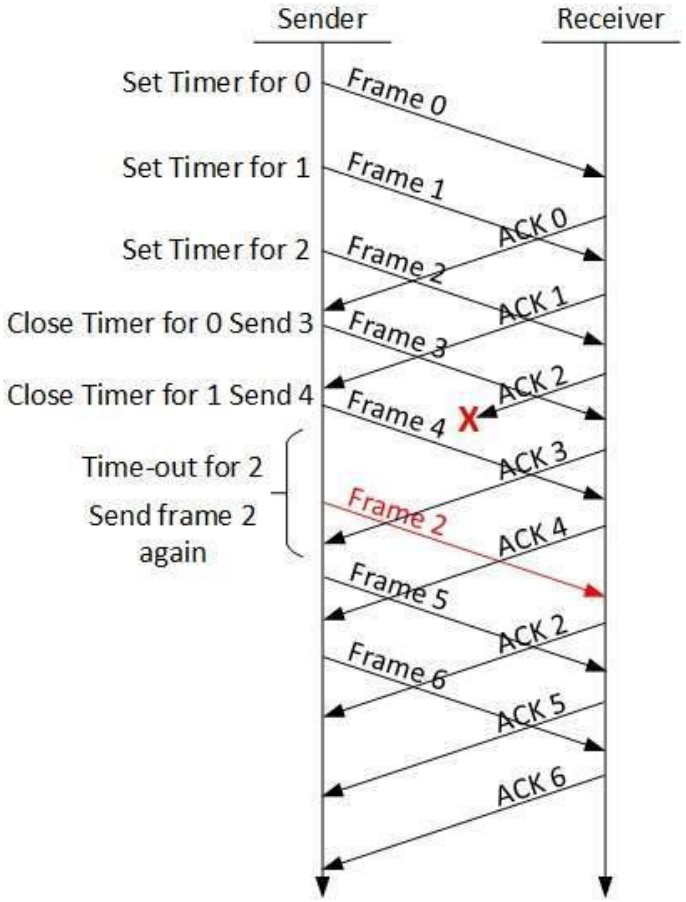


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

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

- Selective Repeat ARQ

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



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

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

3.3.3.2 Go-back-N ARQ The most popular ARQ protocol is the go-back-N ARQ, where the sender sends the frames continuously without waiting for acknowledgement. That is why it is also called as *continuous ARQ*. As the receiver receives the frames, it keeps on sending ACKs or a NACK, in case a frame is incorrectly received. When the sender receives a NACK, it retransmits the frame in error plus all the succeeding frames as shown in Fig.3.3.9. Hence, the name of the protocol is go-back-N ARQ. If a frame is lost, the receiver sends NAK after receiving the next frame as shown in Fig. 3.3.10. In case there is long delay before sending the NAK, the sender will resend the lost frame after its timer times out. If the ACK frame sent by the receiver is lost, the sender resends the frames after its timer times out as shown in Fig. 3.3.11.

Assuming full-duplex transmission, the receiving end sends piggybacked acknowledgement by using some number in the ACK field of its data frame. Let us assume that a 3-bit sequence number is used and suppose that a station sends frame 0 and gets back an RR1, and then sends frames 1, 2, 3, 4, 5, 6, 7, 0 and gets another RR1.This might either mean that RR1 is a cumulative ACK or all 8 frames were damaged. This ambiguity can be overcome if the maximum window size is limited to 7, i.e. for a k-bit sequence number field it is limited to 2k-1. The number N (=2k-1) specifies how many frames can be sent without receiving acknowledgement.

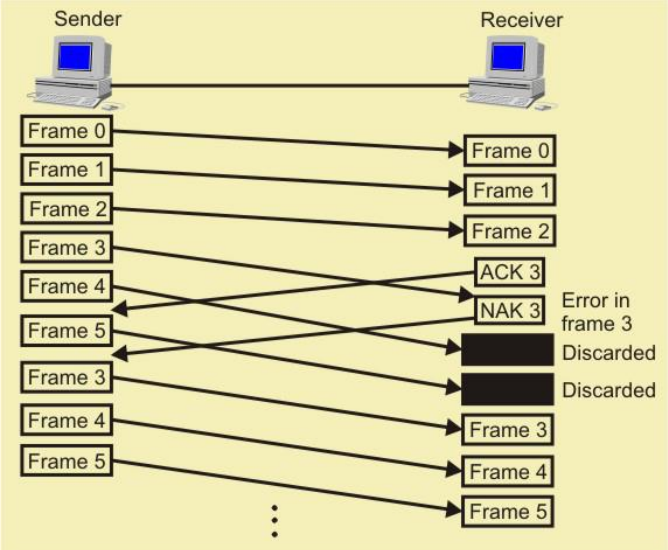


Figure 1 Frames in error in go-Back-N ARQ Version 2 CSE IIT, Kharagpur

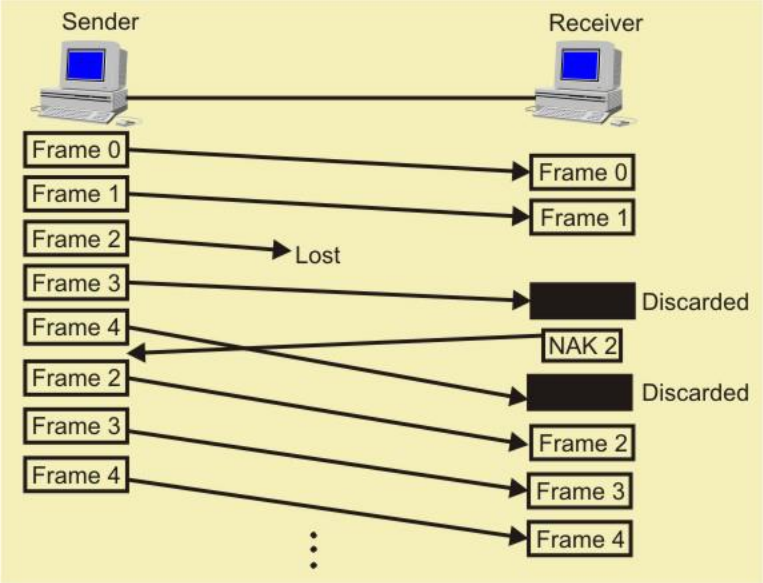


Figure 2 Lost Frames in Go-Back-N ARQ

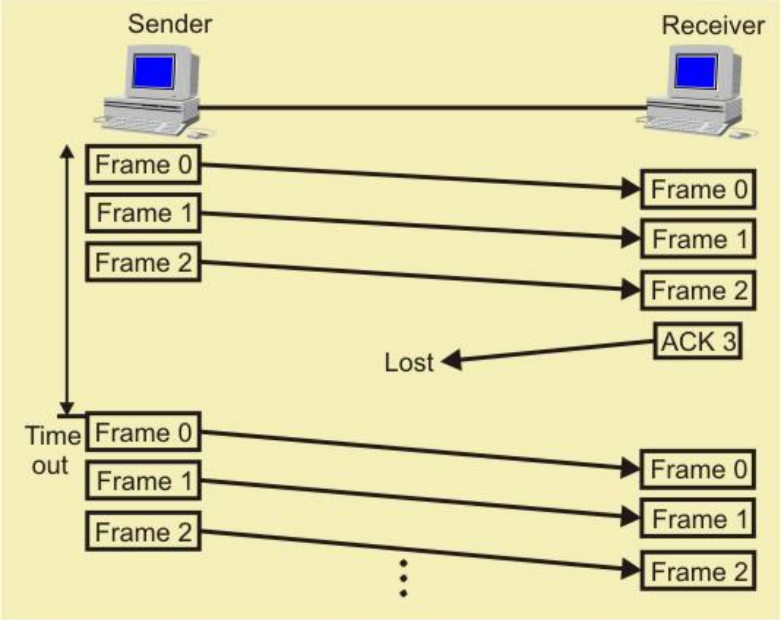


Figure 3 Lost ACK in Go-Back-N ARQ If no acknowledgement is received after sending N frames, the sender takes the help of a timer. After the time-out, it resumes retransmission. The go-

back-N protocol Version 2 CSE IIT, Kharagpur also takes care of damaged frames and damaged ACKs. This scheme is little more complex than the previous one but gives much higher throughput. Assuming full-duplex transmission, the receiving end sends piggybacked acknowledgement by using some number in the ACK field of its data frame. Let us assume that a 3-bit sequence number is used and suppose that a station sends frame 0 and gets back an RR1, and then sends frames 1, 2, 3, 4, 5, 6, 7, 0 and gets another RR1.This might either mean that RR1 is a cumulative ACK or all 8 frames were damaged. This ambiguity can be overcome if the maximum window size is limited to 7, i.e. for a k-bit sequence number field it is limited to 2k-1. The number N (=2k-1) specifies how many frames can be sent without receiving acknowledgement. If no acknowledgement is received after sending N frames, the sender takes the help of a timer. After the time-out, it resumes retransmission. The go-back-N protocol also takes care of damaged frames and damaged ACKs. This scheme is little more complex than the previous one but gives much higher throughput

POSSIBLE QUESTIONS

PART A – Multiple Choice Questions

1. Transmission errors are usually detected at the…….layer of OSI model
A)physical B)datalink C)network D)transport

2. Transmission errors are usually corrected at the……..layer of OSI model
A)network B)transport C)datalink D)physical

3. Datalink layer imposes a …….mechanism to avoid overwhelming the receiver
A)flow control B)error control C)access control D)none of the above

4. Error control mechanism of datalink layer is achieved through a ……..added to the end of frame.
A)header B)trailer C)address D)frames

5. The datalink layer is responsible for moving……from one hop to next
A)packets B)frames C)signals D)message

PART B – 2 Mark Questions

1. What are the three protocols used for noisy channels?
2. What are the various types of connecting devices?
3. What do you mean by RARP?
4. What are the responsibilities of Data Link Layer?
5. What is the frequency range of Bluetooth devices?
6. What is the maximum length of a datagram**?**

PART C – 8 Mark Questions

1. Give an account of Error correction and Detections in detail.
2. Explain go back n ARQ with neat sketch.
3. Illustrate data-link control with proper diagram.
4. Describe stop and wait ARQ with neat sketch.
5. Explain Point to Point Protocol on Internet

Prepared by : A.Jeevarathinam,Dept of CS,CA & IT,KAHE

KARPAGAM ACADEMY OF HIGHER EDUCATION

DEPARTMENT OF CS,CA & IT

II B.Sc CS

COMPUTER NETWORKS (16CSU303)

UNIT III

SL NO	QUESTIONS	CHOICE 1	CHOICE 2	CHOICE 3	CHOICE 4	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 overwhelming the receiver	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 of frame.	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 bit	two	three	first corrupted bit to last
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 unit	a single bit is inverted per transmission	any of the above	a single bit is inverted per
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 possible pairs in a set of words	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 block code must be …..	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 a block code must be …..	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 d(min)=2	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 …… codewords of our frame	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 sender	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 and 0's	a non-zero remainder	a non-zero remainder
30	……. Is a regulation of data transmission so that the receiver buffer do not become overwhelmed	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 from other message to other destinations	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 in text	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 the data.	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 retransmission of data	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 and process is called	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 quantisation	automatic retransmission request	automatic repeat
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 included in the data frames in a technique called	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 retransmitting of the frame when time expires	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 called…….control	logical	media access	A and B	all the above	logical
47	The MAC(media access control)sublayer co-ordinates the datalink task within a specified…….	LAN	MAN	WAN	LAN and MAN	LAN
48	The lower sublayer that is responsible for multiple access resolution is called ……control	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 time	transit	received	A and B	none of the above	transit
50	The sliding window of the sender expands to the ……..when acknowledgement are received	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 reliable link and is responsible for node_to_node delivery	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 is…….	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 d_{min}	3	1	0	2	2
58	……..mechanism of datalink layer is achieved through added to the trailer added to the end of frame.	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

UNIT IV

Multiple ACSUess 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.

