Biyani's Think Tank

Concept based notes

Data Communication & Computer Networks

BCA V- Semester

Mr. Himanshu Mathur

Asst. Professor

Dept. of IT

Biyani Girls College, Jaipur

BIYANI

Where you can trust

Published by :

Think Tanks
Biyani Group of Colleges

Concept & Copyright :

©Biyani Shikshan Samiti
Sector-3, Vidhyadhar Nagar,
Jaipur-302 023 (Rajasthan)
Ph: 0141-2338371, 2338591-95 Fax: 0141-2338007
E-mail : acad@biyanicolleges.org
Website :www.gurukpo.com; www.biyanicolleges.org

ISBN :

Edition: 2025

While every effort is taken to avoid errors or omissions in this Publication, any mistake or omission that may have crept in is not intentional. It may be taken note of that neither the publisher nor the author will be responsible for any damage or loss of any kind arising to anyone in any manner on account of such errors and omissions.

Leaser Type Setted by :

Biyani College Printing Department

Preface

I am glad to present this book, especially designed to serve the needs of the students. The book has been written keeping in mind the general weakness in understanding the fundamental concepts of the topics. The book is self-explanatory and adopts the “Teach Yourself” style. It is based on question-answer pattern. The language of book is quite easy and understandable based on scientific approach.

Any further improvement in the contents of the book by making corrections, omission and inclusion is keen to be achieved based on suggestions from the readers for which the author shall be obliged.

I acknowledge special thanks to Mr. Rajeev Biyani, *Chairman* & Dr. Sanjay Biyani, *Director* (*Acad.*) Biyani Group of Colleges, who are the backbones and main concept provider and also have been constant source of motivation throughout this Endeavour. They played an active role in coordinating the various stages of this Endeavour and spearheaded the publishing work.

I look forward to receiving valuable suggestions from professors of various educational institutions, other faculty members and students for improvement of the quality of the book. The reader may feel free to send in their comments and suggestions to the under mentioned address.

Author

BCA-75T-305: Data Communication & Computer Networks

UNIT-I

Introduction: Network definition, Network topologies, Types of Network, Layered network architecture, Categories of Network, protocol, Standards and interface.

Network Models :client-server, peer-to-peer, OSI reference model, Architecture and functions of layers. TCP/IP protocol suite.

UNIT-II

Data Communication Fundamentals: Analog and digital signal, Data-rate limits, Digital to digital & Digital to analog modulation. Guided and Unguided Transmission media

Data Link Layer and Network Devices Data link layer: framing, error detection and Corrections, flow control, Network devices: switches, routers, bridges, etc., MAC addressing and Ethernet standards.

UNIT-III

Networks Layer Functions and Protocols: Routing, Routing algorithms, Network layer protocol of Internet-IP protocol.

Transport Layer Functions and Protocols: Transport services, Berkeley socket interface overview, Transport layer protocol of Internet-UDP and TCP. Overview of Application layer protocol, DNS protocol, WWW &**HTTP** protocols.

UNIT-IV

Circuit Switching : Simple Circuit Switching, Circuit Switching Networks, Space Division switching, Time Division Multiplexing, Routing in Switching Networks, Control Signals & Channels. Packet Switching concepts and principles.

Network Security and Wireless Networks Network security concepts: encryption, firewalls, VPN, Wireless networks and technologies.

Chapter-1

Introduction to Computer Network

Q.1. What is Computer Network? What are the different classifications of Computer Network?

Ans.: A network consists of two or more computers that are linked in order to share resources such as printers and CD-ROMs, exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Computer network can be classified on the basis of following features :

By Scale : Computer networks may be classified according to the scale :

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

By Connection Method : Computer networks can also be classified according to the hardware technology that is used to connect the individual devices in the network such as Optical fibre, Ethernet, Wireless LAN.

By Functional Relationship (Network Architectures) : Computer networks may be classified according to the functional relationships which exist between the elements of the network. This classification also called computer architecture. There are two type of network architecture :

- Client-Server
- Peer-to-Peer Architecture

By Network Topology : Network Topology signifies the way in which intelligent devices in the network see their logical or physical relations to one another.Computer networks may be classified according to the network topology upon which the network is based, such as :

- Bus Network
- Star Network
- Ring Network
- Mesh Network
- Star-Bus Network
- Tree or Hierarchical Topology Network

Q.2. What is Computer Networking?

Ans.: To share data and network resources among the computers in a network is known as networking. Computer networking is a core part of the whole information technology field because without it computers can never communicate with each other locally and remotely. Just imagine that if you work in a bank or in a corporate office and all the computers in your office are without networking. How difficult it would be for you and for the other employees of your office to communications, shares data such as word documents, financial reports, client‟s feedback, graphical reports and other important work with the other employees.

Q.3. What are the different type of Computer Network?

Ans.: Computer network are of following type :

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)

Local Area Network : A **local-area network** is a computer network covering a small geographic area, like a home, office, or groups of buildings e.g. a school. For example, a library will have a wired or wireless LAN for users to interconnect local devices e.g., printers and servers to connect to the internet.

The defining characteristics of LANs, in contrast to wide-area networks (WANs), includes their much higher data-transfer rates, smaller geographic range, and lack of need for leased telecommunication lines. Although switched Ethernet is now the most common protocol for LAN. Current Ethernet or other IEEE 802.3 LAN technologies operate at speeds up to 10 Gbit/s.IEEE has projects investigating the standardization of 100 Gbit/s, and possibly 40 Gbit/s. Smaller LANs generally consist of a one or more switches linked to each other - often with one connected to a router, cable modem, or

DSL modem for Internet access. LANs may have connections with other LANs via leased lines, leased services.

Wide Area Network : A WAN is a data communications network that covers a relatively broad geographic area i.e. one city to another and one country to another country and that often uses transmission facilities provided by common carriers, such as telephone companies.

Any network whose communications links cross metropolitan, regional, or national boundaries. Or, less formally, a network that uses routers and public communications links. Contrast with local area networks (LANs) or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area respectively. The largest and most well-known example of a WAN is the Internet.

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects to the LAN on one side and a hub within the WAN on the other. Leased lines can be very expensive. Network protocols including TCP/IP deliver transport and addressing functions.

Several options are available for WAN connectivity.Transmission rate usually range from 1200 bits/second to 6 Mbit/s, although some connections such as ATM and Leased lines can reach speeds greater than 156 Mbit/s. Typical communication links used in WANs are telephone lines, microwave links & satellite channels.

Metropolitan Area Network : Metropolitan area networks, or **MAN**s, are large computer networks usually spanning a city. They typically use wireless infrastructure or Optical fiber connections to link their sites.

A Metropolitan Area Network is a network that connects two or more Local Area Networks or Campus Area Networks together but does not extend beyond the boundaries of the immediate town, city, or metropolitan area. Multiple routers, switches & hubs are connected to create a MAN.

According to IEEE, "A MAN is optimized for a larger geographical area than 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 local networks. Metropolitan area networks can span up to 50km, devices used are modem and wire/cable."

Q.4. What is Internetworking?

Ans.: When two or more networks or network segments are connected using devices such as a router then it is called as internetworking. Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an internetwork.

In modern practice, the interconnected networks use the Internet Protocol. There are three variants of internetwork, depending on who administers and who participates in them :

- Intranet
- Extranet
- Internet

Intranets and extranets may or may not have connections to the Internet. If connected to the Internet, the intranet or extranet is normally protected from being accessed from the Internet without proper authorization. The Internet is not considered to be a part of the intranet or extranet, although it may serve as a portal for access to portions of an extranet.

Intranet : An intranet is a set of interconnected networks, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a single administrative entity. That administrative entity closes the intranet to the rest of the world, and allows only specific users. Most commonly, an intranet is the internal network of a company or other enterprise. A large intranet will typically have its own web server to provide users with browseable information.

Extranet : An extranet is a network or internetwork that is limited in scope to a single organisation or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities .Technically, an extranet may also be categorized as a MAN, WAN, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

Internet : A specific internetwork, consisting of a worldwide interconnection of governmental, academic, public, and private networks based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense – also home to the World Wide Web

(WWW) and referred to as the 'Internet' with a capital 'I' to distinguish it from other generic internetworks. Participants in the Internet, or their service providers, use IP Addresses obtained from address registries that control assignments.

Q.5. What are differnet Computer Network Devices?

OR

What are the different Hardware Componenets of Computer Network?

Ans.: All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required like communication media. Followings are the basic hardware components for computer network:

Network Interface Card : A **network card**, **network adapter** or **NIC** (network interface card) is a piece of computer hardware designed to allow computers to communicate over a **computer network**. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

Repeater : A **repeater** is an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable runs longer than 100 meters.

Hub : A hub contains multiple ports. When a packet arrives at one port, it is copied to all the ports of the hub. When the packets are copied, the destination address in the frame does not change to a broadcast address. It does this in a rudimentary way; it simply copies the data to all of the Nodes connected to the hub.

If the hub fails to work, the communication between the computers stops till the hub again starts working. Hub broadcasts the data to its every port, and then finding the destined computer, the data sent toward it. Hub broadcasts the data to its every port, and then finding the destined computer, the data sent toward it.

Bridge : A **network bridge** connects multiple network segments at the data link layer of the OSI model. Bridges do not promiscuously copy traffic to all ports, as a hub do, but learns which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Switch : A switch normally has numerous ports with the intention that most or all of the network be connected directly to a switch, or another switch that is in turn connected to a switch.

Switches is a marketing term that encompasses routers and bridges, as well as devices that may distribute traffic on load or by application content .Switches may operate at one or more OSI layers, including physical, data link, network, or transport . A device that operates simultaneously at more than one of these layers is called a multilayer switch.

The switch is an advance form of the hub similar in functions but the advanced switches has a switching table in them. An advanced switch stores the MAC address of every attached computer and the data is only sent to the destined computer, unlike the hubs where data is sent to all ports.

Router : A router is a key device in the internet communication and wan communication system. A router has software called routing table and the source and destination addresses are stored in the routing table.

Routers are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. Routers work at the network layer of the TCP/IP model or layer 3 of the OSI model. Routers also provide interconnectivity between like and unlike media. This is accomplished by examining the Header of a data packet, and making a decision on the next hop to which it should be sent. They use preconfigured static routes, status of their hardware interfaces, and routing protocols to select the best route between any two subnets. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Some DSL and cable modems, for home and office use, have been integrated with routers to allow multiple home/office computers to access the Internet through the same connection. Many of these new devices also consist of wireless access points (waps) or wireless routers to allow for IEEE 802.11b/g wireless enabled devices to connect to the network without the need for a cabled connection.

The well known routers developing companies are Cisco systems, Nortel, DLink and others. Every ISP, banks, corporate offices and multinational companies use routers for LAN and WAN communications and communication in their private networks.

Server : A server is a computer in network that provides services to the client computers such as logon requests processing, files access and storage, internet access, printing access and many other types of services. Servers are mostly equipped with extra hardware such as plenty of external memory (RAM), more data store capacity (hard disks), high processing speed and other features.

Gateway : Gateways work on all seven OSI layers. The main job of a gateway is to convert protocols among communications networks. A router by itself transfers, accepts and relays packets only across networks using similar protocols. A gateway on the other hand can accept a packet formatted for one protocol (e.g. AppleTalk) and convert it to a packet formatted for another protocol (e.g. TCP/IP) before forwarding it. A gateway can be implemented in hardware, software or both, but they are usually implemented by software installed within a router. A gateway must understand the protocols used by each network linked into the router. Gateways are slower than bridges, switches and (non-gateway) routers.

A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the networks in between are gateways. For example, the computers that control traffic between company networks or the computers used by internet service providers (ISPs) to connect users to the internet are gateway nodes.

Q.6. What are the different step to configure Peer-to-Peer and Client-Server Architecture in Computer Network?

Ans.: Peer-to-Peer Network Model : In the peer to peer network model we simply use the same Workgroup for all the computers and a unique name for each computer.

Additionally, we will have to give a unique IP address of the same class A, B, or C for all the computers in our network and its related subnet mask e.g. if we decide to use class A IP address for our three computers in our Peer-to-Peer network then our IP address/Subnet mask settings can be as follows.

Computer Name	IP Address	Subnet Mask	Workgroup
PC1	100.100.100.1	255.0.0.0	Officenetwork
PC2	100.100.100.2	255.0.0.0	Officenetwork
PC3	100.100.100.3	255.0.0.0	Officenetwork

Please note that the above example is for only illustration purpose so we can choose any IP address, computer name and workgroup name of our interest.

For doing this right click on „My Computer‟ and then click „Properties‟ then go to the Network Identification section and set these.

In a peer to peer network all computers acts as a client because there is not centralized server. Peer to peer network is used where not security is required in the network.

Client/Server Network Model : In the client/server network model a computer plays a centralized role and is known as a server. All other computers in the network are known as clients. All client computers access the server simultaneously for files, database, docs, spreadsheets, web pages and resources like input/output devices and others. In other words, all the client computes depends on the server and if server fails to respond or crash then networking/communication between the server and the client computers stops.

If we want to configure a client-server network model then first prepare the server.

For that we have to follow the following steps :

- Install Windows 2000 or Windows 2003 Server from the CD on the server computer and make a domain.
- We can create a domain by this command on the Run "DCPROMO".
- We can give this command once weinstall the server successfully.
- After wegive the DCPROMO command wewill be asked for a unique domain name.
- All the client computers will use the same unique domain name for becoming the part of this domain.
- This command will install the active directory on the server, DNS and other required things.

- A step by step wizard will run and will guide us for the rest of the steps. Make sure that a network cable is plugged in the LAN card of the server when we you run the DCPROMO.exe command.
- When the Active directory is properly installed on the server, restart the server.
- We can create network users on the server computer and also name/label the network resources like computers/printers etc.
- Once we install the server successfully now come to the client computers.
- Install Windows 2000 professional on our all client computers.
- Once we install the Windows 2000 professional on the clients the next step is to make this computer (client computer) a part of the network.

Configuration Steps :

(1) Choose a unique name for each client computer.

(2) Choose unique IP address for each computer and relevant.

(3) Use the same domain name for all client PCs.

Network/System administrators are required to do these administrative tasks on the server and client computers. Any shared resources on the network either on the server or the clients can be access through the My Network Places in the Windows 2000 platform. There is another way to connect to the shared resources by giving this command in the run \\ComputerName\SharedDriveLetter.

Q.7. What are the different Network Topologies?

Ans.: **Network topology** is the study of the arrangement or mapping of the devices of a network, especially the physical and logical interconnections between nodes.

