3 Telecommunication and Networks

3.1 Introduction

Telecommunication technology is moving towards open, internetworked digital networks for voice, data, video and multimedia whose primary goal is to promote easy and secure access by business professionals and consumers to the resources of the Internet, enterprise Intranets, and inter-organizational Extranets. The major generic components of any telecommunication network are Terminals, Telecommunication processors, Communication Channels, Computers, and Telecommunication Software. Basic types of telecommunication networks include WANs and LANs which are interconnected using client/server, network computing, peer-to-peer, and Internetworking technologies.

Telecommunication processors include modems, multiplexers, internetworked processors, and various devices to help interconnect and enhance the capacity and efficiency of telecommunication channels such as twisted-pair wiring, coaxial cables, fiber-optic cables, terrestrial microwave, communications satellites, cellular and PCS systems, wireless LANs, and other wireless technologies.

3.2 Networking an Enterprise

The Internet and Internet-like networks inside the enterprise are called **Intranets;** between an enterprise and its trading partners are called **Extranets.** Managers, teams, end users, and workgroups use telecommunications networks to electronically exchange data and information anywhere in the world with other end users, customers, suppliers, and business partners.

3.3 Trends in Telecommunication

Major trends that are occurring in the field of telecommunication are as follows:

Trend	Objective
Industry Trends	Towards more competitive vendors, carriers, alliances and network services, accelerated by deregulation and the growth of Internet and WWW.
Technology Trends	Towards extensive use of Internet, digital fiber-optic, and wireless technologies to create high-speed local and global internetworks for voice, data, images, audio, and video-communications.
Business Application Trends	Towards the pervasive use of the Internet, enterprise intranets, and inter-organizational extranets to support electronic business and commerce, enterprise collaboration, and strategic advantage in local and global markets.

3.4 The Business Value of Telecommunications

Information technology, especially in telecommunication-based business applications, helps company overcome barriers to business success. The strategic capabilities of telecommunications and other information technologies include overcoming geographic, time, cost and structural barriers.

3.5 Telecommunication Network

A **Telecommunication Network** is a collection of terminal nodes, links and any intermediate nodes which are connected so as to enable telecommunication between the terminals.

3.5.1 Need and Scope of Networks

Telecommunication network allows file and resource sharing; remotely accessing of data and information via Internet; simultaneous access to the shared databases; implementation of fault tolerance over a network; providing access to the Internet for transferring the document and to access the resources.

3.5.2 Telecommunication Network Model

A simple conceptual model of a telecommunication network consists of five basic categories of components:

Terminals	Any input or output device such as Video Terminals, Microcomputers, Telephones, Office Equipment, Telephone and Transaction Terminals that are used to transmit or receive data.
Telecommunication Processors	Support data transmission and reception between terminals and computers by providing a variety of control and support functions. They include Network Interface Card, MODEM, Multiplexer and Internetworked Processors (such as switch, router, hub, bridge, repeater and gateway).
Telecommunication Media / Channels	These connect the message source with the message receiver by means of Guided/Bound Media (Twisted Pair, Coaxial cable and Fiber optics) or Unguided/Unbound media (Terrestrial Microwaves, Radio waves, Micro Waves, Infrared Waves and Communication Satellites).
Computers	Computers of all sizes and types connected through media to perform their communication assignments and include Host Computers, Front-End Processors and Network Servers.
Telecommunication Control Software	Consists of programs that control and manage the functions of telecommunication networks and include Telecommunication Monitors, Network Operating Systems, Network Management Components and Communication Packages.

3.6 Classification of Telecommunication Networks

On the basis of different factors, telecommunication networks can be classified as follows:

- **Area Coverage Based:** LAN, MAN and WAN.
- **Functional Based:** Client-Server, Peer-to-Peer and Multi-Tier.
- **Ownership Based:** Public Network, Private Network and Virtual Private Network (VPN).

3.6.1 Area Coverage Based Classification

Local Area Network (LAN)	Metropolitan Area Network (MAN)	Wide Area Network (WAN)
It is a group of computers and other network devices which are connected together. These cover manufacturing plant, classrooms, buildings etc.	It is a larger network of computers and other network devices which are connected together and usually spans several buildings of large geographical area. Cable television is an example of MAN.	It is a group of computers and other network devices which are connected together and is not restricted to a geographical location. Internet is a WAN.
All the devices that are part of LAN are within a building or multiple building spanned over limited space.	All the devices that are part of MAN are span across buildings or small town.	All the devices that are part of WAN have no geographical boundaries.
LAN has very high speed mainly due to proximity of computer and network devices.	MAN has lower speed as compared to LAN.	WAN speed varies based on geographical location of the servers. WAN connects several LANs.
LAN connection speeds can be 10Mbps; 100Mbps or 1000Mpbs also.	MAN connection speeds can be 10Mbps or 100Mbps.	WAN connection speeds can be 10 Mbps or 100 Mbps.
LAN uses Guided Media.	MAN uses both Guided Media and Unguided media.	WAN uses Guided Media and Unguided media both.

3.6.2 Functional Based Classification

Client Server Network (C/S)	It is a computer network in which one centralized powerful computer (called Server) is connected to many less powerful PCs or workstations (called Clients). The clients run programs and access data that are stored on the server. Example – WWW/e-Mail.
Peer-to-Peer Network (P2P)	It is a network which is created with two or more PCs connected together and share resources without going through a separate server computer. Example – Napster, Freenet etc.
Multi-Tier Architecture	A tier is a distinct part of hardware or software.
♦ **Single Tier Systems/One-Tier Architecture**	Consists of a single computer that contains a database and a front-end (GUI) to access the database. There is one computer which stores all of the company's data on a single database.
♦ **Two Tier Systems/Two Tier Architecture**	Consists of a client and a server. The database is stored on the server, and the interface used to access the database is installed on the client.
♦ **n-Tier Architecture (Three tier)**	It is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms.

3.6.3 Ownership Based Classification

Public Data Network	It is defined as a network shared and accessed by users not belonging to a single organization. Example – Internet.
Private Data Network	It provides businesses, government agencies and organizations of all sizes as a dedicated network to continuously receive and transmit data critical to both the daily operations and mission critical needs of an organization.
Virtual Private Network	It is a private network that uses a public network (usually the Internet) to connect remote sites or users together.

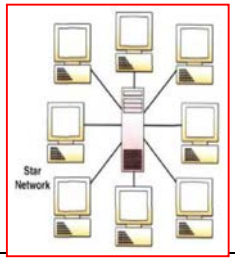
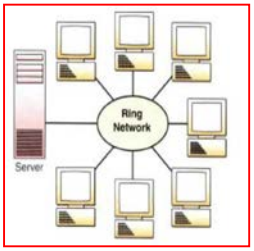
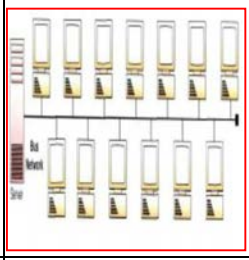
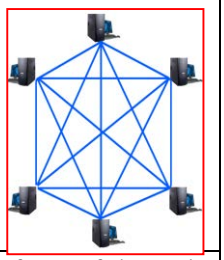
3.7 Network Computing

The network computing concept considers networks as the central computing resource of any computing environment. Features of network computing model include User Interface; System and Application Software; Databases and Database Management. Two basic network computing models are as follows:

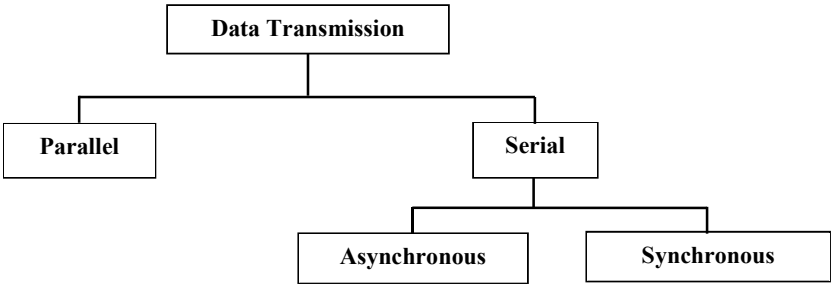
- **Centralized Computing:** Centralized computing is computing done at a central location, using terminals that are attached to a central computer. The computer itself may control all the peripherals directly (if they are physically connected to the central computer) or they may be attached via a terminal server.
- **Decentralized Computing:** Decentralized computing is the allocation of resources, both hardware and software, to each individual workstation, or office location which are capable of running independently of each other. Decentralized systems enable file sharing and all computers can share peripherals such as printers and scanners as well as modems, allowing all the computers in the network to connect to the Internet.

