

5. Computer Networks and Network Security

Q.No.1. What is a Computer Network? What are the different types of computer networks? (N02, RTP)

Computer Network:

- ▶ A computer network is a collection of computers and terminal devices connected together by a communication system.
- ▶ The set of computers may include large-scale computers, medium scale computers, mini computers and micro computers.
- ▶ The set of terminals may include dumb terminals, intelligent terminals, workstations and miscellaneous devices such as telephone lines, printers, etc.
- ▶ There is no specific definition of a computer network. However, Computer networks increase the reliability of computer resources, facilitate overall system development and also satisfy the primary objective of resource sharing such as device sharing, file sharing, program sharing and program segmentation.

Purpose of networks:

- ▶ It allows departments to share hardware devices,
- ▶ It allows information to be shared,
- ▶ It allows electronic transfer of text,
- ▶ It allows decentralization of various data processing functions,
- ▶ It facilitates communication between organizations.

Most commonly found networks:

- ▶ Local Area Networks (LAN)
- ▶ Metropolitan Area Networks (MAN)
- ▶ Wide Area Networks (WAN)
- ▶ Virtual Private Networks (VPN)

Q.No.2. Write short notes on need and scope of computer networks?

Following are some of the ways in which a computer network can be beneficial to a business.

- a. **File Sharing:** File sharing is the most common function provided by networks and consists of grouping all data files together on a server or servers. When all data files in an organization are stored in one place, it is easier for staff to share documents and other data. It also helps to organize the files in a systematic way. Network operating systems also help to restrict access to these files to authorised personnel only.
- b. **Print Sharing:** In a network environment, a single printer can be shared by multiple users. This can reduce the number of printers the organization must purchase, maintain and supply. Network printers are often faster and more capable than those printers which are connected to stand alone computers.
- c. **E-Mail:** Internal or "group e-mail" enables staff in the office to communicate with each other quickly and effectively. Group email applications also provide capabilities for contact management, scheduling and task assignment.
- d. **Fax Sharing:** When a shared modem is connected directly to the network server then it can send/receive fax directly. With this facility users can fax documents directly from their computers without any need for printing them on to paper. Incoming faxes can also be handled by the network and forwarded directly to users' computers via email. With this facility it is not necessary to print a hard copy of every fax.
- e. **Remote Access:** Sometimes staff may require access to their email, documents or other data from remote locations. With the help of this facility users can dial into their organization's network via telephone and access all the network resources as if they are in office. With the help of Virtual Private Network (VPN) even the cost of long-distance telephone calls can be avoided.

- f. **Shared Databases:** This is a subset of file sharing. If the organization maintains an extensive database - for example, a membership, client, grants or financial accounting database - a network is the only effective way to make the database available to multiple users at the same time.
- g. **Fault Tolerance:** Establishing fault tolerance is a process which ensures that there are several lines of defense against accidental data loss. An example of accidental data loss might be a hard drive failure or someone deleting a file by mistake. In a network it can be prevented by maintaining redundant hardware, tape libraries, UPS, etc.
- h. **Internet Access and Security:** When computers are connected through a network, they can share a common network connection to the Internet. This facilitates email, document transfer and access to the resources available on the World Wide Web.
- i. **Communication and collaboration:** A network helps employees to share files, view other people's work and exchange ideas more efficiently. In a big office, one can use e-mail and instant messaging tools to communicate quickly and to store messages for future reference.
- j. **Organization:** Network scheduling software helps to arrange meetings without constantly checking everyone's schedules. This software usually includes other helpful features such as shared address books, to-do lists, etc.

Q.No.3. "Implementation of a computer network in an organization improves its efficiency" – Explain (or) What are the benefits of using a computer network? Describe in brief. (RTP)

As the business grows, good communication between employees is needed. Organisations can improve efficiency by sharing information such as common files, databases and business application software over a computer network. Following are the benefits of using networks:

1. **Can improve communication:** Organisations can improve communication by connecting their computers and working on standardised systems, so that:
 - ▶ Staff, suppliers and customers can share information and get in touch with each other more easily,
 - ▶ Information sharing can make the business more efficient – e.g. in a network it is possible to share a file stored in a common database. With this we can avoid the same data being keyed for multiple times, which would waste time and could result in errors.
 - ▶ Staff can handle the queries in a better way. So, they can deliver better quality of service to their customers.
2. **Reduce costs and improve efficiency:** By storing information in one centralised database and streamlining working practices, organisation can reduce costs and improve efficiency. With this:
 - ▶ Staff can deal with more number of customers at the same time.
 - ▶ Network administration can be centralised. So, less IT support is required.
 - ▶ Costs can be reduced by sharing peripherals such as printers, scanners, external discs, tape drives and Internet access.
3. **Reduction in errors:** All the staff can work from a single source of information. So, organisations can reduce errors and improve consistency because standard versions of manuals and directories can be made available and data can be backed up from a single point on scheduled basis. This ensures consistency.

Q.No.4. What is a Local Area Networks? What are the features of a LAN? (N94, M97, M99 – 5M) (M01 - 3M)

Meaning:

- ▶ LAN is a digital communication system capable of interconnecting large number of computers, terminals and other peripheral devices within a limited geographical area, typically under 1 km.
- ▶ LAN's normally operate within a compact area such as office building or a campus and is owned by the user organisation.

- ▶ Major parameters considered in LAN's are the topology, the transmission media and the speed of transmission. Common topologies include Star, Bus and Ring.
- ▶ One computer, with large capacity disk drive, can become server to other clients. Software can be stored on this central server and used by the whole group.
- ▶ They decentralise the processing from mainframes and mini computers to personal computers.
- ▶ Coaxial and twisted pair cables are used for data transmission.
- ▶ Communication channels are generally owned and maintained by the user organization. These channels are relatively error free (for e.g. a bit error rate of 1 in 10^8 bits transmitted.)
- ▶ The attached computers may be of different types and perform variety of functions such as data processing, word processing and electronic mail.
- ▶ The two main purposes of LAN are to link computers within an organisation so that they can share expensive peripheral devices (for e.g., high speed printers or magnetic disks) and to allow these computers to communicate with each other.

Characteristic features / Important requirements of LAN: ■ (M98, M99)

- a. **Compatibility:** A local area network must be compatible so that software can be easily written and widely distributed. A LAN operating system must be flexible i.e. it must support large variety of hardware.
- b. **Internetworking:** It should be possible to interconnect 2 LANs. Bridge acts as a mediator between LANs of similar topology and protocol. Bridging of different LANs together is one of the most important requirements of any network. Users should easily access resources from all workstations on the bridge network in a transparent way i.e. no special commands should be required to cross the bridge.
- c. **Growth path and Modularity:** Another important feature of a LAN is its modularity. A set of PCs should be easily converted into LAN. It should be able to grow simply by adding additional workstations. For e.g. if more storage is required, one should be able to add another hard disk drive or another server.
- d. **System reliability & maintenance:** In LAN, all computers are prone to system lockups, power failures and other catastrophes ^(=disaster, calamity). If the central processing system goes down, all users connected to it will also fail to work. However, a LAN operating system should be powerful enough to withstand such accidents.