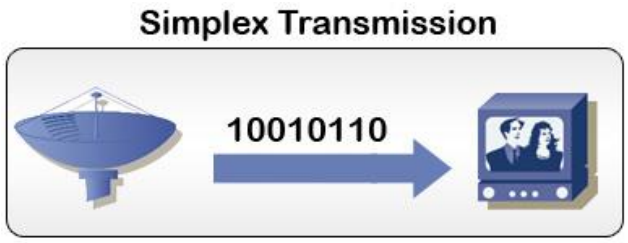
Multiple ACSUess Protocol and Networks

CSMA/CD protocols

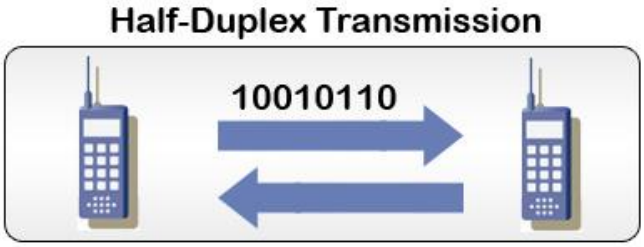
Carrier Sense Multiple Access/Collision Detect (CSMA/CD) is the protocol for carrier transmission access in Ethernet networks. On Ethernet, any device can try to send a frameat any time. Each device senses whether the line is idle and therefore available to be used. If it is, the device begins to transmit 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.

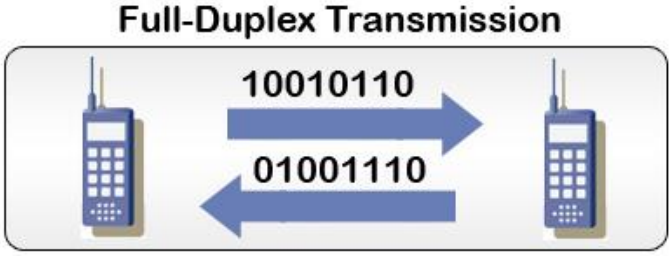


Simplex transmission is, well- simple. It is a connection in which data will always flow in one direction, and will not suffer collisions as a result. Since data flows in one direction, this is poor for mutual communication- so we likely won't see simplex operation in everyday networks. You do, however, 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.



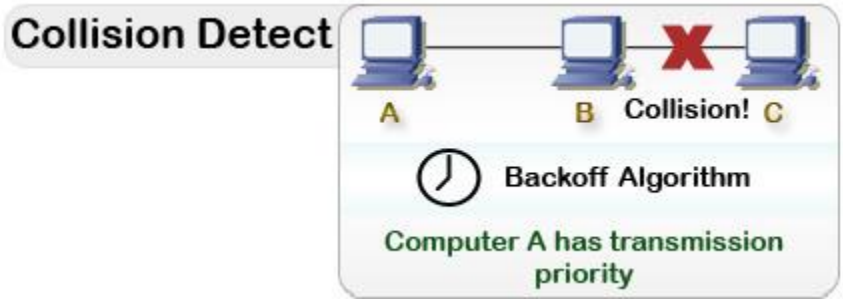
Full-duplex operation is much like half-duplex, only devices can send and receive data at the same time. Virtually no collisions take place on a full-duplex transmission. Perhaps a bigger benefit is the increase in overall throughput- since we are sending and receiving on two different channels, we just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

Second, if you haven't already noticed, CSMA/CD was built for the collision environment. (You won't see it in practical use on a ring topology.)

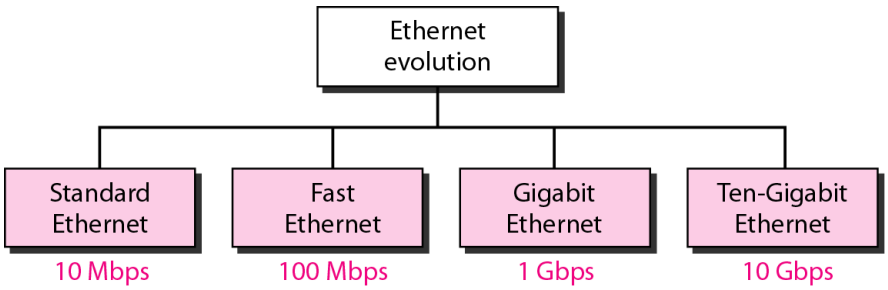
The Collision Detection and Solution Process

- **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.

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.

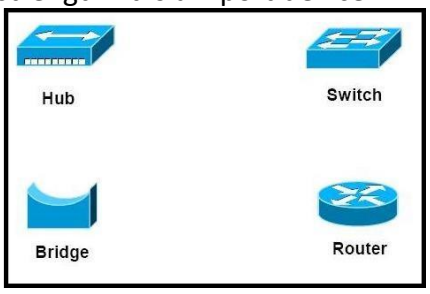
10 Gigabit Ethernet

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.



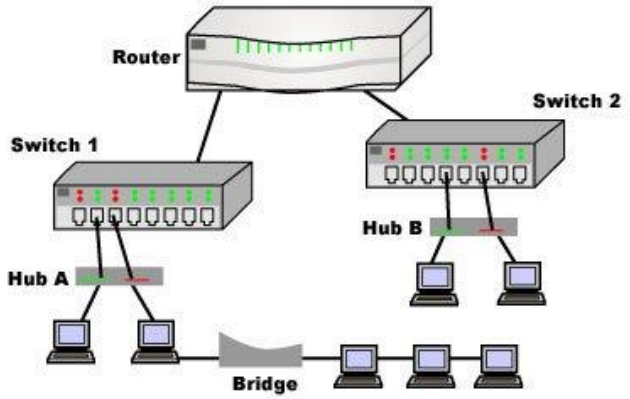
2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected

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 Algorithms

•Adaptive algorithm:
Reflect change in topology
Get information locally from adjacent routers
•Non Adaptive Algorithm
Static routers
Downloaded to routers when network is booted
•Routing:
•Principle of Optimality:
If router I on optimal path from router I to K then optimal path from J to K also on same route!

Routing Algorithms(Static)

•Set of all optimal routes from: Sourceto a given destination
A sink tree!
•Goal of routing algorithm find sink trees that are there!
•Shortest Path Routing:

- Dijkstra
- Uses topology
- Greedy approach
- Possible shorter path of equal length –need not be unique

Routing information is obtained in the two following ways:

- Static routing
- Dynamic routing

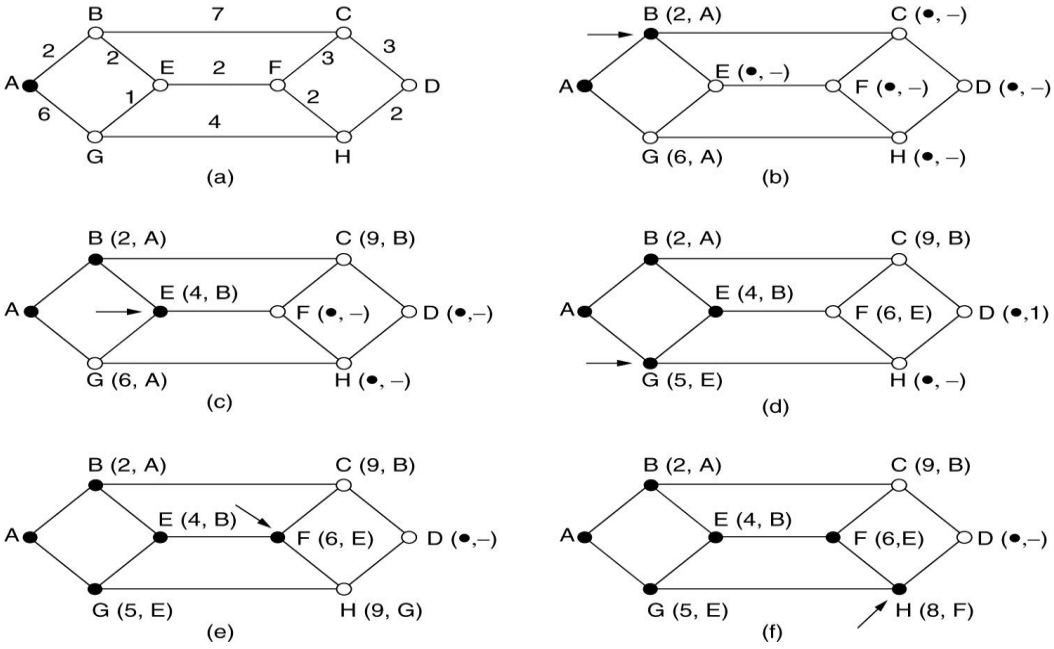
Static routing: This is a function of IP and it requires routing tables to be manually built and manually updated. Because the routing tables are static; static routers do not inform each other in the event of a route change, nor do they exchange routing information with dynamic routers.

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

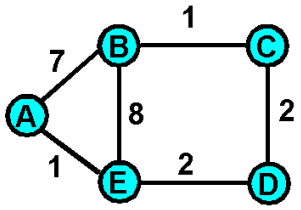
- Distance Vector Routing:
- (Distributed Bellman Ford, Fulkerson)

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

Dynamic Routing

- Distributed Routing:

  Dynamic routing
  Changing topology of the network
  Need to recomputeroute continuously



$D^E()$ — cost to destination via

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

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.

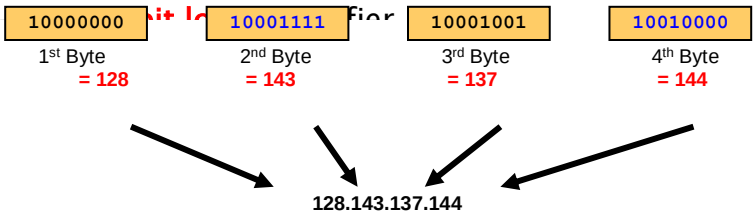
IP provides an unreliable connectionless best effort service

- 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



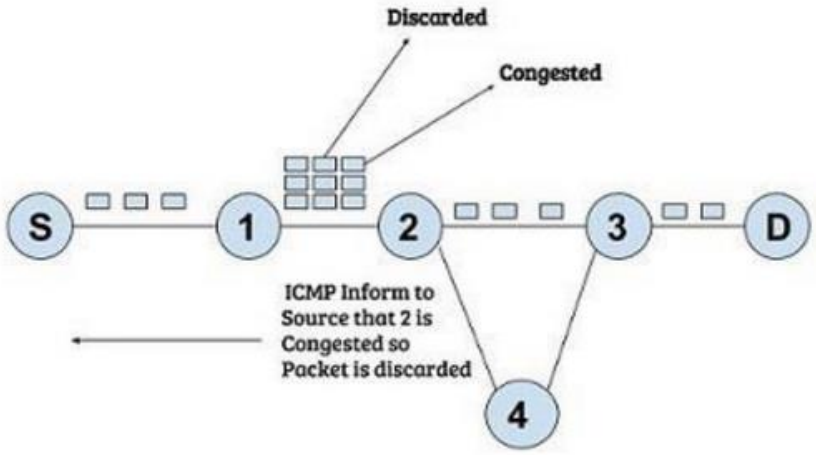
Class Ranges of Internet Addresses

Internet Control Message Protocol (ICMP)