Classification of Network Topologies : There are two basic categories of network topologies :

- Physical Topology
- Logical Topology

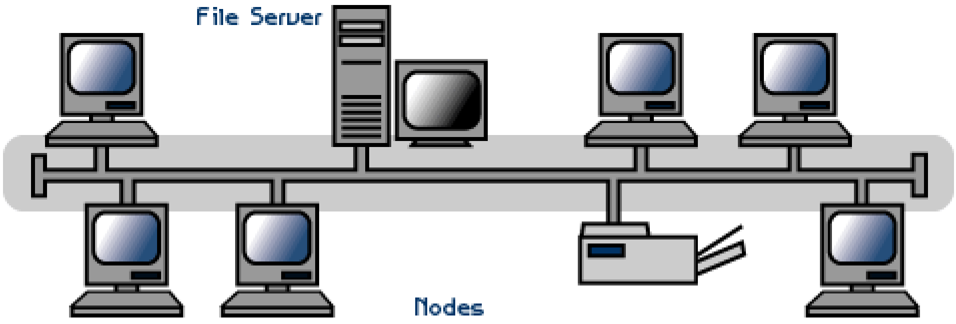
Physical Topology : The mapping of the nodes of a network and the physical connections between them – i.e., the layout of wiring, cables, the locations of nodes, and the interconnections between the nodes and the cabling or wiring system referred as physical topology

Logical Topology : The mapping of the apparent connections between the nodes of a network, as evidenced by the path that data appears to take when traveling between the nodes.

Types of the Topologies :

- Bus
- Star
- Ring
- Mesh
  - partially connected mesh (or simply 'mesh')
  - fully connected mesh
- Tree
- Hybrid

Bus : The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints ;this is the 'bus', which is also commonly referred to as the backbone, or trunk – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network virtually simultaneously.



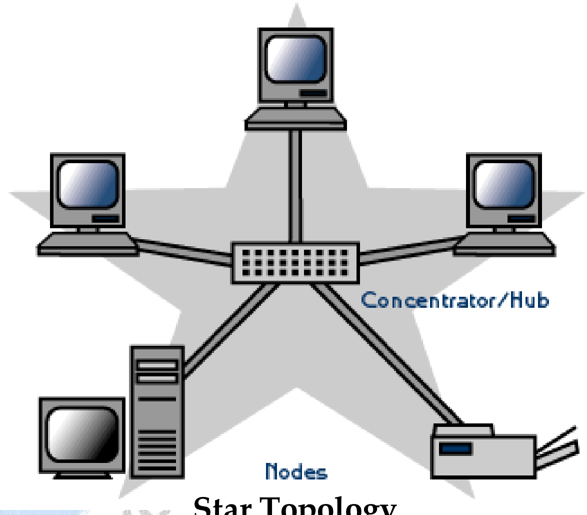
Bus topology

Advantages :

- Easy to connect a computer or peripheral to a bus.
- Requires less cable length than a star topology.

Disadvantages :

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.



Star Topology

Star : The type of network topology in which each of the nodes of the network is connected to a central node with a point-to-point link in a 'hub' and 'spoke' fashion, the central node being the 'hub' and the nodes that are attached to the central node being the 'spokes'. All data that is transmitted between nodes in the network is transmitted to this central node, which is e of device that then retransmits the data to some or all of the other nodes in the network, although the central node may also be a simple common connection point without any active device to repeat the signals.

Advantages :

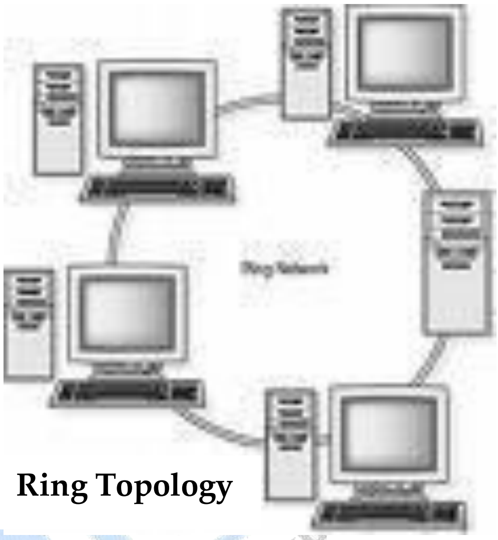
- Easy to install and wire.
- No disruptions to the network then connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages :

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.

Ring : The type of network topology in which each of the nodes of the network is connected to two other nodes in the network and with the first and last nodes being connected to each other, forming a ring – all data that is transmitted between nodes in the network travels from one node to the next node in a circular manner and the data generally flows in a single direction only.

Dual-ring : The type of network topology in which each of the nodes of the network is connected to two other nodes in the network, with two connections to each of these nodes, and with the first and last nodes being connected to each other with two connections, forming a double ring – the data flows in opposite directions around the two rings, although, generally, only one of the rings carries data during normal operation, and the two rings are independent unless there is a failure or break in one of the rings, at which time the two rings are joined to enable the flow of data to continue using a segment of the second ring to bypass the fault in the primary ring.



Ring Topology

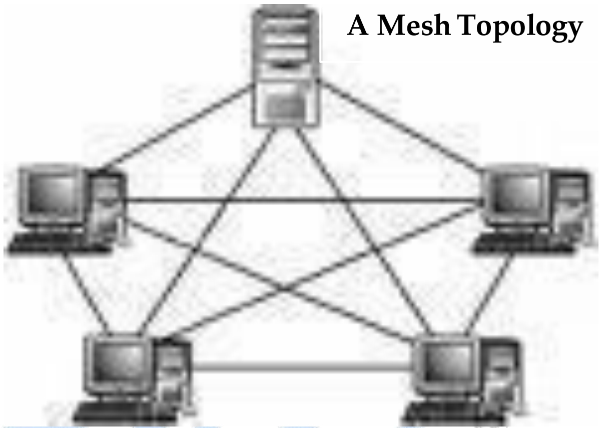
Advantages :

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a star topology under heavy network load
- Does not require network server to manage the connectivity between the computers

Disadvantages :

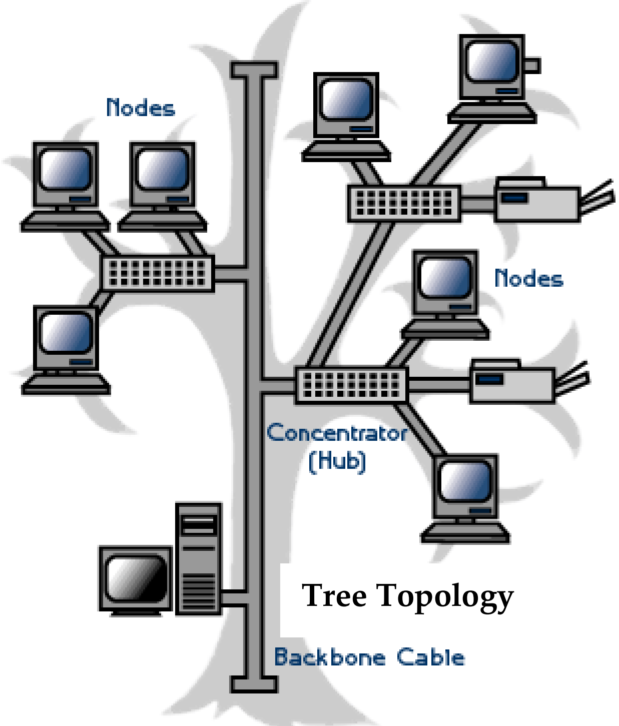
- One malfunctioning workstation or bad port can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Much slower than an bus network under normal load.

Mesh : The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.


A Mesh Topology

Fully Connected : The type of network topology in which each of the nodes of the network is connected to each of the other nodes in the network with a point-to-point link – this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.

The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected.



Tree Topology

Tree or Hierarchical : The type of network topology in which a central 'root' node, the top level of the hierarchy, is connected to one or more other nodes that are one level lower in the hierarchy i.e., the second level, with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy, i.e., the third level, connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy – the hierarchy of the tree is symmetrical, each node in the network having a specific fixed number, f, of nodes connected to it at the next lower level in the hierarchy, the number, f, being referred to as the 'branching factor' of the hierarchical tree.

Advantages :

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages :

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies

Hybrid Network Topologies : The hybrid topology is a type of network topology that is composed of one or more interconnections of two or more networks that are based upon different physical topologies or a type of network topology that is composed of one or more interconnections of two or more networks that are based upon the same physical topology.

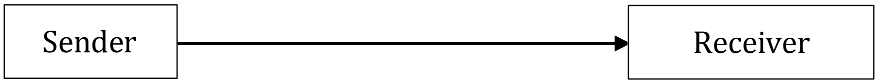
Q.8. What are the different Transmission Modes?

Ans.: There are three ways or **modes of data transmission :**

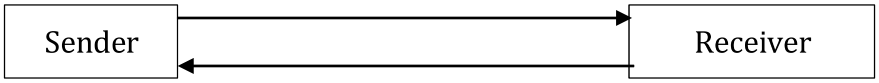
Simplex : Communication can take place in one direction connected to such a circuit are either a send only or a receive only device.

Half Duplex : A half duplex system can transmit data in both directions, but only in one direction at a time.

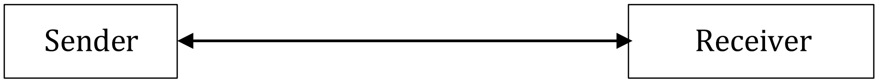
Full Duplex : A full duplex system can transmit data simultaneously in both directions on transmission path.



(a) Simplex



(b) Half Duplex



(c) Full Duplex

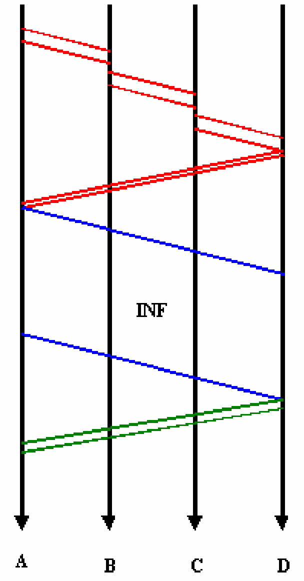
Transmission Modes

Q.9. Write short note on Switching techniques?

Ans.: Apart from determining valid paths between sources and destinations within an interconnection network, a switching technique is needed that specifies how messages are to be fragmented before passing them to the network and how the resources along the path are to be allocated. Furthermore, a switching technique gives preconditions to be fulfilled before a fragment can be moved on to the next network component.

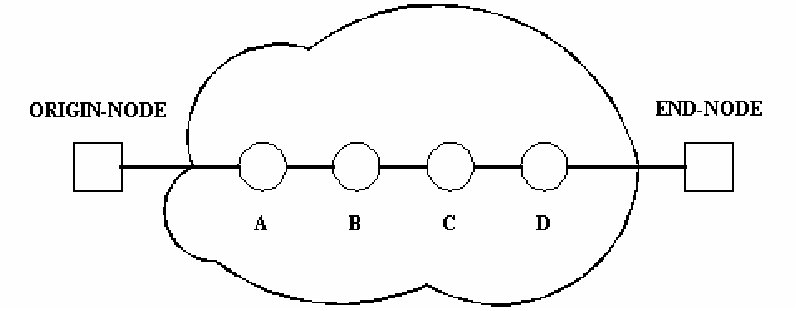
Following are the different **switching techniques :**

Circuit Switching : In circuit switching when a connection is established, the origin-node identifies the first intermediate node (node A) in the path to the end-node and sends it a communication request signal. After the first intermediate node receives this signal the process is repeated as many times as needed to reach the end-node. Afterwards, the end-node sends a communication acknowledge signal to the origin-node through all the intermediate nodes that have been used in the communication request. Then, a full duplex transmission line, that it is going to be kept for the whole communication, is set-up between the origin-node and the end-node.

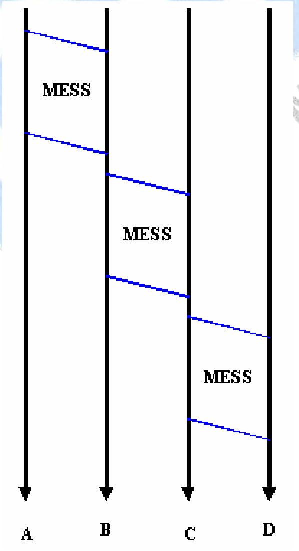


Circuit Switching

To release the communication the origin-node sends a communication end signal to the end-node. In Following figure shows that a connection in a four-node circuit switching network

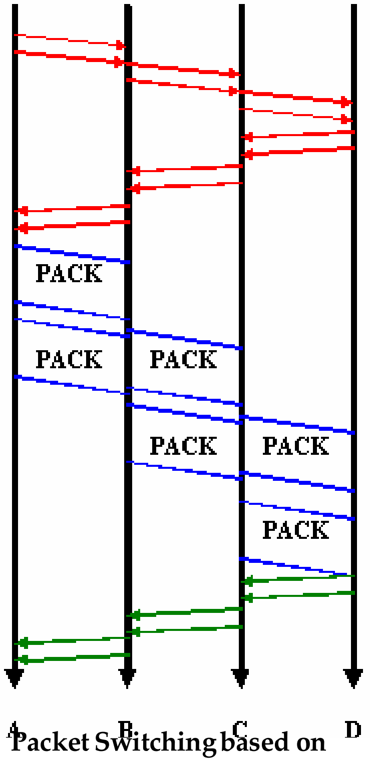


Message Switching : When a connection is established, the origin-node identifies the first intermediate node in the path to the end-node and sends it the whole message. After receiving and storing this message, the first intermediate node (node A) identifies the second one (node B) and, when the transmission line is not busy, the former sends the whole message (store-and-forward philosophy). This process is repeated up to the end-node. As can be seen in figure no communication release or establishment is needed.



Message Switching

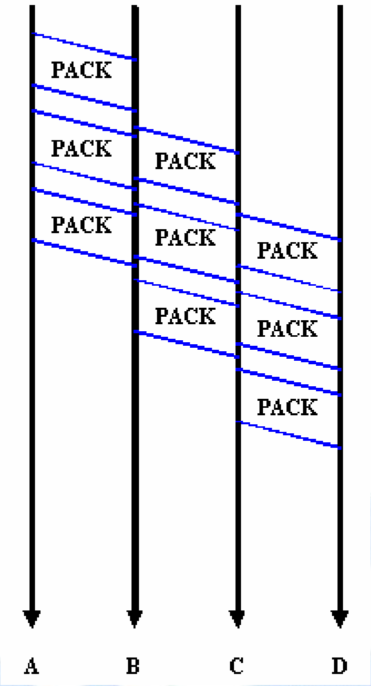
Packet Switching based on Virtual Circuit: When a connection is established, the origin-node identifies the first intermediate node (node A) in the path to the end-node and sends it a communication request packet. This process is repeated as many times as needed to reach. Then, the end-node sends a communication acknowledge packet to the origin-node through the intermediate nodes (A, B, C and D) that have been traversed in the communication request. The virtual circuit established on this way will be kept for the whole communication. Once a virtual circuit has been established, the origin-node begins to send packets (each of them has a virtual circuit identifier) to the first intermediate node. Then, the first intermediate node (node A) begins to send packets to the following node in the virtual circuit without waiting to store all message packets received from the origin-node. This process is repeated until all message packets arrive to the end-node. In the communication release, when the origin-node sends to the end-node a communication end packet, the latter answers with an acknowledge packet. There are two possibilities to release a connection :



Packet Switching based on Virtual Circuit

- No trace of the virtual circuit information is left, so every communication is set-up as if it were the first one.
- The virtual circuit information is kept for future connections.