Q.No.5. Why users prefer Local Area Networks? (Or) Of late many users are going for LAN system. Explain why? (Or) Factors contributed to the growth of LANs. (N03, N07 – 5M)

In the environment of LAN, users can have their own independent processing stations while sharing expensive computer resources like hard disks, printers and plotters. Because of this advantage many users preferred LAN's. But, today, there are several reasons that are making the users to move towards LAN. These include:

- a. **Security:** Security for programs and data can be achieved using servers that are locked physically and logically ^(i.e. through passwords, etc). Diskless nodes also offer security by not allowing users to download important data on floppies or upload unwanted software or virus.
- b. **Expanded PC usage through inexpensive workstation:** Once LAN is set up, it is very easy and economical to accommodate additional employees through diskless PCs. On the other hand existing PCs can be easily converted into nodes by adding network interface cards.
- c. **Electronic mail and Message Broadcasting:** Electronic mail allows users to communicate easily with other employees. Each user can be assigned a mail-box on the server. Messages to other users can be dropped into the mail-box and read by them when they log into the network. If a particular message has to be communicated to everyone in the office, **broadcasting** facility can be used.
- d. **Organisational benefits:** Benefits of LANs are numerous. These include reduced costs in computer hardware, software, peripherals and drastic reduction in time and cost of training and retraining man power to use the systems. Managers and executives can communicate with each other more easily and quickly. Further, information flow becomes easier and smoother.

- e. **Data management benefits:** Since data is located centrally on the server, it is easy to manage it and also to maintain back up copies. It is not necessary to transfer files through floppies.
- f. **Software cost and upgradation:** If the organisation wants to purchase licensed software, purchasing a network version can save lot of money. Software upgradation is also easy and cheap.

Q.No.6. What is meant by LAN? Describe its basic components. (M04-5M) (M05-10M) (N07-5M)

A typical local area network has five basic components. They are:

- a. **File Server:** It is a computer system used for the purpose of managing the files, servicing the network printers, handling network communications and other functions. A server may be dedicated or non-dedicated. A server should have huge amount of RAM because it is required to serve the requests of several users. Thus a Pentium system is preferable for better overall performance of the network.
- b. **Network operating system:** It is loaded in the server's hard disk along with system management tools and user utilities. Thus DOS or Windows operating system is no longer valid. However, most DOS/Windows programs can be run as usually.
- c. **Workstations:**
 - ▶ Workstations are attached to the server through network interface card and cables.
 - ▶ Workstations are normally intelligent systems, such as IBM PC. Dumb terminals that are used in mainframes and mini computers are not supported on LANs because they are not capable of processing on their own. In other words only intelligent terminals are used in LANs.
 - ▶ PCs load programs and data from server and do the processing on their own. After processing the files are again stored in the server.
 - ▶ Workstation can also be a diskless PC. In such a case operating system is loaded from the file server.
 - ▶ In short, a PC + LAN card = Workstation.
- d. **Network interface card:** Every device connected to a LAN needs a Network Interface Card (NIC) to plug into the LAN. For e.g. to connect a PC to Ethernet LAN, it must have Ethernet card.
- e. **Network Cabling:** Once the server, workstations and network interface cards are arranged, network cabling is used to connect everything together. The most popular type of network cables are twisted-pair cables, co-axial and fiber optic cables. It is important that cables and cards should match each other.

Q.No.7. Write about different kinds of cables commonly used in LAN's?

Following are the most commonly used cables in Local Area Networks:

- a. **Twisted – Pair cables:** Twisted-pair wires or cables are similar to cables used for home and office telephone system. Two insulated wires are twisted around each other. It is inexpensive and easy to install. Due to technological improvements, capacity of twisted-pair cables has increased. Now they can handle data communications with speeds up to 10 mbps (= million of bits per second) over limited distances.
- b. **Coaxial Cable:** It is a well established and long-used cabling system for terminals and computers. These cables come in a variety of sizes to suit different purposes. Coaxial cables are commonly used to connect computers and terminals in a local area such as an office, floor, building or campus. This cable is conventionally used for cable television network.
- c. **Fiber Optic Cables:** Fiber optic cables use light as the communication medium. To create the on-and-off bit code needed by computers, light is rapidly turned on and off inside channel. Fiber optic cables are light weight and can handle huge amount of data. They can be installed in environments hostile (=not suitable) to copper wire, such as wet areas or areas subject to electromagnetic interference. Data is more secure in fiber optic networks.

	Difference	Twisted pair	Co-axial	Fiber-optic
1.	Medium of transmission	Copper wire	Copper wire	Glass fiber
2.	Electromagnetic interference	High interference	Moderate interference	No interference at all.
3.	Cost	Inexpensive	Moderate	Expensive
4.	Band width	Low	Moderate	High
5.	Speed	Slow	Moderate	High speed
6.	Maintenance	Easy	Moderate	Difficult

Q.No.8. Explain the basic features & usage of Wide Area Networks? (M94, M96, N97, RTP-5M)
Meaning:

- ▶ WAN is a digital communication system which interconnects different sites, computers and user terminals that are spread over a wide area (a state, a country or even world wide). It also helps LANs to communicate with each other.
- ▶ It covers a wider geographical area with various communication facilities such as long distance telephone lines, satellite transmission and even under sea cables.
- ▶ This type of communication network may be developed to operate nationwide or worldwide.
- ▶ It is a commercial data network that provides data communication services for business and government agencies.
- ▶ Using WAN, users can send electronic messages, data, graphics, programs, documents and even video information rapidly and economically.
- ▶ Examples of WANs are inter state banking networks, airline reservation systems, etc.

Characteristics of WAN:

- ▶ The transmitting and receiving equipments are distributed over wider geographical area.
- ▶ The basic components in a common WAN include a host computer which is linked through various inter connected communication lines to sub-ordinate computers.
- ▶ Communication channels between machines are usually furnished (= provided by) by a third party (for e.g. Telephone Company, public data network, satellite carrier, etc.).
- ▶ WAN typically operate at lower link speeds (about 1 MBPS)
- ▶ Channels are of relatively low capacity.
- ▶ Channels are relatively error prone (a bit error rate of 1 in 10^5 bits transmitted)

Q.No.9. Local Area Network (LAN) Vs. Wide Area Network (WAN) (N02, N05, RTP-4M)

No.	Difference	Local Area Network	Wide Area Network
1.	Spread/ Coverage	A LAN is restricted to a limited geographical coverage of few kilometers.	WAN spreads over greater distance and may operate nationwide or even worldwide
2.	Data transmission errors.	Fewer data transmission errors occur in case of LAN because the distance covered is less.	When compared to LAN, error rate is more because the distance covered is more.
3.	Data transmission speed.	Data transmission speed is much higher in LAN than in WAN. Typical transmission speeds in LAN'S are 1 to 10 MBPS.	In a WAN the data transmission speed ranges from 180 to 9600 Bits per second
4.	How nodes are connected?	In a LAN, computers, terminals and peripheral devices are usually connected with wires and coaxial cables.	But in WAN there may not be direct physical connection between various computers.

