Q3. Give detailed answers to the following questions.

i. Discuss different types of expansion cards.

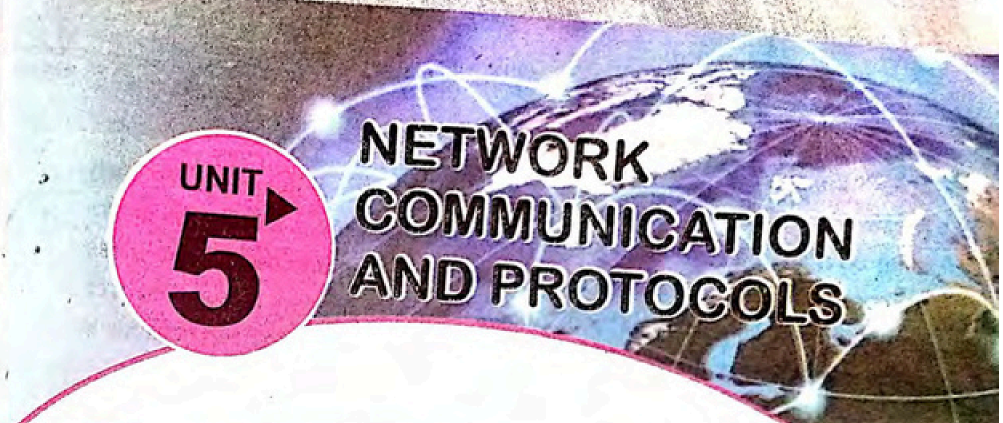
ii. What is port? Explain different types of ports in computers.

iii. Explain different types of ribbon cables.

iv. Discuss different types of memory chips.

v. What is Bus? Explain different types of buses in computers.

vi. Write note on SDRAM and DDR SDRAM.



UNIT 5 NETWORK COMMUNICATION AND PROTOCOLS

After the completion of Unit - 5, the Students will be able to:

- explain basic network components (Sender, Receiver and Medium).
- explain modes of communication (simplex, half-duplex and full-duplex).
- describe communication media (Guided and Un-guided).
- explain communication devices (Switch, Router and Gateway).
- explain network architecture (Client, Server and Peer-to-Peer).
- explain network types (LAN, MAN, WAN and VPN).
- explain network topologies (Star, Ring, Bus and Mesh).
- identify the purpose of communication standards.
- understand OSI Model and concepts of its layers.
- provide examples of protocols and devices at each layer of OSI Model.
- describe TCP/IP protocol suite used for communication over the Internet.
- compare the TCP suite with OSI Model.
- differentiate between circuit switching and packet switching.
- describe IP addressing schemes (Classes, Masks and Subnets).

5.1 COMPUTER NETWORK

A network is a collection of computers or nodes that communicate with each other on a shared network medium. A computer network is a collection of two or more connected computers to share the resources and data. When these computers are joined in a network, people can share different files and devices such as modems, printers and tape drives. A typical computer network is shown in Figure 5.1.

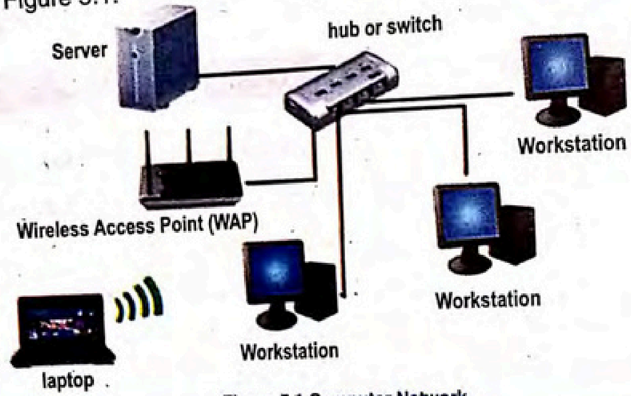


Figure 5.1 Computer Network

5.1.1 Basic Data Communication Components

The data communication is the movement or transmission of data between two devices or computers. OR, it is the transfer of data between two points either in analog or digital form via a communication medium.

A data communication system consists of five basic components.

a. Sender
b. Message
c. Medium
d. Protocol
e. Receiver

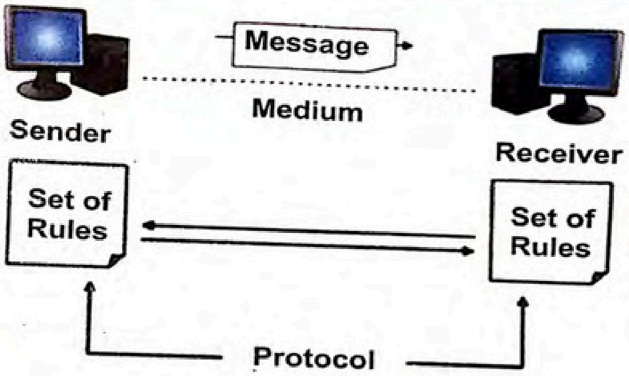


Figure 5.2 Basic Network components

a. Sender

Sender or Transmitter is a device that sends the message. It may be a computer, workstation, telephone handset or video camera. The transmitter converts the electrical signal into a form that is suitable for transmission through the physical channel or transmission medium. For example, TV broadcast, there is a specific frequency range for each channel. Hence the sender (TV broadcast station) must translate the information signal to be sent into the appropriate frequency range that matches the frequency assigned to the sender. Thus the signals transmitted by multiple channels do not interfere with another.

b. Message

Message is the data or information that is to be transmitted. Message can be number, video, text or any combination of these.

c. Medium

Medium is the physical path that message uses to travel from source to destination. It can be fiber optic cable, coaxial cables, twisted pair cable and even can be wireless media. Medium is also called a channel. Telephone system, Internet, and many other electronic systems use wires. Television and radio can use electromagnetic radiations (wireless medium).

d. Receiver

Receiver is the device which receives transmitted message. It can be a computer, workstation, telephone handset or television set. The data received from the transmission medium may not be in proper form to be accepted to the receiver and it must be converted to appropriate form before it is received. There are five receiving steps in the process of communication; i.e. Receive, Understand, Accept, Use, and Give a Feedback. Without these steps communication process may not be completed and successful.

e. Protocol

A protocol is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol, two devices connected may not able to communicate with each other.

5.1.2 Modes of Communication

Modes of data transmission refer to the methods or ways information is transmitted from one place to another. Following are the different categories of data transmission modes which are: .

a. Simplex, half-duplex and full-duplex
b. Synchronous and Asynchronous

a. Simplex, half-duplex and full-duplex

i. Simplex mode

In Simplex mode, the communication takes place in only one direction. In this mode, a node can only send data and cannot receive or it can only receive data but cannot send. In this mode communication is uni-directional, for example communication from a central computer to a dumb terminal. The communication can only take place in one direction and it is not possible for the receiver to send data back. Another example of simplex transmission would be data being sent to an electronic notice board such as those found in train stations and airports.

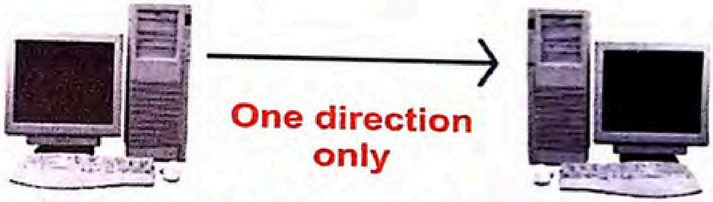


Figure 5.3 Simplex Mode

ii. Half-Duplex mode

In half-duplex mode, each station can both transmit and receive data, but not at the same time. Each end of the communications link acts as sender and receiver. An example of this type of communication is the use of walkie-talkies, where each of the persons communicating must indicate when they have finished speaking.

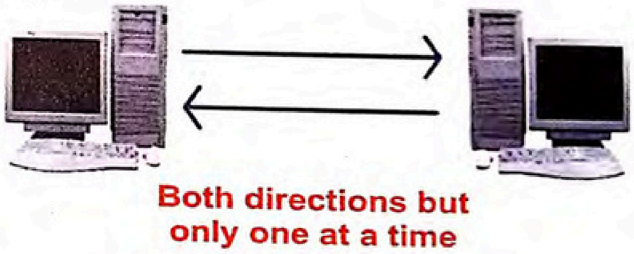


Figure 5.4 Half-duplex Mode

iii. Full-Duplex mode

In full-duplex mode, both stations can send and receive the data simultaneously, for example two or more computers connected to a network device such as a switch that provides full duplex activity. It is the fastest bi-directional mode of communication. The full-duplex mode is like a two way eet, with traffic flowing in both directions at the same time. In full-duplex ode, signals going in one direction share the capacity bandwidth of the ıedium with signals going in the other direction. This sharing can occur in two vays, either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

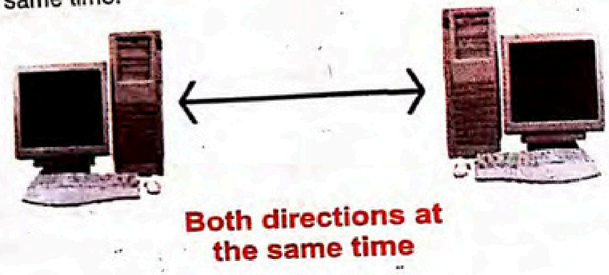


Figure 5.5 Full-duplex Mode

b. Synchronous and Asynchronous

Another way of classifying data communications flow is as synchronous or asynchronous.

i. Synchronous Transmission

In synchronous transmission, large volumes of information can be transmitted at a time. In this type of transmission, data is transmitted block-by-block or word-by-word simultaneously. Each block may contain several bytes of data. In synchronous transmission, a special communication device known as synchronized clock is required to schedule the transmission of information. With synchronous transmission, large blocks of bytes are transmitted at regular intervals without any start/stop signals. Synchronous transmission requires that both the sending and receiving devices be synchronized before data is transmitted. Synchronous transmission requires more expensive

equipment but provides greater speed and accuracy than asynchronous transmission. This type of transmission is appropriate for computer systems that need to transmit great quantities of data quickly.