Packet Switching based on Datagram : The origin-node identifies the first intermediate node in the path and begins to send packets. Each packet carries an origin-node and end-node identifier. The first intermediate node (node A) begins to send packets, without storing the whole message, to the following intermediate node. This process is repeated up to the end-node. As there are neither connection establishment nor connection release, the path follow for each packet from the origin-node to the end-node can be different and therefore, as a consequence of different propagation delays, they can arrive disordered.



Packet Switching based on Datagram

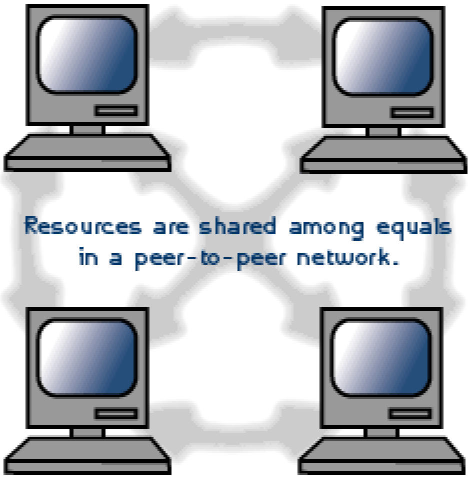
Cell Switching : Cell Switching is similar to packet switching, except that the switching does not necessarily occur on packet boundaries. This is ideal for an integrated environment and is found within Cell-based networks, such as ATM. Cell-switching can handle both digital voice and data signals.

Comparison of Switching Techniques : If a connection (path) between the origin and the end node is established at the beginning of a session we are talking about circuit or packet (virtual circuit) switching. In case it does not, we refer to message and packet (datagram) switching. On the other hand, when considering how a message is transmitted, if the whole message is divided into pieces we have packet switching (based either on virtual circuit or datagram) but if it does not, we have circuit and message switching.

Q.10. What are the different Computer Architectures?

Ans.: The two major types of network architecture systems are :

- Peer-to-Peer
- Client-Server


Resources are shared among equals in a peer-to-peer network.

Peer-to-peer network

Peer-to-Peer : Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source. In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. AppleShare and Windows for Workgroups are examples of programs that can function as peer-to-peer network operating systems.

Advantages of a Peer-to-Peer Network :

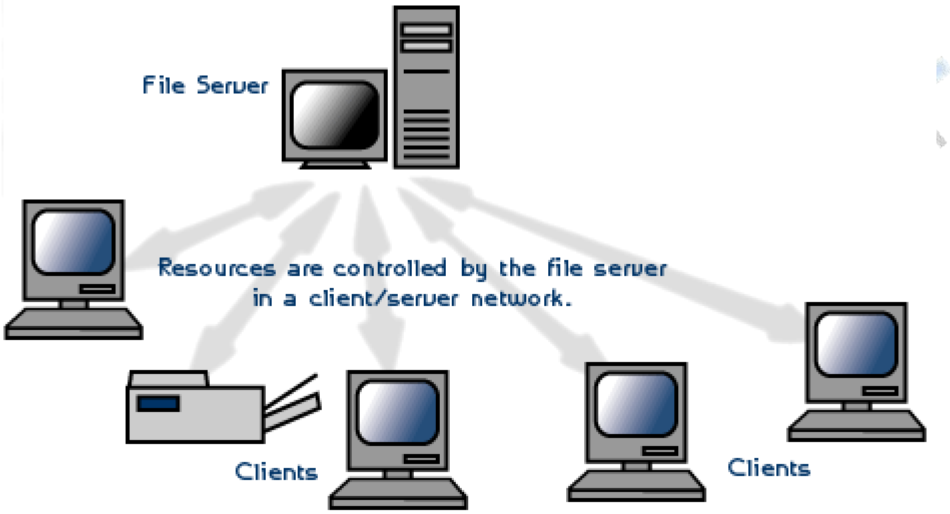
- Less initial expense - No need for a dedicated server.
- Setup - An operating system such as Windows XP already in place may only need to be reconfigured for peer-to-peer operations.

Disadvantages of Peer-to-Peer Network :

- Decentralized - No central repository for files and applications.
- Security - Does not provide the security available on a client/server network.

Client-Server : A network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers), or network traffic (network servers). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated servers. The servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location.


File Server
Resources are controlled by the file server in a client/server network.
Clients
Clients

Client-Server Network

Advantages of Client/Server Network :

- Centralized - Resources and data security are controlled through the server.
- Scalability - Any or all elements can be replaced individually as needs increase.
- Flexibility - New technology can be easily integrated into system.
- Interoperability - All components: client/network/server, work together.
- Accessibility - Server can be accessed remotely and across multiple platforms.

Disadvantages of Client/Server Network:

- Expense - Requires initial investment in dedicated server.

- Maintenance - Large networks will require a staff to ensure efficient operation.
- Dependence - When server goes down, operations will cease across the network

□ □ □

Chapter-2

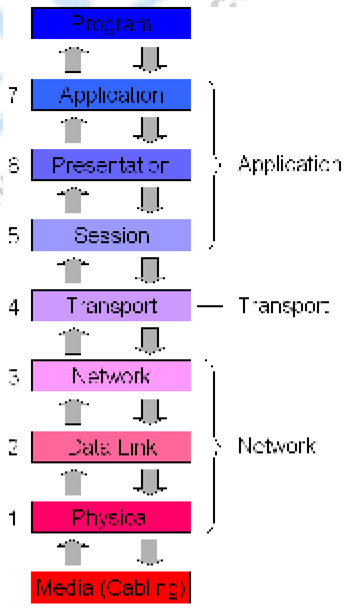
Introduction to Network Layers

Q.1. Describe OSI Model.

Ans.: **Open System Interconnection**, an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Open Systems Interconnection (OSI) model is developed by ISO (International organization for standardization) in 1984. OSI reference model is a logical framework for standards for the network communication. OSI reference model is now considered as a primary standard for internetworking and inter computing. Today many network communication protocols are based on the standards of OSI model. In the OSI model the network/data communication is defined into seven layers.

The seven layers can be grouped into three groups - Network, Transport and Application.

- **Network :** Layers from this group are low-level layers that deal with the transmission and reception of the data over the network.
- **Transport :** This layer is in charge of getting data received from the network and transforming them in a format nearer to the data format understandable by the program. When the computer is transmitting data, this vides it into several packets to be transmitted over the network. When your computer is receiving data, this layer gets the received packets and put them back together.



The OSI Reference Model

- **Application :** These are high-level layers that put data in the data format used by the program

Layer 7 – Application Layer : The application layer serves as the window for users and application processes to access network services. The application layer makes the interface between the program that is sending or is receiving data and the protocol stack. When you download or send e-mails, your e-mail program contacts this layer. This layer provides network services to the end-users like Mail, ftp, telnet, DNS.

Function of Application Layer :

- Resource sharing and device redirection.
- Remote file access.
- Remote printer access.
- Inter-process communication.
- Network management.
- Directory services.
- Electronicmessaging (such as mail).
- Network virtual terminals.

Protocols used at application layer are FTP, DNS, SNMP, SMTP, FINGER, TELNET.

Layer 6 – Presentation Layer : Presentation layer is also called translation layer. The presentation layer presents the data into a uniform format and masks the difference of data format between two dissimilar systems

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, and then translate the common format to a format known to the application layer at the receiving station. Presentation layer provides :

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

Layer 5 - Session : The session protocol defines the format of the data sent over the connections. Session layer establish and manages the session between the two users at different ends in a network. Session layer also manages who can transfer the data in a certain amount of time and for how long. The examples of session layers and the interactive logins and file transfer sessions. Session layer reconnect the session if it disconnects. It also reports and logs and upper layer errors.

The session layer allows session establishment between processes running on different stations. It provides:

- Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging and so on.

Protocols : The protocols that work on the session layer are NetBIOS, Mail Slots, Names Pipes, RPC.

Layer 4 - Transport : Transport layer manages end to end message delivery in a network and also provides the error checking and hence guarantees that no duplication or errors are occurring in the data transfers across the network. Transport layer also provides the acknowledgement of the successful data transmission and retransmits the data if no error free data was transferred.

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides :

- Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
- Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

- Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions.

Protocols : These protocols work on the transport layer TCP, SPX, NETBIOS, ATP and NWLINK.

Layer 3 - Network : This layer is in charge of packet addressing, converting logical addresses into physical addresses, making it possible to data packets to arrive at their destination. This layer is also in charge of setting the route. The packets will use to arrive at their destination, based on factors like traffic and priorities.

The network layer determines that how data transmits between the network devices. It also translates the logical address into the physical address e.g computer name into MAC address. It is also responsible for defining the route, managing the network problems and addressing

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides :

- **Routing :** Routes frames among networks.
- **Subnet Traffic Control :** Routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- **Frame Fragmentation :** If it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- **Logical-Physical Address Mapping :** translates logical addresses, or names, into physical addresses.
- **Subnet Usage Accounting :** has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

Protocols : These protocols work on the network layer IP, ICMP, ARP, RIP, OSI, IPX and OSPF.

Layer 2 - Data Link layer : The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.

Data Link layer defines the format of data on the network. A network data frame, packet, includes checksum, source and destination address, and data. The data link layer handles the physical and logical connections to the packet's destination, using a network interface.

This layer gets the data packets send by the network layer and convert them into frames that will be sent out to the network media, adding the physical address of the network card of your computer, the physical address of the network card of the destination, control data and a checksum data, also known as CRC. The frame created by this layer is sent to the physical layer, where the frame will be converted into an electrical signal to do this, the data link layer provides :

- **Link Establishment and Termination :** Establishes and terminates the logical link between two nodes.
- **Frame Traffic Control :** Tells the transmitting node to "back-off" when no frame buffers are available.
- **Frame Sequencing :** Transmits/receives frames sequentially.
- **Frame Acknowledgment :** Provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- **Frame Delimiting :** Creates and recognizes frame boundaries.
- **Frame Error Checking :** Checks received frames for integrity.
- **Media Access Management :** determines when the node "has the right" to use the physical medium.

Layer 1 – Physical : The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. Physical layer defines and cables, network cards and physical aspects. It also provides the interface between network and network communication devices.

This layer gets the frames sent by the Data Link layer and converts them into signals compatible with the transmission media. If a metallic cable is used, then it will convert data into electrical signals; if a fiber optical cable is used, then it will convert data into luminous signals; if a wireless network is used, then it will convert data into electromagnetic signals; and so on. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together and check for its integrity.

Physical layer provides :

Data Encoding : Modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

- What signal state represents a binary 1.
- How the receiving station knows when a "bit-time" starts.
- How the receiving station delimits a frame.

Physical Medium Attachment, Accommodating Various Possibilities in the Medium :

- Will an external transceiver (MAU) be used to connect to the medium?
- How many pins do the connectors have and what is each pin used for?

Transmission Technique : determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.

Physical Medium Transmission : transmits bits as electrical or optical signals appropriate for the physical medium, and determines:

- What physical medium options can be used.
- How many volts/db should be used to represent a given signal state, using a given physical medium.

Protocols used at physical layer are ISDN, IEEE 802 and IEEE 802.2.

Q.2. What is Congestion Control? Describe the Congestion Control Algorithm commonly used.

Ans.: Congestion is a situation in which too many packets are present in a part of the subnet, performance degrades. In other words when too much traffic is offered, congestion sets in and performance degrades sharply

Factors causing Congestion :

- The input traffic rate exceeds the capacity of the output lines.
- The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).
- The routers' buffer is too limited.

How to correct the Congestion Problem :

- **Increase the Resource :**
  - Using an additional line to temporarily increase the bandwidth between certain points.
  - Splitting traffic over multiple routes.
  - Using spare routers.
- **Decrease the Load :**
  - Denying service to some users,
  - Degrading service to some or all users, and
  - Having users schedule their demands in a more predictable way.

The Leaky Bucket Algorithm : The leaky bucket algorithm is commonly used congestion control algorithm. In this algorithm following steps are used to control the congestion:

- Each host is connected to the network by an interface containing a leaky bucket - a finite internal queue.
- The outflow is at a constant rate when there is any packet in the bucket and zero when the bucket is empty.
- **If a** packet arrives at the bucket when it is full, the packet is discarded.

Q.3. What is Routing? Describe the different Routing Algorithms.

Ans.: Routing is the process of selecting paths in a network along which to send data on physical traffic. In different network operating system the network layer perform the function of routing. In TCP/IP the IP protocol is the ability to form connections between different physical networks. A system that performs this function is called an *IP router*. This type of device attaches to two or more physical networks and forwards packets between the networks. When sending data to a remote destination, a host passes packet to a local router. The router forwards the packet toward the final destination. They travel from one router to another until they reach a router connected to the destination‟s LAN segment. Each router along the end-to-end path selects the *next hop* device used to reach the destination. The next hop represents the next device along the path to reach the destination. It is located on a physical network connected to this intermediate system. Because this physical network differs from the one on which the system originally received the datagram, the intermediate host has *forwarded* (that is, routed) the packets from one physical network to another.

There are two **types of routing algorithm :**

- Static
- Dynamic

Static Routing : Static routing uses preprogrammed definitions representing paths through the network. Static routing is manually performed by the network administrator. The administrator is responsible for discovering and propagating routes through the network. These definitions are manually programmed in every routing device in the environment. After a device has been configured, it simply forwards packets out the predetermined ports. There is no communication between routers regarding the current topology of the network. In small networks with minimal redundancy, this process is relatively simple to administer.

Dynamic Routing : Dynamic routing algorithms allow routers to automatically discover and maintain awareness of the paths through the network. This automatic discovery can use a number of currently available dynamic routing protocols.

Following are the **routing algorithms for networks :**

- Distance Vector Algorithm
- Link State Algorithm
- Path Vector Algorithm
- Hybrid Algorithm

Distance Vector Routing : Distance vector algorithms use the Bellman-Ford algorithm. Distance vector algorithms are examples of dynamic routing protocols. Algorithms allow each device in the network to automatically build and maintain a local routing table or matrix. Routing table contains list of destinations, the total cost to each, and the next hop to send data to get there.

This approach assigns a number, the cost, to each of the links between each node in the network. Nodes will send information from point A to point B via the path that results in the lowest total cost i.e. the sum of the costs of the links between the nodes used.

The algorithm operates in a very simple manner. When a node first starts, it only knows of its immediate neighbours, and the direct cost involved in reaching them. The routing table from the each node, on a regular basis, sends its own information to each neighbouring node with current idea of the total cost to get to all the destinations it knows of. The neighbouring node(s) examine this information, and compare it to what they already 'know'; anything which represents an improvement on what they already have, they insert in their own routing table(s). Over time, all the nodes in the network will discover the best next hop for all destinations, and the best total cost.

The main advantage of distance vector algorithms is that they are typically easy to implement and debug. They are very useful in small networks with limited redundancy.