5.	Cost of transmission	The cost to transmit data in a LAN is negligible since the transmission medium is usually owned by the user organisation.	Cost will be high because the transmission medium used is leased lines or public systems such as telephone lines, microwaves and satellite links.
6.	Communication Mode	Communication may take place just by a way of direct cabling.	Communication takes place by way of telecommunication cables, satellites or microwaves.
7.	Security	Security is not that much important because the network runs within the organisation.	Security is very important because the network has to run outside organisation also.

Q.No.10. Write about Metropolitan Area Network?

- A Metropolitan Area Network (MAN) is some where between a LAN and a WAN.
- Sometimes MAN refers to a network that connects systems or local area networks within a metropolitan area (roughly 40 kms in length from one point to another).
- MANs are based on fiber optic transmission technology and provide high speed interconnection between sites (10 MBPS or so).
- MAN can support both data and voice.
- Cable television networks are best examples of MANs that distribute television signals.

Q.No.11. Write about Virtual Private Network?

A VPN is a private network that uses a public network (usually Internet) to connect remote sites or users together. It will not use a dedicated, real-world connection such as leased line. It uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

Types of VPN: Following are the 2 most common types of VPN

1. Remote-access:

Meaning:

- ▶ This is a user-to-LAN connection used by a company that needs to connect to the private network from various remote locations.
- ▶ It is also called as **Virtual Private Dial-Up Network (VPDN)**.

Working:

- ▶ Generally, a company that wishes to set up a large remote-access VPN will outsource it to an **Enterprise Service Provider (ESP)**.
- ▶ The **ESP** sets up a **Network Access Server (NAS)** and provides **desktop client software** to all the computers of remote users.
- ▶ Employees can dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network.
- ▶ They provide secure, encrypted connections between a company's private network and remote users through a third-party service provider.

Suitability: It is suitable for a company with large number of employees spread over wide area. For example a company with hundreds of sales people in the field needs a remote-access VPN.

- Site-to-Site VPN:** Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as Internet. Site-to-site VPNs can be one of the following two types:

- a. **Intranet based:** If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.
- b. **Extranet based:** When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN. With this, various companies can work in a shared environment.

Q.No.12. What is a computer network? Describe various network architectures? (N02)

The terms LAN or WAN indicates the physical area covered by the network. The way in which individual computers (called nodes) on a network interact with other computers depends on how they are organised. The scheme of organizing network is called network architecture. There are only two basic types of architecture:

Server-based (Client-Server Model) ■ (N96, N99, M07 – 5M)

- a. This type of network consists of certain machines and devices (called servers) that are fully dedicated to provide various services to the other computers (called clients).
- b. Server can be either dedicated or non-dedicated.
- c. Different types of specialised servers include file, fax, printer, modem, E-mail, database server, etc.
- d. The most common type of client server arrangement is a LAN composed of microcomputers connected to a network server. The network serves all clients (users) of the LAN.
- e. A client program running on one of the microcomputers can request specific data from the server. The server program retrieves the requested data from its database and returns it to the client.
- f. Server can also answer the queries raised by client computers.
- g. This way, a LAN permits all the computers connected to it to share hardware, software and data. The most commonly shared resources are disk-storage devices and printers.
- h. The architecture is used when there are large numbers of nodes in the network.

Peer to peer: ■

- a. In peer-to-peer architecture, there are no dedicated servers. All computers are equal. That is why they are termed as peers.
- b. Normally, each of these machines function both as a client and as a server. This arrangement is suitable when
 - ▶ there are limited numbers of users (10 or less),
 - ▶ users are located in a small area and
 - ▶ security is not an important issue.
- c. Users can freely access data and programs that reside ^(=lie) on other computers across the network.
- d. The network does not depend completely on a particular computer. In a server based system if the server fails, the entire network fails. But in a peer to peer network only that particular computer is affected and other systems continue to function as usually.
- e. Linking computers in a peer to peer network is very straight forward because there is no central server to which all the computers have to be connected. The computers can be connected to the network in any convenient manner. This can save lot of time and money.
- f. The architecture is very simple and easy to maintain.

Q.No.13. Peer to peer Vs. Client Server architecture? (N04, M07 - 4M)

Aspect	Peer – to – Peer	Client – Server
Structure	Independent stand-alone systems are interconnected. Each of the system is called a Peer and acts as both server and a client.	Systems with no / limited independence (called Clients) are linked to a Central Computer called Server.

Server	There is no server concept. All computers are equal, and are termed as peers.	Server is available to provide various services to clients.
Working	Any peer can access any other peer on the network for sharing and retrieving data. It does not depend on any particular system.	Client requests specific data from the server. The server program retrieves the requested data and returns it to the client.
Simplicity	It is simple in design and maintenance.	It is complex in design and maintenance.
Security and Control	Does not provide adequate security and control over data and resources.	Provide adequate security and control over data and resources.
Suitability	Suitable for environment with a limited number of users.	Suitable for environment with a large number of users.
Reliability	Network does not depend on a particular computer.	Network totally depends on File Server.

Q.No.14. State the components of a data communication system?

Following are the 5 basic components found in any data communication network:

- ▶ The sending device,
- ▶ The communications interface devices,
- ▶ The communications channel,
- ▶ The receiving device,
- ▶ Communications software.

Q.No.15. Write about various communication interface devices. (or) Explain any 5 Communication interface devices? (N05 - 5M, RTP)

1. Network Interface cards: ■

- ▶ NIC is an adapter that provides a connector to attach network cable to a server or workstation.
- ▶ It is a microprocessor based device containing hardware and software which supplies the intelligence to communicate across the network and to perform all communication processing.
- ▶ It is a PCB installed in the microcomputer. It may be called as Network card, Network adaptor or NIU.
- ▶ The on-board circuitry provides the required protocols and commands.
- ▶ An NIC has additional memory for buffering incoming and outgoing data packets. This improves network performance.
- ▶ Network interface cards are available in 8 bit or 16 bit bus standards (today even 32 bit)
- ▶ But a NIC is required only when networking ability is not already present in the micro computer.

2. Modem: ■ (N95, N98, M03, N05 - 1M)

- ▶ Modem is a communication device used to transmit computer data through ordinary telephone lines because computer data is in digital form but telephone lines are analog.
- ▶ It is an encoding as well as decoding device used in data transmission. It converts digital computer signal into analog telephone signal (modulation) and converts analog telephone signal into digital computer signal (demodulation).
- ▶ The speed of modem is measured in KBPS (Kilo Bits Per Second). Today a 56.6 kbps modem is standard.
- ▶ It helps to access remote computers. Thus employees at home can access computer files at office. They can also exchange files with other employees and exchange e-mail messages.
- ▶ MODEM is required only when a computer network is developed using telephonel lines.



Types:

- ▶ Modems can be categorized according to speed, price and other features. But most commonly, people classify them as internal and external.
- ▶ Internal modems look like sound cards and video cards that fit inside the computer as daughter cards.
- ▶ On the other hand External modems are connected to the serial port of the computer.
- ▶ On the other hand PCMCIA modems are used with laptop computers. They are small - about the size of a visiting card and are quite expensive.