3.7.1 Network Topology

The term 'Topology' defines the physical or logical arrangement of links in a network.

Star Network	Ring Network	Bus Network	Mesh Network
The central unit (server) in the network acts as the traffic controller among all the other computers tied to it.	Local computer processors are tied together sequentially in a ring with each device being connected to two other devices under a decentralized approach.	A single length of wire, cable, or optical fiber connects a number of computers.	Each node is connected by a dedicated point to point link to every node.
			
A node failure does not bring down the entire network. Failure of server affects the whole network.	Failure of one computer on the network can affect the whole network.	If one of the microcomputer fails, it will not affect the entire network.	If one of the node fails, the network traffic can be redirected to another node.
New nodes can be added easily without affecting rest of the network.	Ring topology is considered to be inefficient as data can only travel in one route to reach its destination, and the data usually travels to several points prior to reaching its intended destination.	It is easy to install, easily extendable and inexpensive.	A mesh topology is the best choice when we require fault tolerance, however, it is very difficult to setup and maintain.

3.7.2 Digital Data Transmission



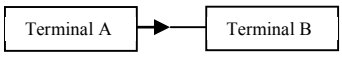
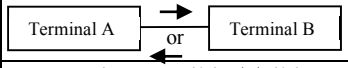
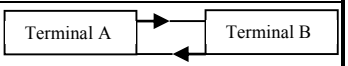
A. Serial versus Parallel Mode: Depends on number of bits sent simultaneously.

- **Serial Transmission –** Data bits are transmitted serially one after another over a single wire, and thus relatively slower.
- **Parallel Transmission –** Data bits are transmitted simultaneously over eight different wires and thus relatively faster.

The two ways of transmitting serial binary data – Asynchronous and Synchronous

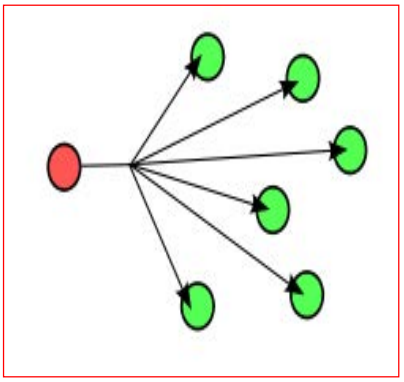
- **Asynchronous Transmission –** In this, each character is sent at irregular intervals in time as in the case of characters entered at the keyboard in real time. So, the sender provides a synchronization signal to the receiver before starting the transfer of each message.
- **Synchronous Transmission –** In this, the transmitter and receiver are paced by the same clock. The receiver continuously receives (even when no bits are transmitted) the information at the same rate the transmitter sends it.

B. Transmission Mode: The direction of signal flow **– Simplex, Half-Duplex and Full Duplex Connection.**

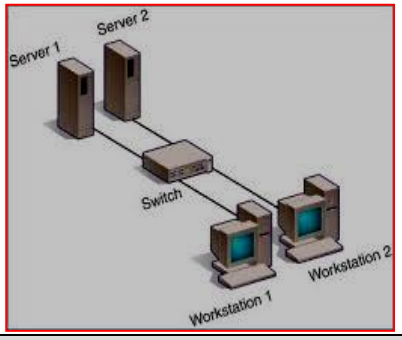
Simplex Connection	Half -Duplex Connection	Full Duplex Connection
Data flows in only one direction.	Data flows in one direction or the other, but not both at the same time.	Data flows in both directions simultaneously.
		
Example – Data from user's computer to the printer or from the mouse to user's computer.	Example – Walkie-Talkie.	Example – Mobile Phones.

C. Transmission Techniques – Based on the techniques used to transfer data, communication networks can be categorized into **Broadcast** and **Switched networks**.

- **Broadcast Networks -** In Broadcast networks, data transmitted by one node is received by many, sometimes all, of the other nodes. This refers to a method of transferring a message to all recipients simultaneously. For example – a corporation or other voluntary association that provides live television or recorded content such as movies, newscasts, sports, public affairs programming, and other television programs for broadcast over a group of radio stations or television stations.



- **Switched Networks -** In switched-communication networks, however, the data transferred from source to destination is routed through the switch nodes. The way in which the nodes switch data from one link to another, as it is transmitted from source to destination node, is referred to as a switching technique. Three common switching techniques are **Circuit Switching, Packet Switching, and Message Switching**.



3.7.3 Network Architectures and Protocols

Network Architecture: Network Architecture refers to the layout of the network, consisting of the hardware, software, connectivity, communication protocols and mode of transmission, such as wired or wireless.

Protocol: A protocol is the formal set of rules for communicating, including rules for timing of message exchanges, the type of electrical connection used by the communications devices, error detection techniques, means of gaining access to communications channels, and so on. A protocol defines the following three aspects of digital communication.

(a) Syntax: The format of data being exchanged, character set used, type of error correction used, type of encoding scheme (e.g., signal levels) being used.

(b) Semantics: Type and order of messages used to ensure reliable and error free information transfer.

(c) Timing: Defines data rate selection and correct timing for various events during data transfer.

Relationship between layers of TCP/IP and OSI Model is shown below:

TCP/IP	The OSI Model	Functions
Application or Process Layer	Application Layer	Provides communications services for end user applications
	Presentation Layer	Provides appropriate data transmission formats and codes
	Session Layer	Supports the accomplishment of telecommunication sessions
Host-to-Host Transport Layer	Transport Layer	Supports the organization and transfer of data between nodes in the network
Internet Protocol (IP)	Network Layer	Provides appropriate routing by establishing connections among network links
Network Interface	Data Link Layer	Supports error-free organization and transmission of data in the network
Physical Layer	Physical Layer	Provides physical transmission of data on the telecommunication media in the network

3.8 Network Risks, Controls and Security

The basic objective for providing network security is to safeguard assets and to ensure and maintain the data integrity. There are two types of systems security – **Physical Security** and **Logical Security**.

- A **Physical Security** is implemented to protect the physical systems assets of an organization like the personnel, hardware, facilities, supplies and documentation.
- A **Logical Security** is intended to control malicious and non-malicious threats to physical security and malicious threats to logical security itself.

3.8.1 Threats and Vulnerabilities

Threat: In context of computer networks, a T**hreat** is a possible danger that can disrupt the operation, functioning, integrity, or availability of a network or system. Network security threats can be categorized into four broad themes – **Unstructured threats, Structured threats, External threats** and **Internal threats**.

Vulnerability: Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat. Software Bugs, Timing Windows, Insecure default configurations, trusting untrustworthy information and end-users are some of the facts responsible for occurrence of vulnerabilities in the software.

3.8.2 Level of Security

A security program is a series of ongoing, regular and periodic review of controls exercised to ensure safeguarding of assets and maintenance of data integrity and involve certain steps.

3.8.3 Network Security

Network Security Protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data by implementing cryptography and encryption techniques. Network security protocols generally implement Digital Signatures, Cryptography and Encryption Techniques.

(a) Privacy: This means that the sender and the receiver expect confidentiality. The transmitted message should make sense to only the intended receiver and the message should be unintelligible to unauthorized users and is achieved by cryptography and encryption techniques.

- **Cryptography:** "Crypto" stands for "hidden, secret", and "graphy" denotes "a process or form of drawing, writing, representing, recording, describing, etc., or an art or science concerned with such a process."
- **Encryption:** In Cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but only authorized parties can. The two basic approaches to encryption are **Hardware encryption** and **Software encryption**.

(b) Authentication: This means that the receiver is sure of the sender's identity and that an imposter has not sent the message.

(c) Integrity: Ensures that the data must arrive at the receiver exactly as it was sent.

(d) Non-Repudiation: Ensures that a receiver must be able to prove that a received message came from a specific sender and the sender must not be able to deny sending it.

3.8.4 Network Security Protocols

Some of the popular network security protocols include **Secure Shell (SSH), Secure File Transfer Protocol (SFTP), HyperText Transfer Protocol Secure (HTTPS)** and **Secure Socket Layer (SSL)** etc.

3.8.5 Network Security Techniques

Several tools/technologies are now available to protect information and systems against compromise, intrusion, or misuse. **Firewall, Intrusion Detection System (IDS), Network Access Control, Anti – malware** and **site blocking** are some of them.

3.9 Network Administration and Management

In computer networks, **Network Management** refers to the activities, methods, procedures, and tools that pertain to the **Operation, Administration, Maintenance, and Provisioning** of networked systems. The common characteristics of network management are **FCAPS** - **Fault, Configuration, Accounting, Performance and Security**

3.10 The Internet Revolution

The Internet is the largest "network of networks" today, and the closest model we have to the information superhighway of tomorrow. Internet includes strategic capabilities that overcome geographic, time, cost and structural barriers along with their business applications.