When one of the nodes involved goes down, those nodes which used it as their next hop for certain destinations discard those entries, and create new routing-table information. They then pass this information to all adjacent nodes, which then repeat the process. Eventually all the nodes in the network receive the updated information, and will then discover new paths to all the destinations which they can still "reach".

Link State Routing : A link state is the description of an interface on a router and its relationship to neighboring routers.

When applying link-state algorithms, each node uses as its fundamental data a map of the network in the form of a graph. To produce this, each node floods the entire network with information about what other nodes it can connect to, and each node then independently assembles this information into a map. Using this map, each router then independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra's algorithm. The result is a tree rooted at the current node such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node.

Shortest-Path First (SPF) Algorithm : The SPF algorithm is used to process the information in the topology database. It provides a tree-representation of the network. The device running the SPF algorithm is the root of the tree. The output of the algorithm is the list of shortest-paths to each destination network. Because each router is processing the same set of LSAs, each router creates an identical link state database. However, because each device occupies a different place in the network topology, the application of the SPF algorithm produces a different tree for each router.

Path Vector Routing : Distance vector and link state routing are both intra-domain routing protocols. They are used inside an autonomous system, but not between autonomous systems. Both of these routing protocols become intractable in large networks and cannot be used in Inter-domain routing. Distance vector routing is subject to instability if there are more than few hops in the domain. Link state routing needs huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding.

Path vector routing is used for inter-domain routing. It is similar to Distance vector routing. In path vector routing we assume there is one node (there can be many) in each autonomous system which acts on behalf of the entire autonomous system. This node is called the speaker node. The speaker node creates a routing table and sends information to its neighboring speaker nodes in neighboring autonomous systems. The idea is the same as Distance vector routing except that only speaker nodes in each autonomous system can communicate with each other. The speaker node sends information of the path, not the metric of the nodes, in its autonomous system or other autonomous systems.

The path vector routing algorithm is somewhat similar to the distance vector algorithm in the sense that each border router advertises the destinations it can reach to its neighboring router. However, instead of advertising networks in terms of a destination and the distance to that destination, networks are sends information as destination addresses and path descriptions to reach those destinations. A route is defined as a pairing between a destination and the attributes of the path to that destination, thus the name, path vector routing, where the routers receive a vector that contains paths to a set of destinations. The path, expressed in terms of the domains traversed so far, is carried in a special path attribute that records the sequence of routing domains through which the reachability information has passed. The path represented by the smallest number of domains becomes the preferred path to reach the destination.

The main advantage of a path vector protocol is its flexibility.

Hybrid Routing : This algorithm attempt to combine the positive attributes of both distance vector and link state protocols. Like distance vector, hybrid algorithm use metrics to assign a preference to a route. However, the metrics are more accurate than conventional distance vector algorithm. Like link state algorithms, routing updates in hybrid algorithm are event driven rather than periodic. Networks using hybrid algorithm tend to converge more quickly than networks using distance vector protocols. Finally, algorithm potentially reduces the costs of link state updates and distance vector advertisements.

Q.4. What are Transmission Errors?

Ans.: External electromagnetic signals can cause incorrect delivery of data. By this, data can be received incorrectly, data can be lost or unwanted data can be generated. Any of these problems are called transmission errors.

Q.5. What is Error Correction and Detection?

Ans.: **Error detection and correction** has great practical importance in maintaining data (information) integrity across noisy channels and less-than-reliable storage media.

Error Correction : Send additional information so incorrect data can be corrected and accepted. Error correction is the additional ability to reconstruct the original, error-free data.

There are two basic ways to design the channel code and protocol for an error correcting system :

- **Automatic Repeat-Request (ARQ) :** The transmitter sends the data and also an error detection code, which the receiver uses to check for errors, and request retransmission of erroneous data. In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time.

- **Forward Error Correction (FEC) :** The transmitter encodes the data with an error-correcting code (ECC) and sends the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives into the "most likely" data. The codes are designed so that it would take an "unreasonable" amount of noise to trick the receiver into misinterpreting the data.

Error Detection : Send additional information so incorrect data can be detected and rejected. Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.

Error Detection Schemes : In telecommunication, a redundancy check is extra data added to a message for the purposes of error detection.

Several schemes exist to achieve error detection, and are generally quite simple. All error detection codes transmit more bits than were in the original data. Most codes are "systematic": the transmitter sends a fixed number of original data bits, followed by fixed number of check bits usually referred to as redundancy which are derived from the data bits by some deterministic algorithm. The receiver applies the same algorithm to the received data bits and compares its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a "non-systematic" code, such as some raptor codes, data bits are transformed into at least as many code bits, and the transmitter sends only the code bits.

Repetition Schemes : Variations on this theme exist. Given a stream of data that is to be sent, the data is broken up into blocks of bits, and in sending, each block is sent some predetermined number of times. For example, if we want to send "1011", we may repeat this block three times each.

Suppose we send "1011 1011 1011", and this is received as "1010 1011 1011". As one group is not the same as the other two, we can determine that an error has occurred. This scheme is not very efficient, and can be susceptible to problems if the error occurs in exactly the same place for each group e.g. "1010 1010 1010" in the example above will be detected as correct in this scheme.

The scheme however is extremely simple, and is in fact used in some transmissions of numbers stations.

Parity Schemes : A parity bit is an error detection mechanism . A *parity bit* is an extra bit transmitted with a data item, chose to give the resulting bits even or odd parity.

Parity refers to the number of bits set to 1 in the data item. There are 2 types of parity

- ***Even parity*** - an even number of bits are 1

  Even parity - data: 10010001, parity bit 1

- ***Odd parity*** - an odd number of bits are 1

  Odd parity - data: 10010111, parity bit 0

The stream of data is broken up into blocks of bits, and the number of 1 bits is counted. Then, a "parity bit" is set (or cleared) if the number of one bits is odd (or even).This scheme is called even parity; odd parity can also be used.

There is a limitation to parity schemes. A parity bit is only guaranteed to detect an odd number of bit errors (one, three, five, and so on). If an even number of bits (two, four, six and so on) are flipped, the parity bit appears to be correct, even though the data is corrupt.

For exapmle

- Original data and parity: 10010001+1 (even parity)
- Incorrect data: 10110011+1 (even parity!)

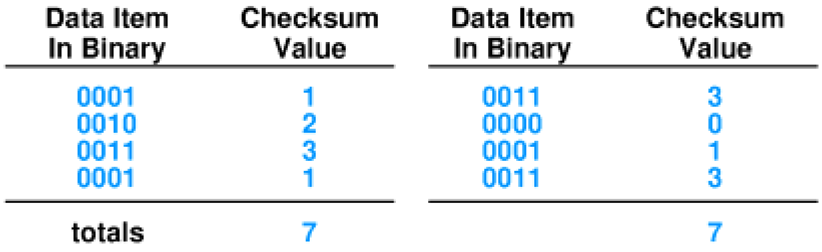
Parity usually used to catch one-bit errors

Checksum : A checksum of a message is an arithmetic sum of message code words of a certain word length, for example byte values, and their carry value. The sum is negated by means of ones-complement, and stored or transferred as an extra code word extending the message. On the receiver side, a new checksum may be calculated, from the extended message. If the new checksum is not 0, error is detected.Checksum schemes include parity bits, check digits, and longitudinal redundancy check.

Suppose we have a fairly long message, which can reasonably be divided into shorter words (a 128 byte message, for instance). We can introduce an accumulator with the same width as a word (one byte, for instance), and as each word comes in, add it to the accumulator. When the last word has been added, the contents of the accumulator are appended to the message (as a 129th byte, in this case). The added word is called a *checksum*.

Now, the receiver performs the same operation, and checks the checksum. If the checksums agree, we assume the message was sent without error.

Example for Checksum :



Data Item In Binary	Checksum Value	Data Item In Binary	Checksum Value
0001	1	0011	3
0010	2	0000	0
0011	3	0001	1
0001	1	0011	3
totals	7		7

Checksum Error Detection

Hamming Distance Based Checks : If we want to detect d bit errors in an n bit word we can map every n bit word into a bigger n+d+1 bit word so that the minimum Hamming distance between each valid mapping is d+1. This way, if one receives n+d+1 bit word that doesn't match any word in the mapping (with a Hamming distance x <= d+1 from any word in the mapping) it can successfully detect it as an errored word. Even more, d or fewer errors will never transform a valid word into another, because the Hamming distance between each valid word is at least d+1, and such errors only lead to invalid words that are detected correctly. Given a stream of m*n bits, we can detect x <= d bit errors successfully using the above method on every n bit word. In fact, we can detect a maximum of m*d errors if every n word is transmitted with maximum d errors.

The *Hamming distance* between two bit strings is the number of bits you have to change to convert one to the other. The basic idea of an error correcting code is to use extra bits to increase the dimensionality of the hypercube, and make sure the Hamming distance between any two valid points is greater than one.

- If the Hamming distance between valid strings is only one, a single-bit error results in another valid string. This means we can't detect an error.
- If it's two, then changing one bit results in an invalid string, and can be detected as an error. Unfortunately, changing just one more bit can result in another valid string, which means we can't detect which bit was wrong; so we can detect an error but not correct it.

- If the Hamming distance between valid strings is three, then changing one bit leaves us only one bit away from the original error, but two bits away from any other valid string. This means if we have a one-bit error, we can figure out which bit is the error; but if we have a two-bit error, it looks like one bit from the other direction. So we can have single bit correction, but that's all.
- Finally, if the Hamming distance is four, then we can correct a single-bit error and detect a double-bit error. This is frequently referred to as a SECDED (Single Error Correct, Double Error Detect) scheme.

Cyclic Redundancy Checks : For CRC following some of Peterson & Brown's notation here . . .

- ***k*** is the length of the message we want to send, *i.e.,* the number of information bits.
- ***n*** is the total length of the message we will end up sending the information bits followed by the check bits. Peterson and Brown call this a *code polynomial*.
- ***n-k*** is the number of check bits. It is also the degree of the generating polynomial. The basic (mathematical) idea is that we're going to pick the n-k check digits in such a way that the code polynomial is divisible by the generating polynomial. Then we send the data, and at the other end we look to see whether it's still divisible by the generating polynomial; if it's not then we know we have an error, if it is, we hope there was no error.

The way we calculate a CRC is we establish some predefined n-k+1 bit number P (called the Polynomial, for reasons relating to the fact that modulo-2 arithmetic is a special case of polynomial arithmetic). Now we append n-k 0's to our message, and divide the result by P using modulo-2 arithmetic. The remainder is called the Frame Check Sequence. Now we ship off the message with the remainder appended in place of the 0's. The receiver can either recompute the FCS or see if it gets the same answer, or it can just divide the whole message (including the FCS) by P and see if it gets a remainder of 0.

As an example, let's set a 5-bit polynomial of 11001, and compute the CRC of a 16 bit message :

```
---------------------------
11001)10011101010101100000
          11001
```

```
- - - - -
  1010101010101100000
  11001
  - - - - -
    110001010101100000
    11001
     - - - - -
       00011010101100000
       11001
       - - - - -
         0011101100000
         11001
         - - - - -
          100100000
          11001
          - - - - -
            10110000
            11001
            - - - - -
              1111000
              11001
                 - - - - -
                 11100
                 11001
                  - - - - -
                    0101
```

In division don‟t bother to keep track of the quotient; we don't care about the quotient. Our only goal here is to get the remainder (0101), which is the FCS.

CRC's can actually be computed in hardware using a shift register and some number of exclusive-or gates.

Q.6. Describe the MAC Layer Protocols?

Ans.: The Media Access Control (MAC) data communication protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the data link layer specified in the seven-layer OSI model. The medium access layer was made necessary by systems that share a common communications medium. Typically these are local area networks. In LAN nodes uses the same communication channel for transmission. The MAC sub-layer has two primary responsibilities:

- Data encapsulation, including frame assembly before transmission, and frame parsing/error detection during and after reception.
- Media access control, including initiation of frame transmission and recovery from transmission failure.

Following Protocols are used by Medium Access Layer :

- **ALOHA :** ALOHA is a system for coordinating and arbitrating access to a shared communication channel. It was developed in the 1970s at the University of Hawaii. The original system used terrestrial radio broadcasting, but the system has been implemented in satellite communication systems. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.
- **Carrier Sensed Multiple Access (CSMA) :** CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear. Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time. On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it. There are two methods for avoiding these so-called collisions, listed here :
    - **CSMA/CD (Carrier Sense Multiple Access/Collision Detection) :** CD (collision detection) defines what happens when two devices sense a clear channel, then attempt to transmit at the same time. A collision occurs, and both devices stop transmission, wait for a random amount of time, and then retransmit. This is the technique used to access the 802.3 Ethernet network channel. This method handles collisions as

they occur, but if the bus is constantly busy, collisions can occur so often that performance drops drastically. It is estimated that network traffic must be less than 40 percent of the bus capacity for the network to operate efficiently. If distances are long, time lags occur that may result in inappropriate carrier sensing, and hence collisions.

- **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) :** In CA collision avoidance), collisions are avoided because each node signals its intent to transmit before actually doing so. This method is not popular because it requires excessive overhead that reduces performance.

- **Ethernet : IEEE 802.3 Local Area Network (LAN) Protocols :** Ethernet protocols refer to the family of local-area network (LAN) covered by the IEEE 802.3. In the Ethernet standard, there are two modes of operation: half-duplex and full-duplex modes. In the half duplex mode, data are transmitted using the popular Carrier-Sense Multiple Access/Collision Detection (CSMA/CD) protocol on a shared medium. The main disadvantages of the half-duplex are the efficiency and distance limitation, in which the link distance is limited by the minimum MAC frame size. This restriction reduces the efficiency drastically for high-rate transmission. Therefore, the carrier extension technique is used to ensure the minimum frame size of 512 bytes in Gigabit Ethernet to achieve a reasonable link distance.

Four data rates are currently defined for operation over optical fiber and twisted-pair cables :

- 10 Mbps - 10Base-T Ethernet (IEEE 802.3)
- 100 Mbps - Fast Ethernet (IEEE 802.3u)
- 1000 Mbps - Gigabit Ethernet (IEEE 802.3z)
- 10-Gigabit - 10 Gbps Ethernet (IEEE 802.3ae).

The **Ethernet System** consists of three basic elements :

(1) The physical medium used to carry Ethernet signals between computers,

(2) a set of medium access control rules embedded in each Ethernet interface that allow multiple computers to fairly arbitrate access to the shared Ethernet channel, and

(3) an Ethernet frame that consists of a standardized set of bits used to carry data over the system.

As with all IEEE 802 protocols, the ISO data link layer is divided into two IEEE 802 sub-layers, the Media Access Control (MAC) sub-layer and the MAC-client sub-layer. The IEEE 802.3 physical layer corresponds to the ISO physical layer.

Each Ethernet-equipped computer operates independently of all other stations on the network: there is no central controller. All stations attached to an Ethernet are connected to a shared signaling system, also called the medium. To send data a station first listens to the channel, and when the channel is idle the station transmits its data in the form of an Ethernet frame, or packet.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface located in each station. The medium access control mechanism is based on a system called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

As each Ethernet frame is sent onto the shared signal channel, all Ethernet interfaces look at the destination address. If the destination address of the frame matches with the interface address, the frame will be read entirely and be delivered to the networking software running on that computer. All other network interfaces will stop reading the frame when they discover that the destination address does not match their own address.