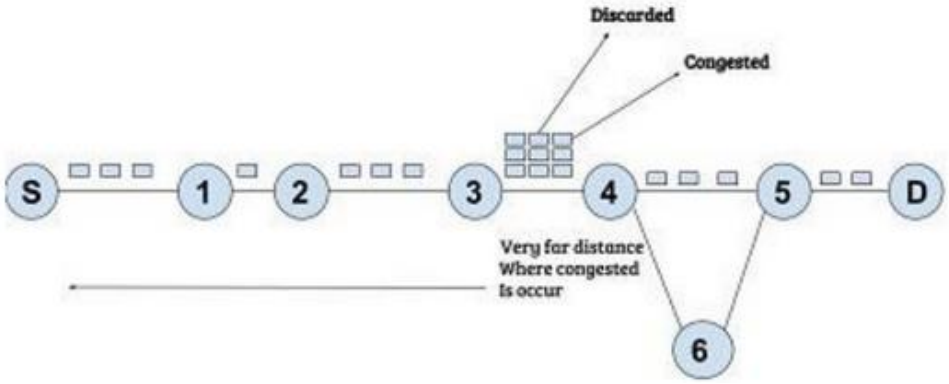
Since IP does not have a inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries. It is a supporting protocol and used by networks devices like routers for sending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



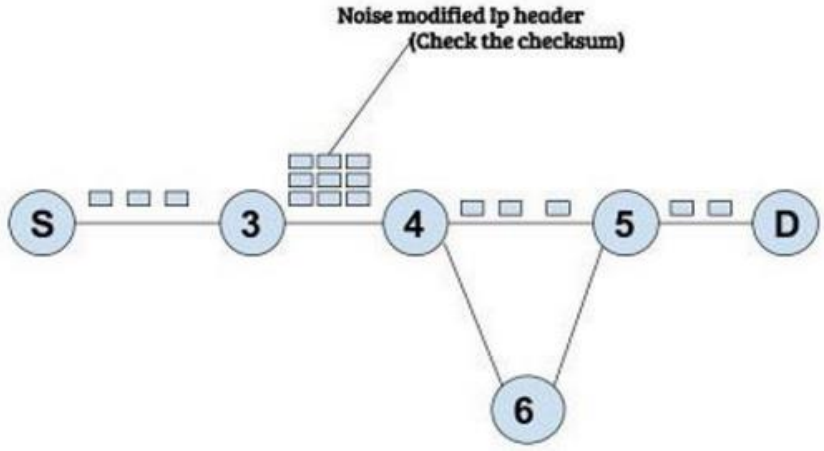
ICMP will take source IP from the discarded packet and informs to source by sending source quench message.
Then source will reduce the speed of transmission so that router will free for congestion.



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 :

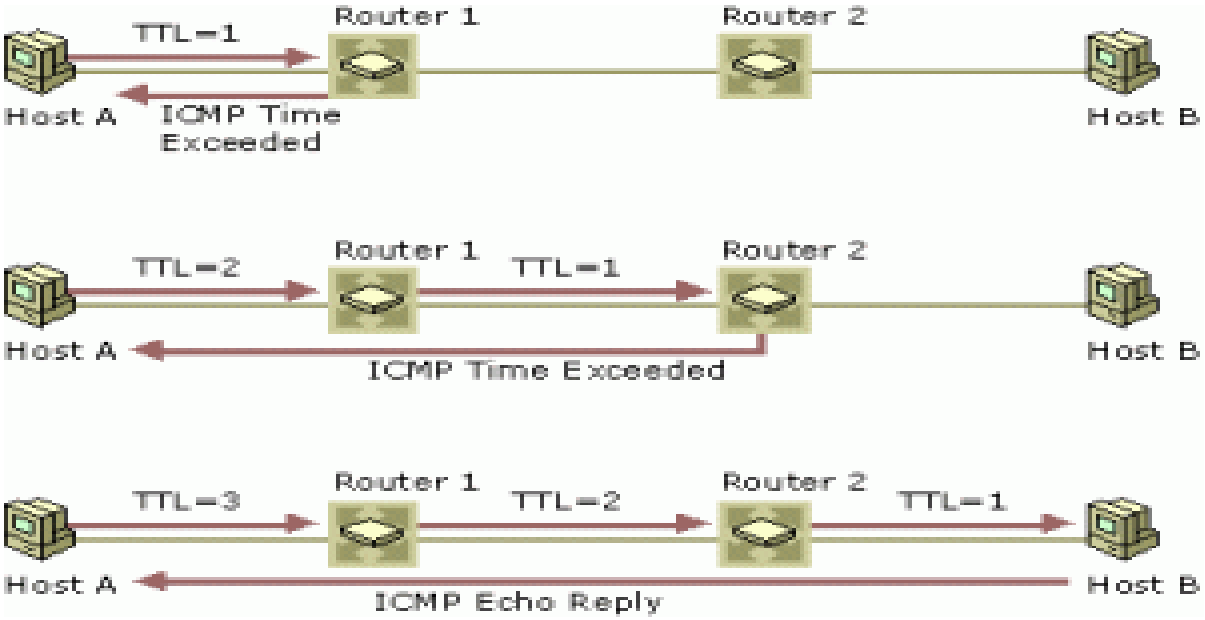
Whenever packets come to the router then calculated header checksum should be equal to recieved header checksum then only packet is accepted by the router.



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.

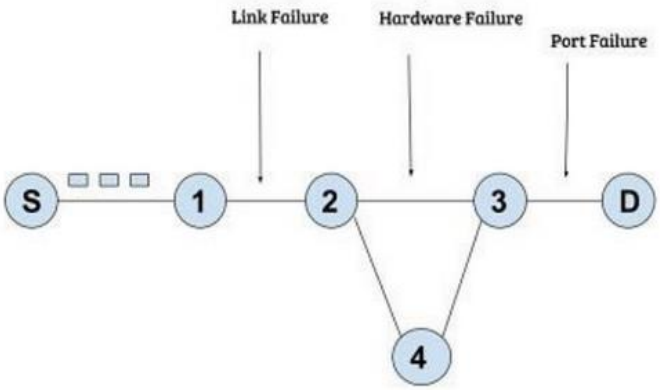
Time exceeded message :



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.

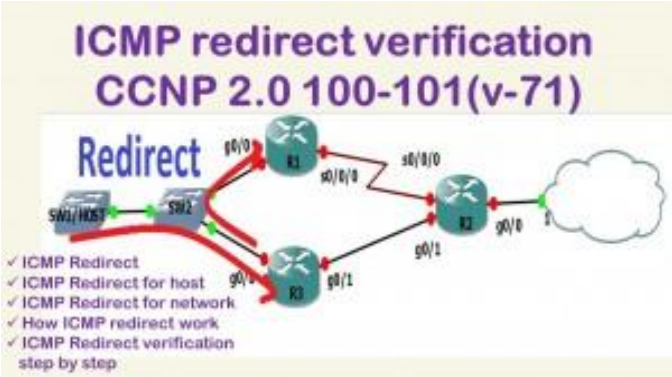


There is no necessary condition that only router give the ICMP error message some time destination host send ICMP error message when any type of failure (link failure,hardwarefailure,port failure etc) happen in the network.

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 – Multiple Choice Questions

1. Internetwork is made of_____networks.
   A) 3 LANs and 2 WANs B) 2 LANs and 3 WANs
   C)4 LANs and 1 WAN D)1 LAN and 4 WANs

2. Internet at the network layer is a_____network.
   A) packet-switched B)LAN C)connection D)connectionless

3. Internet has chosen the datagram approach to_____in network layer
   A)routers B)packets C)switching D)protocol

4. Internet is made of so many_____networks.
   A)homogenous B)heterogeneous C)MAN D)multipoint

5. Communication at network layer in the internet is_____.
   A)connectionless B)point-to-point
   C)connection oriented D)packet-switched

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?

PART C – 8 Mark Questions

1. Describe CSMA/CD protocols.
2. 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

Prepared by : A.Jeevarathinam,Dept of CS,CA & IT,KAHE

KARPAGAM ACADEMY OF HIGHER EDUCATION

DEPARTMENT OF CS,CA & IT

II B.Sc CS

COMPUTER NETWORKS (16CSU303)

UNIT IV

S.NO	QUESTION	CHOICE 1	CHOICE 2	CHOICE 3	CHOICE 4	ANSWER
1	Internetwork is made of_____networks.	3 LANs and 2 WANs	2 LANs and 3 WANs	.4 LANs and 1 WAN	1 LAN and 4 WANs	.4 LANs and 1 WAN
2	Internet at the network layer is a_____network.	packet-switched	.LAN	connection	connetionless	packet-switched
3	Internet has chosen the datagram approach to_____in network layer	routers	packets	switching	protocol	protocol
4	Internet is made of so many_____networks.	homogenous	hetrogeneous	MAN	multipoint	hetrogeneous
5	Communication at network layer in the internet is_____.	connectionless	point-to-point	connection oriented	packet-switched	connectionless
6	What is the abbrevation for IPV4_____.	Inter Protocol Versus 4	Inter Position Version 4	internet protocol version 4	internet Position Versus 4	Internet protocol
7	IPV4 provides the term 'best-effort' means that_____.	no error control	error control	error detection	datagram	no error control
8	Packets in the IPV4 layer are called_____.	frames	datagroup	switching	datagrams	datagrams

9	A datagram is a variable length packet consisting of_____parts.	one	six	two	three	two
10	The total length field defines the total length of the datagram including_____.	footer	header	flags	frames	header
11	Abbravation for MTU_____.	Minimum Transfer Unit	Maximum Transfer Unit	Maximum Travel Unit	Minimum Travel Unit	Maximum Transfer Unit
12	_____in the IPV4 packet covers only header,not the data.	Check subtract	Check sum	options	Check product	Check sum
13	Options can be used for network testings and_____.	checking	packets	types	debugging	debugging
14	A no-operation option is a _____ byte used as a filler between option.	three	six	one	four	one
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	In packet format,the extension headers and data from the upper layer conains upto_____bytes of information.	65.033	65.535	65.536	65.035	65.535
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	Delivery has_____types.	3	4	5	2	2
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	The flags are_____.	U,G,H,D,M	G,H,S,S,D	U,G,H	none of these	U,G,H,D,M
38	The one of the flag is not present,the router is down_____.	G	U	H	D	U
39	D means_____.	added by direction	added	added by redirection	none	added by redirection
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
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	In TCP,one end can stop sending data while still receiving data is _____.	full-close	full-open	half-close	none	half-close
60	The value of RTO is dynamic in TCP and is updated based on _____segment.	RTO	RTT	ACK	none	RTT

UNIT V

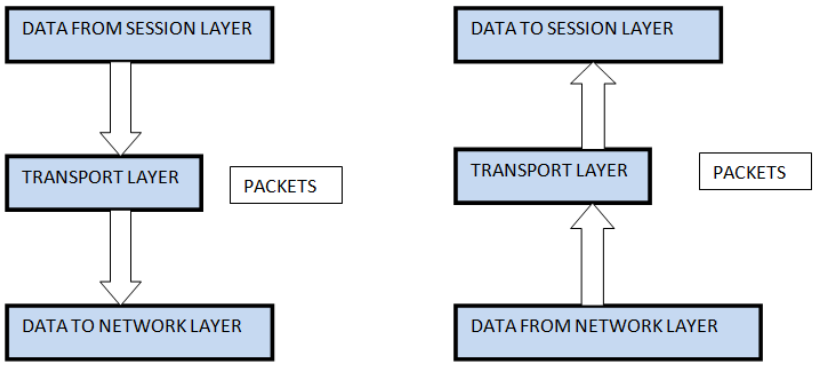
Transport Layer Functions and Protocols: Transport services- error and flow control, Connection establishment and release- three way handshake; **Overview of Application layer protocol**: Overview of DNS protocol; overview of WWW &HTTP protocol.

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.