3.10.1 Networks and the Internet

A computer network is two or more computers linked together to share information and/or resources. There are several types of computers networks, but the types most important to the topic of accounting information systems are Local Area Network (LAN), the Internet, Extranet, and Intranet.

3.10.2 Internet Architecture

(a) To join the Internet, the computer is connected to an Internet Service Provider (ISP) from whom the user purchases Internet access or connectivity.

(b) ISP's architecture is made up of long-distance transmission lines that interconnect routers at Point of Presence (POP) in different cities that the ISPs serve. This equipment is called the backbone of the ISP.

(c) ISPs connect their networks to exchange traffic at IXPs (Internet eXchange Points). The connected ISPs are said to peer with each other.

(d) The path a packet takes through Internet depends on the peering choices of the ISPs.

3.10.3 Internet Applications

Email, e-Commerce, electronic discussion forums, real-time conversations, search engines, downloading software and information files are some of the Internet applications.

3.10.4 Business Use of the Internet

Some of the business uses of the Internet include providing customer and vendor support, marketing, sales, and customer service applications, growth of cross-functional business applications, collaboration among business partners, e-commerce and attracting new customers with innovative marketing and products.

3.10.5 Intranet

An **Intranet** is a network inside an organization that uses Internet technologies such as web browsers and servers, TCP/IP network protocols. An Intranet is protected by security measures such as passwords, encryption, and firewalls, and thus can be accessed by authorized users through the Internet.

3.10.6 Extranets

Extranets are network links that use Internet technologies to interconnect the Intranet of a business with the Intranets of its customers, suppliers, or other business partners. Companies can use Extranets to establish direct private network links between themselves, or create private secure Internet links between them.

3.10.7 Information Systems and Telecommunication

Telecommunications give an organization the capability to move information rapidly between distant locations and to provide the ability for the employees, customers, and suppliers to collaborate from anywhere, combined with the capability to bring processing power to the point of the application.

3.11 Electronic Commerce

Electronic Commerce refers to the use of technology to enhance the processing of commercial transactions between a company, its customers and its business partners. It involves the automation of a variety of business-to-business and business-to-consumer transactions through reliable and secure connections.

3.11.1 Benefits of e-Commerce Application and Implementation

E-Commerce presents immense benefits to individual organizations, consumers, and society as a whole. Reduction in advertising costs, errors, time, and overhead cost to buyers, and reduction in time to complete business transactions are some of the major benefits of e-Commerce transactions.

3.11.2 Risks involved in e-Commerce

Problem of anonymity, repudiation of contract, lack of authenticity of transactions, data loss or theft or duplication, attack from hackers, denial of service are some of the risks that are associated with e-Commerce.

3.11.3 Types of e-Commerce

The general classes of e-Commerce applications are as follows:

(a) **Business-to-Business (B2B) e-Commerce –** This refers to the exchange of services, information and/or products from one business to another.

(b) **Business-to-Consumer (B2C) e-Commerce -** This is defined as the exchange of services, information and/or products from a business to a consumer, as opposed to between one business and another.

(c) **Consumer-to-Business (C2B) e-Commerce -** Consumers directly contact with business vendors by posting their project work online so that the needy companies review it and contact the consumer directly with bid.

(d) **Consumer-to-Consumer (C2C) e-Commerce –** It is an Internet-facilitated form of commerce that has existed for the span of history in the form of barter, flea markets, swap meets, yard sales and the like.

(e) **Business-to-Government (B2G) e-Commerce -** This refers to the use of information and communication technologies to build and strengthen relationships between government and employees, citizens, businesses, non-profit organizations, and other government agencies.

(f) **Business-to-Employee (B2E) e-Commerce -** This provides the means for a business to offer online products and services to its employees.

3.11.4 Key aspects to be considered in implementing e-Commerce

Successful implementation of e-Commerce requires involvement of key stakeholders and should ideally include representatives from accounting/ finance, internal audit, IT security, telecommunication, end users, system analysts, and legal.

3.12 Mobile Commerce

Mobile Commerce or m-Commerce is about the explosion of applications and services that are becoming accessible from Internet-enabled mobile devices. It is buying and selling of goods and services through wireless handheld devices such as cellular telephone and PDAs.

3.13 Electronic Fund Transfer

Electronic Funds Transfer (EFT) represents the way the business can receive direct deposit of all payments from the financial institution to the company bank account. Once the user "Signs Up", money comes to him directly and sooner than ever before. Some examples of EFT systems in operation are Automated Teller Machines (ATMs), Point-of-Sale (PoS) Transactions, Preauthorized and Telephone Transfers.

Question 1

Define the following terms briefly:

(a) Network Interface Card (NIC)
(b) MODEM
(c) Multiplexer
(d) Internetwork Processors
(e) Switch
(f) Router
(g) Hub
(h) Bridge
(i) Repeater
(j) Gateway
(k) Server
(l) Protocol

Answer

(a) Network Interface Card (NIC) – Network Interface Card (NIC) is a computer hardware component that connects a computer to a computer network. It has additional memory for buffering incoming and outgoing data packets, thus improving the network throughput.

(b) MODEM – A MODEM is a device that converts a digital computer signal into an analog telephone signal (i.e. it modulates the signal) and converts an analog telephone signal into a digital computer signal (i.e. it demodulates the signal) in a data communication system.

(c) Multiplexer – A multiplexer is a communication processor that allows a single communication channel to carry simultaneous data transmissions from many terminals. A multiplexer merges the transmission of several terminals at one end of a communication channel while a similar unit separates the individual transmissions at the receiving end.

(d) Internetwork Processors – Telecommunication networks are interconnected by special-purpose communication processors called internetwork processors such as switches, routers, hubs, bridges, repeaters and gateways.

(e) Switch – Switch is a communication processor that makes connections between telecommunication circuits in a network so that a telecommunication message can reach its intended destination.

(f) Router – Router is a communication processor that interconnects networks based on different rules or protocols, so that a telecommunication message can be routed to its destination.

(g) Hub – Hub is a port-switching communication processor. This allows for the sharing of the network resources such as servers, LAN workstations, printers, etc.

(h) Bridge – Bridge is a communication processor that connects number of Local Area Networks (LAN). It magnifies the data transmission signal while passing data from one LAN to another.

(i) Repeater – Repeater is a communication processor that boosts or amplifies the signal before passing it to the next section of cable in a network.

(j) Gateway – Gateway is a communication processor that connects networks and use different communication architectures.

(k) Server – A server is one or more multi-user processors with shared memory providing computing, connectivity and the database services and the interfaces relevant to the business need.

(l) Protocol – A protocol is the formal set of rules for communicating, including rules for timing of message exchanges, the type of electrical connection used by the communications devices, error detection techniques, means of gaining access to communications channels, and so on.

Question 2

Differentiate between the following:

(a) Guided Media and Unguided Media

(b) Client Server Network and Peer-to-Peer Network

(c) Serial Transmission and Parallel Transmission

(d) Synchronous Transmission and Asynchronous Transmission

Answer

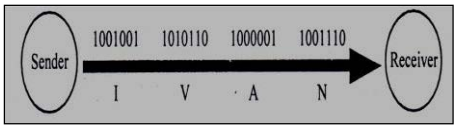
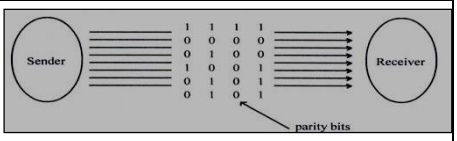
(a) The differences between Guided Media and Unguided Media are given below:

Guided Media	Unguided Media
Guided Media are those media that provide a conduit from one device to another.	Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path.
Guided Transmission Media uses a "cabling" system that guides the data signals along a specific path.	It passes through a vacuum; it is independent of a physical pathway.
Example – Coaxial Cable, Twisted Pair, Fiber Optic Cable.	Example – Infrared Waves, Micro Waves, Radio Waves etc.