3. Multiplexer: ■ (N96, N04, M07, M08 - 1M, RTP)

- ▶ It is a form of data transmission in which one communication channel carries several transmissions at the same time.
- ▶ Multiplexer is a device that combines large number of low speed transmission lines into high speed line.
- ▶ Thus Multiplexer can divide a single communication line between number of terminals.
- ▶ Multiplexer can scan each device to collect and transmit data on a single line to the CPU. It can also transmit data from CPU to appropriate terminal linked to the Multiplexer.
- ▶ This function may be very complex and on some systems a separate computer processor is devoted to this activity and it is known as "front-end-processor".
- ▶ For e.g. telephone lines can carry thousands of our conversations at the same time using multiplexing.
- ▶ The exact number of transmissions depends on the type of communication channel and the communication rate.

4. Front-end communication processor: ■ (RTP)

- ▶ These are programmable devices which control the functions of communication system.
- ▶ They support the operations of a mainframe computer by performing some functions, which a mainframe computer has to perform by itself.
- ▶ It is like a mini computer which sits between the mainframe computer and MODEM.
- ▶ These functions include code conversions, editing and verification of data, terminal recognition and control of transmission lines.
- ▶ With this, the mainframe computer can devote its time on data processing rather than on data transmission.

5. Protocol Converters: ■ (N05 - 1M)

- ▶ Dissimilar devices can't communicate with each other unless a strict set of communication standards are followed. Such standards are commonly known as communication protocols.
- ▶ A Protocol is a set of rules required to initiate and maintain communication between sending and receiving device.
- ▶ Generally an organisation uses several types of computers, transmission channels, transmission modes and data codes. Protocol converters help to communicate data between such diverse components and computers.
- ▶ For example it may be necessary to convert data from ASCII to EBCDIC.
- ▶ Protocol conversion can be done by hardware, software or a combination of hardware and software.

6. Hub: (M04 - 1M)

- ▶ A hub is a hardware device that provides a common wiring point in a LAN.
- ▶ Each node is connected to the hub by means of simple twisted pair wires.
- ▶ The hub then provides a connection over a higher speed link to other LANs, the company's WAN, or the Internet.
- ▶ Generally it works on half duplex mode.
- ▶ A Hub can be either active or passive.

- 7. Switches:** These are hardware devices used to direct messages across a network. Switches create temporary point to point links between two nodes on a network and send all data along that link.
- 8. Repeaters: (M05, N06, N07 - 1M, RTP)** When data is transmitted through several cables, signal gets degraded. To avoid such problems repeaters are used. Repeater boosts or amplifies the signal before passing it through the next section of cable.
- 9. Bridges: (M06 – 1M, RTP)** The main task of a bridge is to receive and pass data between two LAN's that use **similar protocol and topology**. In order to transmit this data successfully, bridge magnifies the signal. Thus a bridge acts as a repeater as well as a link.
- 10. Gateway: (N04, M07 - 1M)** Gateways are similar to bridges because they are also used to transfer data from one network to another network. But Gateways are used to transfer data between 2 networks that use **dissimilar protocols and terminals**. For e.g. several years ago, the sales department of a company installed LAN. Today accounting department wants to install LAN but wants to use latest technology. Now these networks are using 2 different topologies and protocols. Now these 2 different LANs can be connected using a gateway.
- 11. Routers: (N06, M03, M07 - 1M, RTP)** Routers are used to **route data** between several nodes in the network. Router computers are **similar to bridges** but can also provide network management utilities to the user. It plays a very key role in managing network traffic. Their job is to ensure that data arrives at proper destination.
- ▶ Generally Routers are not needed for LAN because the network itself can handle its internal traffic.
 - ▶ Routers come into play when data is sent between different networks.
 - ▶ Routers examine packets to determine their destination. They take into account the volume of activity on the network and they send the packets to another router – one that is closer to the packet's final destination.
 - ▶ If one network is out of order, router can route the data through another appropriate route.
- 12. Remote Access Devices:** Remote access devices are modem banks that serve as gateways to the Internet or to private corporate networks. Their function is to properly route all incoming and outgoing connections.

Q.No.16. What is meant by Network Structure or Topology? Write about different network structures available? (M00 - 5M) (M03 - 10M)

The geometrical arrangement of computer resources, remote devices, and communication facilities is known as network structure or network topology. A computer network consists of nodes and links. A node is the end point of any branch in a computer. It can be either terminal device, workstation or an interconnecting equipment facility. A link is a communication path between two nodes.

A network structure determines how one computer in the network can communicate with other computers. Following are the most commonly used network topologies:

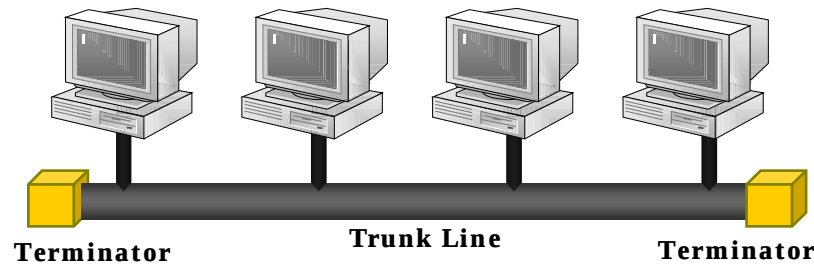
- ▶ Bus topology / Bus form of Network,
- ▶ Star topology / Star form of Network,
- ▶ Ring topology / Ring form of Network and
- ▶ Mesh topology / Mesh form of Network.

Q.No.17. Outline the meaning, advantages and disadvantages of a bus network?

Meaning:

- ▶ A bus network topology is a network architecture in which a set of clients are connected via a shared communications line, called a bus.
- ▶ Bus networks are the simplest way to connect multiple clients, but often have problems when two clients want to transmit at the same time on the same bus.
- ▶ This structure is very popular for local area networks.

- ▶ In this structure or topology, a single network cable runs in the building or campus and all nodes are linked along with this communication line.
- ▶ Two ends of the cable are terminated with terminators.



Advantages:

- ▶ It is a highly reliable in small networks. Any line breakdown does not affect the communication between two computers.
- ▶ Easy to use and understand.
- ▶ Requires least amount of cable to connect the computers together.
- ▶ Less expensive than other cabling arrangements because only a single cable is used.
- ▶ It is easy to extend the network. 2 Cables can be joined together with a connector, making a longer cable. With this more number of computers can be connected to the network.
- ▶ A repeater can also be used to improve the quality of signal.
- ▶ Well suited for temporary or small networks not requiring high speeds (quick setup)

Disadvantages:

- ▶ Heavy traffic can slow down the network. This is so because only one computer can transmit at any time. But networks do not coordinate when information is sent. Computers interrupting each other can use lot of bandwidth.
- ▶ Each new connection weakens the signal. (because the length of cable increases)
- ▶ It is difficult to troubleshoot bus network. It is difficult to find out break or malfunction of a cable and can cause the whole network to stop functioning.
- ▶ If there is a problem with main cable, the entire network goes down.
- ▶ Maintenance costs may be higher in the long run.
- ▶ It is slower than the other topologies.

Suitability: It works best with limited number of nodes.