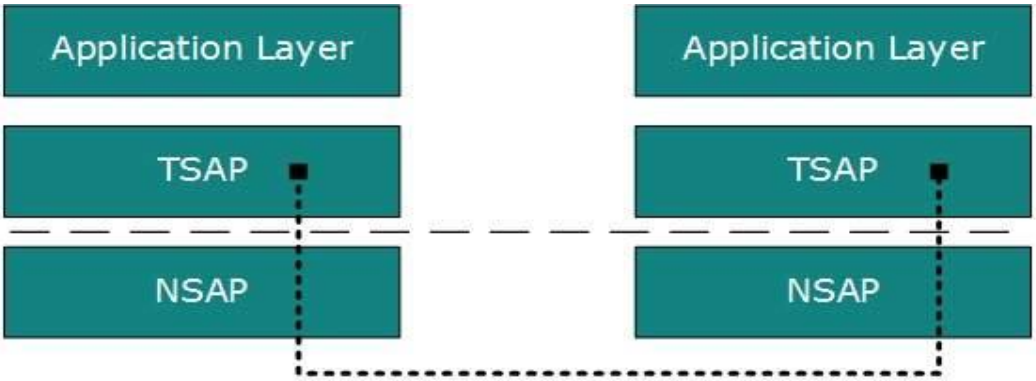
Transport layer offers peer-to-peer and end-to-end connection between two processes on remote hosts. Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.

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.

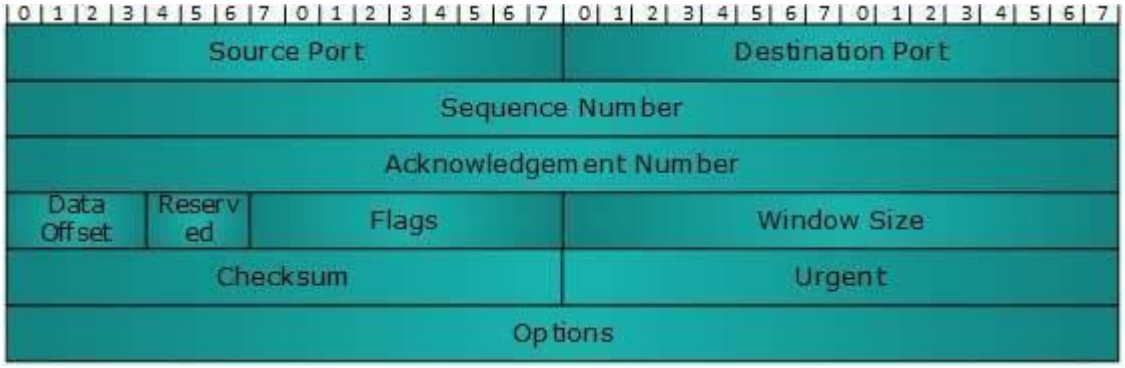
Features

- 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 field has significance. If ACK is 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.

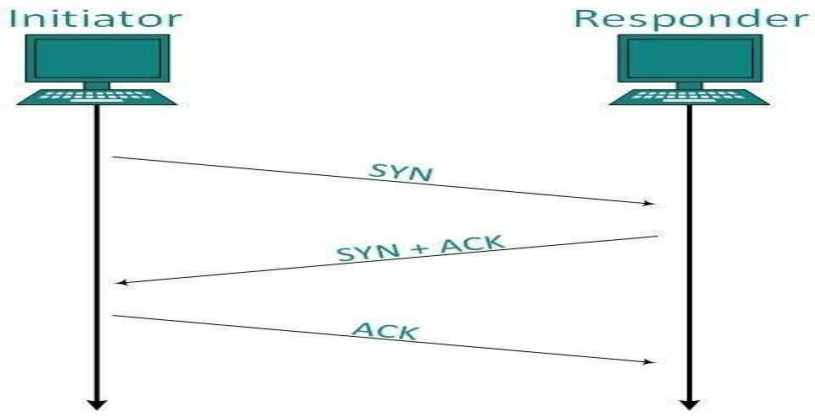
Addressing

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 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

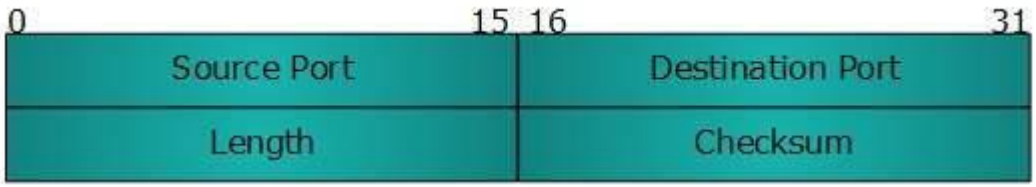
A question may arise, why do we need an unreliable protocol to transport the data? We deploy UDP where the acknowledgement packets share significant amount of bandwidth along with the actual data. For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging 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:

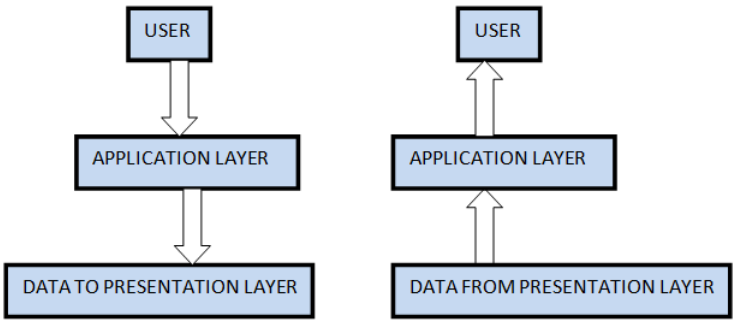
- Domain Name Services

- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

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:

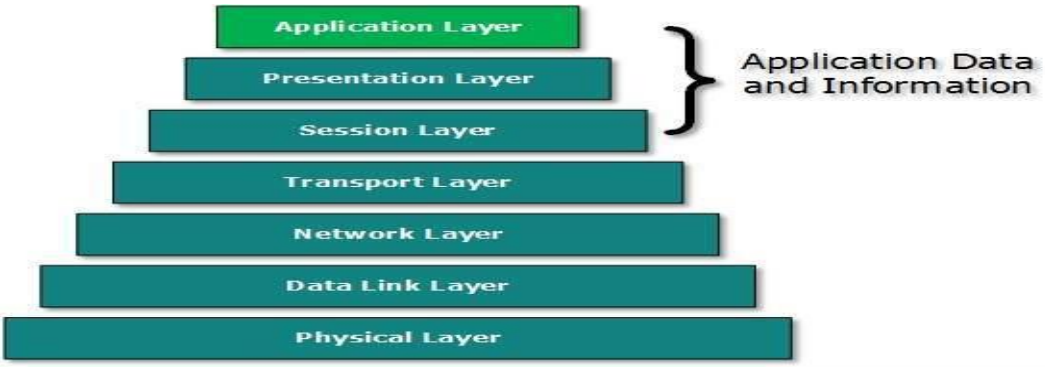
1. **Mail Services :** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal :** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn 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 Layer Introduction

Application layer is the top most layer in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

A user may or may not directly interacts with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote host.

When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.



There'is an ambiguity in understanding Application Layer and its protocol. Not every user application can be put into Application Layer. except those applications which interact with the communication system. For example, designing software or text-editor cannot be considered as application layer programs.

On the other hand, when we use a Web Browser, which is actually using Hyper Text Transfer Protocol (HTTP) to interact with the network. HTTP is Application Layer protocol.

Another example is File Transfer Protocol, which helps a user to transfer text based or binary files across the network. A user can use this protocol in either GUI based software like FileZilla or CuteFTP and the same user can use FTP in Command Line mode.

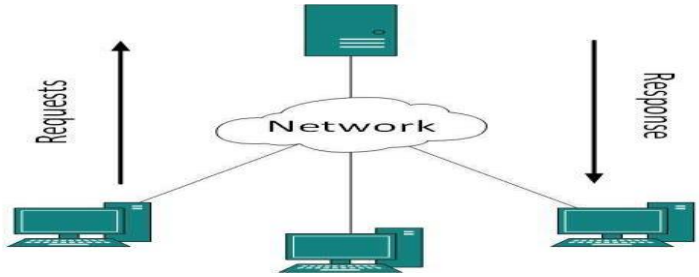
Hence, irrespective of which software you use, it is the protocol which is considered at Application Layer used by that software. DNS is a protocol which helps user application protocols such as HTTP to accomplish its work.

DCN - Client Server Model

Two remote application processes can communicate mainly in two different fashions:

- **Peer-to-peer:** Both remote processes are executing at same level and they exchange data using some shared resource.
- **Client-Server:** One remote process acts as a Client and requests some resource from another application process acting as Server.

In client-server model, any process can act as Server or Client. It is not the type of machine, size of the machine, or its computing power which makes it server; it is the ability of serving request that makes a machine a server.



A system can act as Server and Client simultaneously. That is, one process is acting as Server and another is acting as a client. This may also happen that both client and server processes reside on the same machine.

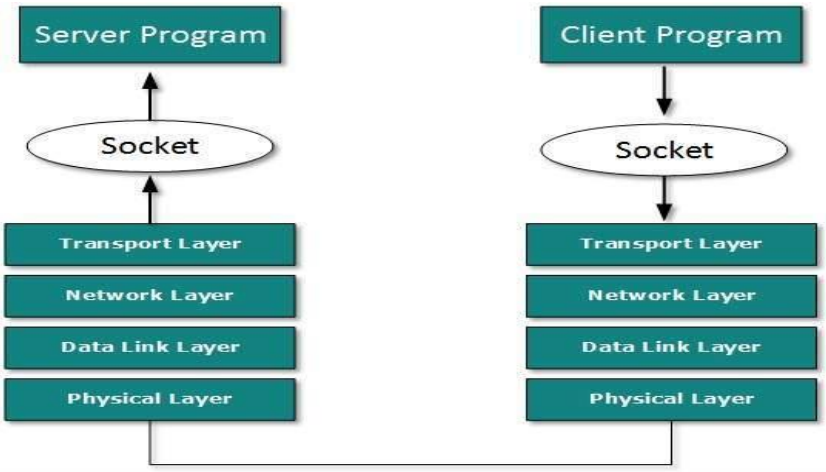
Communication

Two processes in client-server model can interact in various ways:

- Sockets
- Remote Procedure Calls (RPC)

Sockets

In this paradigm, the process acting as Server opens a socket using a well-known (or known by client) port and waits until some client request comes. The second process acting as a Client also opens a socket but instead of waiting for an incoming request, the client processes 'requests first'.



When the request is reached to server, it is served. It can either be an information sharing or resource request.

Remote Procedure Call

This is a mechanism where one process interacts with another by means of procedure calls. One process (client) calls the procedure lying on remote host. The process on remote host is said to be Server. Both processes are allocated stubs. This communication happens in the following way:

- The client process calls the client stub. It passes all the parameters pertaining to program local to it.
- All parameters are then packed (marshalled) and a system call is made to send them to other side of the network.
- Kernel sends the data over the network and the other end receives it.
- The remote host passes data to the server stub where it is unmarshalled.
- The parameters are passed to the procedure and the procedure is then executed.
- The result is sent back to the client in the same manner.

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

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:

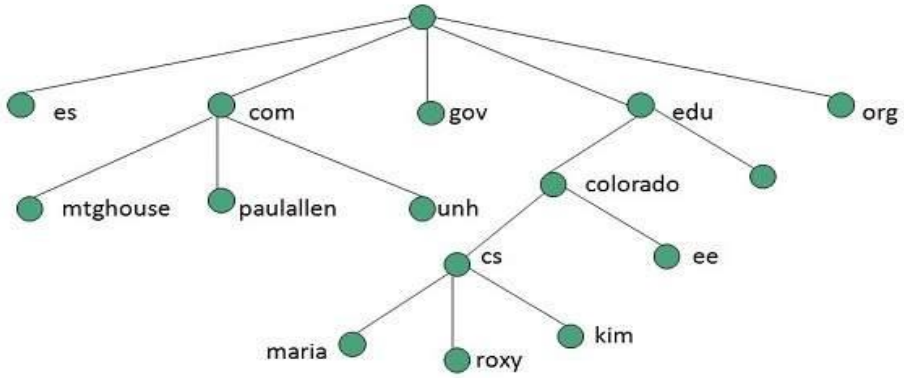
Domain Name	Meaning
Com	Commercial business
Edu	Education
Gov	U.S. government agency
Int	International entity
Mil	U.S. military
Net	Networking organization
Org	Non profit organization

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.