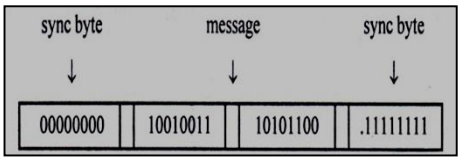
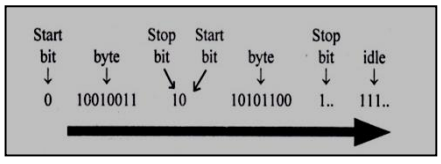
(b) The differences between Client Server Network and Peer-to-Peer Network are given below:

Client Server Network	Peer-to-Peer Network
A client computer typically communicates only with servers, not with other clients.	Every computer is equal and can communicate with any other computer on the network to which it has been granted access rights.
A central server handles all security and file transactions.	Each machine shares its own resources and handles its own security.
It is more expensive as it requires a central file server, server software and client licenses.	It is relatively less expensive as it does not require a dedicated machine, server software or special client licenses.
More secure.	Lesser secure as the network control is handed to the end-users.
Backup is centralized on the server; managed by network administrator. Backup by device and media only required at server.	Backup is decentralized; managed by users. Backup devices and media are required at each workstation.
The performance is relatively high as the server is dedicated and does not handle other tasks.	The performance is relatively low.
In case of failure of server, the whole network fails.	No single point of failure in the network.
C/S model relies on the power and stability of a single computer i.e. Server.	P2P gives each workstation equivalent capabilities and relies heavily on the power and bandwidth of each individual computer.
Example - Email, network printing, and the World Wide Web.	Example - Napster, Gnutella, Freenet, BitTorrent and Skype.

(c) The differences between Serial Transmission and Parallel Transmission are given below:

Serial Transmission	Parallel Transmission
In this, the data bits are transmitted serially one after another.	In this, the data bits are transmitted simultaneously.
Data is transmitted over a single wire and is thus relatively slower.	Data is transmitted over eight different wires and is thus relatively faster.
It is a cheaper mode of transferring data.	It is relatively expensive mode of transferring data.
	
It is useful for long distance data transmissions.	Not practical for long distance communications.

(d) The differences between Synchronous Transmission and Asynchronous Transmission are given below:

Synchronous Transmission	Asynchronous Transmission
Allows characters to be sent down the line without Start-Stop bits.	Each data word is accompanied with start and stop bits.
Transmission is faster as in absence of Start and Stop bits, many data words can be transmitted per second.	Extra Start and Stop bits slow down the transmission process relatively.
The synchronous device is more expensive to build as it must be smart enough to differentiate between the actual data and the special synchronous characters.	It is relatively cheaper.
Chances of data loss are relatively higher.	More reliable as the start and stop bits ensure that the sender and the receiver remain in step with one another.
It is more efficient.	It is relatively less efficient.
	

Question 3

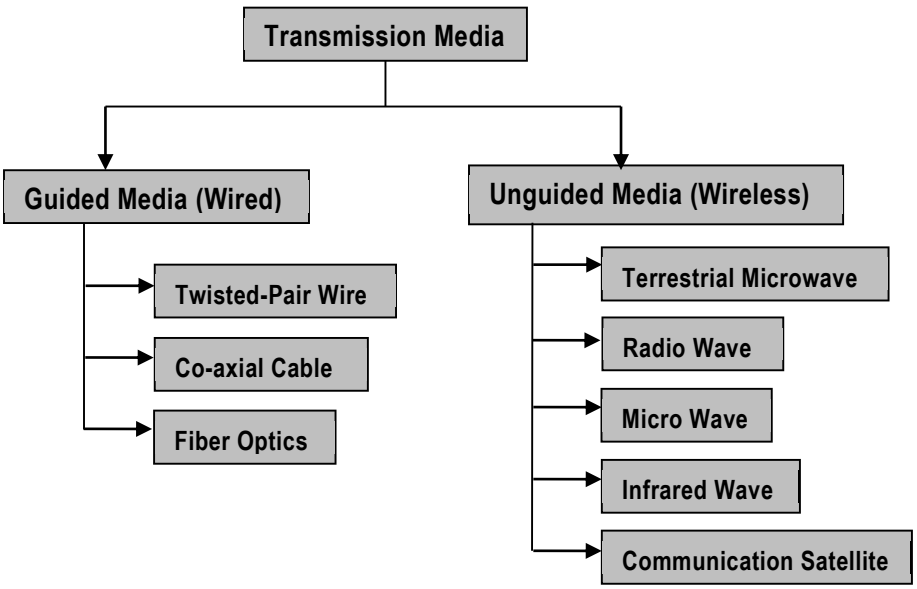
Discuss Transmission Media in detail.

Answer

Transmission Media connects the message source with the message receiver by means of Guided or Unguided Media.

Guided Media/Bound Media: Guided Transmission Media uses a "cabling" system that guides the data signals along a specific path. Some of the common examples of guided media are Twisted Pair, Coaxial cable and Fiber optics.

- **Twisted-Pair Wire:** Twisted-pair is ordinary telephone wire, consisting of copper wire twisted into pairs. It is the most widely used media for telecommunications and is used for both voice and data transmissions. It is used extensively in home and office telephone systems and many LANs and WANs.
- **Coaxial Cable:** This telecommunication media consists of copper or aluminum wire wrapped with spacers to insulate and protect it. Coaxial cables can carry a large volume of data and allows high-speed data transmission used in high-service metropolitan areas for cable TV systems, and for short-distance connection of computers and peripheral devices. It is used extensively in office buildings and other work sites for local area networks.
- **Fiber Optics:** This media consists of one or more hair-thin filaments of glass fiber wrapped in a protective jacket. Signals are converted to light form and fired by laser in bursts. Optical fibers can carry digital as well as analog signals and provides increased speed and greater carrying capacity than coaxial cable and twisted-pair lines.



Unguided Media/Unbound Media: Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not

bound to a cabling media. Some of the common examples of unguided media are Terrestrial Microwave, Radio Waves, Micro Waves, Infrared Waves and Communication Satellites.

- **Terrestrial Microwave:** Terrestrial microwave media uses the atmosphere as the medium through which to transmit signals and is used extensively for high-volume as well as long-distance communication of both data and voice in the form of electromagnetic waves.
- **Radio Waves:** Radio waves are an invisible form of electromagnetic radiation that varies in wavelength from around a millimeter to 100,000 km, making it one of the widest ranges in the electromagnetic spectrum. Radio waves are most commonly used transmission media in the wireless Local Area Networks.
- **Micro Waves:** Microwaves are radio waves with wavelengths ranging from as long as one meter to as short as one millimeter, or equivalently, with frequencies between 300 MHz (0.3 GHz) and 300 GHz. These are used for communication, radar systems, radio astronomy, navigation and spectroscopy.
- **Infrared Waves:** Infrared light is used in industrial, scientific, and medical applications. Night-vision devices using infrared illumination allow people or animals to be observed without the observer being detected.
- **Communication Satellites:** Communication satellites use the atmosphere (microwave radio waves) as the medium through which to transmit signals. A satellite is some solar-powered electronic device that receives, amplifies, and retransmits signals; the satellite acts as a relay station between satellite transmissions stations on the ground (earth stations). They are used extensively for high-volume as well as long-distance communication of both data and voice.

Question 4

How can Client Computers be classified?

Answer

Client Computers can be classified as **Fat Client, Thin Client or Hybrid Client**.

(i) **Fat / Thick Client:** A Fat Client or Thick Client is a client that performs the bulk of any data processing operations itself, and does not necessarily rely on the server. Thick clients do not rely on a central processing server because the processing is done locally on the user system, and the server is accessed primarily for storage purposes. For that reason, thick clients often are not well-suited for public environments. To maintain a thick client, IT needs to maintain all systems for software deployment and upgrades, rather than just maintaining the applications on the server. For example – Personal Computer.

(ii) **Thin Client:** A Thin Client use the resources of the host computer. A thin client generally only presents processed data provided by an application server, which performs the bulk of any required data processing. A thin client machine is going to communicate with a central processing server, meaning there is little hardware and software installed on the user's machine. A device using web application (such as Office Web Apps) is a thin client.

(iii) **Hybrid Client:** A Hybrid Client is a mixture of the above two client models. Similar to a fat client, it processes locally, but relies on the server for storing persistent data. This approach offers features from both the fat client (multimedia support, high performance) and the thin client (high manageability, flexibility). Hybrid clients are well suited for video gaming.

Question 5

Discuss some of the characteristics and issues of Client Server (C/S) architecture.

Answer

Some of the prominent characteristics of C/S architecture are as follows:

- **Service:** C/S provides a clean separation of function based on the idea of service. The server process is a provider of services and the client is a consumer of services.
- **Shared Resources:** A server can service many clients at the same time and regulate their access to the shared resources.
- **Transparency of Location:** C/S software usually masks the location of the server from the clients by redirecting the service calls when needed.
- **Mix-and-Match:** The ideal C/S software is independent of hardware or Operating System software platforms.
- **Scalability:** In a C/S environment, client workstations can either be added or removed and also the server load can be distributed across multiple servers.
- **Integrity:** The server code and server data is centrally managed, which results in cheaper maintenance and the guarding of shared data integrity. At the same time, the clients remain personal and independent.