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

The token and frames of data are passed from one station to another following the numeric sequence of the station addresses. Thus, the token follows a logical ring rather than a physical ring. The last station in numeric order passes the token back to the first station. The token does not follow the physical ordering of workstation attachment to the cable. Station 1 might be at one end of the cable and station 2 might be at the other, with station 3 in the middle.

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

- **IEEE 802.5 Token Ring :** Token ring is the IEEE 802.5 standard for a token-passing ring network with a star-configured physical topology. Internally, signals travel around the network from one station to the next in a ring. Physically, each station connects to a central hub called a MAU (multistation access unit). The MAU contains a "collapsed ring," but the physical configuration is a star topology. When a station is attached, the ring is extended out to the station and then back to the MAU . If a station goes offline, the ring is reestablished with a bypass at the station connector. Token ring was popular for an extended period in the late 1980s and 1990s, especially in IBM legacy system environments. IBM developed the technology and provided extensive support for connections to SNA systems. More recently, Ethernet, Fast Ethernet, and Gigabit Ethernet technologies have pushed token ring and other LAN technologies to the sidelines.

Q.7. Describe the different Transmission Media.

Ans.: The first layer (physical layer) of the OSI Seven layer model is dedicated to the transmission media. Due to the variety of transmission media and network wiring methods, selecting the most appropriate media can be confusing - what is the optimal cost-effective solution???

When choosing the transmission media, what are the factors to be considered?

- Transmission Rate
- Distances
- Cost and Ease of Installation
- Resistance to Environmental Conditions

There are two **types of transmission media :**

- Guided
- Unguided

Guided Media :

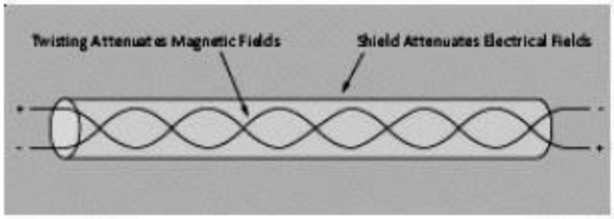
- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair
- Coaxial Cable
- Optical Fiber

Unshielded Twisted Pair (UTP) : UTP is the copper media, inherited from telephony, which is being used for increasingly higher data rates, and is rapidly becoming the de facto standard for horizontal wiring, the connection between, and including, the outlet and the termination in the communication closet. A **Twisted Pair** is a pair of copper wires, with diameters of 0.4-0.8 mm, twisted together and wrapped with a plastic coating. The twisting increases the electrical noise immunity, and reduces the bit error rate (BER) of the data transmission. A UTP cable contains from 2 to 4200 twisted pairs.

UTP is a very flexible, low cost media, and can be used for either voice or data communications. Its greatest disadvantage is the limited bandwidth, which restricts long distance transmission with low error rates.

Shielded Twisted Pair (STP) : STP is heavier and more difficult to manufacture, but it can greatly improve the signaling rate in a given transmission scheme Twisting provides cancellation of magnetically induced fields and currents on a pair of conductors. Magnetic fields arise around other heavy current-carrying conductors and around large electric motors. Various grades of copper cables are available, with Grade 5 being the best and most expensive.

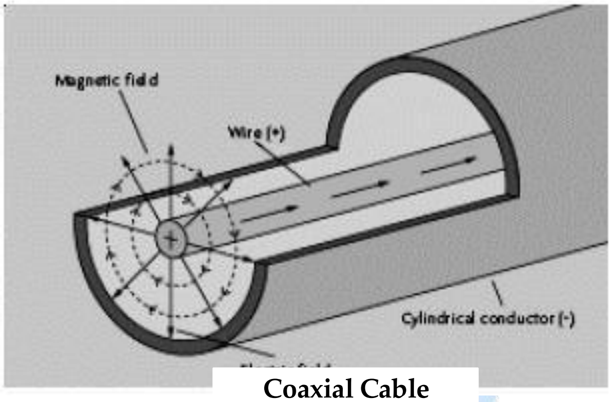
Grade 5 copper, appropriate for use in 100-Mbps applications, has more twists per inch than lower grades. More twists per inch means more linear feet of copper wire used to make up a cable run, and more copper means more money.


Twisting Attenuates Magnetic Fields
Shield Attenuates Electrical Fields
+
-
-
+

Shielded Twisted Pair

Shielding provides a means to reflect or absorb electric fields that are present around cables. Shielding comes in a variety of forms from copper braiding or copper meshes to aluminized.

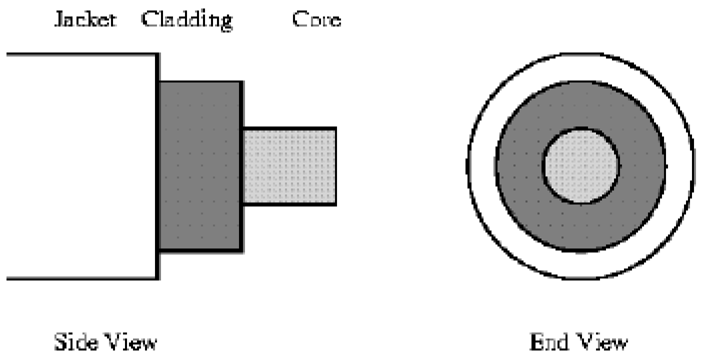
Mylar tape wrapped around each conductor and again around the twisted pair.



Coaxial Cable

Coaxial Cable : Coaxial cable is a two-conductor cable in which one conductor forms an electromagnetic shield around the other. The two conductors are separated by insulation. It is a constant impedance transmission cable. This media is used in base band and broadband transmission. Coaxial cables do not produce external electric and magnetic fields and are not affected by them. This makes them ideally suited, although more expensive, for transmitting signals.

Optical Fiber : Optical fiber consists of thin glass fibers that can carry information at frequencies in the visible light spectrum and beyond. The typical optical fiber consists of a very narrow strand of glass called the core. Around the core is a concentric layer of glass called the cladding. A typical core diameter is 62.5 microns .Typically cladding has a diameter of 125 microns. Coating the cladding is a protective coating consisting of plastic, it is called the Jacket. An important characteristic of fiber optics is refraction. Refraction is the characteristic of a material to either pass or reflect light. When light passes through a medium, it “bends” as it passes from one medium to the other. An example of this is when we look into a pond of water If the angle of incidence is small, the light rays are reflected and do not pass into the water. If the angle of incident is great, light passes through the media but is bent or refracted. Optical fibers work on the principle that the core refracts the light and the cladding reflects the light. The core refracts the light and guides the light along its path. The cladding reflects any light back into the core and stops light from escaping through it - it bounds the medium!



Optical Fiber

Unguided Media : Transmission media then looking at analysis of using them unguided transmission media is data signals that flow through the air. They are not guided or bound to a channel to follow.

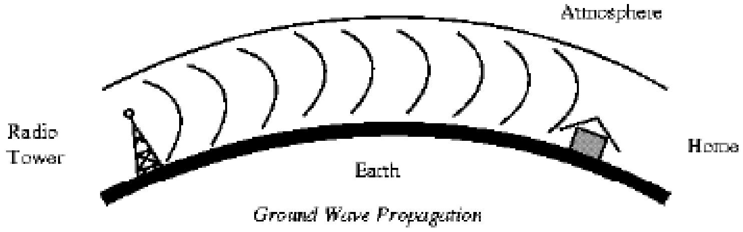
Following are unguided media used for data communication :

- Radio Transmission
- Microwave
- Satellite Communication

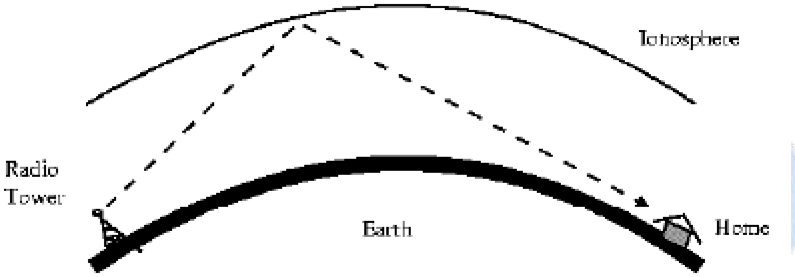
. **RF Propagation :** There are three types of RF (radio frequency) propagation :

- Ground Wave
- Ionospheric
- Line of Sight (LOS)

Ground wave propagation follows the curvature of the Earth. Ground waves have carrier frequencies up to 2 MHz. AM radio is an example of ground wave propagation.

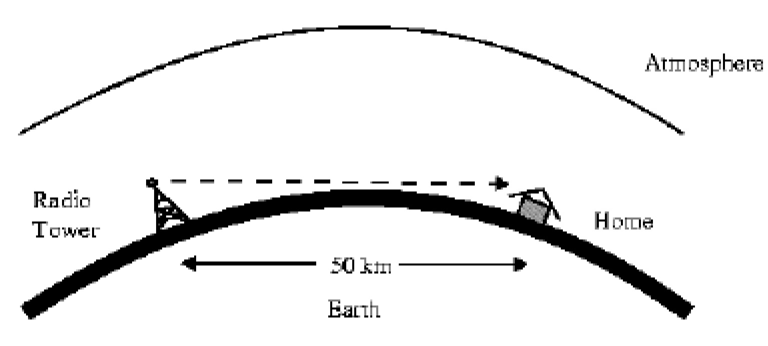


Ionospheric propagation bounces off of the Earth‟s ionospheric layer in the upper atmosphere. It is sometimes called double hop propagation. It operates in the frequency range of 30 - 85 MHz. Because it depends on the Earth‟s ionosphere, it changes with the weather and time of day. The signal bounces off of the ionosphere and back to earth. Ham radios operate in this range.



Ionospheric propagation

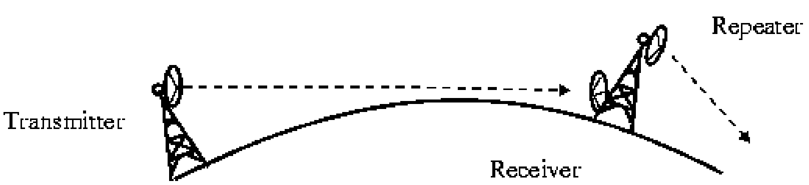
Line of sight propagation transmits exactly in the line of sight. The receive station must be in the view of the transmit station. It is sometimes called space waves or tropospheric propagation. It is limited by the curvature of the Earth for ground-based stations (100 km, from horizon to horizon). Reflected waves can cause problems. Examples of line of sight propagation are: FM radio, microwave and satellite.



Line of sight

Radio Frequencies : The frequency spectrum operates from 0 Hz (DC) to gamma rays (1019 Hz). Radio frequencies are in the range of 300 kHz to 10 GHz. We are seeing an emerging technology called wireless LANs. Some use radio frequencies to connect the workstations together, some use infrared technology.

Microwave : Microwave transmission is line of sight transmission. The transmit station must be in visible contact with the receive station. This sets a limit on the distance between stations depending on the local geography. Typically the line of sight due to the Earth‟s curvature is only 50 km to the horizon! Repeater stations must be placed so the data signal can hop, skip and jump across the country.



Microwave Transmission

Microwaves operate at high operating frequencies of 3 to 10 GHz. This allows them to carry large quantities of data due to their large bandwidth.

Advantages :

(a) They require no right of way acquisition between towers.

(b) They can carry high quantities of information due to their high operating frequencies.

(c) Low cost land purchase: each tower occupies only a small area.

(d) High frequency/short wavelength signals require small antennae.

Disadvantages :

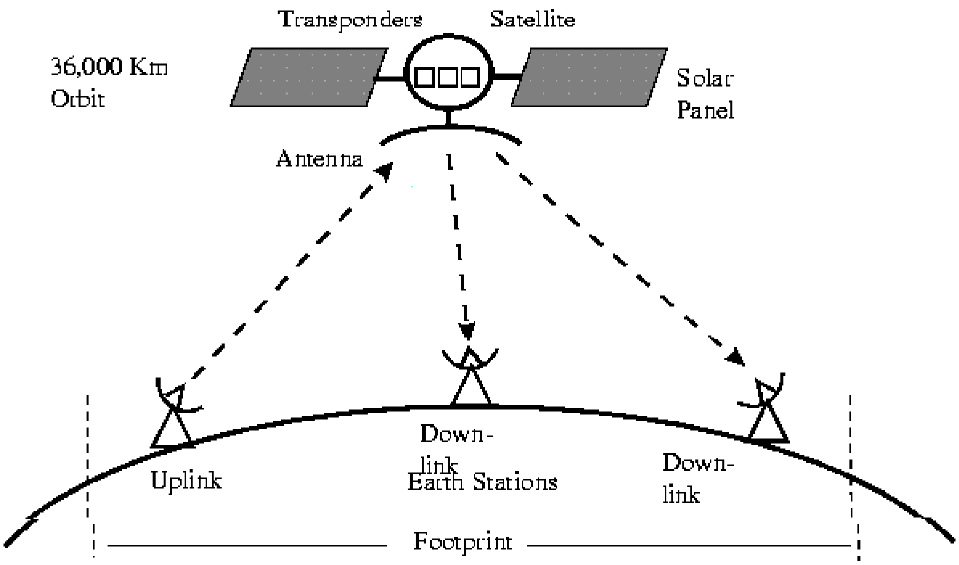
(a) Attenuation by solid objects: birds, rain, snow and fog.

(b) Reflected from flat surfaces like water and metal.

(c) Diffracted (split) around solid objects.

(d) Reflected by atmosphere, thus causing beam to be projected away from receiver.

Satellite : Satellites are transponders (units that receive on one frequency and retransmit on another) that are set in geostationary orbits directly over the equator. These geostationary orbits are 36,000 km from the Earth‟s surface. At this point, the gravitational pull of the Earth and the centrifugal force of Earth‟s rotation are balanced and cancel each other out. Centrifugal force is the rotational f0000000orce placed on the satellite that wants to fling it out into space.



The uplink is the transmitter of data to the satellite. The downlink is the receiver of data. Uplinks and downlinks are also called Earth stations because they are located on the Earth. The footprint is the "shadow" that the satellite can transmit to, the shadow being the area that can receive the satellite‟s transmitted signal.

Q.8. What are the different Transmission Modes?

Ans.: In communications, the transmission of a unit of data from one node to another node takes place. It is responsible for ensuring that the bits received are the same as the bits sent. Following are the major categories of transmission :

Asynchronous Transmission : Originating from mechanical teletype machines, asynchronous transmission treats each character as a unit with start and stop bits appended to it. It is the common form of transmission between the serial port of a computer or terminal and a modem. ASCII, or teletype, protocols provide little or no error checking. File transfer protocols, provide data link services and higher-level services, collectively known as transport services.

Synchronous Transmission : Developed for mainframe networks using higher speeds than teletype terminals, synchronous transmission sends contiguous blocks of data, with both sending and receiving stations synchronized to each other. Synchronous protocols include error checking.