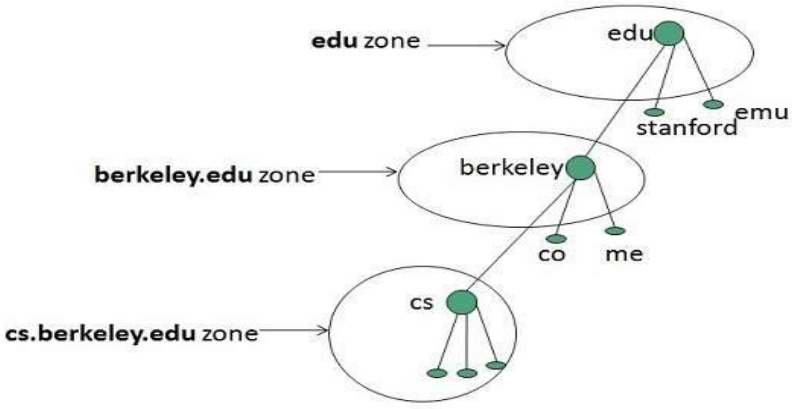
Name Server

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

Overview

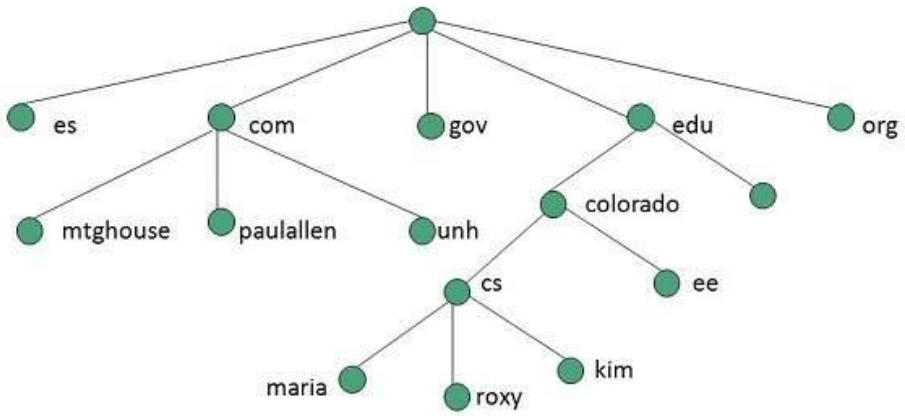
WWW stands for **World Wide Web.** A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

A broader definition comes from the organization that Web inventor **Tim Berners-Lee** helped found, the **World Wide Web Consortium (W3C).**

The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.

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.

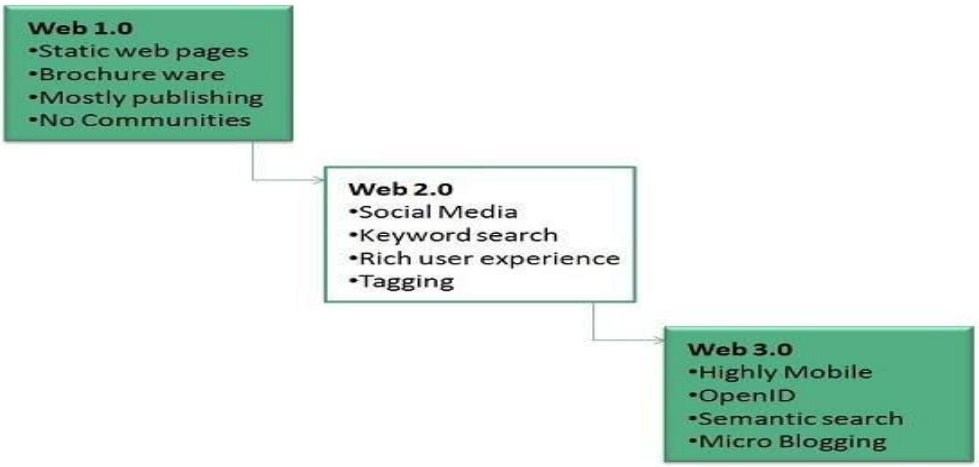
Internet and **Web** is not the same thing: Web uses internet to pass over the information.



Evolution

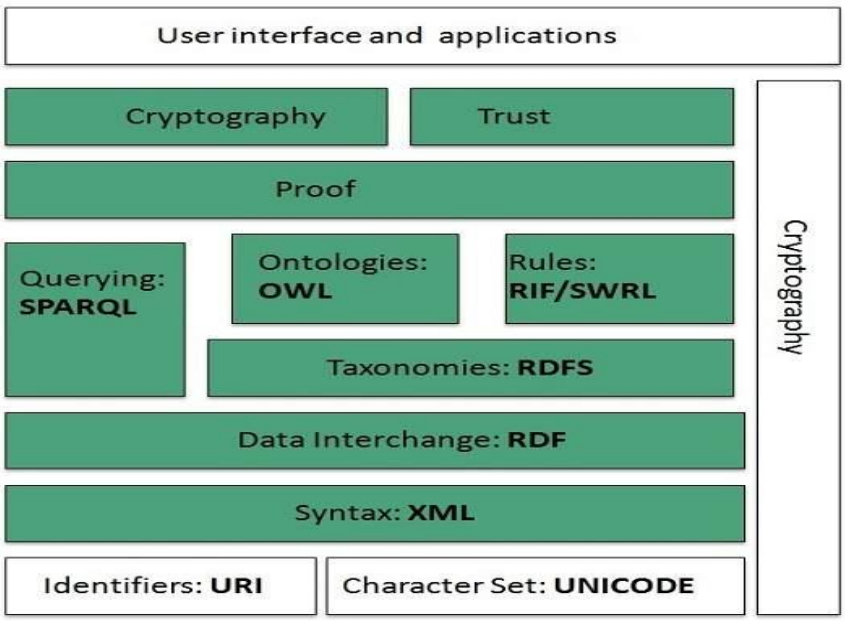
World Wide Web was created by **Timothy Berners Lee** in 1989 at **CERN** in **Geneva.** World Wide Web came into existence as a proposal by him, to allow researchers to work together effectively and efficiently at **CERN.** Eventually it became **World Wide Web.**

The following diagram briefly defines evolution of World Wide Web:



WWW Architecture

WWW architecture is divided into several layers as shown in the following diagram:



Identifiers and Character Set

Uniform Resource Identifier (URI) is used to uniquely identify resources on the web and **UNICODE** makes it possible to built web pages that can be read and write in human languages.

Syntax

XML (Extensible Markup Language) helps to define common syntax in semantic web.

Data Interchange

Resource Description Framework (RDF) framework helps in defining core representation of data for web. RDF represents data about resource in graph form.

Taxonomies

RDF Schema (RDFS) allows more standardized description of **taxonomies**and other **ontological** constructs.

Ontologies

Web Ontology Language (OWL) offers more constructs over RDFS. It comes in following three versions:

- OWL Lite for taxonomies and simple constraints.
- OWL DL for full description logic support.
- OWL for more syntactic freedom of RDF

Rules

RIF and **SWRL** offers rules beyond the constructs that are available from **RDFs** and **OWL.** Simple Protocol and **RDF Query Language (SPARQL)** is SQL like language used for querying RDF data and OWL Ontologies.

Proof

All semantic and rules that are executed at layers below Proof and their result will be used to prove deductions.

Cryptography

Cryptography means such as digital signature for verification of the origin of sources is used.

User Interface and Applications

On the top of layer **User interface and Applications** layer is built for user interaction.

WWW Operation

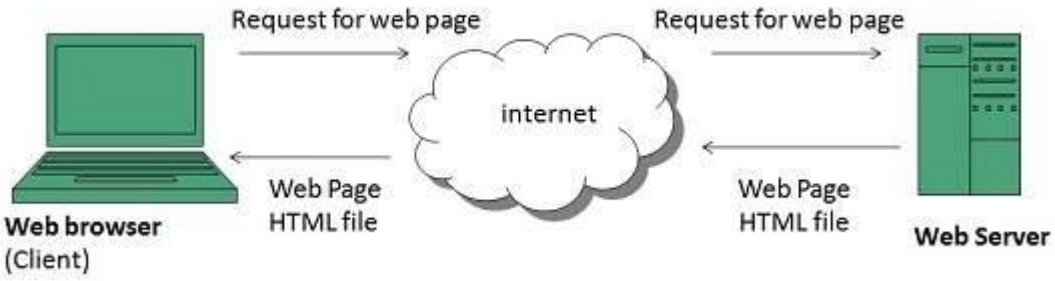
WWW works on client- server approach. Following steps explains how the web works:

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.



Future

There had been a rapid development in field of web. It has its impact in almost every area such as education, research, technology, commerce, marketing etc. So the future of web is almost unpredictable.

Apart from huge development in field of WWW, there are also some technical issues that W3 consortium has to cope up with.

User Interface

Work on higher quality presentation of 3-D information is under deveopment. The W3 Consortium is also looking forward to enhance the web to full fill requirements of global communities which would include all regional languages and writing systems.

Technology

Work on privacy and security is under way. This would include hiding information, accounting, access control, integrity and risk management.

Architecture

There has been huge growth in field of web which may lead to overload the internet and degrade its performance. Hence more better protocol are required to be developed.

An overview of HTTP

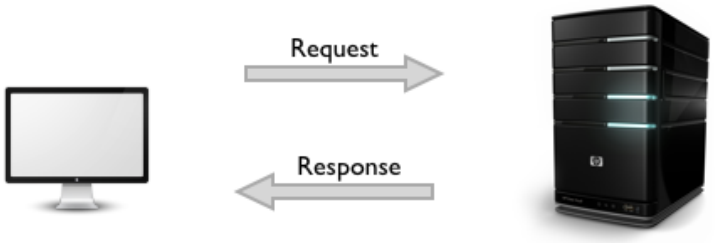
HTTP is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and a client-server protocol, which means requests are initiated by the recipient, usually the Web browser. A complete document is reconstructed from the different sub-documents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

HTTP Basics

HTTP allows for communication between a variety of hosts and clients, and supports a mixture of network configurations.

To make this possible, it assumes very little about a particular system, and does not keep state between different message exchanges.

This makes HTTP a **stateless** protocol. The communication usually takes place over TCP/IP, but any reliable transport can be used. The default port for TCP/IP is **80**, but other ports can also be used.



Custom headers can also be created and sent by the client.

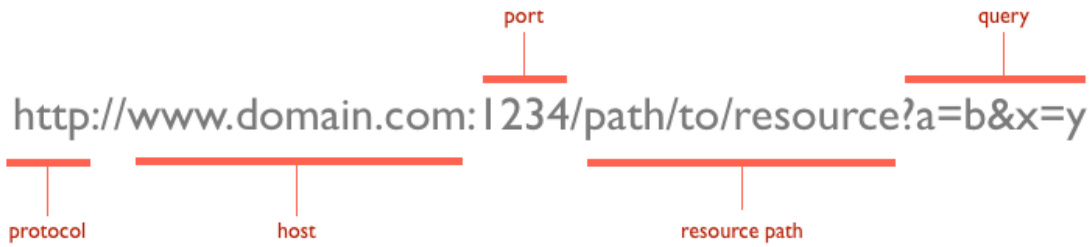
Communication between a host and a client occurs, via a **request/response pair**. The client initiates an HTTP request message, which is serviced through a HTTP response message in return. We will look at this fundamental message-pair in the next section.

The current version of the protocol is **HTTP/1.1**, which adds a few extra features to the previous 1.0 version. The most important of these, in my opinion, includes *persistent connections*, *chunked transfer-coding* and *fine-grained caching headers*. We'll briefly touch upon these features in this article; in-depth coverage will be provided in part two.