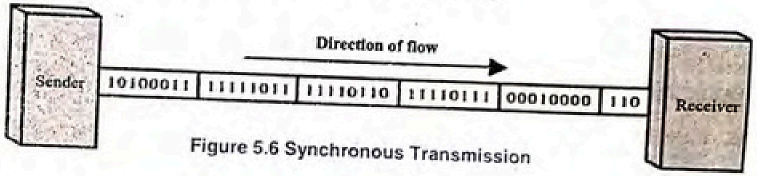


Figure 5.6 Synchronous Transmission

ii. Asynchronous Transmission

In asynchronous transmission, data is transmitted one byte at a 'time'. This type of transmission is most commonly used by microcomputers. The data is transmitted character-by-character. In asynchronous transmission, transmission does not occur at predetermined or regular intervals (i.e., not synchronized). A sending device can transmit bytes at any time, and the receiving device must be ready to accept them as they arrive. A start bit marks the beginning of a byte and a stop bit marks the end of the byte. An additional bit called a parity bit is sometimes included at the end of each byte to allow for error checking. Asynchronous transmission usually involves communications in which data can be transmitted intermittently instead of in a steady stream. It is so named because the timing of the signal is not important. Asynchronous transmission is relatively slow.

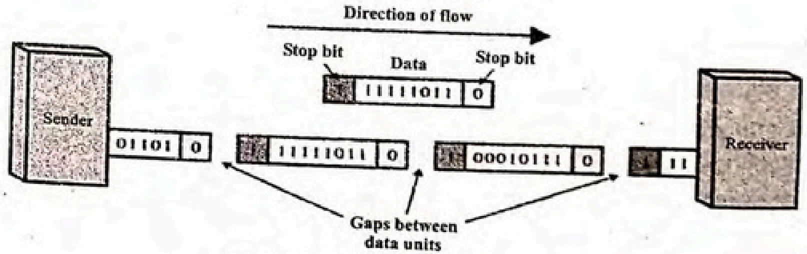


Figure 5.7 Asynchronous Transmission

5.1.3 Communication Media

Communication media are the links that provide paths for communicating devices. It is an important part of communication model. Transmission medium should provide communication with good quality.

Communication media can be classified into two main types.

a. Guided Communication Media

b. Unguided Communication Media

a. Guided Communication Media

Guided media are the physical links in which signals are confined along a narrow path. These are also called bounded media. Three common types of bounded media are:

i. Twisted Pair Cable

ii. Coaxial Cable

iii. Fiber Optic Cable

i. Twisted Pair Cable

Twisted Pair Cable is formed of two insulated copper wires twisted together. The wires are twisted with each other to minimize interference from other twisted pairs cable. Twisted wire pairs have fewer bandwidths than coaxial cable or optical fiber cable.

There are two types of twisted pair cables; shielded and unshielded.

Unshielded Twisted Pair (UTP) Cable:

UTP is the most commonly used networking wire. It is inexpensive, flexible, and light, thus making it very easy to work with. The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. The unshielded twisted pair provides a bandwidth of 100 Kbps (Cat 1) to 1000 Mbps (Cat 7).The standard connector for unshielded twisted pair cabling is an RJ-45 connector.

Shielded Twisted Pair (STP) Cable

The difference between the UTP and STP is that the STP uses metallic shield wrapped to protect the wire from interference. Shielded cables can help to extend the maximum distance of the cables. Data rate of STP is from 16 to 155 Mbps. It costs more than UTP.

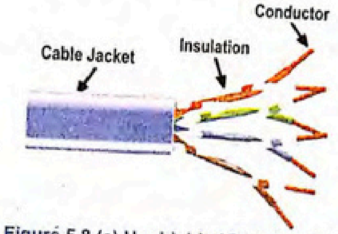


Figure 5.8 (a) Unshielded Twisted Pair Cable

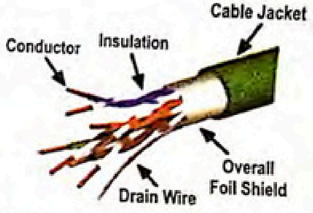


Figure 5.8 (b) Shielded Twisted Pair Cable

ii. Coaxial Cable (Coax)

A Coaxial Cable (Coax) has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping is a second conductor to complete the circuit and shield against noise. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Because coaxial cables have very little distortion and are less prone to interference, they have low error rates. Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable.

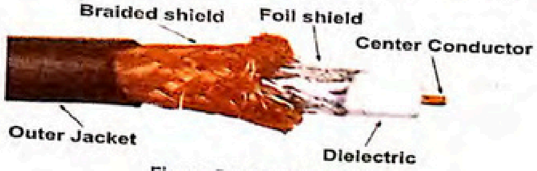


Figure 5.9 Coaxial Cable

iii. Optical Fiber Cable

An optical fiber consists of a very narrow strand or fiber of glass called the core. The core is surrounded by a concentric layer of glass called Cladding. The cladding is covered by a protective coating of plastic jacket. It transmits signals in the form of light rather than electronic signals. This eliminates the problem of electrical interference. The Fiber optic uses total internal reflection to guide light signals through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in the density of the two materials causes the beam of light moving through the core. No light escapes the glass core because of this reflective cladding.

The fiber-optic cable is becoming more popular. Now a days, telephone, Internet and television companies are replacing their existing cables with fiber optic cables. Fiber optic cable has bandwidth more than 2 Gbps (Gigabytes per Second).

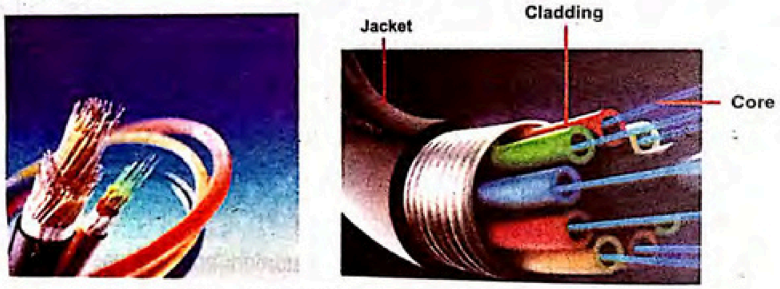


Figure 5.10 (a) Fiber Optic Cable

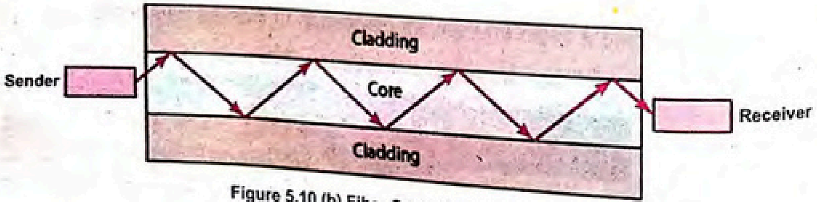


Figure 5.10 (b) Fiber Optic Mechanism

b. Unguided Communication Media

Unguided media also called Wireless media transports signals without using any physical conductor between the two devices communicating. Signals are normally broadcast through the air and thus are available to anyone who has the device capable of receiving them.

The commonly used wireless transmission media are:

i. Radio waves

ii. Micro waves

iii. Infrared waves

i. RADIO WAVES

Radio wave distributes radio signals through the air over long distances such as between cities, regions, and countries, and short distances such as within an office or home. Radio waves are normally multi-directional. When an antenna transmits radio waves, they are propagated in all directions. The multi-directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. It has frequency between 10 KHz to 1 GHz. Our AM and FM radio stations, cordless phones and televisions are examples of multicasting.

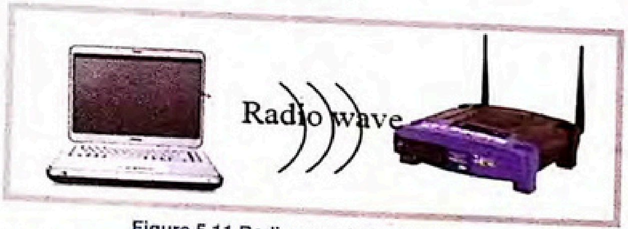


Figure 5.11 Radio wave Transmission

ii. MICRO WAVES

Micro wave is a wireless transmission technology that travels at high frequency than radio waves and provides high throughput as a wireless network media. Micro wave transmission requires the sender to be in line of sight of the receiver. Electronic waves with frequencies between 1 GHz to 300 GHz are normally called microwaves. Micro waves are used to transmit wireless signals across a few miles. Unlike radio waves, microwaves are unidirectional, in which the sending and receiving antennas need to be aligned. Microwave stations or antennas are usually installed on the high towers or buildings. Microwaves propagation is line-of-sight therefore towers with mounted antennas need to be in direct sight of each other. Mobile telephone companies use microwave technology.