Issues in Client/Server Network

(i) When the server goes down or crashes, all the computers connected to it become unavailable to use.

(ii) Simultaneous access to data and services by the user takes little more time for server to process the task.

Question 6

Discuss advantages and disadvantages of following:

(a) Peer-to-Peer Network
(b) Single Tier Systems
(c) Two Tier Systems
(d) Three Tier Systems
(e) Centralized Computing
(f) Decentralized Computing
(g) Star Topology
(h) Ring Topology
(i) Bus Topology
(j) Mesh Topology

Answer

(a) Peer-to-Peer Network

Advantages: Following are the major advantages of Peer-to-Peer networks:

(i) Peer-to-Peer Networks are easy and simple to set up and only require a Hub or a Switch to connect all the computers together.

(ii) It is very simple and cost effective.

(iii) If one computer fails to work, all other computers connected to it continue to work.

Disadvantages: The major disadvantages of peer-to-peer networks are as below:

(i) There can be a problem in accessing files if computers are not connected properly.

(ii) It does not support connections with too many computers as the performance gets degraded in case of high network size.

(iii) The data security is very poor in this architecture.

(b) Single Tier Systems

Advantages: A single-tier system requires only one stand-alone computer. It also requires only one installation of proprietary software which makes it the most cost-effective system available.

Disadvantages: It can be used by only one user at a time. A single tier system is impractical for an organization which requires two or more users to interact with the organizational data stores at the same time.

(c) Two Tier Systems

The advantages of Two-Tier systems are as follows:

- The system performance is higher because business logic and database are physically close.
- Since processing is shared between the client and server; more users could interact with system.
- By having simple structure, it is easy to setup and maintain entire system smoothly.

The disadvantages of Two-Tier systems are as follows:

- Performance deteriorates if number of users increases.
- There is restricted flexibility and choice of DBMS since data language used in server is proprietary to each vendor.

(d) Three Tier Systems

The following are the advantages of Three-Tier systems:

- **Clear separation of user-interface-control and data presentation from**

application-logic: Through this separation, more clients are able to have access to a wide variety of server applications. The two main advantages for client-applications are quicker development through the reuse of pre-built business-logic components and a shorter test phase.

- **Dynamic load balancing:** If bottlenecks in terms of performance occur, the server process can be moved to other servers at runtime.
- **Change management:** It is easy and faster to exchange a component on the server than to furnish numerous PCs with new program versions.

The disadvantages of Three-Tier systems are as below:

- It creates an increased need for network traffic management, server load balancing, and fault tolerance.
- Current tools are relatively immature and are more complex.
- Maintenance tools are currently inadequate for maintaining server libraries.

(e) Centralized Computing

Advantages are as follows:

- **Ease of management** – There are relatively few computers to manage;
- **Enhanced security** – The physical and logical securing of the computing environment can be more easily managed since there is only one location and a few computers;
- **Ease of control** – The introduction of change can be managed closely since there is only one location and a few computers;
- **Reduced cost of ownership** – Fewer computing elements to manage and therefore few people needed to manage them;
- **Multiple types of workload** – All of the work associated with the business runs at the central computing location.

Disadvantages are as follows:

- The central computer performs the computing functions and controls the remote terminals. In case of failure of central computer, the entire system will go down.
- Central computing relies heavily on the quality of administration and resources provided to its users. Empowerment of the central computer should be adequate by all means, else the usage suffers greatly.

(f) Decentralized Computing

Advantages are as follows:

- A decentralized system utilizes the potential of desktop systems to maximize the potential performance of the business applications.

Disadvantages are as follows:

- All computers have to be updated individually with new software, unlike a centralized computer system.

(g) Star Topology

Advantages are as follows:

- Several users can use the central unit at the same time.
- It is easy to add new nodes and remove existing nodes.
- A node failure does not bring down the entire network.
- It is easier to diagnose network problems through a central hub.

Disadvantages are as follows:

- The whole network is affected if the main unit "goes down," and all communications stop. If it fails, there is no backup processing and communications capability and the local computers will be cut off from the corporate headquarters and from each other.
- Cost of cabling the central system and the points of the star network together are very high.

(h) Ring Topology

Advantages are as follows:

- Ring networks neither require a central computer to control activity nor does it need a file server.
- Each computer connected to the network can communicate directly with the other computers in the network by using the common communication channel, and each computer does its own independent applications processing.
- The ring network is not as susceptible to breakdowns as the star network, because when one computer in the ring fails, it does not necessarily affect the processing or communications capabilities of the other computers in the ring.
- Ring networks offer high performance for a small number of workstations or for larger networks where each station has a similar workload.
- Ring networks can span longer distances than other types of networks.
- Ring networks are easily extendable.

Disadvantages are as follows:

- Relatively expensive and difficult to install.
- Failure of one computer on the network can affect the whole network.

- It is difficult to troubleshoot a ring network.
- Adding or removing computers can disrupt the network.

(i) Bus Topology

Advantages are as follows:

- There is no host computer or file server which makes bus network reliable as well as easy to use and understand.
- If one of the microcomputers fails, it will not affect the entire network.
- Requires the least amount of cable to connect the computers together and therefore is less expensive than other cabling arrangements.
- Is easy to extend. Two cables can be easily joined with a connector, making a longer cable for more computers to join the network.
- A repeater can also be used to extend a bus configuration.

Disadvantages are as follows:

- Heavy network traffic can slow a bus considerably since any computer can transmit at any time.
- Each connection between two cables weakens the electrical signal.
- The bus configuration can be difficult to troubleshoot. A cable break or malfunctioning computer can be difficult to find and can cause the whole network to stop functioning.

(j) Mesh Topology

Advantages are as follows:

- Yields the greatest amount of redundancy in the event that if one of the nodes fails, the network traffic can be redirected to another node.
- Network problems are easier to diagnose.

Disadvantages are as follows:

- Installation and maintenance cost is very high as more cable is required in Mesh Topology.

Question 7

Discuss the common Switching techniques used in computer networking.

Answer

The common switching techniques used in computer networking are – **Circuit switching, Packet Switching and Message Switching.**

- **Circuit Switching:** When two nodes communicate with each other over a dedicated communication path, it is called Circuit Switching. An important property of circuit switching is the need to set up an end-to-end path before any data can be sent which can either be

permanent or temporary. Applications which use circuit switching may have to go through three phases: **Establish a circuit, Transfer of data** and **Disconnect the circui**t. The bandwidth is reserved all the way from sender to receiver and all the data packets follow the same path, thus, ensuring the sequence of data packets are in order.

- **Packet Switching:** The entire message is broken down into smaller transmission units called packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store smaller size packets and they do not take much resources either on carrier path or in the switches' internal memory. In packet switched network, first packet of a multi-packet message may be forwarded before the second one has fully arrived, thus reducing delay and improving throughput. Since, there is no fixed bath, different packets can follow different path and thus they may reach to destination out of order.
- **Message Switching/ Store-and-Forward:** In message switching, no physical path is established between sender and receiver in advance. The whole message is treated as a data unit and is transferred in its entirety which contains the entire data being delivered from the source to destination node. A switch working on message switching first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits. E-mail and voice mail are examples of message switching systems.

Question 8

Explain the OSI Model of communication in detail.

Answer

OSI Model – The International Standards Organization (ISO) developed a seven-layer Open Systems Interconnection (OSI) model to serve as a standard model for network architectures. Seven layers of OSI include the following:

- **Layer 7 or Application Layer:** This layer is closest to the end user and interacts with software applications and provides user services by file transfer, file sharing, etc. At this layer, communication partners are identified; quality of service is identified; user authentication and privacy are considered; any constraints on data syntax are identified; and database concurrency and deadlock situation controls are undertaken.
- **Layer 6 or Presentation Layer:** Also, referred as **Syntax Layer**, this layer is usually a part of an operating system that 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). It further controls onscreen display of data, transforms data to a standard application interface, encryption and data compression.
- **Layer 5 or Session Layer:** This layer sets up, coordinates, and terminates conversations; exchanges and dialogs between the applications at each end. It deals with session and connection coordination and provides for full-duplex, half-duplex, or simplex operation, and

establishes check pointing, adjournment, termination, and restart procedures.