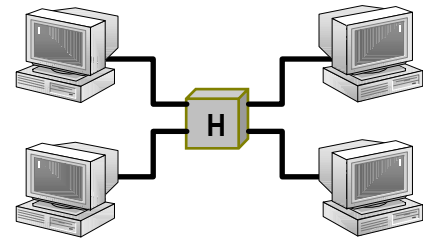
Q.NO.18. Write short notes on Star Network?

Meaning:

- ▶ This is the most commonly used structure or topology.
- ▶ Here communication channels emanate ^(=come) from centralized computer system. That is, processing nodes in a star network interconnect directly with a central system.
- ▶ In its simplest form, a star network consists of one central switch, hub or computer, which acts as a medium to transmit messages.
- ▶ Each terminal, small computer or large main frame, can communicate only with the central site and not with other nodes in the network.
- ▶ If a node wants to transmit information from one node to another, it can be done by sending the details to the central node, which in turn sends them to the destination.

Advantages:

- ▶ It is easy to add and remove nodes. So, it is easy to expand a star network.
- ▶ A node failure does not bring down the entire network
- ▶ Connection of additional computers does not slow down the communication between any 2 computers.
- ▶ It is easier to diagnose network problems through a central hub.
- ▶ Very Robustic.

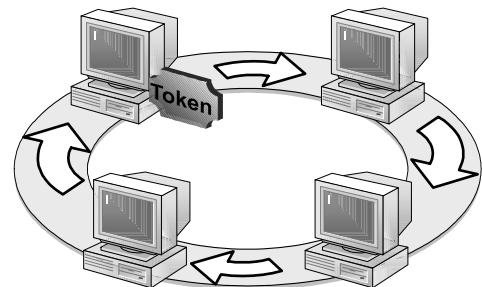
**Disadvantages:**

- ▶ More dependence on central hub. If the central hub fails, the entire network ceases to function.
- ▶ It is costlier than other topologies (more cable is required than bus or ring network).
- ▶ The performance and scalability of the network depends upon the capabilities of the hub. Network size is also limited by the number of connections that a hub can handle.

Suitability: A star network is particularly appropriate for organisations that require centralized database or centralized processing facility.

Q.No.19. Write about Ring form of Network?
Meaning:

- ▶ It is another structure used for local area networks.
- ▶ It is a decentralised network topology in which number of nodes are arranged around a closed loop cable.
- ▶ In this topology, the network cable passes from one node to another until all nodes are connected in the form of a loop or ring.
- ▶ There is a direct point-to-point link between two neighboring nodes.
- ▶ These links are unidirectional. It ensures that transmission by a node passes the whole ring and comes back to the node that made the transmission.

**Advantages:**

- ▶ It offers high performance for a small number of workstations.
- ▶ Ring networks can spread over longer distances than other types of networks.
- ▶ It is also easy to expand ring network.
- ▶ It is more reliable since communication between 2 computers is not dependent on a single host computer.
- ▶ Does not require network server to manage the connectivity between the computers
- ▶ Performs better than star topology under heavy network load

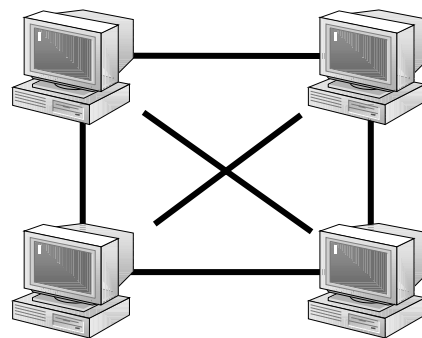
Disadvantages:

- ▶ Relatively expensive and difficult to install.
- ▶ Failure of one computer on the network can affect the whole network.
- ▶ It is difficult to trouble shoot a ring network.
- ▶ Adding or removing computers can disturb the network.
- ▶ Addition of computers to the network increases the communication time between 2 computers.

Suitability: Ring networks offer high performance for a small number of workstations. It can also be used for large networks where each station has a similar workload.

Q.No.20. Write about Mesh form of Network?**Meaning:**

- ▶ Mesh networking is a way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around broken or blocked paths by “hopping” from node to node until the destination is reached.
- ▶ In a mesh network structure, the nodes are randomly connected using communication links.
- ▶ But in real life network connections, it may be fully connected or connected with only partial links. In a fully inter connected topology, each node is connected by a dedicated point-to-point link to every other node. In partially connected topology, computer nodes are widely scattered.
- ▶ When every node is connected to every other node, a mesh network with ‘n’ nodes will have $n(n-1)/2$ number of links and the number of links coming from every node is (n-1).
- ▶ This concept is applicable to wired and wireless networks.
- ▶ This architecture is typically used in Wireless mesh networks.

**Advantages:**

- ▶ This topology is very reliable. If direct link between 2 nodes breaks down, there exists an alternate path.
- ▶ Mesh networks are self-healing. The network can still operate even when a node breaks down or a connection goes bad.
- ▶ Gives the greatest amount of redundancy. Even if one node fails, network traffic can be redirected to another node.
- ▶ It allows the network to isolate and prioritize communications from different computers.

Disadvantages:

- ▶ It is very difficult to diagnose network problems.
- ▶ Adding or replacing a node will disturb the entire network.
- ▶ The cost of installation and maintenance is high (more cable is required than any other topology)

Suitability: Only military organizations, that need high degree of redundancy, use this type of networks.

Q.No.21. Star Network Vs. Ring Network. (N01 - 5M, N04 – 4M)

No.	Difference	Star Network	Ring Network
1.	Meaning	It is a type of network topology in which all nodes are connected to a central computer/hub through dedicated cables.	It is a type of network topology in which all nodes are connected in the form of a circular chain.
2.	Communication between nodes.	The communication takes place between the nodes through the hub/computer only i.e. all communication between terminals must pass through hub/computer.	The communication takes place by each node to receive and check for the message i.e. every node receives message and passes it to the next node.
3.	Break in connection	A broken connection between hub/central computer and node does not affect the rest of the network.	A broken connection between nodes leads to failure of entire network.
4.	Failure of the system	Failure in the hub/central computer affects all nodes connected to that hub.	Failure in one node does not affect the entire system.
5.	Repeaters	The signal becomes weak when it has to travel long distances. To avoid it, repeaters are required to be used.	Repeaters are not needed. Every computer acts as a repeater.

6.	Adding / Removing nodes	It is very easy to add/remove a node from the network.	It is difficult to add/remove a node from the system.
----	-------------------------	--	---

Q.No.22. Serial Transmission Vs. Parallel Transmission. (M06 - 4M)

Serial Transmission: Serial Transmission is the most commonly used method of communication. In serial transmission bits of each byte are transmitted one after the other along a single path. Then the receiver assembles the incoming bit stream into characters. In serial transmission, the bits of each byte are sent along a single path one after another. An example is the serial port (RS-232), used for Mouse or MODEM. Serial transmission can occur in any of the two ways - Asynchronous & Synchronous transmission.

Advantages:

- ▶ It is a cheap mode of transferring data.
- ▶ It is suitable to transmit data over long distances.

Disadvantage: This method is not efficient (i.e. slow) because it transfers data in series.