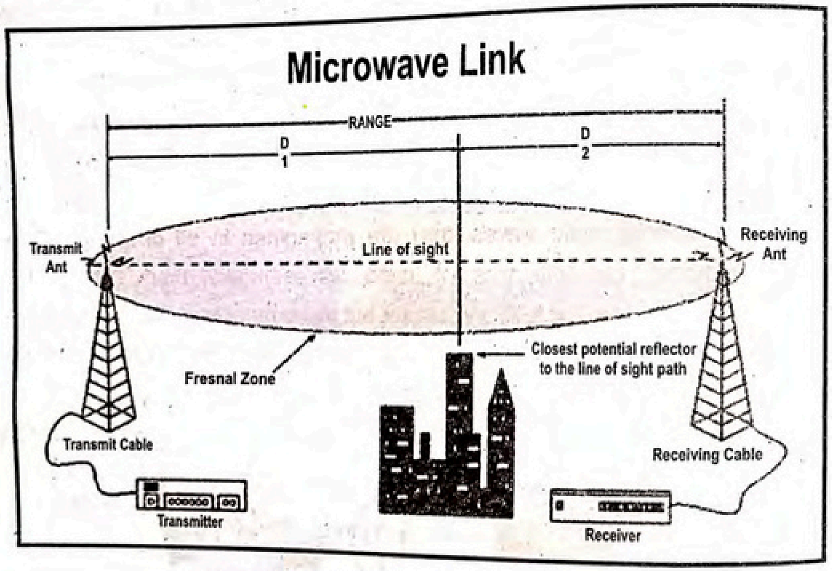


Figure 5.12 Microwave transmission

For long distance communication **Satellite Microwave** technology is used. A communications satellite is a device that receives microwave signals from an earth-based station, amplifies the signals, and broadcasts the signals back over a wide area to any number of earth-based stations. Satellite micro wave transmission is used to transmit signals throughout the world.

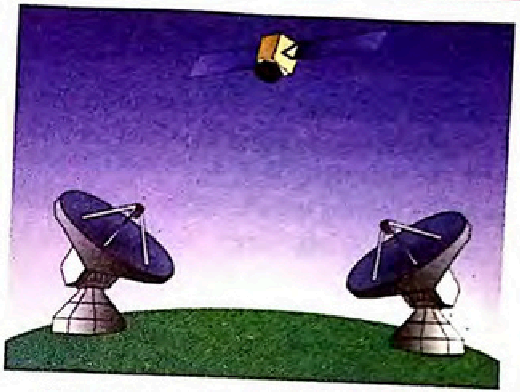


Figure 5.13 Satellite Transmission System

iii. Infrared

Infrared is a short-distance wireless transmission medium that sends signals using infrared light waves. Infrared frequencies are just below visible light. These high frequencies allow high speed data transmission. This technology is similar to the use of a remote control for a TV. Infrared transmission can be affected by objects obstructing sender or receiver.

Infrared is used in devices such as the mouse, wireless keyboard and printers. With infrared, computers can transfer files and other digital data bi-directionally. Infrared adapters are installed in many laptops, handheld personal devices and mobile phones.

Figure 5.14 Infrared

5.1.4 Communication Devices

Communication devices are used for communication between the computers or other devices. The following are some important communication devices.

a. Switch

b. Router

c. Gateway

a. Switch

A network switch or hub is a device that connects network nodes to a central location. Switch is also called layer 2 device because it operates on OSI data link layer. Switch does not generally encompass unintelligent device such as hubs and repeaters. Network switches appear nearly identical to network hubs but a switch generally contains more intelligence than a hub because it maintains MAC table. Unlike hubs, network switches are capable of inspecting data packets as they are received determining the source and destination device of each packet and forwarding them.

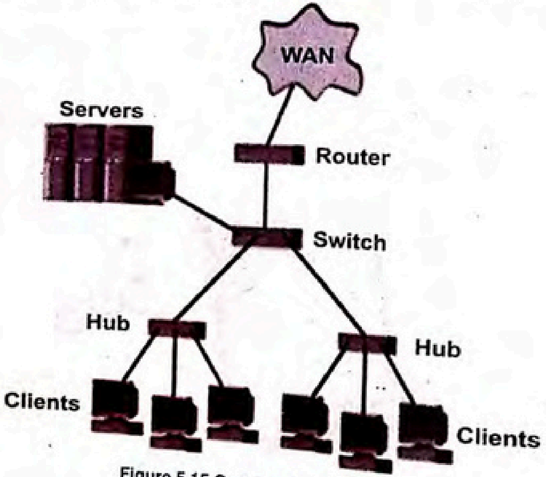


Figure 5.15 Communication Devices

b. Router

data

Router is a device that forwards data packets across different networks. A router performs traffic directing functions on the Internet. A router is a microprocessor controlled device that is connected to two or more data lines from different networks. When a data packet comes in, the router reads the destination address in the packet. Using information in its routing table it directs the packet to the next network. A data packet is typically passed from node to node until it reaches the destination. Router operates on Network layer of OSI Model. Routing can be static or dynamic. Router determines the best route for the packets to destination.

A router normally connects LANs and WANs in the Internet with the help of routing table. For example a router can be used to distribute one Internet connection to many computers in a University or College LAN.

c. Gateway

A gateway is a hardware device or a computer running software that allows communication between networks with dissimilar network protocols or architectures. The gateway has an interface to each of the networks to which it is connected. Generally, congestion on connected networks is avoided by keeping local traffic confined to the network on which it originates, except when the packets are destined for another network. The gateway has the responsibility of acting as the switch that allows such packets to go from one network to another.

Gateways are very intelligent devices. A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model.

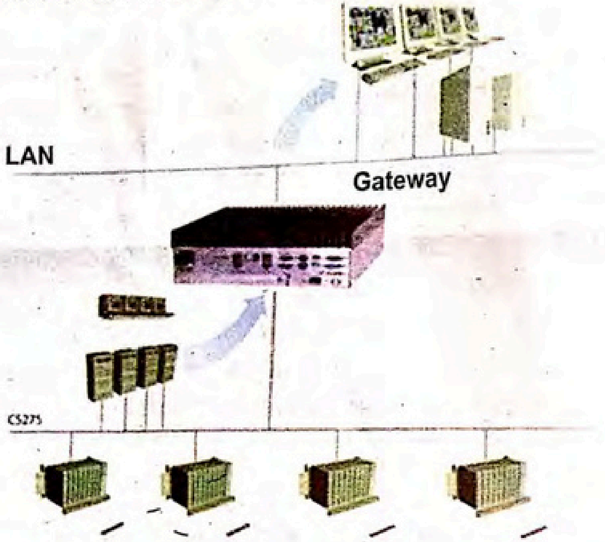


Figure 5.16 Network Gateway

5.1.5 Network Architecture

A computer network is a collection of computers and devices interconnected by communications channels that facilitate communications among users and allow users to share resources and data. Network Architecture is the complete framework of any computer network. It refers to the logical and structural layout of the network, consisting of the hardware, software, connectivity, communication protocols and mode of transmission, such as wired or wireless. The following are some important network architectures.

a. Client Server Network Architecture

b. Peer to Peer Network Architecture

a. Client/Server Network Architecture

Server is a powerful computer that provides centralized administration of the network and serves up the resources that are available on the network, such as printers and files.

Client on the other hand is a network device that participates in a client/server relationship by requesting a service from a server. It may be a computer that allows a user or users to log on to the network and take advantage of the resources available on the network.

The client/server Architecture is particularly recommended for networks requiring a high degree of reliability. The term Client/server refers to the concept of sharing the work involved in processing data between the client computer and the server computer.

The client begins the exchange by requesting data from the server. The server responds by sending one or more streams of data to the client. In addition to the actual data transfer, this exchange may also require control information, such as user authentication and the identification of a data file to be transferred.

Example:

One example of a client/server network is a corporate environment where employees use a company e-mail server to send, receive and store e-mail. The e-mail client on an employee computer issues a request to the e-mail server for any unread mail. The server responds by sending the requested e-mail to the client. Data transfer from a client to a server is referred to as an upload and data from a server to a client as a download.