- **Layer 4 or Transport Layer:** This layer ensures reliable and transparent transfer of data between user processes; assembles and disassembles message packets and provides error recovery and flow control. Multiplexing and encryption are undertaken at this layer level.
- **Layer 3 or Network Layer:** The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer makes a choice of the physical route of transmission; creates a virtual circuit for upper layers to make them independent of data transmission and switching; establishes, maintains, terminates connections between the nodes and ensure proper routing of data.
- **Layer 2 or Data Link Layer:** The Data Link Layer responds to service requests from the Network Layer and issues service requests to the Physical Layer. This layer transfers data between adjacent network nodes in a WAN or between nodes on the same LAN segment. This layer also specifies channel access control method and ensures reliable transfer of data through the transmission medium. It provides the functional and procedural means to transfer data between network entities and detects and possibly corrects errors that may occur in the Physical Layer.
- **Layer 1 or Physical Layer:** The Physical Layer is a hardware layer which specifies mechanical features as well as electromagnetic features of the connection between the devices and the transmission. Establishment and termination of a connection to a communications medium; participation in the process whereby the communication resources are effectively shared among multiple users; and modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel are the major tasks of this layer.

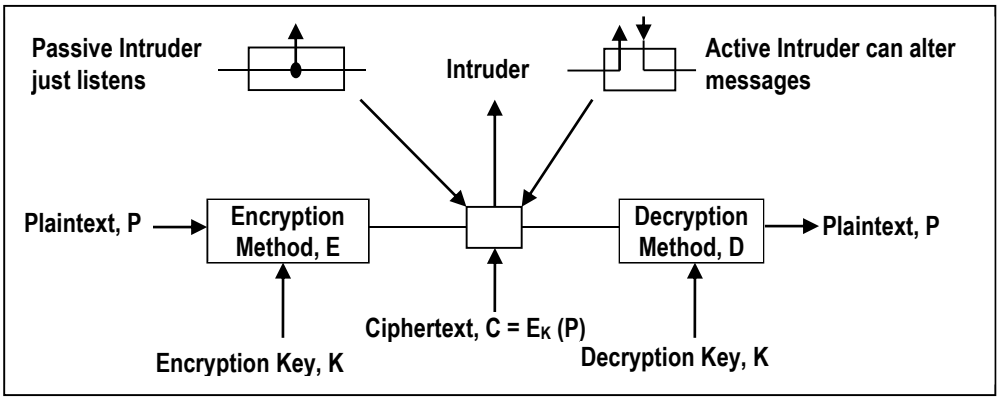
Question 9

Discuss Encryption Model in computer network.

Answer

In Cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but only authorized parties can. The Encryption Model defines the encryption of plaintext into ciphertext and decryption of ciphertext into plaintext.

- **Plaintext** is the message that is to be encrypted. It is transformed by a function that is parameterized by a key.
- **CipherText** is the output of the encryption process that is transmitted often by a messenger or radio.



Encryption Model – The intruder may hear and accurately copies down the complete ciphertext. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder). The art of breaking ciphers is known as **Cryptanalysis**, and the art of devising them (**Cryptography**) are collectively known as **Cryptology**.

Question 10

Discuss in brief, some of the popular Network Security Protocols.

Answer

Some of the popular network security protocols include **Secure Shell (SSH), Secure File Transfer Protocol (SFTP), HyperText Transfer Protocol Secure (HTTPS)** and **Secure Socket Layer (SSL)** etc.

- **SSH –** Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker cannot play back the traffic or hijack the connection when encryption is enabled. During ssh login; the entire login session including transmission of password is encrypted; therefore it is almost impossible for an outsider to collect passwords.
- **SFTP –** The SSH File Transfer Protocol (also known as Secure FTP and SFTP) is a computing network protocol for accessing and managing files on remote file systems. Unlike standard File Transfer Protocol (FTP), SFTP encrypts commands and data both, preventing passwords and sensitive information from being transmitted in the clear over a network.
- **HTTPS –** HyperText Transfer Protocol Secure (HTTPS) is a communication protocol for secure communication over a computer network with especially wide deployment on the

Internet. The security of HTTPS uses long term public and secret keys to exchange a short term session key to encrypt the data flow between client and server.

- **SSL –** It is a protocol that provides a secure channel between two machines operating over the Internet or an internal network. It is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet. In practice, SSL is used to secure online credit card transactions system logins and any sensitive information exchanged online; to secure the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange, to secure intranet based traffic such as internal networks, file sharing, extranets, and database connections etc.

Question 11

Discuss FCAPS model of network management.

Answer

FCAPS is the ISO Telecommunications Management Network model and framework for network management. It is an acronym for **Fault, Configuration, Accounting, Performance and Security.**

(i) Fault Management – A fault is an event that has a negative significance. The goal of fault management is to recognize, isolate, correct and log faults that occur in the network. Most fault management systems poll the managed objects for error conditions and present this information to the network manager. Fault management identifies and isolates network issues; proposes problem resolution; and subsequently logs the issues and associated resolutions.

(ii) Configuration Management – Monitors network and system configuration information so that the impact on network operations (hardware and software elements) can be tracked and managed. Network changes, additions, and deletions need to be coordinated with the network management personnel.

(iii) Accounting Management – Accounting management is concerned with tracking network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes. For non-billed networks, accounting refers to administration whose primary goal is to administer the set of authorized users by establishing users, passwords, and permissions and to administer the operations of the equipment such as by performing software backup and synchronization.

(iv) Performance Management – Measures and makes network performance data available so that performance can be maintained and acceptable thresholds. It enables the manager to prepare the network for the future, as well as to determine the efficiency of the current network. The network performance addresses the throughput, network response times, packet loss rates, link utilization, percentage utilization, error rates and so forth.

(v) Security Management – Controls access to network resources as established by organizational security guidelines. Most network management systems address security regarding network hardware such as someone logging into a router. Security management

functions include managing network authentication, authorization, and auditing, such that both internal and external users only have access to appropriate network resources, configuration and management of network firewalls, intrusion detection systems, and security policies (such as access lists).

Question 12

Discuss strategic capabilities of Internet along with their business applications.

Answer

The strategic capabilities of Internet include the following:

(i) **Overcome geographic barriers:** Capture information about business transactions from remote locations. This provides better customer service by reducing delay in filling orders and improves cash flow by speeding up the billing of customers. For example - Use the Internet and Extranet to transmit customer orders from travelling salespeople to a corporate data centre for order processing and inventory control.

(ii) **Overcome time barriers:** Provide information to remote locations immediately after it is requested. Credit inquiries can be made and answered in seconds. For example - Credit authorization at the point of sale using online POS networks.

(iii) **Overcome cost barriers:** Reduce the cost of more traditional means of communication. This reduces expensive business trips; allows customers, suppliers, and employees to collaborate, thus improving the quality of decisions reached. For example - Desktop videoconferencing between a company and its business partners using the Internet, Intranet and Extranet.

(iv) **Overcome structural barriers:** Support linkages for competitive advantage. Fast, convenient services lock in customers and suppliers. For example - Business-to-business electronic commerce websites for transactions with suppliers and customers using the Internet and Extranet.

Question 13

What do you understand by the term 'e-Commerce"? Discuss its benefits and risks involved.

Answer

e-Commerce is the process of doing business electronically. It refers to the use of technology to enhance the processing of commercial transactions between a company, its customers and its business partners. It involves the automation of a variety of business-to-business and business-to-consumer transactions through reliable and secure connections.

Benefits of e-Commerce Application and Implementation are as follows:

- Reduction in costs to buyers from increased competition in procurement as more suppliers are able to compete in an electronically open marketplace.

- Reduction in errors, time and overhead costs in information processing by eliminating requirements for re-entering data.
- Reduction in costs to suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.
- Reduction in time to complete business transactions, particularly from delivery to payment.
- Creation of new markets through the ability to easily and cheaply reach potential customers.
- Easier entry into new markets especially geographically remote markets for enterprises regardless of size and location.
- Better quality of goods as specifications are standardized and competition is increased and improved variety of goods through expanded markets and the ability to produce customized goods.
- Faster time to market as business processes are linked, thus enabling seamless processing and eliminating time delays.
- Optimization of resource selection as businesses form cooperative teams to increase the chances of economic successes, and to provide the customer products and capabilities more exactly meeting the requirements.
- Reduction in inventories and risk of obsolete inventories as the demand for goods and services is electronically linked through just-in-time inventory and integrated manufacturing techniques.
- Reduction in overhead costs through uniformity, automation, and large-scale integration of management processes.
- Reduction in use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects).
- Reduction in advertising costs.