Parallel Transmission:

- ▶ In parallel transmission all the bits of each byte are transmitted simultaneously i.e. each bit will have a unique channel dedicated to it. For ASCII character we need eight channels. All bits are transmitted together and arrive at the destination together.
- ▶ Example – Parallel port being used for printers.

Advantages: Data can be transmitted at a very high speed.

Disadvantage:

- ▶ As it uses parallel paths, cross talk may occur. So, it is not suitable for transferring data over long distances. To minimise cross talk, cable length should be limited.
- ▶ It is costly. (Because, there should be separate channel for each bit)

No.	Difference	Serial transmission	Parallel transmission
1.	Path	The bits of each byte are sent along a single path one after the other.	In parallel transmission, there are separate parallel paths corresponding to each bit of byte.
2.	Data transmission	Bits in a byte are transmitted one by one.	All character bits are transmitted in parallel, at a time.
3.	Distance	It is used to transfer data over long distances.	It is used to transfer data to limited distances.
4.	Speed	The rate of data transmission is very slow.	The rate of data transmission is very high.
5.	Where is it used?	It is used where less volume of data is to be transmitted.	It is used where more volume of data is to be transmitted.
6.	Cost	It is economical.	It is costly.

Q.No.23. Write about Synchronous and Asynchronous methods of data transmission. (M03 - 4M) (M05 - 4M) (N07 - 4M)

Synchronous Transmission: ■

- ▶ In this method characters are transmitted as groups, preceded and followed by control characters.
- ▶ The transmission and receiving intervals are precisely timed, permitting grouping of bits into identifiable characters.

- ▶ In this method data bytes are sent one after the other at regular intervals. The data form a continuous stream of bits spaced at equal intervals, with no space between consecutive bytes.
- ▶ This method is mainly used for computers but is also used for human operation of buffered terminals.

Advantages: It can transfer data at a very high speed since fewer bits are needed to identify the beginning and ending of the character coding.

Disadvantages:

- ▶ Its main drawback is inaccuracy.
- ▶ This method requires high quality communication channels.
- ▶ It is expensive because the device built has to be smart enough to differentiate actual data and special synchronous characters.

Asynchronous Transmission: ■ (N03 - 1M)

- ▶ In this method each character is transmitted separately i.e. one character at a time.
- ▶ The character is preceded by a start bit, which tells the receiving device where the character coding begins, and is followed by a stop bit, which tells the receiving device where the character coding ends after which there is an interval of idle time on the channel.
- ▶ Then the next character is sent, start bits first, character bits next, stop bits last.
- ▶ The start and stop bits (and the interval of time between consecutive characters) allow the receiving and sending computers to synchronise the transmission.
- ▶ This is the most common mode world wide, especially for operation of interactive computer terminals and teletypewriters.

Advantages:

- ▶ Reliable as the start and stop bits ensure that the sender and receiver remain in step with one another.
- ▶ It is less expensive.

Disadvantages: This method is not efficient because the extra start and stop bits slow down the data transmission when huge volume of data is to be transmitted.

No.	Synchronous	Asynchronous
1.	In this transmission technique bits are transmitted at fixed rate.	In this method transmission takes place in the form of words accompanied by stop and stop bits.
2.	This allows characters to be sent down the line without start-stop bits.	Transfers the data with start-stop bits.
3.	It allows data to be sent as a multi-word blocks.	Data transfer takes place in the form of words.
4.	Uses a group of synchronization bits.	No special synchronization bits are used to synchronize the equipment.
5.	Data transfer rate is fast.	The data transfer rate is slow.

Q.No.24. Write about different modes of data communication? (N98 - 6M) (N06,M02 - 5M) (M07 - 4M)

There are three different modes of data communication:

- Simplex:** In this mode data is transmitted in one direction only. The sending station cannot receive data. A terminal connected to such line may send only or receive only.
- Half duplex:** Under this mode, data can be transmitted in both the directions but only one side at a time. Thus every terminal can send and receive data but only one activity at a time. For example, all terminal devices are connected to the CPU in half-duplex mode.
- Full duplex:** A full duplex connection can simultaneously transmit and receive data between two stations. It is the most commonly used communication mode. A full duplex line is faster because it avoids the delay that occur in half-duplex mode (for changing the direction of transmission) Full-duplex transmission uses two separate circuits for communication i.e. one for each direction. It is costlier than half- duplex but easy to use.

Q.No.25. Discuss various data transmission techniques used in a computer network? (M04 - 5M)**Circuit switching: ■**

- ▶ Circuit Switching is the simplest method of data communication. Landline telephone network uses this method to establish connection between two subscribers.
- ▶ Circuit switching establishes a physical connection between two devices and the physical path that is established remains open until the end of the session.
- ▶ At any point of time only two communication devices can transmit information to each other. These devices could be either telephones or computers.
- ▶ Once a circuit is established between two stations, it is exclusively used by the two parties and the dedicated link becomes unavailable to others till the call is terminated by either party.
- ▶ This will be the experience of every person using the telephone. We make a call and either we get our destination party or encounter a busy signal.
- ▶ A single circuit is used for the entire duration of call.

Message Switching: ■ (RTP)

- ▶ Message switching is a system which uses computer techniques to transmit, receive, store and retrieve textual information.
- ▶ A message is a logical unit of information and can be of any length. In this method, if a station wants to send a message to another station, the destination address is attached to the message and then transmitted to the destination through intermediary nodes.
- ▶ The intermediary node receives the message, stores it temporarily, inspects for errors and transmits the message to the next node on the basis of availability of channel. This process goes on till the message reaches its intended destination.
- ▶ Organisations with heavy volume of data transmission use this method.
- ▶ It causes long delay because the message is stored at the exchange until suitable circuits are available to transmit message.
- ▶ For message switching it is not necessary to establish a dedicated path between 2 stations.
- ▶ Examples are telegrams, electronic mail, computer files, transaction queries and responses.

Packet switching: ■ (N02 - 1M)

- ▶ It is a sophisticated technique of maximizing transmission capacity of networks.
- ▶ Here the message is broken into transferable units of fixed size called packets. Depending on the availability of channel these packets are routed individually through the network.
- ▶ Each packet contains source and destination address, synchronizing error correction and control bits. The packets are routed using these source and destination addresses.
- ▶ Passwords and all types of data can be included within the packet.
- ▶ Now transmission is done by packets and it is possible that different packets of the same message can be routed across different paths and they will be combined at the destination.
- ▶ Transmission cost is by packet and not by message, route or distance.
- ▶ This method is currently being used to transmit data in Internet.

Aspect	Circuit Switching	Message Switching	Packet Switching
Dedicated Communication Path or Channel	Required	Not Required	Not Required
Availability of Recipients and Sender at the same time	Required	Not Required	Not Required
Use of source address & destination address to transmit a message	Not Required	Required	Required
Full Message Required at each node for transmission	Yes	Yes	No
Breaking or Division of Data into Packets	No	No	Yes

Q.No.26. Write about Communication channels? What are the important characteristics of a communication channel?