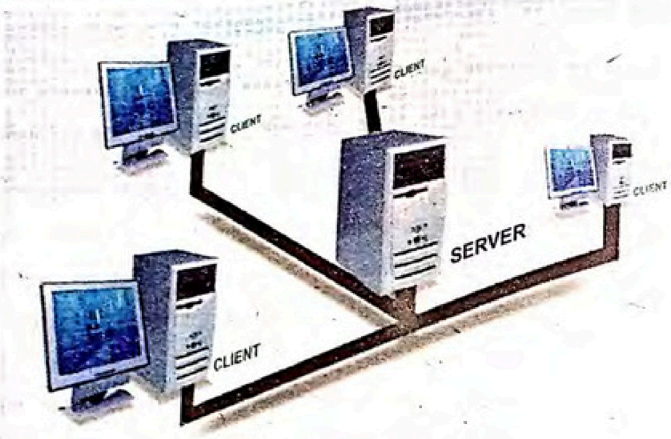


Figure 5.17 Client/Server Network

Advantages of a client/server network

- **Centralized Resources**: Server is the centre of the network and it can manage resources that are common to all users.
- **Improved security:** Server provides better security to network users.
- **Scalable network:** It is possible to remove or add clients without affecting the operation of the network and without the need for major changes.
- **Flexibility:** New technology can be easily integrated into the system.
- **Interoperability:** All components (client/network/server) work together.

Disadvantages of a client/server network

- **Expensive:** Requires high initial investment in dedicated server.
- **Maintenance:** Large networks will require a staff to ensure efficient operation and maintenance.
- **Dependence:** When server goes down, operations will cease across the network.

Most LANs consist of many clients and a few servers. While one server always controls user logons, other servers can specialize in providing certain types of resources.

b. Peer-to-Peer Network Architecture

In peer-to-peer networking there are no dedicated servers or hierarchy among the computers. Peers i.e. computers are equally privileged nodes in the network. Peer-to-peer network allow users to share resources and files located on their computers and to access shared resources found on other computers. In a peer-to-peer network, all computers have equal status and therefore known as peers. 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. Nearly all modern desktop operating systems, such as Macintosh OSX, Linux, and Windows, can support peer-to-peer network. A peer computer basically acts as both a client and a server computer.

The only requirements for building a peer-to-peer network include installing an operating system on the PCs that supports peer-to-peer networking and then physically connecting the PCs through some medium.

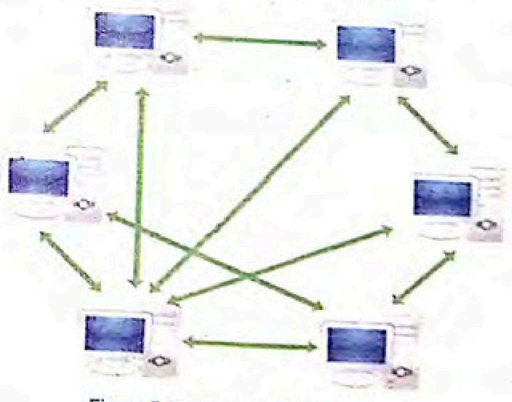


Figure 5.18 Peer-to-peer Network

Advantages of a peer-to-peer network

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

Disadvantages of a peer-to-peer network

- **Decentralization:** No central storage for files and applications.
- **Less Secure:** Does not provide the security available as on a client/server network.

5.1.6 Network Types

Network can be classified into following types.

a. Local Area Network (LAN)

b. Metropolitan Area Network (MAN)

c. Wide Area Network (WAN)

d. Virtual Private Network (VPN)

a. LAN (Local Area Network)

LAN (Local Area Network) is a network that connects computers and devices in a limited geographical area like home, school, and office building. Each computer or device on the network is called a node. LANs are most likely to be based on Ethernet technology. A LAN is useful for sharing resources like files, printers, games or other applications. A LAN can be wired or wireless. A wired LAN requires Ethernet cable to physically connect all computers on the network to a central device called a switch or hub. A wireless LAN uses radio waves to communicate.

Data transfer speeds over a local area network can reach up to 10 Mbps (such as for an Ethernet network) and 1 Gbps (as with FDDI or Gigabit Ethernet). A local area network can reach as many as 100, or even 1000, users.

A local area network's linkages usually are accomplished with either telephone, coaxial, or fiber-optic cables.

There are two basic reasons for developing a LAN:

- Information sharing: This refers to having users who access the same data files, exchange information via electronic mail, or search the Internet for information. The main benefit of information sharing is improved decision making, which makes it generally more important than resource sharing.
- Resource sharing: It refers to one computer sharing a hardware device (e.g., a printer) or a software package with other computers on the network. The main benefit of resource sharing is cost savings.

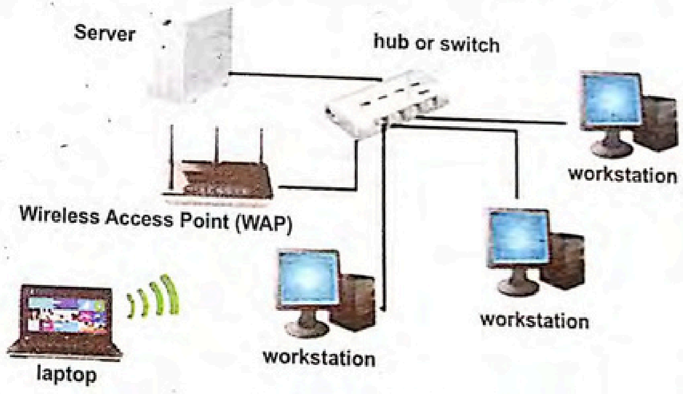


Figure 5.19 Local Area Network

b. MAN (Metropolitan Area Network)

A metropolitan area network is a computer network that usually spans a city or in a large metropolitan area. MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology. MAN might be owned and managed by a single organization.

Metropolitan Area Network connects multiple geographically nearby LANs to one another (over an area of up to a few dozen kilometers). Recent use of MAN technology has been the rapid development of cellular phone systems.

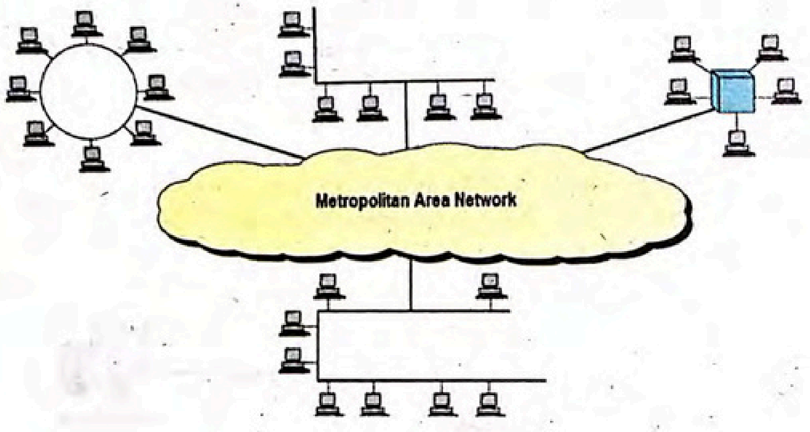


Figure 5.20 Metropolitan Area Network

c. WAN (Wide Area Networks)

WAN (Wide Area Network) covers large distance for communication between computers. Its nodes may span cities, states, or even countries. It interconnects many LANs and MANs. WAN uses fiber optics, microwaves and satellites technology for communication. For example, nationwide ATM (Automated Teller Machines) used in banking represent a common application of a wide area network.

The most well-known WAN is the Internet, which may cover the entire globe. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management.

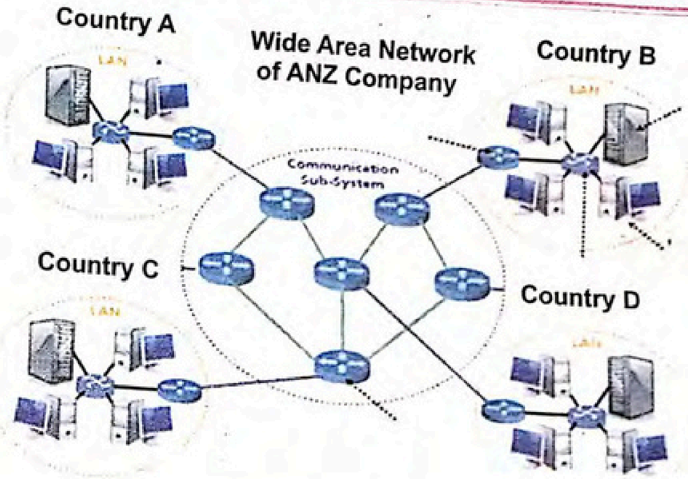


Figure 5.21 Wide Area Network

d. VPN (Virtual Private Network)

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet or a private network owned by a service provider to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures.

Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network. In order to gain access to the private network, a user must be authenticated using a unique identification and a password.