URLs

At the heart of web communications is the request message, which are sent via Uniform Resource Locators (URLs). I'm sure you are already familiar with URLs, but for completeness

sake, I'll include it here. URLs have a simple structure that consists of the following components:



The protocol is typically `http`, but it can also be `https` for secure communications. The default port is `80`, but one can be set explicitly, as illustrated in the above image. The resource path is the *local path* to the resource on the server.

HTTP Request Methods

HTTP protocol defines a set of request methods. A client can use one of these request methods to send a request message to an HTTP server. The methods are:

- ✓ GET: A client can use the GET request to get a web resource from the server.
- ✓ HEAD: A client can use the HEAD request to get the header that a GET request would have obtained. Since the header contains the last-modified date of the data, this can be used to check against the local cache copy.
- ✓ POST: Used to post data up to the web server.
- ✓ PUT: Ask the server to store the data.
- ✓ DELETE: Ask the server to delete the data.
- ✓ TRACE: Ask the server to return a diagnostic trace of the actions it takes.
- ✓ OPTIONS: Ask the server to return the list of request methods it supports.
- ✓ CONNECT: Used to tell a proxy to make a connection to another host and simply reply the content, without attempting to parse or cache it. This is often used to make SSL connection through the proxy.
- ✓ Other extension methods.

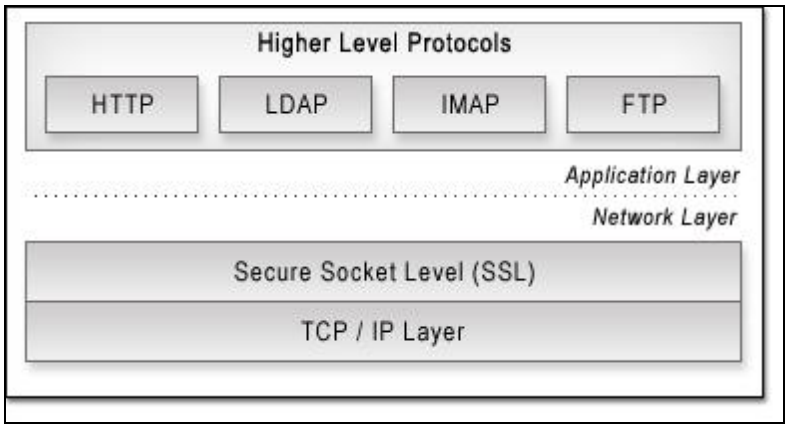
Introduction to SSL

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.

SSL Architecture

The Transmission Control Protocol/Internet Protocol (TCP/IP) governs the transport and routing of data over the Internet. Other protocols, such as the HyperText Transport Protocol (HTTP), Lightweight Directory Access Protocol (LDAP), or Internet Messaging Access Protocol (IMAP) run "on top of" TCP/IP in the sense that they all use TCP/IP to support typical application tasks, such as displaying Web pages or running e-mail servers.



The SSL protocol runs on top of TCP/IP and below higher-level protocols, such as HTTP, IMAP, FTP, etc. It uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

These capabilities address fundamental concerns about "secure" communication over the Internet and other TCP/IP networks.

The SSL Protocol includes two Sub-Protocols, namely SSL Record Protocol and SSL Handshake. SSL Record Protocol defines the format used to transmit data. SSL Handshake Protocol uses SSL Record Protocol to exchange series of messages between SSL-enabled Client and SSL-enabled Server when SSL Connection is first established between them.

Features of SSL

Data Privacy

SSL Provides data privacy for all the data transmitted via the SSL and between the Web Server and Client. 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. This sort of tamper-proof confidentiality is a prerequisite for being able to exchange sensitive data through a network.

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 – Multiple Choice Questions

1. In ----------the rate of data flow changes in time, whith the change smooth instead of sudden and sharp
A)constant-bit-rate B)variable-bit-rate C)both a & b D)bit rate

2. In the ----------the data rate changes suddenly in a very short times
A)variable-bit-rate B)constant-bit-rate
C)bursty data D)constant-bit-rate

3 Congestion control is divided into--------types
A)1 B)2 C)3 D)4

4. If the sender feels that a sent packets is lost ,the packet needs to ----------
A)transmission B)delete C)retransmission D)None

5. The type of ---------- at the sender may also affect congestion
A)closed-loop B)window C)control D)discarding

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. Explain the overview of WWW
2. Illustrate router and gateways with proper diagram
3. Elaborate IP protocol with neat sketch
4. Elucidate the principles of WWW and HTTP.
5. Describe in detail about Transport services.
6. Give a detail note on - three way handshake.

KARPAGAM ACADEMY OF HIGHER EDUCATION

DEPARTMENT OF CS,CA & IT

II B.Sc CS

COMPUTER NETWORKS (16CSU303)

UNIT V

S.NO	QUESTION	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWER
1	---------- are qualitative values that represent a flow data	data traffic	data descriptor	data traffic and data descriptor	traffic data	data descriptor
2	the----- define the maximum data rate of the traffic	peak data rate	maximum burst size	bandwith	effective bandwith	peak data rate
3	the----- define the maximum length of time the traffic is generated in the peak rate	effective bandwith	constant rate	peak data rate	maximum burst size	maximum burst size
4	the------- is the bandwith that the network needs to allocate for the flow of traffic	effective bandwith	peak data rate	maximum burst size	data descriptor	effective bandwith
5	a constant-bit-rate is also called as -------	fixed_rate	nonfixed rate	both a & b	none	fixed_rate
6	in ----------the rate of data flow changes in time, whith the change smooth instead of sudden and sharp	constant-bit-rate	variable-bit-rate	both a & b	bit rate	variable-bit-rate
7	in the ----------the data rate changes suddenly in a very short times	variable-bit-rate	constant-bit-rate	bursty data	constant-bit-rate	bursty data
8	congestion control is divided into--------types	1	2	3	4	2

9	a ----------is mechanism that can prevent before and after it happens	open-loop	closed-loop	congestion control	none	congestion control
10	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
11	if the sender feels that a sent packets is lost ,the packet needs to ----------	transmission	delete	retransmission	none	retransmission
12	the type of ---------- at the sender may also affect congestion	closed-loop	window	control	discarding	window
13	the -------- policy imposed by the receiver may also effect	acknowledgment	discarding	admission	window	acknowledgment
14	a good ------- policy by the routers may prevent congestion and the same time may not harm the integrity network	admission	window	discarding	acknowledgment	discarding
15	an---------- policy , which is a quality of service mechanism	acknowledgment	window	daiscarding	admission	admission
16	a ----------is mechanism try to alleviate congestion after it happens	open-loop	closed-loop	congestion control	none	closed-loop
17	the technique od--------- refer to congestion control mechanism in which a congestion node stops receiving data from the immediate	choke packet	control	window	backpressure	backpressure
18	in---------- is anodeto node congestion control that start with a node and propagates	backpressure	choke packet	none	window	backpressure
19	a---------- is apacket sent by anode to the source to inform it of congestion	control	choke packet	admission	backpressure	choke packet
20	in ----------there is no communication between the congested nodes and source	explict signaling	left side	implicit signaling	both a&c	implicit signaling
21	lack of reliablity means losing a ----------	packet	control	data flow	admission	packet

22	a ---------- in a file transfer or E-mail is less important	jitter	delay	reliablity	none	delay
23	a ---------- in the variation in delay for packets belonging to the same flow	jitter	reliablity	delay	none	jitter
24	different application need different ----------	maximum burst size	effective bandwith	bandwith	peak data rate	bandwith
25	packets from different flows arrive at ----------	scheduling	fifo	bandwith	switch	switch
26	a good ---------- technique treats the different flows in apair in appropriate manner	bandwith	scheduling	admission	window	scheduling
27	several scheduling are designed to improve ----------	quality of service	quality of data	quality of control	quality of data flow	quality of service
28	in -------- queuing , packets wait in a buffer(queue) until the node is ready to process them	lifo	linked	fifo	none	fifo
29	in --------- queuing , packets are first assigned to a priorety class	fifo	lifo	circular	priority	priority
30	in priority the packets in a---------- priority queue are processed first	lowest	highest	medium	none	highest
31	a better scheduling method is---------- queuing, in this ,the packets are still assigned to different classes	weighted fair	priority	both a & b	fair queuing	weighted fair
32	the-------- is amechanism to control the amount and rate of traffic sent to the network	priority	data descriptor	traffic shaping	weighted fair	traffic shaping
33	the ---------- does not credit an idle host	token bucket	leak bucket	both a & b	empty bucket	leak bucket
34	a---------- algorithm shapes bursty traffic into fixed-rete traffic by averaging the data rate	leak bucket	token bucket	empty bucket	both a & b	leak bucket

35	the ------- bucket allows the bursty traffic at aregulated maximum rate	empty bucket	leak bucket	token bucket	none	token bucket
36	the---------- can be combained to credit an idle host and at the same time regulate the traffic	leak bucket	token bucket	empty bucket	both a & b	both a & b
37	_____allows us to send message include text,auido and video .	mail	internet	E-mail	all the above	E-mail
38	the_____client established a connection with MTA server on the system	MTA	alice	UA	system server	MTA
39	the first component of an electrionic mail system is the_____	alice	server	user agent	services provider	user agent
40	_____is the example of user agents are mail,pine,and elm	user agent	command driven	GUI-based	E-mail	command driven
41	_____ define the names of aspecial files	local part	domain name	mime	both a & b	local part
42	the second part of address is_____	system server	internet	domain name	local part	domain name
43	MIME is_____	multiple internet mail extensions	multipurpose interface mail extensions	multipurpose internet mail exchange	multipurpose internet mail extensions	multipurpose internet mail
44	_____ has delete and keep mode	pop	pop2	pop3	none	pop3
45	_____is the mechanism provided by TCP/IP for copying a file from one host to another	FTP	MIME	UA	pop3	FTP
46	_____ is the default formate for transferring text files	image	ASCII	data structure	record structure	ASCII
47	_____ is the default formate for transferring binary files	image	data structure	record structure	ASCII	image

48	in the _____ formate, the file is a continuous stream of byte	file structure	record structure	data structure	image	file structure
49	the service provider is distrubuted over many location called _____	internet	sites	www	http	sites
50	theweb page store at the _____	hard disk	disk	client	server	server
51	the _____ is the computer on which the information is located	path	sites	host	cookies	host
52	_____is the pathname of the file where the information is located	host	path	server	sites	path
53	_____ is language for creating web pages	HTML	C	C++	java	HTML
54	a_____ is created by a web server whenever a browser request the document	common gate way	dynamic document	script	all the above	dynamic document
55	_____ is the protocol used mainly to access data on the world wide web	communicatio	network	WWW	HTTP	HTTP
56	a_____ replaces one symbol with another	substitution cipher	monoalphabetic ciphet	traditional cipher	none	substitution cipher
57	a_____ reorders (permutes) symbols in a block of symbols	traditional cipher	substitution cipher	transposition cipher	monoalphabetic ciphet	transposition cipher
58	the _____ is sometimes referred to as the caesar cipher	monoalphabetic ciphet	shift cipher	traditional cipher	transposition cipher	shift cipher
59	a _____ is a techique that emplys the morden block ciphers such as DES and AES	modes	modes of operation	operating server	none	modes of operation
60	the most common public key algorithm is _____	RSA	RSSA	RSS	none	RSA

61	_____means that the data can must arrive at the receiver exactly as they were sent	integrity	message integrity	authentication	message authentication	message integrity
62	_____ is the service beyond message integrity	message authentication	message integrity	integrity	authentication	message authentication
63	a digital signature needs a _____ system	private-key	primary-key	public-key	none	public-key
64	a digital signature today provides _____	message authentication	integrity	message integrity	authentication	message integrity
65	a_____ keys between two parties is used only once	session	primary-key	private-key	public-key	session

Reg .No…….