Risks involved in e-Commerce are as follows:

- **Problem of anonymity:** There is need to identify and authenticate users in the virtual global market where anyone can sell to or buy from anyone, anything from anywhere.
- **Repudiation of contract:** There is possibility that the electronic transaction in the form of contract, sale order or purchase by the trading partner or customer may be denied.
- **Lack of authenticity of transactions:** The electronic documents that are produced in the course of an e-Commerce transaction may not be authentic and reliable.
- **Data Loss, Theft or Duplication:** The data transmitted over the Internet may be lost, duplicated, tampered with or replayed.
- **Attack from hackers:** Web servers used for e-Commerce may be vulnerable to hackers.

- **Denial of Service:** Service to customers may be denied due to non-availability of system as it may be affected by viruses, e-mail bombs and floods.
- **Non-recognition of electronic transactions:** e-Commerce transactions as electronic records and digital signatures may not be recognized as evidence in courts of law.
- **Lack of audit trails:** Audit trails in e-Commerce system may be lacking and the logs may be incomplete, too voluminous or easily tampered with.
- **Problem of piracy:** Intellectual property may not be adequately protected when such property is transacted through e-Commerce.

Question 14

What are the different types of e-Commerce?

Answer

The general classes of e-Commerce applications are as follows:

(i) **Business-to-Business (B2B) e-Commerce:** B2B refers to the exchange of services, information and/or products from one business to another. B2B electronic commerce typically takes the form of automated processes between trading partners and is performed in much higher volumes than Business-to-Consumer (B2C) applications. B2B can also encompass marketing activities between businesses and not just the final transactions that result from marketing.

(ii) **Business-to-Consumer (B2C) e-Commerce:** It is defined as the exchange of services, information and/or products from a business to a consumer, as opposed to between one business and another. This model saves time and money by doing business electronically but customers must be provided with safe and secure as well as easy-to-use and convenient options when it comes to paying for merchandise. This minimizes internal costs created by inefficient and ineffective supply chains and creates reduces end prices for the customers.

(iii) **Consumer-to-Business (C2B) e-Commerce:** In C2B e-Commerce model, consumers directly contact with business vendors by posting their project work online so that the needy companies review it and contact the consumer directly with bid. The consumer reviews all the bids and selects the company for further processing. Some examples are guru.com, rentacoder.com, getacoder.com, freelancer.com.

(iv) **Consumer-to-Consumer (C2C) e-Commerce:** C2C e-Commerce is an Internet-facilitated form of commerce that provides a virtual environment in which consumers can sell to one another through a third-party intermediary.

(v) **Business-to-Government (B2G) e-Commerce:** B2G e-Commerce, also known as e-Government, refers to the use of information and communication technologies to build and strengthen relationships between government and employees, citizens, businesses, non-profit organizations, and other government agencies.

(vi) **Business-to-Employee (B2E) e-Commerce:** B2E e-Commerce, from an intra-organizational perspective provides the means for a business to offer online products and services to its employees.

Question 15

Differentiate between Host Based & Network Intrusion Detection System.

Answer

Differences between Host Based Intrusion Detection System and Network Based Intrusion Detection System are as follows:

	Host Based Intrusion Detection System	Network Based Intrusion Detection System
Deterrence	Strong deterrence for insiders	Strong deterrence for outsiders
Detection	Strong insider detection, weak outsider detection	Strong outsider detection, weak insider detection
Attack Anticipation	Good at trending and detecting suspicious behavior patterns	None
Damage Assessment	Excellent for determining extent of compromise	Very weak damage assessment capabilities
Response	Weak real-time response, good for long term attacks	Strong response against outsider attacks
Scope	Narrow in scope, monitors specific activities	Broad in scope
Dependency	Host dependent	Host independent.

Question 16

Write short note on the following:

(a) Internet

(b) Intranet

(c) Extranet

(d) HTTPS

(e) Firewall

Answer

(a) Internet: The Internet is the massive global system that connects computer networks around the world together. Millions of private, public, academic, business and government networks worldwide connect with each other over the internet to share massive amounts

of information, resources and services. The Internet uses the standard Internet protocol suite (TCP/IP) to allow us to connect to each other. It has numerous information resources and services, such as the web pages of the World Wide Web (WWW), games, videos, images, e-mail, social networking, etc.

The Internet carries information from all streams; traditional, such as newspaper, book and other print publishing; and modern such as blogging and web feeds. It also enables new forms of human interactions through, instant messaging, e-mail, Internet forums, and social networking.

(b) Intranet: Intranet is an internal network used by companies to connect their computers on a network. Intranet is accessible only by the organization's members, employees, or others with authorization. A firewall surrounds an Intranet that fends off unauthorized access. The Intranet is based on TCP/IP protocol and is inaccessible from the outside. An Intranet resides behind a firewall and is accessible only to people who are members of the same company or organization.

Intranet is mainly used by corporations as it is a secure network and is much less expensive to build and manage than private networks based on proprietary protocols. Only the members of the corporation with authorized access may log on and access the network and the data on the network. Like all networks, the Intranet is mainly used to share data, information, resources, company programs, software applications, as well as facilitate communication between people or work groups within the company. Intranet improves the data sharing capability and overall knowledge base of the company's employees.

(c) Extranet: Extranet is basically an internal network that can be accessed externally. The extranet can be thought as an extension of the company's intranet. People from outside the company can have a limited access to the company's internal network for business or education related purposes. The access may be granted to the organization's partners, vendors, suppliers, current and potential customers, etc. Extranet refers to an Intranet that is partially accessible to authorized outsiders. An Extranet provides various levels of accessibility to outsiders having a valid username and password.

The Extranet requires security and privacy, so that the information on the network is not wrongly accessed or misused by external parties. In order to protect the network, the extranets can incorporate firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of virtual private networks (VPNs) that tunnel through the public network.

(d) HTTPS: HyperText Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. The security of HTTPS uses long term public and secret keys to exchange a short term session key to encrypt the data flow between client and server.

(e) Firewall: Firewall is a device that forms a barrier between a secure and an open environment when the latter environment is usually considered hostile, for example, the

Internet. It acts as a system or combination of systems that enforces a boundary between more than one networks. Access controls are common form of controls encountered in the boundary subsystem by restricting the use of system resources to authorized users, limiting the actions authorized users can take with these resources and ensuring that the users obtain only authentic system resources.

Question 17

Define Virtual Private Networks (VPN).

Answer

Virtual Private Network: It is a private network that uses a public network (usually the Internet) to connect remote sites or users together. By using a VPN, businesses ensure security – anyone intercepting the encrypted data can't read it. VPN is a secure network that uses the Internet as its main backbone network, but relies on the firewalls and other security features of the Internet and Intranet connections and those of participating organizations.

Question 18

What do you mean by threat and vulnerability? Explain any three facts responsible for occurrence of vulnerabilities in the software.

Answer

Threat: A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system.

Vulnerability: Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat.

The following facts are responsible for occurrence of vulnerabilities in the software:

- **Software Bugs** - Software bugs are so common that users have developed techniques to work around the consequences, and bugs that make saving work necessary every half an hour or crash the computer every so often are considered to be a normal part of computing. For example - buffer overflow, failure to handle exceptional conditions, access validation error, input validation errors are some of the common software flaws.
- **Timing Windows** - This problem may occur when a temporary file is exploited by an intruder to gain access to the file, overwrite important data, and use the file as a gateway for advancing further into the system.
- **Insecure default configurations** - Insecure default configurations occur when vendors use known default passwords to make it as easy as possible for consumers to set up new systems. Unfortunately, most intruders know these passwords and can access systems effortlessly.
- **Trusting Untrustworthy information** - This is usually a problem that affects routers, or those computers that connect one network to another. When routers are not programmed

to verify that they are receiving information from a unique host, bogus routers can gain access to systems and do damage.

- **End users** - Generally, users of computer systems are not professionals and are not always security conscious. For example, when the number of passwords of a user increases, user may start writing them down, in the worst case to places from where they are easy to find. In addition to this, users do human errors, for example save confidential files to places where they are not properly protected.

Question 19

How Extranets are used by Business Organization?

Answer

The Extranets can be used by business organizations in some of the following ways:

- Share product catalogs exclusively with wholesalers or those "in the trades".
- Collaborate with other companies on joint development efforts.
- Jointly develop and use training programs with other companies.
- Provide or access services provided by one company to a group of other companies; and
- Share news of common interest exclusively with partner companies.
- Establish direct private network links between themselves, or create private secure internet links between them called virtual private networks.
- Use the unsecured internet as the extranet link between its intranet and consumers and others, but rely on encryption of sensitive data and its own firewall systems to adequate security.