A communication channel is the medium that connects the sender and the receiver in data communications network. Common communication channels include telephone lines, fiber optic cables, microwaves, satellite, etc. Different communication channels possess different characteristics that can affect the network's reliability, cost and security. They are:

- a. **Bandwidth: (N03, N07, - 1M)** It refers to a channel's information carrying capacity. Technically bandwidth represents the difference between highest and lowest frequencies that can be used to transmit data. It is usually measured in terms of Bits per Second (BPS). A communication channel with greater bandwidth will be more useful, because it can transmit more information in less time. Higher bandwidth is essential for applications like real-time video, audio, etc.
- b. **Transmission Rate:** It is the data transmission capacity of a telecommunication channel. It depends on the bandwidth. The greater the bandwidth higher will be the transmission rate.
- c. **Transmission Mode:** It is the mode in which data are transmitted over the network. There are 2 modes of data transmission namely synchronous and asynchronous transmission.
- d. **Transmission Direction:** It is the direction in which data is transmitted. It is categorized into 3 ways – Simplex, Half Duplex and Full Duplex.

Q.No.27. Briefly explain various types of communication services used to transmit data. (N04 - 5M)

Normally, an organization uses one of the common carrier services to carry messages from one station to another station. Following is a brief description of these services:

- a. **Narrow band service:** Usually, this service is used where data volume is relatively low. The transmission rate range from 45 to 300 bits per second. Example of this are telephone companies' typewriters exchange service (TWX), Telex service.
- b. **Voice band services:** Voice band services use ordinary telephone lines to send data messages. Transmission rates vary from 300 to 9600 bits per second or higher.
- c. **Wide band Services:** Wide band services provide data transmission rates from several thousands to several million bits per second (9600 to 256000). These services are limited to high-volume users. Such services generally use coaxial cable or microwave communication. Space satellites are using this service to transmit data from one part of the world to another part of the world.

Communication services may be either **leased** or **dialed up**.

- ▶ A leased line can be exclusively used by the user. It is used when there are continuing data-transmission needs.
- ▶ The dial-up variety requires the person to dial the computer. This alternative is appropriate when there are periodic data to transmit.

Q.No.28. Communication software is an essential requirement of data communication system. Explain the various functions of this data communication software? (N03, N05 - 5M)

Communication software is a software that manages the flow of data across a network. Following are the important functions of communication software:

- a. **Access control:**
 - ▶ Linking and disconnecting different devices;
 - ▶ automatically dialing and answering telephones;
 - ▶ restricting access to authorized users;
 - ▶ establishing parameters such as speed, mode, and direction of transmission.
- b. **Network management:**
 - ▶ Polling (=checking) devices to see whether they are ready to send or receive data;

- ▶ queuing input and output;
 - ▶ determining system priorities;
 - ▶ routing messages,
 - ▶ logging network activity, use and errors.
- c. **Data and file transmission:** Controlling the transfer of data, files and messages among various devices.
- d. **Error detection and control:** Ensuring that data sent is actually data received.
- e. **Data security:** Protecting data during transmission from unauthorized access.

Q.No.29. Communication or Transmission protocols. (M98, N03, N07 - 5M)**Communication Protocols:**

- ▶ For any network to exist, there must be connections between computers and agreements or what is termed as protocols in communications language. Protocols are software that performs a variety of actions necessary for data transmission between computers.
- ▶ Protocols are a set of rules for inter-computer communication that have been agreed upon and implemented by many vendors, users and standard bodies. Ideally, protocols allow heterogeneous computers to talk to each other.
- ▶ At the most basic level, protocols define the physical aspects of communication, such as how the system components will be interfaced and at what voltage levels data will be transmitted, etc.
- ▶ At higher level, protocols define the way data will be transferred such as the establishment and termination of “sessions” between computers and the synchronisation of those transmissions. At still higher levels, protocols can standardise the way data is encoded and compressed for transmission.

Aspects defined by protocols: A transmission protocol is a set of conventions or rules that must be followed by both the parties to ensure that the information is correctly exchanged. A protocol defines the following 3 aspects of digital communication.

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

Layers: Communication protocols are defined in layers.

- ▶ The first layer is the physical layer which defines the manner in which nodes in a network are connected to each other.
- ▶ Subsequent layers describe how messages are packaged for transmission, how messages are routed through the network, security procedures and the manner in which messages are displayed.
- ▶ The number of subsequent layers depends upon the protocol.

Examples: Several protocols are in common use. For example,

- ▶ X.12 is the standard for Electronic Data Interchange;
- ▶ X.75 is used for interconnection between networks of different countries;
- ▶ XON/XOFF is the de-facto standard for microcomputer data communication;
- ▶ XMODEM is used for uploading and downloading files.
- ▶ TCP/IP – protocol being used in internet.

Q.No.30. Write about Open System Interconnection.

Meaning: OSI or the Open System Interconnection has been outlined by International Organization for Standardization (ISO). It facilitates communication of heterogeneous hardware or software platforms with each other.

Layers: It is defined with the help of following seven layers of functions with their associated controls:

- a. **Layer 1 or Physical Layer** is a hardware layer which specifies mechanical features as well as electromagnetic features. Network topology is a part of this layer.
- b. **Layer 2 or Data Link Layer** is also a hardware layer which specifies channel access control method and ensures reliable transfer of data through the transmission medium.
- c. **Layer 3 or Network Layer** makes a choice of the physical route of transmission of data. It establishes, maintains, terminates, connections between the nodes and ensures proper routing of data.
- d. **Layer 4 or Transport Layer** ensures reliable transfer of data between user processes, assembles and disassembles message packets, provides error recovery and flow control. Multiplexing and encryption are undertaken at this layer level.
- e. **Layer 5 or Session Layer** establishes, maintains and terminates sessions between user processes. Identification and authentication are undertaken at this layer level.
- f. **Layer 6 or Presentation Layer** controls on screen display of data, transforms data to a standard application interface. Encryption, data compression can also be undertaken at this layer level.
- g. **Layer 7 or Application Layer** provides user services by file transfer, file sharing, etc. Database concurrency and deadlock situation controls are undertaken at this layer.

Q.No.31. Write short notes on network protocols.

Meaning: Network protocols which are essentially software are sets of rules for –

- ▶ Communicating, timings, sequencing, formatting, and error checking for data transmission.
- ▶ Providing standards for data communication

Where they are stored? These rules are embedded or built into the software which reside either in –

- ▶ Computer's memory or
- ▶ Memory of transmission device

Need for protocols: Different protocols cannot talk to each other. To solve this problem, standard protocols have been developed.

Functions of Protocols:

- a. The entire operation of data transmission over a network is broken down into systematic steps. Each step has its own rules or protocols. For example, in OSI model each of the seven layers use different protocols. Accordingly, steps must be implemented in a consistent order. This order is same for every computer in the network, either receiving or sending data.
- b. At the sending computer, protocols:
 - ▶ Breakdown data into packets,
 - ▶ Add destination address to the packet,
 - ▶ Prepares data for transmission through Network Interface Card (NIC)
- c. At the receiving computer, protocols:
 - ▶ Take data packets from the cable,
 - ▶ Bring packets into computer through Network Interface Card (NIC)
 - ▶ Strip the packets off any transmitting information,
 - ▶ Copy data from packet to a buffer for reassembly,
 - ▶ Pass the reassembled data to the application.