Q.9. Which are the sub-layers in Data Link layer?

Ans.: In LAN data link layer is divided in the 2 layers :

- Logical Lick Control Sub-layer
- Medium Access Layer

Logical Link Control Sublayer : The uppermost sublayer is Logical Link Control (LLC). This sublayer multiplexes protocols running atop the data link layer, and optionally provides flow control, acknowledgment, and error recovery. The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

Media Access Control Sublayer : The sublayer below it is Media Access Control (MAC). Sometimes this refers to the sublayer that determines who is allowed to access the media at any one time. Other times it refers to a frame structure with MAC addresses inside. There are generally two forms of media access control: distributed and centralized. Both of these may be compared to communication between people:

The Media Access Control sublayer also determines where one frame of data ends and the next one starts. There are four means of doing that: a time based, character counting, byte stuffing and bit stuffing.

□ □ □

Chapter-3

Introduction to TCP/IP

Q.1. What is TCP/IP Protocol Suit? Describe all layers of TCP/IP.

Ans.: The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide. Its simplicity and power has led to its becoming the single network protocol of choice in the world today.

TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network. It was developed by a community of researchers centered around the ARPAnet. Certainly the ARPAnet is the best-known TCP/IP network.

The most accurate name for the set of protocols is the "Internet protocol suite". TCP and IP are two of the protocols in this suite. The Internet is a collection of networks. Term "Internet" applies to this entire set of networks.

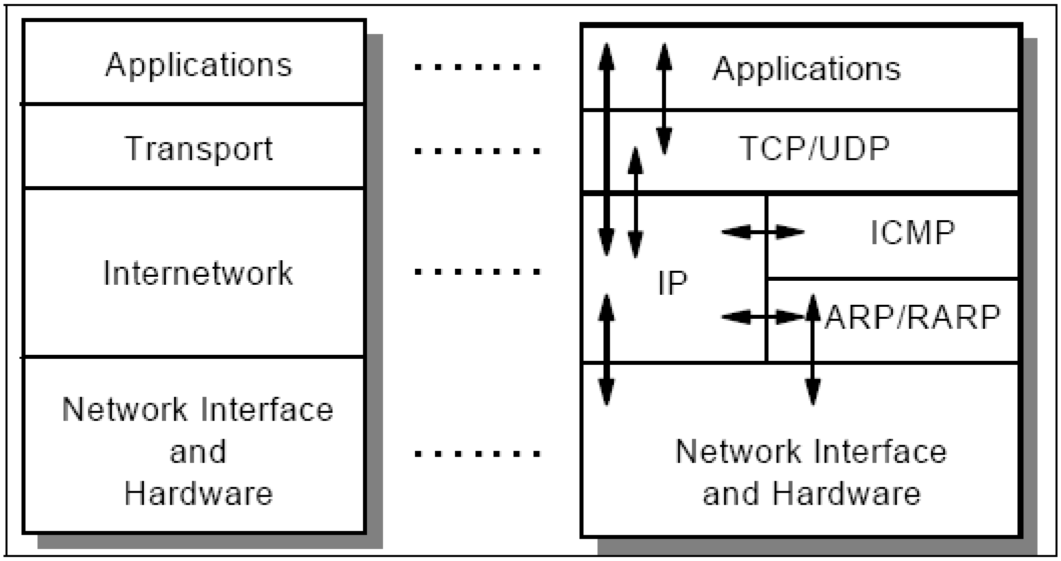
Like most networking software, TCP/IP is modeled in layers. This layered representation leads to the term protocol stack, which refers to the stack of layers in the protocol suite. It can be used for positioning the TCP/IP protocol suite against others network software like Open System Interconnection (OSI) model.

By dividing the communication software into layers, the protocol stack allows for division of labor, ease of implementation and code testing, and the ability to develop alternative layer implementations. Layers communicate with those above and below via concise interfaces. In this regard, a layer provides a service for the layer directly above it and makes use of services provided by the layer directly below it. For example, the IP layer provides the ability to transfer data from one host to another without any guarantee to reliable delivery or duplicate suppression.

TCP/IP is a family of protocols. A few provide "low- level" functions needed for many applications. These include IP, TCP, and UDP. Others are protocols for doing specific tasks, e.g. transferring files between computers, sending mail, or finding out who is logged in on another computer. Initially TCP/IP was used mostly between minicomputers or mainframes. These machines had their own disks, and generally were self- contained.

Application Layer : The application layer is provided by the program that uses TCP/IP for communication. An application is a user process cooperating with another process usually on a different host (there is also a benefit to application communication within a single host). Examples of applications include Telnet and the File Transfer Protocol (FTP).

Transport Layer : The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer. Multiple applications can be supported simultaneously. The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides connection-oriented reliable data delivery, duplicate data suppression, congestion control, and flow control.



The TCP/IP Protocol Suit

Another transport layer protocol is the User Datagram Protocol It provides connectionless, unreliable, best-effort service. As a result, applications using

UDP as the transport protocol have to provide their own end-to-end integrity, flow control, and congestion control, if desired. Usually, UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

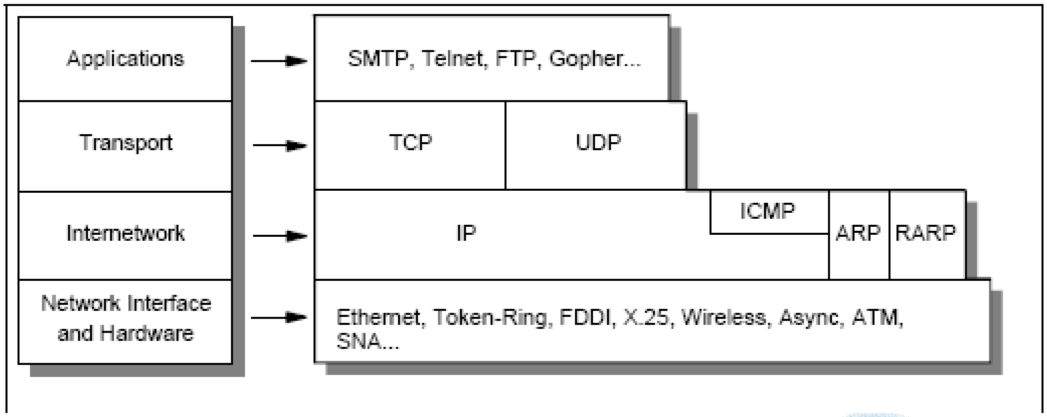
Internetwork Layer : The internetwork layer, also called the **internet layer or the network layer**, provides the "virtual network" image of an internet this layer shields the higher

levels from the physical network architecture below it. Internet Protocol (IP) is the most important protocol in this layer. It is a connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control, or error

recovery. These functions must be provided at a higher level. IP provides a routing function that attempts to deliver transmitted messages to their destination. A message unit in an IP network is called an **IP datagram**. This is the basic unit of information transmitted across TCP/IP networks. Other internetwork-layer protocols are IP, ICMP, IGMP, ARP, and RARP.

Network Interface Layer : The network interface layer, also called **the link layer or the data-link layer**, is the interface to the actual network hardware. This interface may or may not provide reliable delivery, and may be packet or stream oriented. In fact, TCP/IP does not specify any protocol here, but can use almost any network interface available, which illustrates the flexibility of the IP layer. Examples are IEEE 802.2, X.25, ATM, FDDI, and even SNA.TCP/IP specifications do not describe or standardize any network-layer protocols, they only standardize ways of accessing those protocols from the internet work layer.

The following figure shows the TCP/IP protocol suit with their Protocol.


Applications
SMTP, Telnet, FTP, Gopher...
Transport
TCP
UDP
Internetwork
IP
ICMP
ARP
RARP
Network Interface and Hardware
Ethernet, Token-Ring, FDDI, X.25, Wireless, Async, ATM, SNA...

Detail TCP/IP Protocol

Q.2. Write short note on -

A) TCP

B) IP

C) FTP

D) TELNET

E) DNS

F) DHCP

G) BOOTS

Ans.: A) TCP : TCP is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

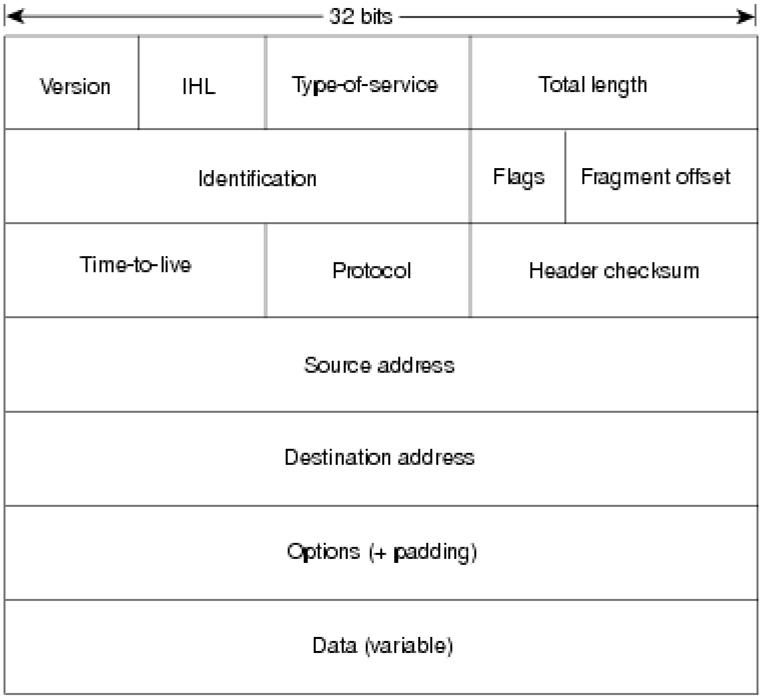
The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite. TCP provides reliable, in-order delivery of a stream of bytes, making it suitable for applications like file transfer and e-mail. It is so important in the Internet protocol suite that sometimes the entire suite is referred to as "TCP/IP." TCP manages a large fraction of the individual conversations between Internet hosts, for example between web servers and web clients. It is also responsible for controlling the size and rate at which messages are exchanged between the server and the client.

TCP consists of a set of rules, the protocol, that are used with the Internet Protocol, the IP, to send data “in a form of message units” between computers over the Internet. At the same time that the IP takes care of handling the actual delivery of the data, the TCP takes care of keeping track of the individual units of data “packets” that a message is divided into for efficient routing through the net. For example, when an HTML file is sent to you from a web server, the TCP program layer of that server takes the file as a stream of bytes and divides it into packets, numbers the packets, and then forwards them individually to the IP program layer. Even though every packet has the same destination IP address, they can get routed differently through the network. When the client program in your computer gets them, the TCP stack (implementation) reassembles the individual packets and ensures they are correctly ordered as it streams them to an application.

TCP is used extensively by many of the Internet's most popular application protocols and resulting applications, including the World Wide Web, E-mail, File Transfer Protocol, Secure Shell, and some streaming media applications.

B) **Internet Protocol (IP) :** The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.

IP Packet Format : An IP packet contains several types of information, as illustrated in following figure :



<table>
<tr><td colspan="5">32 bits</td></tr>
<tr><td>Version</td><td>IHL</td><td>Type-of-service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time-to-live</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Options (+ padding)</td></tr>
<tr><td colspan="5">Data (variable)</td></tr>
</table>

IP Packet Format

The following discussion describes the IP packet fields illustrated in :

- *Version*—Indicates the version of IP currently used.
- *IP Header Length* **(IHL)**—Indicates the datagram header length in 32-bit words.
- *Type-of-Service*—Specifies how an upper-layer protocol would like a current datagram to be handled, and assigns datagrams various levels of importance.
- *Total Length*—Specifies the length, in bytes, of the entire IP packet, including the data and header.
- *Identification*—Contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.
- *Flags*—Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit

specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.

- *Fragment Offset*—Indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.
- *Time-to-Live*—Maintains a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.
- *Protocol*—Indicates which upper-layer protocol receives incoming packets after IP processing is complete.
- *Header Checksum*—Helps ensure IP header integrity.
- *Source Address*—Specifies the sending node.
- *Destination Address*—Specifies the receiving node.
- *Options*—Allows IP to support various options, such as security.
- *Data*—Contains upper-layer information.

IP Addressing : As with any other network-layer protocol, the IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetworks.

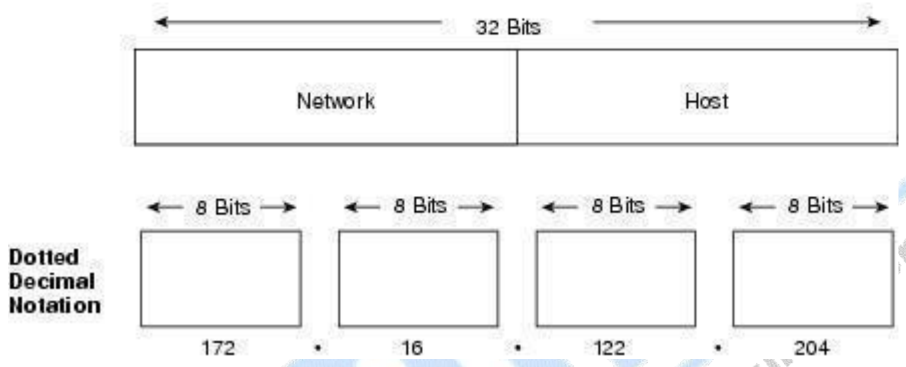
Each host on a TCP/IP network is assigned a unique 32-bit logical address that is divided into two main parts :

- The network number
- The host number

The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet. An Internet Service Provider (ISP) can obtain blocks of network addresses from the InterNIC and can itself assign address space as necessary. The host number identifies a host on a network and is assigned by the local network administrator.

IP Address Format : The 32-bit IP address is grouped eight bits at a time, separated by dots, and represented in decimal format (known as *dotted decimal notation*). Each bit in the octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1). The minimum value for an octet is 0, and the maximum value for an octet is 255. illustrates the basic format of an IP address.

Following figure shows an IP address consists of 32 bits, grouped into four octets.



IP address

IP Address Classes : IP addressing supports five different address classes: A, B, C, D, and E. only classes A, B, and C are available for commercial use. The left-most (high-order) bits indicate the network class. It provides reference information about the five IP address classes.