[16CSU303]

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Under section 3 of UGC Act 1956)

COIMBATORE – 641 021

(For the candidates admitted from 2016 onwards)

B.Sc DEGREE EXAMINATION

Third Semester

First Internal Examination – JULY 2017

COMPUTER SCIENCE

COMPUTER NETWORKS

Date : 19 – 07 – 17 **Time** : 2:00 Hrs

Class : II.B.Sc CS (A & B) **Maximum** : 50

SECTION A – (20*1 = 20 Marks)
Answer All Questions

1. MAN stands for _____
   a. Metropolitician area network b. Metropolitan area network
   c. Metropolitical area network d. Macro area network
2. In physical layer we can transfer data into _____
   a. Frame b. packet c. bit d. byte
3. FTP_____
   a. file transmit protocol b. file transmission protocol
   c. file transfer protocol d. flip transfer protocol
4. A_____ is the set of rules.
   a. Protocols b. transmission mode c. networks d. ip
5. The _____is the number of bits sent in a second.
   a. Bit length b. bandpass c. bandwidth d. bit rate
6. The_____layer is responsible for providing services to the user.
   a. Presentation b. data link c. application d. network

7. RARP is _____

   a. Reverse address resolution protocol b. reverse address revolutionized protocol

   b. reverse address result protocol d. reverse address research protocol

8. As frequency increases, the period_____

   a. Decreases b. increases c. remains the same d. doubles

9. A_____signal is a composite analog signal with an infinite bandwidth

   a. simple b. composite c. digital d. Analog

10. A_____connection provides a dedicated link between two devices.

   a. Point-to-point b. multi-point c. mesh d. physical

11. The _____layer is responsible for process to process delivery.

   a. physical b. presentation c. networks d. transport

12. Which multiplexing technique transmits analog signals

   a. FDM b. TDM c. WDM d. none

13. A_____is a set of devices connected by communication links.

   a. Protocols b. networks c. computer d. printer

14. The _____layer is responsible for movements of bits from one hop to next.

   a. data link b. physical c. transport d. session

15. One long cable acts as a _____to link all the devices in a network.

   a. Bus b. mesh c. hub d. backbone

16. ---are network meant for one person

   a. LAN b.PAN c. WAN d. MAN

17. The short range wireless network called --- are used to connect components without wires.

   a. Blue tooth b. wireless mobile c. Headsets d. camera

18. UDP stands for ----

   a. User data protocol b. User data control protocol

   c. User datagram protocol d.user data transfer protocol

19. One of the oldest and still most common transmission media is ----

   a. Co-axial cables b. Fibre-optics cable

   c. Twisted-Pair cables d. wireless transmission

20. In cilent-server model, the data are stored on powerful computers called---

   a. Servers b. clients c. network d. Router

SECTION B – (3*2 = 6 Marks)

Answer All Questions

21. Define networks

22. Differentiate analog and digital signals.

23. What are the elements of data communication?

SECTION C – (3*8 = 24 Marks)

Answer the Questions

24. a) Discuss the layered architecture of OSI reference model with a neat diagram.

[OR]

b) Write note on pulse code modulation with suitable diagram

25. a) Describe in detail about classifications of networks with neat sketch.

[OR]

b).Write a note on the transmission modes.

26. a). Explain the various network topologies with a neat diagram

[OR]

b) Explain multiplexing techniques with neat diagram.

Reg .No…….
[16CSU303]

KARPAGAM UNIVERSITY
(Under section 3 of UGC Act 1956)
COIMBATORE – 641 021
(For the candidates admitted from 2016 onwards)

B.Sc DEGREE EXAMINATION

Third Semester

First Internal Examination – JULY 2017

COMPUTER SCIENCE

COMPUTER NETWORKS

Date : 19 – 07 – 17 **Time** : 2:00 Hrs
Class : II.B.Sc CS (A & B) **Maximum** : 50

SECTION A – (20*1 = 20 Marks)
Answer All Questions

1. MAN stands for _____
   a. Metropolitician area network **b. Metropolitan area network**
   c. Metropolitical area network d. Macro area network
2. In physical layer we can transfer data into _____
   a. Frame b. packet **c. bit** d. byte
3. FTP_____
   a. file transmit protocol b. file transmission protocol
   c. file transfer protocol d. flip transfer protocol
4. A_____ is the set of rules.
   a. Protocols b. transmission mode c. networks d. ip
5. The _____is the number of bits sent in a second.
   a. Bit length b. bandpass c. bandwidth **d. bit rate**
6. The_____layer is responsible for providing services to the user.
   a. Presentation b. data link **c. application** d. network

7. RARP is _____

a. **Reverse address resolution protocol** b. reverse address revolutionized protocol

b. reverse address result protocol d. reverse address research protocol

8. As frequency increases, the period_____

a. Decreases **b. increases** c. remains the same d. doubles

9. A_____signal is a composite analog signal with an infinite bandwidth

a. simple b. composite **c. digital** d. Analog

10. A_____connection provides a dedicated link between two devices.

a. Point-to-point b. multi-point c. mesh d. physical

11. The _____layer is responsible for process to process delivery.

a. physical b. presentation c. networks **d. transport**

12. Which multiplexing technique transmits analog signals

a. FDM b. TDM c. WDM d. none

13. A_____is a set of devices connected by communication links.

a. Protocols **b. networks** c. computer d. printer

14. The _____layer is responsible for movements of bits from one hop to next.

a. data link **b. physical** c. transport d. session

15. One long cable acts as a _____to link all the devices in a network.

a. Bus b. mesh c. hub **d. backbone**

16. ---are network meant for one person

a. LAN **b.PAN** c. WAN d. MAN

17. The short range wireless network called --- are used to connect components without wires.

a. Blue tooth b. wireless mobile c. Headsets d. camera

18. UDP stands for ----

a. User data protocol b. User data control protocol

c. User datagram protocol d.user data transfer protocol

19. One of the oldest and still most common transmission media is ----

a. Co-axial cables b. Fibre-optics cable

c. Twisted-Pair cables d. wireless transmission

20. In cilent-server model, the data are stored on powerful computers called---

a. Servers b. clients c. network d. Router

SECTION B – (3*2 = 6 Marks)

Answer All Questions

21. Define networks

A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data. An excellent example of a network is the Internet, which connects millions of people all over the world. Below is an example image of a home network with multiple computers and other network devices all connected to each other and the Internet.

22. Differentiate analog and digital signals.

	Analog	Digital
Signal	Analog signal is a continuous signal which represents physical measurements.	Digital signals are discrete time signals generated by digital modulation.
Waves	Denoted by sine waves	Denoted by square waves
Representation	Uses continuous range of values to represent information	Uses discrete or discontinuous values to represent information
Example	Human voice in air, analog electronic devices.	Computers, CDs, DVDs, and other digital electronic devices.
Technology	Analog technology records waveforms as they are.	Samples analog waveforms into a limited set of numbers and records them.
Data transmissions	Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.

23. What are the elements of data communication?

- Transmitter
- Receiver
- Medium
- Message
- Protocol

SECTION C – (3*8 = 24 Marks)

Answer the Questions

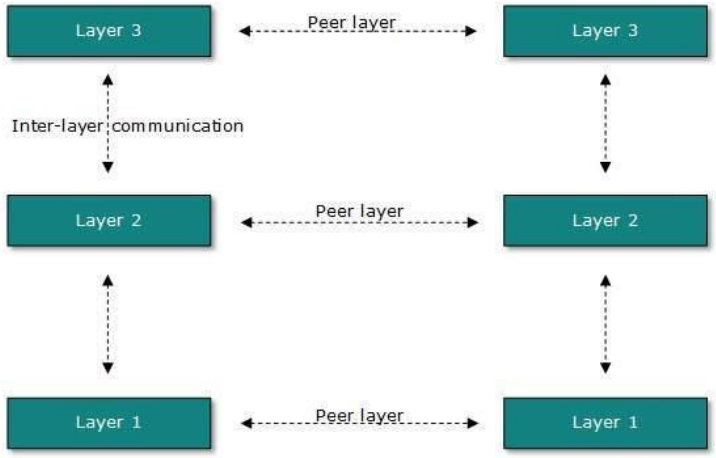
24. a) Discuss the layered architecture of OSI reference model with a neat diagram.

LAYERED NETWORK ARCHITECTURE

Layered Tasks

In layered architecture of Network Model, 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 the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.



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

Definition

An **architecture** in which data moves from one defined level of processing to another. Communications protocols are a primary example.

- **Layers:** grouping the common functions

- **Benefits of layers**:
  - Simplicity: easy to design once layers and their interaction are defined clearly
  - Flexibility: easy to modify and develop networks by separate layers modifications
  - Incremental changes: add new layers, add new functions to a layer

Three obvious tasks (layers)

- Transport of data across the network from one end to the other
- Routing/forwarding of packets across multiple hops
- Transfer of a frame from one interface to another (i.e., one hop).

Big picture of layered architectures

- Web browsing and e-mail examples
- OSI reference model (Seven layers)
- TCP/IP architecture
- Detailed end-to-end examples to complete big picture of layered architectures
- Socket API and other utilities

[OR]

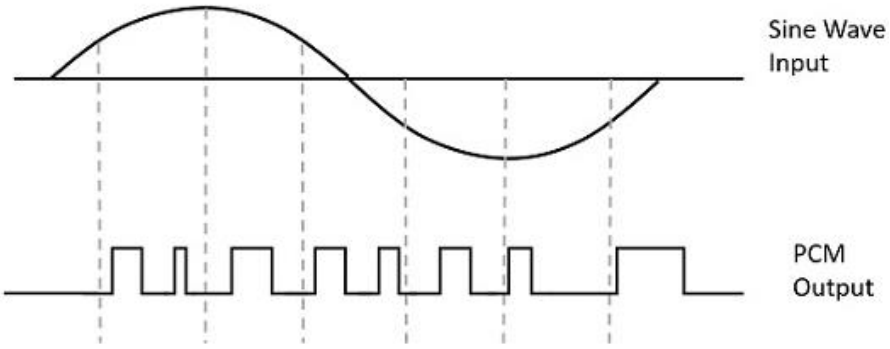
b) Write note on pulse code modulation with suitable diagram

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.



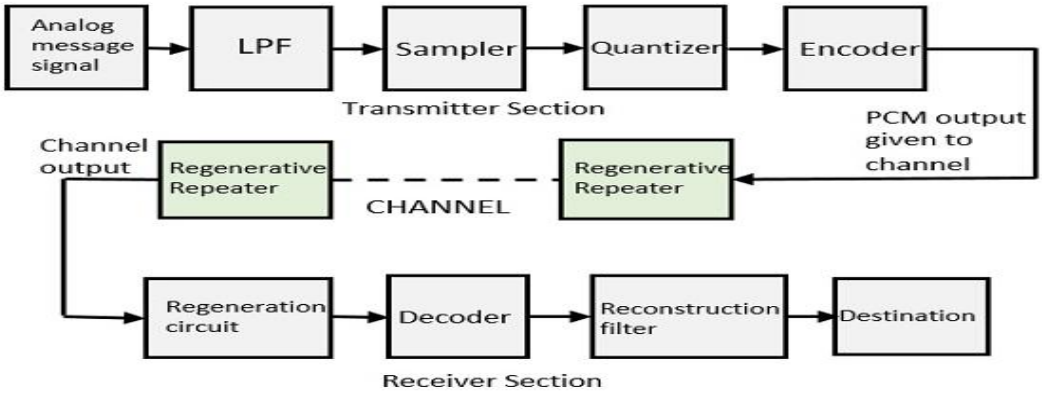
Instead of a pulse train, PCM produces a series of numbers or digits, and hence this process is called as **digital**. Each one of these digits, though in binary code, represent the approximate amplitude of the signal sample at that instant.

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

25. a) Describe in detail about classifications of networks with neat sketch.