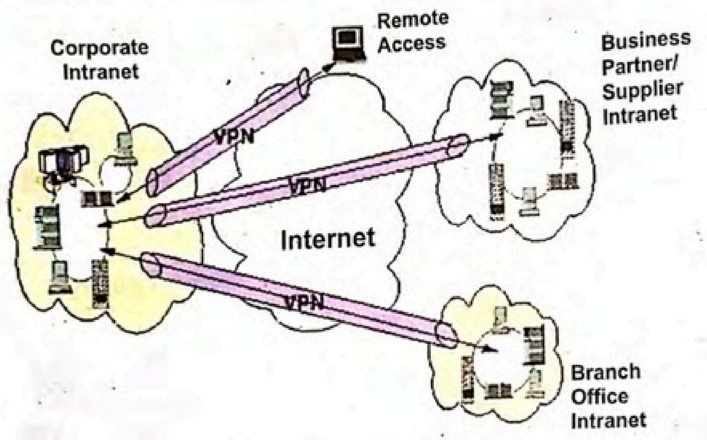


Figure 5.22 Virtual Private Network

5.1.7 Network Topologies

Network Topology refers to the physical layout and connectivity of computers in a network. Network topologies are categorized into the following four basic types.

a. Star
b. Ring
c. Bus
d. Mesh

a. Star Topology

In a star topology all the nodes (server, workstations, peripherals) on the network are connected directly to a centralized connectivity device called a hub, switch, or router. Each computer is connected with its own cable to a port on the hub. Data on a star network passes through the hub, switch, or router before continuing to its destination. The hub, switch, or router manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

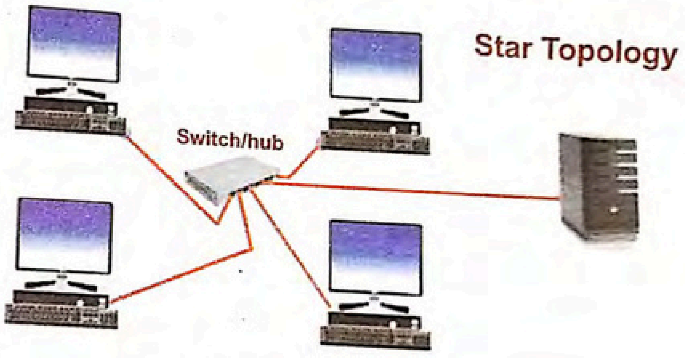


Figure 5.23 Star Topology

Advantages of a Star Topology

- Centralized management. It helps in monitoring the network.
- Easy to install and configure.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.
- Failure of one node or link doesn't affect the rest of network.

Disadvantages of a Star Topology

- Requires more cable than a Bus topology.
- If the hub, switch, or concentrator fails, nodes attached become disable.
- More expensive than linear bus topologies because of the cost of the hubs.

b. Ring Topology

In a ring topology, every node is logically connected to two other preceding and succeeding nodes, forming a ring. Traffic flows through the entire ring until it reaches its destination.

Data packets travel in a single direction around the ring from one network device to the next. Each network device acts as a repeater, meaning it regenerates the signal the packets they receive and then send them on to the next computer in the ring.

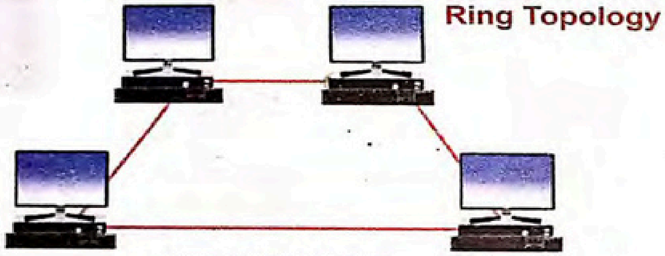


Figure 5.24 Ring Topology

Advantages of Ring Topology

- Even when the load on the network increases, its performance is better than that of Bus topology.
- There is no need for network server to control the connectivity between workstations.
- Additional components do not affect the performance of network.
- Each computer has equal access to resources.

Disadvantages of Ring Topology

- Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- If one workstation or port goes down, the entire network gets affected.

- Network is highly dependent on the wire which connects different components.
- Ring topologies can be difficult to troubleshoot.
- Adding or removing computers from this type of topology can disrupt the operation of the network.

c. Bus Topology

In the bus topology, each node (computer, server or peripheral device) is attached to a single common cable. This topology type is considered a passive topology because the computers on a bus just sit and listen. When they "hear" data on the wire that belongs to them, they accept that data. When they are ready to transmit, they make sure no one else on the bus is transmitting and then they send their packets of information on the network.

Bus network typically uses coaxial networking cable hooked in to each computer using a T-connector. Each end of the network is terminated using a terminator specific to a cable.

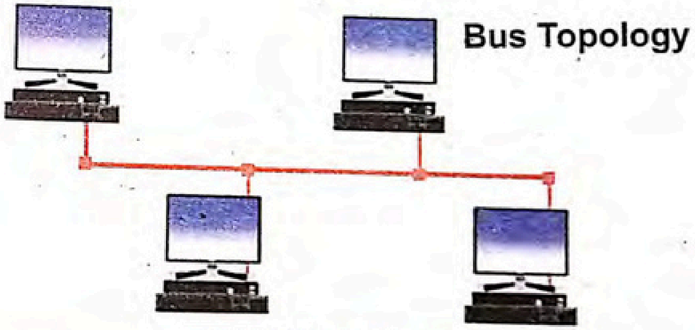


Figure 5.25 Bus Topology

Advantages of a Bus Topology

- Bus topology costs very less.
- Easy to connect a computer or peripheral to a linear bus.

- Requires less cable length than a other topologies.
- It is easy to set-up and extend bus network.
- Linear Bus network is mostly used in small networks.

Disadvantages of a Bus Topology

- Entire network shuts down if there is a break in the main cable. Loose and detached connections may also affect the entire network.
- There is a limit on central cable length and number of nodes that can be connected.
- Proper termination is required to dump signals. Use of terminators is must.
- It is difficult to detect and troubleshoot fault at individual station.
- It is not suitable for networks with heavy traffic.

d. Mesh Topology

In a mesh network topology, each of the network node, computer and other devices, are interconnected with one another.

In a full mesh, every device in the network is connected to every other device. In reality, a partial mesh is commonly used in backbone environments to provide fault-tolerant connections between critical servers and network devices. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. This type of topology is very expensive as there are many redundant connections, thus it is not mostly used in computer networks. It is commonly used in wireless networks. Flooding or routing technique is used in mesh topology.

Nehmat

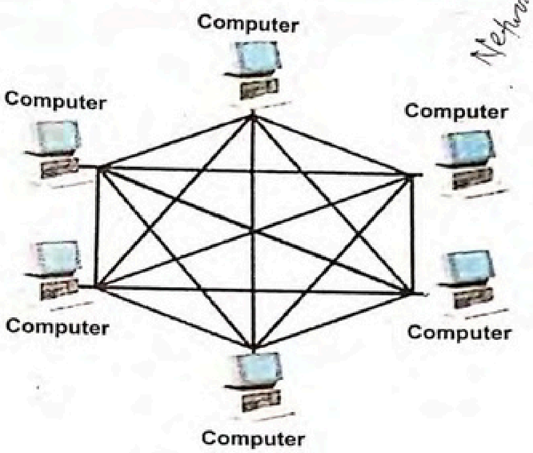


Figure 5.26 Mesh Topology

Advantages of Mesh topology

- Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.
- Even if one of the components fails there is always an alternative link present. So data transfer doesn't get affected.
- Expansion and modification in topology can be done without disrupting other nodes.

Disadvantages of Mesh topology

- There are high chances of redundancy in many of the network connections.
- Overall cost of this network is too high as compared to other network topologies.
- Set-up and maintenance of this topology is very difficult. Even administration of the network is challenging.

▶ 5.2 DATA COMMUNICATION STANDARDS

Data communication standards, also called Network protocols, are set of rules that coordinate the exchange of information in Computer networks.

5.2.1 Purpose of Communication Standards

Communication Standards provide guidelines (also called rules or protocols) to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity of networks for communication. These standards define how computers identify one another on a network, the form that the data should take in during transmission, and how this information is processed once it reaches its final destination. Some examples of communication standards are TCP/IP (for UNIX, Windows NT, Windows 95 and other platforms), IPX (for Novell NetWare), DECnet (for networking Digital Equipment Corp. computers), AppleTalk (for Macintosh computers), and NetBIOS/NetBEUI (for LAN Manager and Windows NT networks).

5.2.2 Open System Interconnection (OSI) Model

OSI Model is developed by International Standards Organization (ISO), which is a multinational body dedicated to worldwide agreements on International Standards. An OSI model covers all aspects of Network Communication. It is an Open System because it allows two different systems to communicate over their primary network.

The OSI model deals with the following:

- How a device on a network transmits its data and how it knows when and where to send.
- How a node on a network receives its data and how it know where to search.
- How nodes using different languages communicate with each other.
- How nodes on a network are physically connected to each other.

- How different protocols work with devices on a network to arrange data.

OSI MODEL LAYERS

The OSI model defines a networking framework for implementing protocols in seven different layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

The OSI model divides communications into seven different layers, where each include multiple hardware standards, protocols, or, other types of services. The OSI model has following seven layers.

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

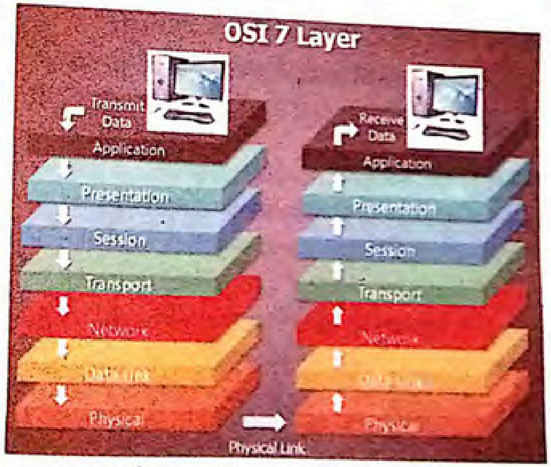


Figure 5.27 OSI Model Layers

Layer 1: PHYSICAL LAYER

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. It provides the following functions.