Reference Information about the Five IP Address Classes :

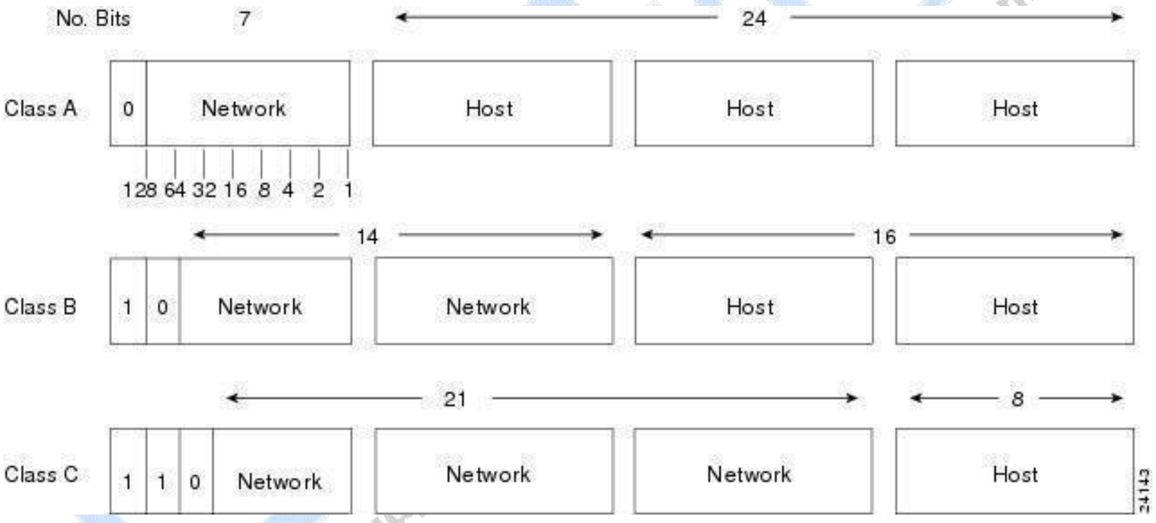
IP Address Class	Format	Purpose	High-Order Bit(s)	Address Range	No. Bits Network/ Host	Max. Hosts
A	N.H.H.H	Few large organizations	0	1.0.0.0 to 126.0.0.0	7/24	16777214 $(2^{24}- 2)$
B	N.N.H.H	Medium-size organizations	1, 0	128.1.0.0 to 191.254.0.0	14/16	65534 $(2^{16}- 2)$
C	N.N.N.H	Relatively small organizations	1, 1, 0	192.0.1.0 to 223.255.254.0	21/8	254 $(2^{8}- 2)$
D	N/A	Multicast	1, 1, 1, 0	224.0.0.0 to	N/A (not for	N/A

		groups (RFC 1112)		239.255.255.255	commercial use)	
IP Address Class	**Format**	**Purpose**	**High-Order Bit(s)**	**Address Range**	**No. Bits Network/ Host**	**Max. Hosts**
E	N/A	Experimental	1, 1, 1, 1	240.0.0.0 to 254.255.255.255	N/A	N/A

N = Network number, H = Host number.

One address is reserved for the broadcast address, and one address is reserved for the network.

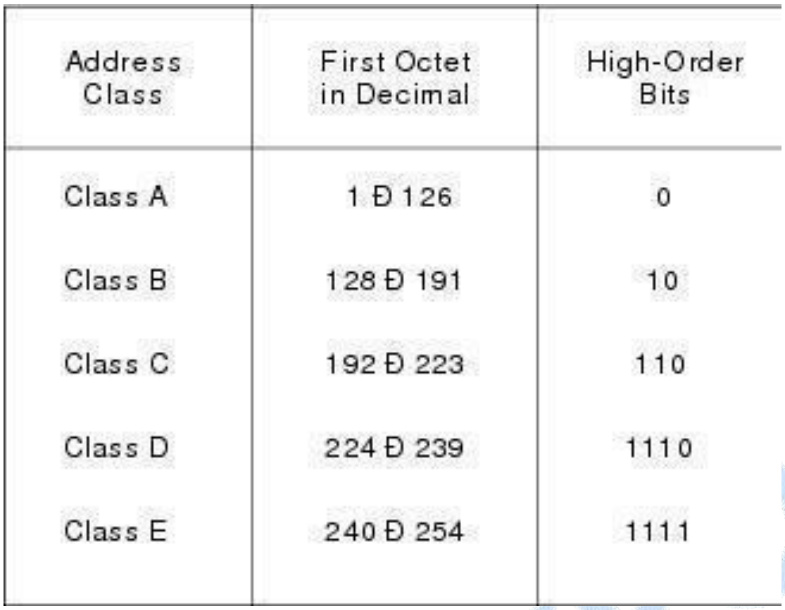
Following figure shows IP address formats A, B, and C are available for commercial use.



IP Address Formats A, B, and C

The class of address can be determined easily by examining the first octet of the address and mapping that value to a class range in the following table. In an IP address of 172.31.1.2, for example, the first octet is 172. Because 172 fall between 128 and 191, 172.31.1.2 is a Class B address.

Following table describe a range of possible values exists for the first octet of each address class.



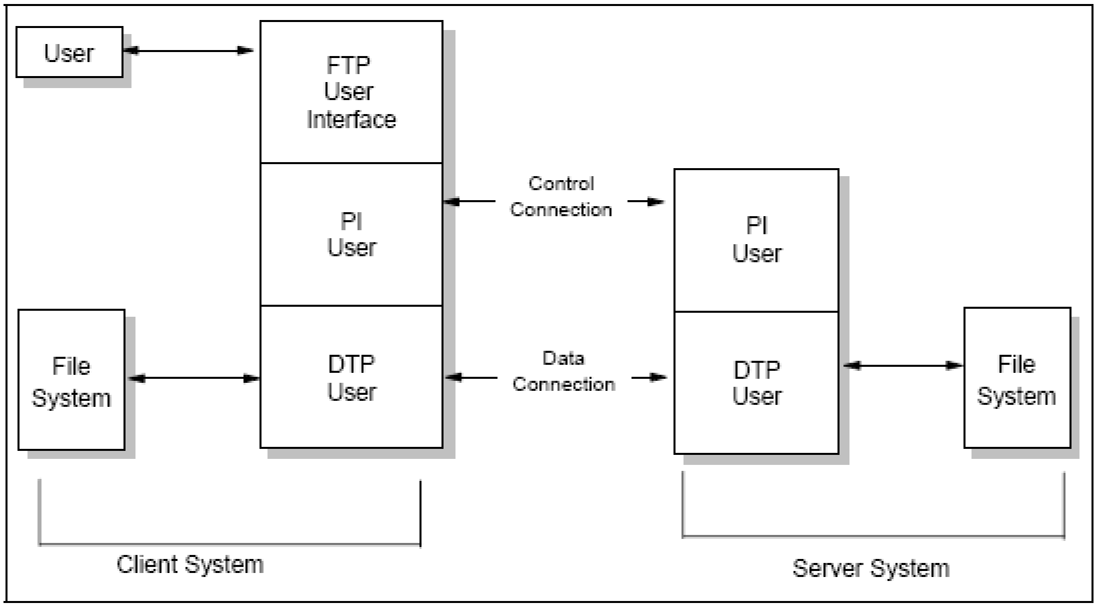
Address Class	First Octet in Decimal	High-Order Bits
Class A	1 Ð 126	0
Class B	128 Ð 191	10
Class C	192 Ð 223	110
Class D	224 Ð 239	1110
Class E	240 Ð 254	1111

C) **File Transfer Protocol (FTP) :** Transferring data from one host to another is one of the most frequently used operations. Both the need to upload data: transfer data from a client to a server and download data: retrieve data from a server to a client, are addressed by FTP. Additionally, FTP provides security and authentication measures to prevent unauthorized access to data.

It allows a user on any computer to get files from another computer, or to send files to another computer. Security is handled by requiring the user to specify a user name and password for the other computer. Provisions are made for handling file transfer between machines with different character set, end of line conventions, etc. This is not quite the same thing as more recent "network file system" or "netbios" protocols. Rather, FTP is a utility that you run any time you want to access a file on another system. You use it to copy the file to your own system. You then work with the local copy.

FTP uses TCP as transport protocol to provide reliable end-to-end connections and implements two types of connections in managing data transfers. The FTP client initiates the first connection, referred to as the control connection. It is on this port that an FTP server listens for and accepts new connections. The control connection is used for all of the control commands a client user uses to log on to the server, manipulate files, and terminate a session. This is also the connection across which the FTP server will send messages to the client in response to these control commands. The second connection used by FTP is referred to as the data connection. It is across this connection that FTP transfers the data. FTP only opens a data connection when a client issues a command requiring a data transfer, such as a request to retrieve a file, or to view a list of the files available. Therefore, it is possible for an entire FTP session to open and close without a data connection ever having been opened. Unlike the control connection, in which commands and replies can flow both from the client to the server and from the server to the client, the data connection is unidirectional. FTP can transfer data only from the client to the server, or from the server to the client, but not both. Also, unlike the control connection, the data connection can be initiated from either the client or the server. Data connections initiated by the server are active, while those initiated by the client are passive.

The client FTP application is built with a protocol interpreter (PI), a data transfer process (DTP), and a user interface. The server FTP application typically only consists of a PI and DTP.



The FTP Model

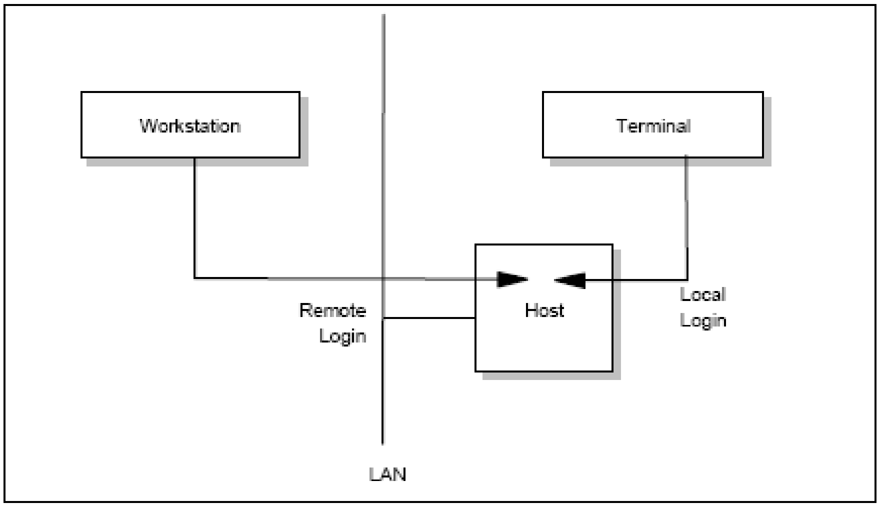
D) **TELNET : TELNET** (**TEL**ecommunication **NET**work) is a network protocol used on the Internet or local area network (LAN) connections. It was developed in 1969 beginning with RFC 15 and standardized as IETF STD 8, one of the first Internet standards.

The network terminal protocol (TELNET) allows a user to log in on any other computer on the network. We can start a remote session by specifying a computer to connect to. From that time until we finish the session, anything we type is sent to the other computer.

The Telnet program runs on the computer and connects your PC to a server on the network. We can then enter commands through the Telnet program and they will be executed as if we were entering them directly on the server console. This enables we to control the server and communicate with other servers on the network. To start a Telnet session, we must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

The term **telnet** also refers to software which implements the client part of the protocol. TELNET clients have been available on most Unix systems for many years and are available virtually for all platforms. Most network equipment and OSs with a TCP/IP stack support some kind of TELNET service server for their remote configuration including ones based on Windows NT.

TELNET is a client-server protocol, based on a reliable connection-oriented transport. Typically this protocol used to establish a connection to TCP port 23, where a getty-equivalent program (telnetd) is listening, although TELNET predates.



The TELNET Model

TELNET is generally used with the following applications :

(1) Enterprise networks to access host applications, e.g. on IBM Mainframes.

(2) Administration of network elements, e.g., in commissioning, integration and maintenance of core network elements in mobile communication networks.

(3) MUD games played over the Internet, as well as talkers, MUSHes, MUCKs, MOOes, and the resurgent BBS community.

(4) embedded systems.

E) **Domain Name System (DNS) :** The **Domain Name System** (DNS) associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g**. www.example.com**, into IP addresses, e.g. *208.77.188.166*, which networking equipment needs to deliver information.

It also stores other information such as the list of mail servers that accept email for a given domain. In providing a worldwide keyword-based redirection service, the Domain Name System is an essential component of contemporary Internet use.

DNS makes it possible to assign Internet names to organizations independent of the physical routing hierarchy represented by the numerical IP address. Because of this, hyperlinks and Internet contact information can remain the same, whatever the current IP routing arrangements may be, and can take a human-readable form, which is easier to remember than the IP address 208.77.188.166. The Domain Name System distributes the responsibility for assigning domain names and mapping them to IP networks by allowing an authoritative name server for each domain to keep track of its own changes, avoiding the need for a central register to be continually consulted and updated.

At the request of Jon Postel, Paul Mockapetris invented the Domain Name system in 1983 and wrote the first implementation. The original specifications appear in RFC 882 and RFC 883. In November 1987, the publication of RFC 1034 and RFC 1035 updated the DNS specification and made RFC 882 and RFC 883 obsolete. Several more-recent RFCs have proposed various extensions to the core DNS protocols.

The Domain Name System consists of a hierarchical set of DNS servers. Each domain or subdomain has one or more authoritative DNS servers that publish information about that domain and the name servers of any domains "beneath" it. The hierarchy of authoritative DNS servers matches the hierarchy of domains. At the top of the hierarchy stand the root nameservers: the servers to query when looking up a top-level domain name.

Domain names, arranged in a tree, cut into zones, each served by a nameserver.

A domain name usually consists of two or more parts which is conventionally written separated by dots, such as example.com.The rightmost label conveys the top-level domain for example, the address www.example.com has the top-level domain com.Each label to the left specifies a subdomain of the domain above it. For example: example.com comprises a subdomain of the com domain, and www.example.com comprises a subdomain of the domain example.com. In theory, this subdivision can go down 127 levels. Each label can contain up to 63 characters. The whole domain name does not exceed a total length of 253 characters

A hostname refers to a domain name that has one or more associated IP addresses; ie: the 'www.example.com' and 'example.com' domains are both hostnames, however, the 'com' domain is not.

F) **Dynamic Host Configuration Protocol (DHCP) : Dynamic Host Configuration Protocol (DHCP)** is a protocol used by networked devices or clients to obtain the parameters necessary for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configurations.

Dynamic Host Configuration Protocol is a way to administrator network parameter assignment from a single DHCP server, or a group of DHCP servers arranged in a fault-tolerant manner. Even in small networks, Dynamic Host Configuration Protocol is useful because it can make it easy to add new machines to the local network.

DHCP is also recommended even in the case of servers whose addresses rarely change, so that if a server needs to be readdressed, changes can be made in as few places as possible. DHCP can be used to directly assign addresses to servers and desktop machines, and, through a Point-to-Point Protocol (PPP) proxy, to dialup and broadband on-demand hosts, as well as for residential Network address translation (NAT) gateways and routers. DHCP is generally not appropriate for infrastructure such as non-edge routers and DNS servers.

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the BOOTP protocol, adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP consists of two components :

- A protocol that delivers host-specific configuration parameters from a DHCP server to a host
- A mechanism for the allocation of temporary or permanent network addresses to hosts

IP requires the setting of many parameters within the protocol implementation software. Because IP can be used on many dissimilar kinds of network hardware, values for those parameters cannot be guessed at or assumed to have correct defaults. The use of a distributed address allocation scheme based on a polling/defense mechanism, for discovery of network addresses already in use, cannot guarantee unique network addresses because hosts might not always be able to defend their network addresses.