Question 20

Briefly explain three tiers in Three tier architecture.

Answer

The three tiers in Three-tier architecture are as follows:

- **Presentation Tier:** This tier occupies the top level, communicates with other tiers and displays information related to services available on a website.
- **Application Tier:** Also called the Middle tier, Logic tier, Business Logic or Logic tier; this tier controls application functionality by performing detailed processing.
- **Database Tier:** This tier houses the database servers where information is stored and retrieved. Data in this tier is kept independent of application servers or business logic.

Question 21

Which network topology can be used in case of Military Installations with a very small number of nodes and why it should be used? List advantages and disadvantages of such network topology.

Answer

In case of Military installations with a very small number of nodes, **Mesh Network topology** should be used.

In fully interconnected Mesh topology, each node is connected by a dedicated point to point link to every node and thus the reliability is very high which is of prime importance in any military installations. Even if one node fails, Mesh topology provides high degree of redundancy with each node connected to remaining nodes.

Advantages of mesh network are as follows:

- Mesh network topology yields the greatest amount of redundancy in the event that if one of the nodes fails, the network traffic can be redirected to another node.
- Network problems are easier to diagnose.

Disadvantage of mesh network are as follows:

- Mesh networks are not very common because of its high cost of installation and maintenance.
- More cabling is required than any other configuration.

Question 22

Mention the two categories of encryption/decryption methods. What are two basic approaches to encryption?

Answer

(a) The two categories of encryption/decryption methods are: the Secret Key Method and the Public Key Method.

- **Secret Key Method:** In Secret key encryption/decryption method, the same key is used by both sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.
- **Public Key Method:** In Public key encryption, there are two keys: a private key which is kept by the receiver and the public key which is announced to the public.

The two basic approaches to Encryption are as follows:

- **Hardware Encryption:** Hardware encryption devices are available at a reasonable cost, and can support high- speed traffic. If the Internet is being used to exchange information among branch offices or development collaborators, for instance, use of such devices can ensure that all traffic between these offices is secure.

- **Software encryption:** Software encryption is typically employed in conjunction with specific applications. Certain electronic mail packages, for example, provide encryption and decryption for message security.

Question 23

What are the key aspects to be considered in implementing e-commerce?

Answer

The key aspects to be considered in implementing e-commerce are as follows:

- Involvement of stakeholders, key trading partners, and external auditors to obtain insight into the design and deployment of e-commerce solution;
- Implementing appropriate policies, standards and guidelines;
- Performing cost benefit analysis and risk assessment to ensure value delivery;
- Implementing the right level of security across all layers and processes;
- Establishing and implementing the right level of baseline (best practice) controls;
- Integration of e-Commerce with the business process and the physical delivery channels;
- Providing adequate user training; and
- Performing post implementation review to ensure controls are working as envisaged.

Question 24

What are the characteristics of Star Network?

Answer

The characteristics of Star network are as follows:

- ***The star network, a popular network configuration, involves a central unit that has several terminals tied into it. In other words, it ties end user computers to a central computer.***
- ***The central unit in the star network acts as the traffic controller among all the other computers tied to it. The central computer is usually a mainframe (host), which acts as the file server.***
- ***A star network is well suited to companies with one large data processing facility shared by several smaller departments. Many star networks take the form of hierarchical networks with a centralized approach.***

Question 25

What is the basic objective for providing network security? Explain the major functions and services performed by the Physical Layer (Layer 1) of OSI Model of Network Architecture.

Answer

The basic objective for providing network security is two-fold –

- ***To safeguard assets, and***
- ***To ensure and maintain the data integrity. The boundary subsystem is an interface between the potential users of a system and the system itself. Controls in the boundary subsystem have the following purposes:***
- ***To establish the system, resources that the users desire to employ; and***
- ***To restrict the actions undertaken by the users who obtain the system resources to an authorized set.***

The major functions and services performed by the Physical Layer (Layer 1) of OSI Model of Network Architecture are as follows:

- ***Establishment and termination of a connection to a communications medium.***
- ***Participation in the process whereby the communication resources are effectively shared among multiple users. For example – contention, resolution and flow control.***
- ***Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.***

Question 26

What do you understand by n-tier architecture?

Answer

<u>n-tier Architecture:</u> In a client-server architecture in which presentation, application processing, and data management functions are logically separated. By segregating an application into tiers, developers acquire the option of modifying or adding a specific layer, instead of reworking on entire application. For example, an application that uses middleware to service data requests between a user and a database employs multi-tier architecture. The most widespread use of multi-tier architecture is the three-tier architecture.

Question 27

What does FCAPS stand for? Explain it regarding Network Management function.

Answer

A common way of characterizing network management functions is FCAPS - Fault, Configuration, Accounting, Performance and Security. FCAPS is the ISO Telecommunications Management Network model and framework for network management.

(i) Fault Management - A fault is an event that has a negative significance. The goal of fault management is to recognize, isolate, correct and log faults that occur in the network. Most fault management systems poll the managed objects for error conditions and present this information to the network manager. Fault management identifies and isolates network issues, proposes problem resolution, and subsequently logs the issues and associated resolutions.

(ii) Configuration Management - Monitors network and system configuration information so that the impact on network operations (hardware and software elements) can be tracked and managed. Network changes, additions, and deletions need to be coordinated with the network management personnel.

(iii) Accounting Management - Accounting management is concerned with tracking network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes. For non-billed networks, accounting refers to administration whose primary goal is to administer the set of authorized users by establishing users, passwords, and permissions and to administer the operations of the equipment such as by performing software backup and synchronization.

(iv) Performance Management - Measures and makes network performance data available so that performance can be maintained and acceptable thresholds. It enables the manager to prepare the network for the future, as well as to determine the efficiency of the current network. The network performance addresses the throughput, network response times, packet loss rates, link utilization, percentage utilization, error rates and so forth.

(v) Security Management - Controls access to network resources as established by organizational security guidelines. Most network management systems address security regarding network hardware, such as someone logging into a router. Security management functions include managing network authentication, authorization, and auditing, such that both internal and external users only have access to appropriate network resources, configuration and management of network firewalls, intrusion detection systems, and security policies (such as access lists).

Question 28

List out some features of computerized networking in an organization.

Answer

With growth of business, organizations need good communication between employees to maintain consistency and efficiency. It is being achieved by sharing information such as common files, databases and business application software via telecommunication network and computers. Followings features are commonly seen due to computerized networking in an organization:

(i) ***File Sharing:*** ***It provides for sharing and grouping of data files via network.***

(ii) ***User Interface:*** ***In computerized networking, network computers and other thin clients provide a browser based user interface for processing small application programs called applets.***

(iii) ***Hardware Resource Sharing:*** ***It provides sharing of computer hardware resources such as hard disk, printers etc. by multiple users simultaneously that save cost of installing and maintaining multiple resources.***

(iv) ***System and Application Software:*** ***Networks can provide for/include Application Servers for multiuser operating systems, web server software and application software applets.***

(v) ***Remote Access:*** ***Network allows users to remotely access the data and information. from organizations' network via internet in cost effective manner.***

(vi) ***Shared databases:*** ***Network facilitates simultaneous access to shared databases to multiple users at the same time by ensuring the integrity of database.***

(vii) ***Fault Tolerance:*** ***Computerized networking allows for primary and secondary line of data and programs backups to help defense against accidental data losses against faults or failures. Additional measures can also be taken by adding un-interruptible power supply to handle power failures.***

(viii) ***Internet Access and Security:*** ***It provides access to the internet for transfer of document and access world wide web by maintaining security thru firewall in the organization's network.***

Exercise

1. *Discuss the benefits of a computer network in an organization.*
2. *What is Network Management in Computer Networks and what functions does it perform?*
3. *Discuss some of the characteristics of Local Area Network (LAN).*
4. *Discuss the working of Client/Server architecture.*
5. *Discuss Multi-Tier architecture.*
6. *What are various threats to a computer network's security?*
7. *What is Vulnerability? What are the facts that are responsible for occurrence of vulnerabilities in software?*
8. *What are the steps followed by a security program?*
9. *What are the various ways available for a user to connect to an Internet Service Provider?*
10. *Discuss Internet architecture.*

11. *What are the possible ways in which Internet can be used in an effective manner?*
12. *Discuss the business uses of the Internet, Intranet and Extranet.*
13. *What do you understand by the term "Mobile Commerce"?*
14. *What is Electronic Fund Transfer? Discuss some examples of EFT Systems.*
15. Differentiate between Centralized Computing and Decentralized Computing.
16. *Discuss various Network Security Techniques in brief.*