- Defines physical means of sending data over network devices.
- Defines the characteristics of the physical medium.
- Transmission and receipt of data from the physical medium is managed at this layer.
- Interfaces between network medium and devices.
- Defines optical, electrical and mechanical characteristics.
- Conversion of the raw bit stream into electrical impulse, light or radio signal.
- Manages the encoding and decoding of data.
- Determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.

Layer 2: DATA LINK LAYER

The data link layer provides reliable transmission of data across a physical link. Data link layer is used by hubs and switches for their operation. The *data link* layer is concerned with physical addressing, network topology, physical link management, error notification, ordered delivery of frames, and flow control.

The data link layer provides:

- Segmentation of upper layer datagrams into frames in sizes that can be handled by the communications hardware.

- Bit Ordering. The data link layer organizes the pattern of data bits into frames before transmission. The frame formatting issues such as stop and start bits, bit order, parity and other functions are also handled.

Layer 3: NETWORK LAYER

This layer allows the data called packets or datagram to go from one physical network to another. This layer also has its own addressing scheme (network logical address) so that devices can communicate with other devices across multiple networks. Consequently, this layer is also responsible for path determination.

The network layer establishes the route between the sender and receiver across switching points, which are typically routers. The most ubiquitous example of this layer is the IP protocol in TCP/IP. It provides the following functions.

- Translates logical addresses, or names, into physical addresses.
- Management of connectivity and routing between hosts or networks.
- Determines how data are transferred between network devices
- Routes packets according to unique network device addresses
- Provides flow and congestion control to prevent network resource depletion
- Responsible for addressing, determining routes for sending and managing network problems such as packet switching, data congestion and routines.

Layer 4: TRANSPORT LAYER

As its name implies, it handles the transparent transport of data segments between network devices. It is responsible for flow control, error control, data segmentation, and communication reliability.

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications.

The transport layer provides the following functions.

- Accepts a message from the (session) layer above it, splits the message into smaller units, and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- Manages reliable end-to-end message delivery with acknowledgments in network.
- Tells the transmitting station to "back-off" when no message buffers are available.
- Provides reliable and sequential packet delivery through error recovery and flow control mechanisms.
- Provides connectionless oriented packet delivery.

Layer 5: SESSION LAYER

The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications 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.

It also marks significant parts of the transmitted data with checkpoints to allow fast recovery in the event of a connection failure.

In most modern Internet applications, the *session*, *presentation* and *application* layers are usually combined inside the application itself, thus, web browser performs all functions of the *session*, *presentation* and *application* layers.

Layer 6: PRESENTATION LAYER

The presentation layer converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). The presentation layer is sometimes called as the syntax layer. It can be viewed as the translator for the network. The presentation layer provides the following functions.

- Character code translation: for example, ASCII to EBCDIC.
- 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.
- Specifies architecture-independent data transfer format.

Layer 7: APPLICATION LAYER

The application layer serves as the user interface for users and application processes to access network services. The application layer is responsible for displaying data and images to the user in a human-recognizable format. It provides an interface with the presentation layer. Everything at this layer is application-specific. This layer performs the following functions.

- Resource sharing
- Remote file access
- Network management
- Directory services
- Electronic messaging (such as e-mail)

5.2.3 Examples of Devices and Protocols on Layers of OSI Model

The following are some common network devices and protocols and where they are implemented in the OSI model.

OSI LAYER	DEVICES	PROTOCOLS
APPLICATION layer 7	Gateway	SNMP, SMTP, FTP, TELNET, HTTP, NCP, SMB, AppleTalk, FTAM, X.400,X.500, DAP,DNS
PRESENTATION layer 6	Gateway	NCP, AFP, TDI, XDR, SSL, ISO 8823 TLS, PAP, X.226
SESSION layer 5	Gateway	NetBIOS, ASP, ADSP, ZIP, ISO 8327, X.225, SAP, SDP
TRANSPORT layer 4	Gateway	NetBEUI, TCP, SPX, NWlink, UDP, RTP, SCTP, TP0, TP1, TP2, TP3, TP4, OSPF, SPX, RIP, ATP, NBP, AEP, RTMP
NETWORK layer 3	Routers, layer 3 (or IP) switches.	IP, IPX, NWlink, NetBEUI, ICMP, IPsec, ARP, RIP, BGP, X.25 (PLP), CLNP, DDP, IGRP
DATA LINK layer 2	Bridges and switches, Ethernet incorporates both this layer and the Physical layer.	X.25 (LAPB., Token Bus, IEEE 802.3 framing, Ethernet II framing, LocalTalk, TokenTalk, EtherTalk, Apple Remote Access, PPP, HDLC, Q.921
PHYSICAL layer 1	Hubs, repeaters, network adapters, Parallel SCSI buses. Various physical-layers Ethernet incorporates both this layer and the data-link layer. Token ring, FDDI, and IEEE 802.11.	X.25 (X.21bis), EIA/TIA-232, EIA/TIA-449, EIA-530, G.703

▶ 5.3 TCP/IP

Communications between computers on a network is done through protocol suits. The most widely used and most widely available protocol suite is TCP/IP protocol suite. TCP/IP is an industry standard suite of protocols designed for local and wide area networks. It was developed by the United States

Department of Defense (DoD) Advanced Research Projects Agency (ARPA) in 1969 for a research sharing project called ARPANET. Internet was built on the foundation of the original ARPANET project.

5.3.1 TCP/IP Protocol Suite Architecture

A protocol suite is a group of protocols that all work together to allow software or hardware to perform a function. The **TCP/IP** protocol suite is a good example of it. The three important points associated with TCP/IP protocol suit are:

a. TCP/IP Architecture

b. TCP/IP PORTS

c. TCP/IP Applications

a. TCP/IP Architecture

TCP/IP protocol suit consists of a layered architecture where each layer depicts some functionality which can be carried out by a protocol. Each layer usually has more than one protocol options to carry out the responsibility that the layer adheres to. It is named from two of the most important protocols in it. That is Transmission Control Protocol and Internet Protocol. TCP/IP is normally considered to be a 4 layer system. The TCP/IP model breaks down into the following four layers.

- Application Layer
- Transport Layer
- Internet Layer
- Network Access Layer

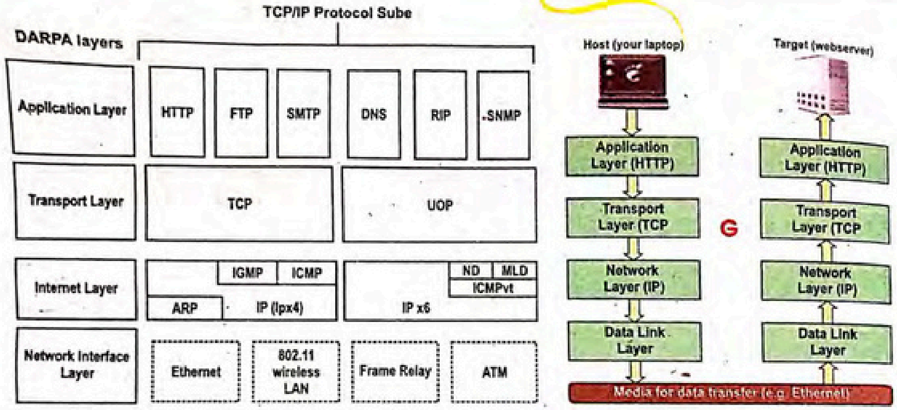


Figure 5.28 The architecture of the TCP/IP protocol suite

All application data, whether it is an e-mail, a file, an instant message, a video or voice call, is divided into data segments and encapsulated in Transport Layer PDU's (TCP or UDP segments). The Transport Layer PDU's (Protocol data Unit) are then encapsulated in Internet Layer's Internet Protocol packets. The Internet Protocol packets are then divided into frames at the Network Access layer and transmitted across the physical media (copper wires, fiber optic cables or the air) to the next station in the network. Figure 5.28 shows the architecture of the TCP/IP protocol suite.

Application Layer

This is the top layer of TCP/IP protocol suite. This layer includes applications or processes that use transport layer protocols to deliver the data to destination computers.

Transport Layer

The Transport Layer provides the means for the transport of data segments across the Internet. The Transport Layer is concerned with host-to-host communication. Transmission Control Protocol provides reliable, connection-

oriented transport of data between two endpoints (sockets) on two computers that use Internet Protocol to communicate.

Internet Layer

The Internet Layer provides a global logical addressing scheme, a process for packetization of data, another process for routing packets to their destination and for providing connectivity between networks. The Internet Layer is concerned with network to network communication. The main protocol used at this layer is IP.