DHCP supports three mechanisms for IP address allocation :

- **Automatic Allocation** : DHCP assigns a permanent IP address to the host.
- **Dynamic Allocation** : DHCP assigns an IP address for a limited period of time. Such a network address is called a lease. This is the only mechanism that allows automatic reuse of addresses that are no longer needed by the host to which it was assigned.

- **Manual Allocation** : The host's address is assigned by a network administrator.

Wherever possible, DHCP-assigned addresses should be dynamically linked to a secure DNS server, to allow troubleshooting by name rather than by a potentially unknown address. Effective DHCP-DNS linkage requires having a file of either MAC addresses or local names that will be sent to DNS that uniquely identifies physical hosts, IP addresses, and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server ensures that all IP addresses are unique, i.e., no IP address is assigned to a second client while the first client's assignment is valid.

G) **Bootstrap Protocol (BOOTP) :** The Bootstrap Protocol (BOOTP) enables a client workstation to initialize with a minimal IP stack and request its IP address, a gateway address, and the address of a name server from a BOOTP server. If BOOTP is to be used in your network, the server and client are usually on the same physical LAN segment. BOOTP can only be used across bridged segments when source-routing bridges are being used, or across subnets, if you have a router capable of BOOTP forwarding.

BOOTP is a draft standard protocol. Its status is recommended. There are also updates to BOOTP, some relating to interoperability with DHCP .BOOTP are draft standards with a status of elective and recommended, respectively. The BOOTP protocol was originally developed as a mechanism to enable diskless hosts to be remotely booted over a network as workstations, routers, terminal concentrators, and so on. It allows a minimum IP protocol stack with no configuration information to obtain enough information to begin the process of downloading the necessary boot code. BOOTP does not define how the downloading is done, but this process typically uses TFTP “Trivial File Transfer Protocol (TFTP)”. Although still widely used for this purpose by diskless hosts, BOOTP is also commonly used solely as a mechanism to deliver configuration information to a client that has not been manually configured.

The BOOTP process involves the following steps :

Terminology

1. Node

- **Definition**: Any device that is connected to a network, such as a computer, printer, or router.

2. IP Address

- **Definition**: A unique numerical label assigned to each device connected to a network. It identifies the device's location on the network.
- **Types**: IPv4 (e.g., 192.168.1.1) and IPv6 (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

3. Router

- **Definition**: A device that forwards data packets between computer networks. Routers determine the best path for data to travel across the network.

4. Switch

- **Definition**: A device that connects devices within a single network segment and uses MAC addresses to forward data to the correct destination.

5. Subnet

- **Definition**: A smaller network within a larger network. Subnetting is the practice of dividing a network into multiple sub-networks to optimize performance and security.

6. Protocol

- **Definition**: A set of rules that govern how data is transmitted over a network. Examples include TCP/IP, HTTP, FTP, and DNS.

7. Bandwidth

- **Definition**: The maximum amount of data that can be transferred over a network in a given period of time, typically measured in bits per second (bps).

8. Latency

- **Definition**: The delay before a transfer of data begins following an instruction for its transfer. It's the time it takes for data to travel from the source to the destination.

9. Packet

- **Definition**: A small chunk of data transmitted over a network. Large pieces of data are broken down into packets to improve the efficiency of transmission.

10. MAC Address (Media Access Control Address)

- **Definition**: A unique identifier assigned to network interfaces for communications on the physical network segment. It operates at the Data Link Layer (Layer 2) of the OSI model.

11. OSI Model (Open Systems Interconnection Model)

- **Definition**: A conceptual framework used to understand network interactions in seven layers, from physical transmission to application. The layers are:
  1. Physical
  2. Data Link
  3. Network
  4. Transport
  5. Session
  6. Presentation
  7. Application

12. TCP/IP (Transmission Control Protocol/Internet Protocol)

- **Definition**: A set of protocols that governs how data is transmitted over the internet. It breaks down data into packets, sends them, and ensures they are correctly reassembled.

13. DNS (Domain Name System)

- **Definition**: A system that translates human-readable domain names (e.g., www.example.com) into IP addresses.

14. Firewall

- **Definition**: A security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

15. VPN (Virtual Private Network)

- **Definition**: A service that encrypts your internet traffic and routes it through a remote server, enhancing security and privacy while using the internet.

16. DHCP (Dynamic Host Configuration Protocol)

- **Definition**: A protocol that automatically assigns IP addresses to devices on a network, eliminating the need for manual IP address configuration.

17. Gateway

- **Definition**: A device that connects different networks, often with different communication protocols, allowing them to communicate with each other.

18. HTTP/HTTPS (Hypertext Transfer Protocol / Secure)

- **Definition**: Protocols used for transferring web pages on the internet. HTTPS is the secure version, using encryption for security.

19. LAN (Local Area Network)

- **Definition**: A network of computers and devices that are connected within a limited geographic area, such as an office or home.

20. WAN (Wide Area Network)

- **Definition**: A network that covers a large geographic area, such as a country or even the entire world. The internet is the largest example of a WAN.

21. VPN (Virtual Private Network)

- **Definition**: A network that extends a private network across a public network, allowing secure communication over unsecured networks.

22. Topology

- **Definition**: The arrangement of different elements (links, nodes, etc.) in a computer network. Common types include star, bus, ring, and mesh.

23. Throughput

- **Definition**: The actual amount of data transmitted successfully over a network in a given period of time. It is often measured in bits per second (bps).

24. NAT (Network Address Translation)

- **Definition**: A method used by routers to translate private IP addresses in a local network to a public IP address for internet communication.

25. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

- **Definition**: Cryptographic protocols designed to provide secure communication over a computer network, commonly used in HTTPS.

26. Access Point

- **Definition**: A device that allows wireless devices to connect to a wired network using Wi-Fi or related standards.

27. Port

- **Definition**: A communication endpoint used by applications for network connections. Ports are identified by numbers (e.g., port 80 for HTTP).

28. Load Balancer

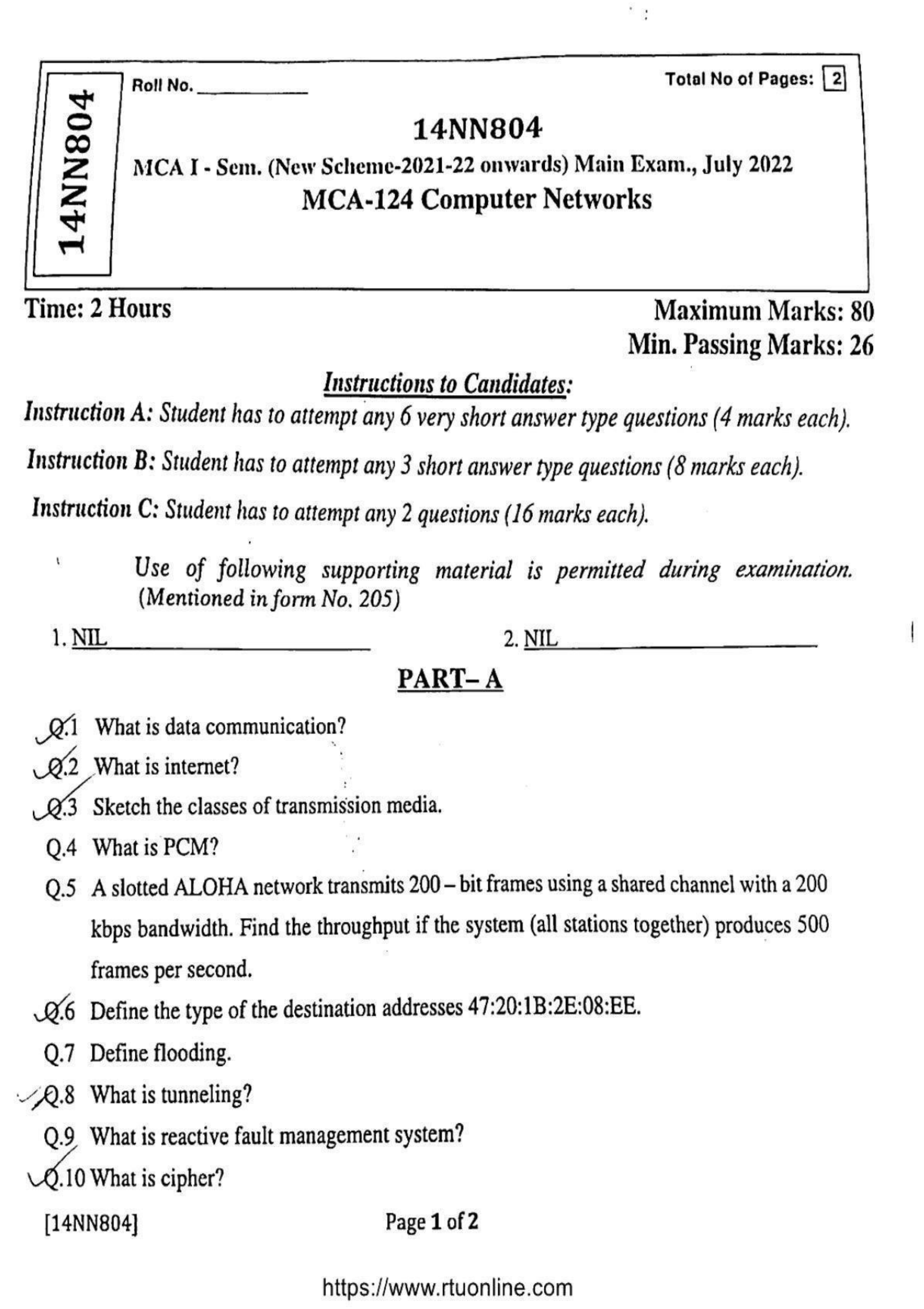
- **Definition**: A device or software that distributes incoming network traffic across multiple servers to ensure no single server is overwhelmed.

29. MTU (Maximum Transmission Unit)

- **Definition**: The largest size of a packet that can be sent in a single network transaction.

30. QoS (Quality of Service)

- **Definition**: A set of technologies that manage traffic to ensure performance, reliability, and availability, often by prioritizing certain types of traffic (e.g., VoIP or video streaming).



14NN804

Roll No. ____________

Total No of Pages: 2

14NN804

MCA I - Sem. (New Scheme-2021-22 onwards) Main Exam., July 2022

MCA-124 Computer Networks

Time: 2 Hours

Maximum Marks: 80

Min. Passing Marks: 26

Instructions to Candidates:

Instruction A: Student has to attempt any 6 very short answer type questions (4 marks each).

Instruction B: Student has to attempt any 3 short answer type questions (8 marks each).

Instruction C: Student has to attempt any 2 questions (16 marks each).

Use of following supporting material is permitted during examination. (Mentioned in form No. 205)

1. NIL 2. NIL

PART– A

Q.1 What is data communication?

Q.2 What is internet?

Q.3 Sketch the classes of transmission media.

Q.4 What is PCM?

Q.5 A slotted ALOHA network transmits 200 – bit frames using a shared channel with a 200 kbps bandwidth. Find the throughput if the system (all stations together) produces 500 frames per second.

Q.6 Define the type of the destination addresses 47:20:1B:2E:08:EE.

Q.7 Define flooding.

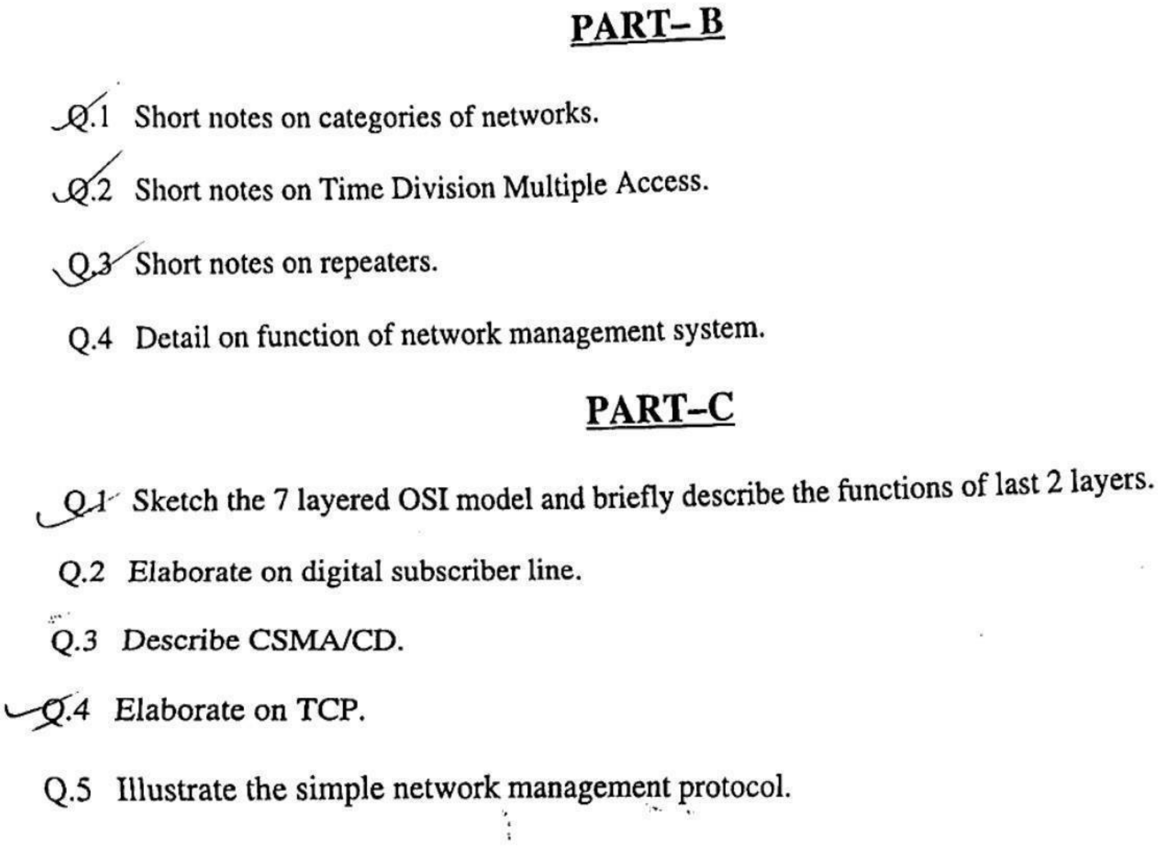
Q.8 What is tunneling?

Q.9 What is reactive fault management system?

Q.10 What is cipher?

[14NN804] Page 1 of 2

https://www.rtuonline.com



PART– B

Q.1 Short notes on categories of networks.

Q.2 Short notes on Time Division Multiple Access.

Q.3 Short notes on repeaters.

Q.4 Detail on function of network management system.

PART–C

Q.1 Sketch the 7 layered OSI model and briefly describe the functions of last 2 layers.

Q.2 Elaborate on digital subscriber line.

Q.3 Describe CSMA/CD.

Q.4 Elaborate on TCP.

Q.5 Illustrate the simple network management protocol.