Classification of Networks by Scale

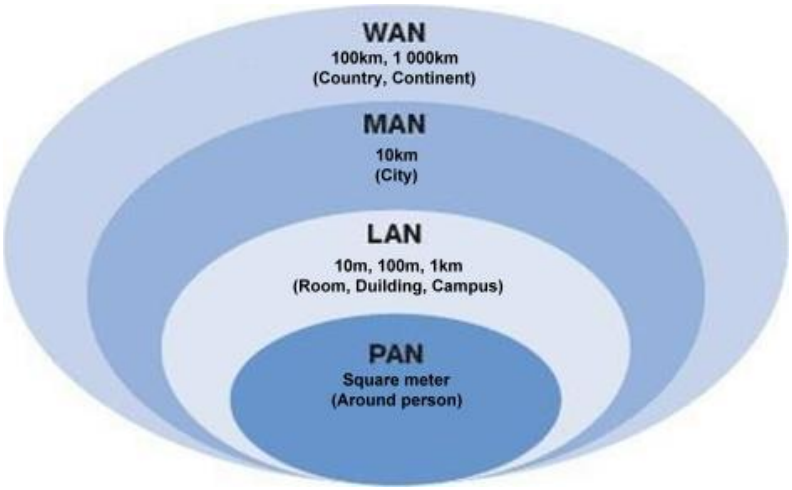
- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Networks (WAN)

Personal Area Network (PAN) - The interconnection of devices within the range of an individual person, typically within a range of 10 meters. For example, a wireless network connecting a computer with its keyboard, mouse or printer is a PAN. Also, a PDA that controls the user's hearing aid or pacemaker fits in this category. Another example of PAN is a Bluetooth. Typically, this kind of network could also be interconnected without wires to the Internet or other networks.

Local Area Network (LAN) - Privately-owned networks covering a small geographic area, like a home, office, building or group of buildings (e.g. campus). They are widely used to connect computers in company offices and factories to share resources (e.g., printers) and exchange information. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps.

Metropolitan Area Network (MAN) - Covers a larger geographical area than is a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of LANs. Metropolitan Area Networks can span up to 50km, devices used are modem and wire/cable.

Wide Area Networks (WAN) - Computer network that covers a large geographical area, often a country or continent. (any network whose communications links cross metropolitan, regional, or national boundaries). Less formally, a network that uses routers and public communications links.



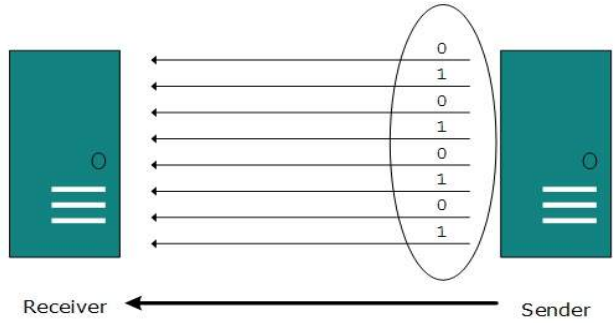
Networks by Scale

[OR]

b).Write a note on the 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.

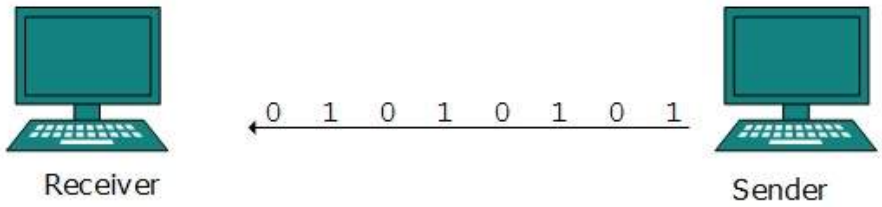
Parallel Transmission



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

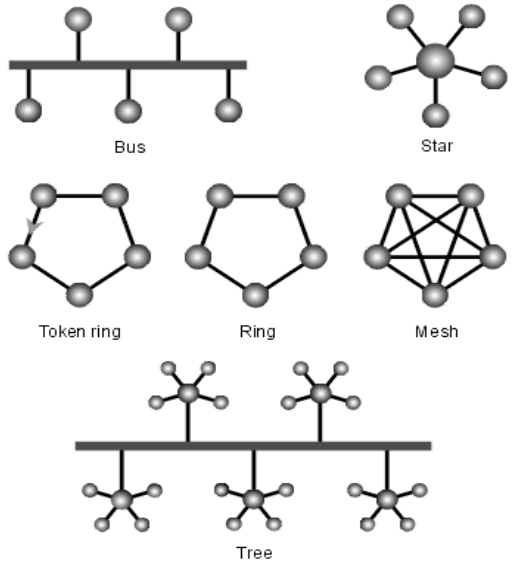
Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits.There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes.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

26. a). Explain the various network topologies with a neat diagram

- A *topology* is a way of "laying out" the network. Topologies can be either physical or logical.
- *Physical topologies* describe how the cables are run.
- *Logical topologies* describe how the network messages travel

- Bus (can be both logical and physical)
- Star (physical only)
- Ring (can be both logical and physical)
- Mesh (can be both logical and physical)



Types of Network Topology

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

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 and 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

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.

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.

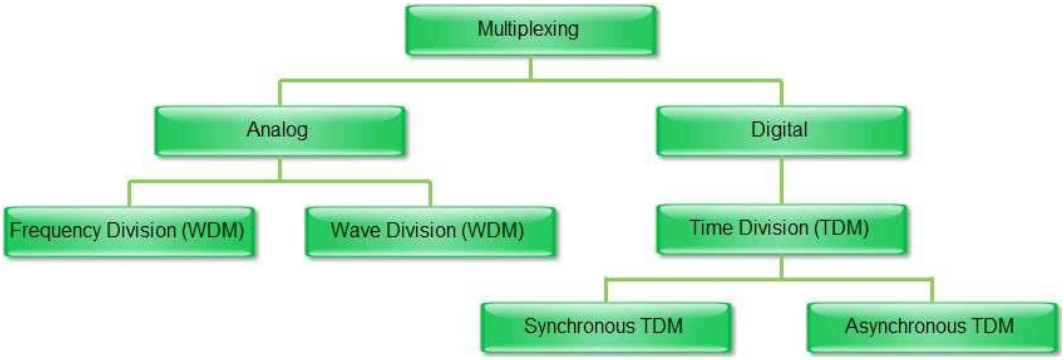
[OR]

b) Explain multiplexing techniques with neat diagram.

A communications device that multiplexes (combines) several signals for transmission over a single medium. A demultiplexer completes the process by separating multiplexed signals from a transmission line. Frequently a multiplexer and demultiplexer are combined into a single

device capable of processing both outgoing and incoming signals. **A multiplexer is sometimes called a mux**.

.

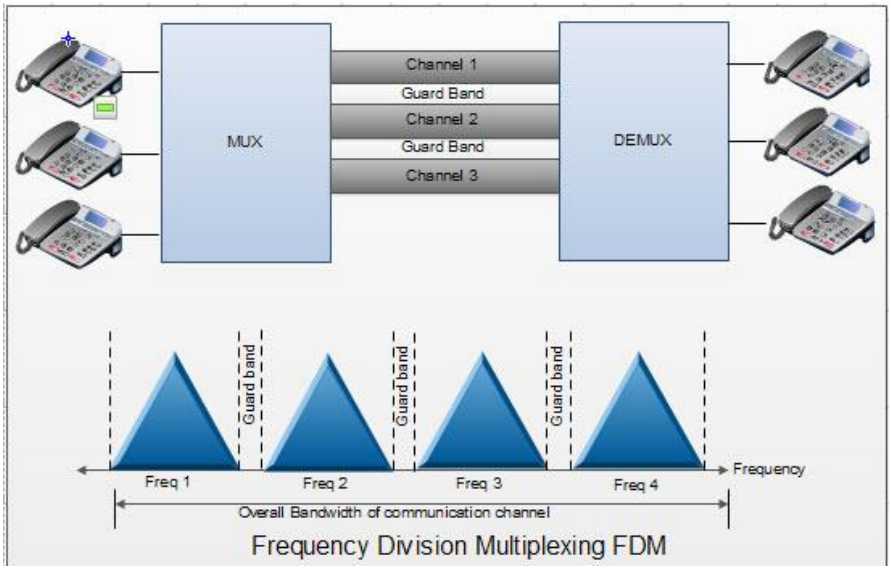


FDM:

Frequency-Division Multiplexing (FDM) is a scheme in which **numerous signals are combined for transmission on a single communications line or channel.** It is analog technique. Each signal is assigned a different frequency (sub channel) within the main channel.

FDM requires that the bandwidth of a link should be greater than the combined bandwidths of the various signals to be transmitted. Thus each signal having different frequency forms a particular logical channel on the link and follows this channel only. These channels are then separated by the strips of unused bandwidth called guard bands. These guard bands prevent the signals from overlapping as shown in Fig.

In FDM, signals to be transmitted must be analog signals. Thus digital signals need to be converted to analog form, if they are to use FDM.



A typical analog Internet connection via a twisted pair telephone line requires approximately three kilohertz (3 kHz) of bandwidth for accurate and reliable data transfer.

Twisted-pair lines are common in households and small businesses. But major telephone cables, operating between large businesses, government agencies, and municipalities, are capable of much larger bandwidths.

Advantages of FDM:

1. A large number of signals (channels) can be transmitted simultaneously.
2. FDM does not need synchronization between its transmitter and receiver for proper operation.
3. Demodulation of FDM is easy.
4. Due to slow narrow band fading only a single channel gets affected.

Disadvantages of FDM:

1. The communication channel must have a very large bandwidth.
2. Intermodulation distortion takes place.
3. Large number of modulators and filters are required.
4. FDM suffers from the problem of crosstalk.
5. All the FDM channels get affected due to wideband fading.

Applications of FDM

1. FDM is used for FM & AM radio broadcasting. Each AM and FM radio station uses a different carrier frequency. In AM broadcasting, these frequencies use a special band from 530 to 1700 KHz. All these signals/frequencies are multiplexed and are transmitted in air. A receiver receives

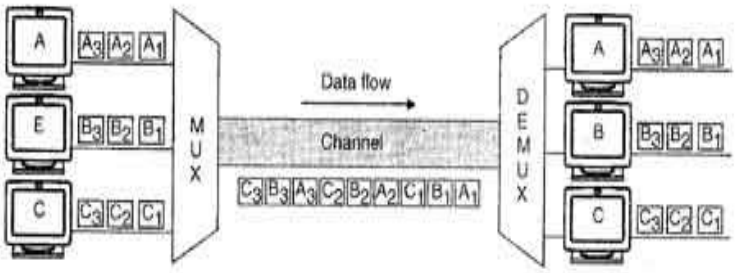
all these signals but tunes only one which is required. Similarly FM broadcasting uses a bandwidth of 88 to 108 MHz

2. FDM is used in television broadcasting.
3. First generation cellular telephone also uses FDM.

Time Division Multiplexer

Short for Time Division Multiplexing, a type of multiplexing that combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel. Within T-Carrier systems, such as T-1 and T-3, TDM combines Pulse Code Modulated (PCM) streams created for each conversation or data stream.

1. TDM is the digital multiplexing technique.
2. In TDM, the channel/link is not divided on the basis of frequency but on the basis of time.
3. Total time available in the channel is divided between several users.
4. Each user is allotted a particular a time interval called time slot or time slice during which the data is transmitted by that user.
5. Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time.
6. In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices.
7. In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one.
8. Thus each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel.
9. The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing.
10. The TDM signal in the form of frames is transmitted on the common communication medium.



Time Division Multiplexing (TDM)

Advantages of TDM :

1. Full available channel bandwidth can be utilized for each channel.
2. lntermodulation distortion is absent.
3. TDM circuitry is not very complex.
4. The problem of crosstalk is not severe.

Disadvantages of TDM :

1. Synchronization is essential for proper operation.
2. Due to slow narrowband fading, all the TDM channels may get wiped out.