Network Access Layer

main
Protocol used layer

The Network Access Layer provides access to the physical network. The data is transmitted and received across the physical network in network access layer. This layer combines the Physical and Data link layers and routes the data between devices on the same network. It also manages the exchange of data between the network and other devices.

b. TCP/IP PORTS

Every computer or device on the Internet must have a unique number assigned to it called the IP address. This IP address is used to recognize each particular computer out of the millions of other computers connected to the Internet. The information sent over the Internet to a particular computer is received by using TCP or UDP ports. There are a total of 65,535 TCP Ports and another 65,535 UDP ports. The Internet Assigned Numbers Authority (IANA) is responsible for assigning TCP and UDP port numbers to specific uses.

For instance, port 23 is used for telnet services, HTTP uses port 80 for providing web browsing service and FTP servers use TCP ports 20 and 21 to send and receive information. There are some ports that are assigned, some reserved and many unassigned which may be utilized by application programs.

The port numbers are divided into three ranges:

- The Well Known Ports.
- The Registered Ports.
- The Dynamic and/or Private Ports.

WELL KNOWN PORT NUMBERS

Well-known ports (0-1023) are used for the major Internet applications, such as Web and e-mail. For example, all port 80 packets (HTTP packets) are directed to and processed by a Web server.

REGISTERED PORT NUMBERS

Registered ports are assigned to applications that are mostly vendor specific, such as Skype and BitTorrent. The Registered Ports are in the range 1024-49151.

DYNAMIC PORT NUMBERS

The Dynamic and/or Private Ports are those in the range 49152–65535. These ports are not used by any defined application.

c. TCP/IP Applications

All modern operating systems support TCP/IP, and most large private networks rely on TCP/IP for much of their traffic. A technology used for connecting dissimilar systems. Many TCP/IP application protocols were designed to access and transfer data between dissimilar systems. These protocols include HTTP, FTP, and Telnet. TCP/IP provides a robust, scalable, cross-platform client/server framework.

The TCP/IP is used by the following applications.

- Web browsers (Internet Explorer, Firefox, Safari, Opera etc.)
- Web Servers
- File Servers
- Terminal Servers

- Online games
- File Transfer applications (WS-FTP etc.)
- Microsoft Windows Update
- Anti-Virus applications

5.3.2 Comparison of TCP/IP and OSI Models

TCP/IP and OSI Model can be compared keeping in view the following characteristics.

SIMILARITIES

The main similarities between the two models include the following:

- They share similar architecture. - Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.
- They share a common application layer: - Both of the models share a common "application layer". However in practice this layer includes different services depending upon each model.
- Both models have comparable transport and network layers: - This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.
- Knowledge of both models is required by networking professionals.
- Both models assume that packets are switched. Basically this means that individual packets may take differing paths in order to reach the same destination.
- Both the models are based on the concept of stack of independent protocols.

DIFFERENCES

The main differences between the two models are as follows:

- TCP/IP combines the presentation and session layer issues into its application layer.
- OSI is a reference model and TCP/IP is an implementation of OSI model.
- TCP/IP Protocols are considered to be standard around which the internet has developed. The OSI model however is a "generic, protocol-independent standard."
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears to be simpler model and this is mainly due to the fact that it has fewer layers.
- The OSI model consists of 7 architectural layers whereas the TCP/IP only has 4 layers.
- In the TCP/IP model of the Internet, protocols are deliberately not as rigidly designed into strict layers as the OSI model.
- The TCP/IP protocol suite comes prior to the OSI model. ISO first introduce the idea of TCP/IP suite. After some time the idea of OSI model comes into existence. So the TCP/IP suite is older than OSI model.
- The TCP/IP suite is based on protocols whereas the OSI model is layer based model.

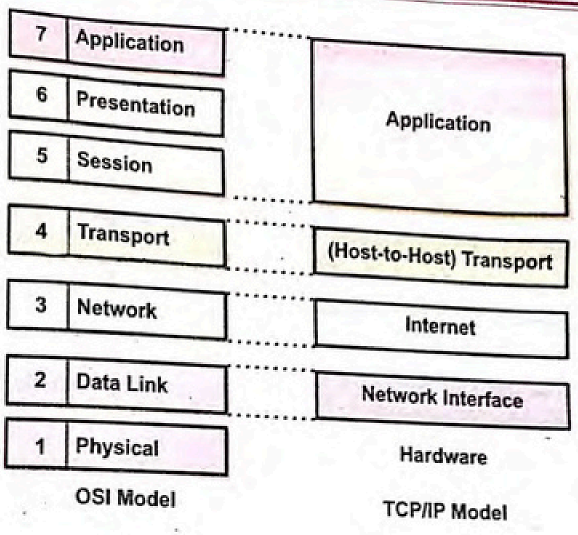


Figure 5.29 OSI Model Versus TCP Model

5.3.3 Packet Switching and Circuit Switching

Packet Switching

Packet switching is a network communication method in which the data get transmitted in blocks, regardless of type and content, called packets based on the destination address in each packet. When received, packets are reassembled in the proper sequence to make up the message. In this kind of switching, the media capacity is used optimally, and the response time is lesser.

Circuit Switching

Circuit switching is a scheme in which the network sets up a dedicated point-to-point connection between nodes and terminals before the communication starts, just like the nodes were already connected.

Difference between Circuit and Packet Switching

	Packet switching	Circuit switching
1	Bandwidth is allocated dynamically.	Fixed bandwidth allocation.
2	May be more economical as not needed dedicated circuit.	Costs more for hardware.
3	The packet needs to be re-transmitted every time when it gets lost, damaged before it is received in this method.	Once connection is established, communication is fast and almost errorless.
4	It can be used for telephony, DSL services and other data transmission services.	This concept is mainly used in telephony systems.
5	It is best used for sending data over the network and audio and video signals can also be sent over the network in the form of packets.	This is best used for transmission of audio signals and not suitable for data transmission.
6	It is usually a connection less service.	This type of switching is connection oriented and may be connectionless also.
7	The Internet being the most common example.	The most common example of a circuit switching network is the telephone system,PBX.

5.3.4 IP Addressing

An Internet Protocol address (IP address) is a number that is used to identify a device, for example a computer, a printer, etc. on the network. Each device on a network must have a unique IP address to communicate with other network devices. A **host** (usually a computer) is a device that sends or receives information on the network. Network devices transmit the data across the network. These devices include hubs, switches and routers. On a LAN, each

host and network device must have an IP address within the same network to be able to communicate with each other.

An IP address can be **static** or **dynamic**. A static IP address will never change and it is a permanent Internet address. A dynamic IP address is a temporary address that is assigned each time a computer or device accesses the Internet. The address is made up of 32 binary bits, which can be divided into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is represented in decimal and separated by a period (dot). For this reason, an IP address is expressed in dotted decimal format (e.g., 172.16.81.100). The value in each octet ranges from 0 to 255 in decimal, or 00000000 - 11111111 in binary.

The following IP address is an example which shows an IP address represented in both binary and decimal formats.

10.   1.   23.   19 (decimal)
00001010.00000001.00010111.00010011 (binary)

These octets can be broken down to provide an addressing scheme that can support/accommodate large and small networks.

a. Classes of IP Addresses

Given an IP address, its class can be determined from the three high-order bits. Figure 5.30 shows the significance in the three high order bits and the range of addresses that fall into each class.

There are five different classes of an IP address, from A to E.

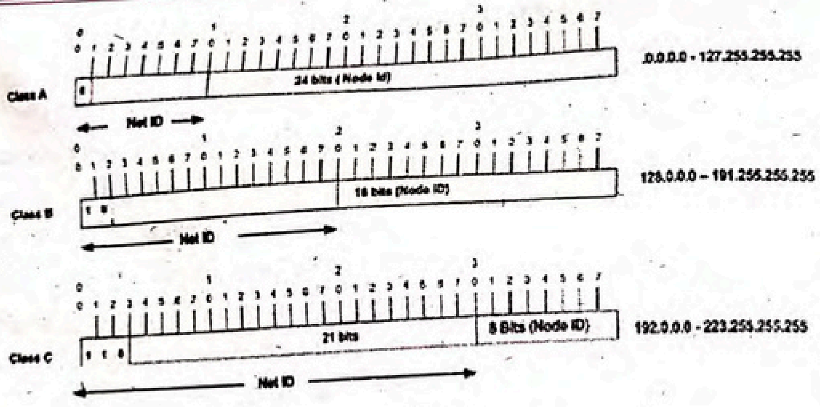


Figure 5.30 Classes of IP Addresses

Class A

Class A is used for the large networks and is implemented by large companies with many network devices. Binary address for the class A starts with 0. Its range is between 1 to 126 and the default subnet mask of this class is 255.0.0.0. Its Network part consists of 1 octet and Host part consists of 3 octets. An example of the class A is 100.10.11.1.

```
bits  0          7-8          15-16         23-24         31.
      +-----------+-------------+-------------+-------------+
      | Network   |             Host                        |
      |  Part     |             Part                        |
      +-----------+-------------+-------------+-------------+
```

1 Octet 3 Octets

Class B

Class B addresses scheme is used for the medium sized networks. The binary address for the class B starts with 10. The range of the IP address in the class B is between 128 to 191 and the default subnet mask of this class B is 255.255.0.0. Its Network part consists of 2 octets and Host part also consists of 2 octets. An example of the class B address is 150.101.110.120. .

```
bits  0
             7-8          15-16         23-24          31
      +-----------+-------------+-------------+-------------+
      |        Network          |                           |
      |         Part            |           Host            |
      |                         |           Part            |
      +-----------+-------------+-------------+-------------+
```

2 Octets 2 Octets

150.101.110.120

Class C

Class C is used for the small networks. The binary address for the class C starts with 110. The range addresses in the class C is between 192 to 223 and the default subnet mask for this class is 255.255.255. Its Network part consists of 3 octets and Host part consists of 1 octet. An example of the Class C IP address is 210.190.100.150.

```
bits  0
             7-8          15-16         23-24          31
      +-----------+-------------+-------------+-------------+
      |                Network                |   Host      |
      |                 Part                  |   Part      |
      +-----------+-------------+-------------+-------------+
```

3 Octets 1 Octet

class

Class D

Class D is for special use for multicasting. The binary addresses for the class D starts with 1110 and the IP address ranges from 224 to 239. An example of the class D IP address is 230.150.110.11

Class E

Class E is under experimental research. The binary address can start with 1111 and the decimal can be in range from 240 to 255. An example of the class E IP address is 245.101.110.110

b. Subnet Masks

Subnet Mask indicates the network portion of an IP address. Like the IP address, the subnet mask is a dotted-decimal number. Usually all hosts within a LAN use the same subnet mask. Subnet mask is a 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host. Figure 5.31 shows default subnet masks for usable IP addresses that are mapped to the first three classes of IP addresses.

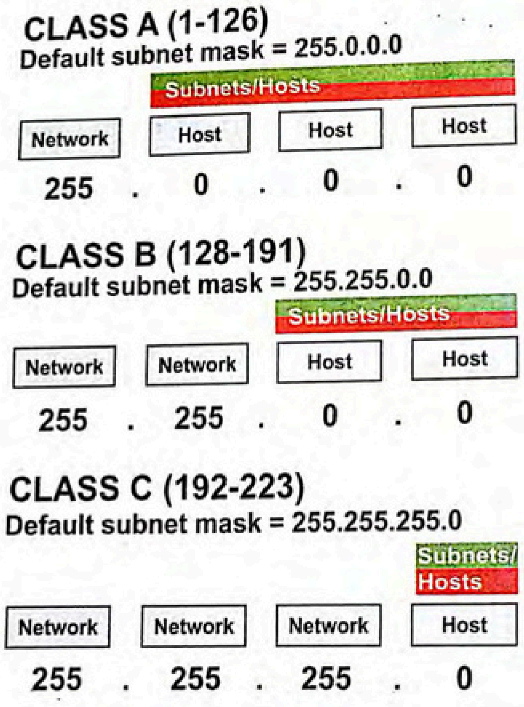


Figure 5.31 Subnet Masks

SUMMARY

- A network is a collection of independent computers or nodes that communicate with each other on a shared network medium. en
- Sender or Transmitter is a device that sends the message.
- Message is the data or information that is to be communicated.
- Medium is the physical path that message uses to travel from source to destination.

message uses +

- Receiver is the device which receives transmitted message.
- A protocol is a set of rules that governs data communications.

takes only

- In Simplex mode, the communication takes place in only one direction.
- In half-duplex mode, each station can transmit and receive data, but not at the same time.
- In Full-duplex mode, both stations can send and receive the data simultaneously
- In synchronous transmission, large volumes of information can be transmitted block-by-block or word-by-word simultaneously.
- In asynchronous transmission, data is transmitted one byte at a 'time'.
- Guided media are the physical links in which signals are confined along a narrow path.
- Unguided media also called Wireless media transports signals without using any physical conductor between the two devices communicating.

med.

- Radio wave wireless transmission medium distributes radio signals through the air over long distances such as between cities, regions, and countries, and short distances such as within an office or home.
- Micro wave is a wireless transmission technology that travels at high frequency than radio waves and provide throughput as a wireless network media.
- Infrared is a short-distance wireless transmission medium that sends signals using infrared light waves.
- A network switch or hub is a device that connects network nodes to a central location.
- Router is a device that forwards data packets across different networks.
- A gateway is a hardware device or a computer running software that allows communication between networks with dissimilar network protocols or architectures.
- Server is a powerful computer that provides centralized administration of the network and serves up the resources, such as printers and files, etc.
- Client is a network device that participates in a client/server relationship by requesting a service from a server.
- In peer-to-peer networking there are no dedicated servers or hierarchy among the computers.
- LAN (Local Area Network) is a network that connects computers and devices in a limited geographical area like home, school, and office building, etc.
- A metropolitan area network is a computer network that usually spans a city or in a large metropolitan area.

- WAN (Wide Area Network) covers large distance for communication between computers.
- A virtual private network (VPN) is a network that uses a public telecommunication infrastructure to provide remote offices or individual users with secure access to their organization's network.
- Network Topology refers to the physical layout and connectivity of computers in a network.
- In a star topology all the nodes (server, workstations, peripherals, etc.) on the network are connected directly to a centralized connectivity device called a hub, switch, or router.
- In a ring topology, every node is logically connected to two other nodes, forming a ring. Traffic flows through the entire ring until it reaches its destination.
- In the bus topology, each node (computer, server, peripheral etc.) attaches to a common cable.
- In a mesh network topology, each of the network node, computer and other devices, are interconnected with one another.
- Communication Standards provide guidelines (also called rules or protocols) to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity of networks for communication.
- OSI model defines a networking framework for implementing protocols in seven different layers.
- Application layer serves as the user interface for users and application processes to access network services.

- Presentation layer converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text).
- Session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications running on different stations.
- Transport layer handles the transparent transport of data segments between network devices.
- Network layer allows the data called packets or datagram to go from one physical network to another.
- Data link layer provides reliable transmission of data across a physical link.
- Physical layer is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium.
- TCP/IP is an industry standard suite of protocols designed for local and wide area networks.
- Packet switching is a network communication method in which the data get transmitted in blocks, regardless of type and content, called packets based on the destination address in each packet.
- Circuit switching is a scheme in which the network sets up a dedicated point-to-point connection between nodes and terminals before the communication starts, just like the nodes were already connected.
- An Internet Protocol address (IP address) is a number that is used to identify a device, for example a computer, a printer, etc. on the network.
- Subnet Mask indicates the network portion of an IP address.

EXERCISE

Q1. Select the best choice for the following MCQs.

i. A collection of two or more connected computers to share the resources and data is called a ____________.

A. Route B. Network
C. Path D. Medium

ii. In which communication mode data can be sent and received in both directions but not at the same time?

A. Simplex B. Full-duplex
C. Half-duplex D. Duplex

iii. ____________ is the data or information that is to be communicated over the network.

A. Message B. Sender
C. Medium D. Receiver

iv. ____________ is a set of rules that governs data communications.

A. Message B. Sender
C. Medium D. Protocol

v. In ____________ mode, both stations can send and receive the data simultaneously.

A. Simplex B. Full-duplex
C. Half-duplex D. Duplex

vi. In which type of transmission data is transmitted one byte at a 'time'.

A. Simplex B. Synchronous
C. Asynchronous D. Duplex

Half

vii. ______ Cable is formed of two insulated copper wires twisted together.

A. Coaxial B. Fiber Optic

C. CAT5 D. Twisted Pair

viii. Which of the following network devices is used to forward data packets across different networks?

A. Switch B. Router

B. Gateway D. Modem

ix. In ______ networking there are no dedicated servers or hierarchy among the computers.

A. Peer-to-Peer B. Server

C. LAN D. WAN

x. ______ works by using the shared public infrastructure while maintaining privacy through security procedures.

A. LAN B. WAN

C. VPN D. MAN

xi. Which of the following topology is most expensive to implement?

A. Star topology B. Bus topology

C. Ring topology D. Mesh topology

xii. How many layers does the OSI model consist of?

A. 4 B. 5

B. 8 D. 7

xiii. Which layer of OSI Model decides which physical path-way the data should take to reach the destination?

A. Data link layer B. Transport layer

C. Network layer D. Session layer

xiv. Which layer performs security, name recognition, logging and similar functions?

A. Transport layer B. Presentation layer

C. Network layer D. Session layer

xv. In ______ topology, each node (computer, server, peripheral etc.) attaches to a common cable.

A. Star B. Tree

C. Ring D. Mesh

Q2. Give short answers to the following questions.

i. Show all the modes of data communication with the help of a diagram.

ii. Differentiate between synchronous and asynchronous transmission.

iii. Differentiate between guided and unguided media.

iv. Differentiate between LAN and WAN.

v. What is OSI Model?

vi. Compare TCP/IP Model with OSI Model.

vii. Differentiate between circuit switched and packet switched networks.

viii. Briefly describe IP Addressing.

Q3. Give detailed answers to the following questions.

i. Explain various modes of data communication.

ii. What is guided media? Explain different types of guided media.

iii. Explain Radio wave and Microwave communications.

iv. Write notes on switch, router and gateway.

v. Explain in detail Client/Server and Peer-to-Peer networks.

vi. Define network topology and explain its types.

vii. Describe the seven layers of OSI Model.

viii. What is TCP/IP? Explain TCP/IP Protocol Suite.