Protocol Stack: A **protocol stack** is a combination of set of protocols. Each layer specifies a different protocol–

- ▶ For handling a function or,
- ▶ As a subsystem of the common process,
- ▶ Each layer has its won set of rules

For example:

- ▶ Application Layer initiates or accepts a request from the user.
- ▶ The Presentation Layer adds formatting, displays and encrypts information to the packet.
- ▶ The Session Layer adds traffic flow information to determine when the packet should be sent or received.
- ▶ Transport Layer adds error handling information.
- ▶ The Network Layer does sequencing and adds address information in the packet.
- ▶ The data Link Layer adds error checking information and prepares the data for going to the destination.

Q.No.32. Write short notes on TCP/IP.

Meaning: The protocol used on the Internet is called TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP protocol consists of 2 parts-

- a. TCP deals with exchange of sequential data.
- b. IP handles packet switching and is used on the Internet.

TCP/IP has four layers:

- a. **Application Layer:** It directly provides services to the users such as e-mail,
- b. **Transport Layer:** It provides end-to-end communication between applications and verifies correct packet arrival.
- c. **Internet Layer:** It provides packet routing for error checking, addressing and integrity.
- d. **Network Interface Layer:** It provides an interface to the network hardware and device drivers. This is also called as Data Link Layer.

Steps in transmission of data: TCP/IP creates a packet-switching network. When a message is to be sent over the Internet,

- ▶ the TCP protocol breaks it up into small packets.
- ▶ A header is given to each packet, which consists of destination address.
- ▶ The packets are then sent individually over the Internet.
- ▶ The IP protocol guides the packets so that they arrive at proper destination.
- ▶ Once the destination is reached, the TCP protocol reassembles the packets into the original message.

Q.No.33. Write about Broadband networks (ISDN).

1. Meaning:

- a. **Integrated Services Digital Network (ISDN)** is a circuit switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds.
- b. ISDN is a set of protocols for establishing and breaking circuit switched connections and for advanced call features for the user.

2. Types of channel:

- a. **Bearer channels (B channels):** Data and voice are carried by these channels having a bandwidth of 64 kilobits per second.
- b. **Delta channels (D channels):** It carries signals and controls. But it can also be used for carrying data.

3. Types of ISDN services:

- a. **Basic Rate Interface (BRI):**
 - ▶ It consists of two 64 kbps B channels and one 16 kbps D channel to form a total of 144 kbps.
 - ▶ It is suitable for individual users.

b. Primary Rate Interface (PRI):

- ▶ It consists of 23 B channels and one 64 kbps D channel to form a total of 1536 kbps.
- ▶ It is suitable for users with higher capacity requirements.

4. Advantages:

- a. Multiple channel operation in same cable:** ISDN allows multiple digital channels to be operated simultaneously through the same regular phone cable which is meant for analog signals. However, this is possible only if the telephone company's switches can support digital connections.
- b. Combines different digital sources:** With ISDN, it is possible to combine several digital data sources and send the information to the proper destination. In a digital line it is easy to reduce noise and interference even after combining these signals.

Q.No.34. Write about different types of traditional computing models.**1. Mainframe architecture: ■**

- ▶ In mainframe architecture, all the intelligence lies in the central host computer (processor)
- ▶ Users can interact with the host computer through dumb terminals.
- ▶ These terminals can capture keystrokes and send that data to the host computer.
- ▶ Centralized, host-based computing model allows users to share a single computer application, database and peripherals.

Limitations:

- ▶ They do not easily support graphical user interface or
- ▶ They don't support access to multiple databases from geographically dispersed sites.
- ▶ The cost of these systems will be thousands of times more than PCs. But they don't do thousands of times more work.

2. Personal Computers & workstations: ■

- ▶ With the introduction of PC and its operating system, independent computing workstations became popular. These are stand alone computing models.

Advantages:

- ▶ They are not connected to the central computer and hence independent.
- ▶ In this model, the processing load on central computer is removed.

Limitations:

- ▶ Disconnected personal computers can't share data and expensive resources like disk drives, printers, modems and other peripheral devices.
- ▶ These problems led to the development of network/file server computing model. It links PCs and workstations together in a Local Area Network. So, they can share data and peripherals.

3. File sharing architecture: ■

- ▶ The original PC networks were based on file sharing architectures. Here the server downloads files from the shared location to the desktop. The requested user's job is then run in the desktop environment.
- ▶ In other words the data sent by the server is processed into information by the workstation.

Limitations:

- ▶ The server will send the entire file over the network even though the workstation only requires a few records in the file.
- ▶ If Graphic User Interface (GUI) is added to this model then it increases network traffic, decreases response time and limits customer service.

- ▶ It is not suitable for multi user applications because of the following reasons: (i) this model does not support data concurrence i.e. simultaneous access to a file by multiple users (ii) when several workstations request and send several files in a LAN, then the overall performance of the network will degrade. It can only satisfy about 12 users simultaneously.
- ▶ With the advent of less expensive but more powerful computer hardware the file server architecture has become outdated.

Q.No.35. Write about Client Server model. (RTP)**Meaning:**

- ▶ Client server technology is an advancement of the traditional computing models.
- ▶ Client/Server (C/S) refers to a computing technology in which the hardware and the software components (i.e., clients and servers) are distributed across a network.
- ▶ It is a technology in which the server software accepts requests for data from client software and returns the results to the client. The client processes the data and presents the results to the user.
- ▶ Client server technology intelligently divides the processing work between the server and the workstation.
- ▶ The server handles all the global tasks while the workstation handles all the local tasks.
- ▶ The server only sends those records to the workstation that are needed to satisfy the information request. As a result network traffic is significantly reduced.
- ▶ This is a versatile, message based and modular infrastructure.
- ▶ It improves usability, flexibility, interoperability and scalability when compared to centralised, mainframe, time sharing computing.
- ▶ This is very fast, secure, reliable, efficient, inexpensive and easy to use.
- ▶ The use of LANs has made the client/server model even more attractive to organisations.

Q.No.36. What is the necessity to shift to client server computing technology?

Introduction: Client/server is described as a 'cost-reduction' technology. These technologies include client/server computing, open systems, fourth generation languages and relational databases. Cost reduction is the main reasons for changing to client server technology. These systems also help to improve control, increase data integrity and security, increase performance and better connectivity.

Following are the main reasons for the adoption of client server technology.

- ▶ Improving the Flow of Management Information
- ▶ Better Services to End-User Departments.
- ▶ Lowering IT costs
- ▶ The ability to manage IT costs better
- ▶ Direct access to required data
- ▶ High flexibility of information processing
- ▶ Direct control of the operating system

Client server technology has been defined as "the provision of information that is required by a user, which is easily accessed despite of the physical location of the data within the organisation".

Q.No.37. Mention some areas where client server systems are being used?

Following are some of the areas where client server technology is currently being used.

- ▶ Online banking application
- ▶ Internal call centre application
- ▶ Applications for end-users that are stored in the server
- ▶ E-commerce online shopping page.

- ▶ Intranet applications.
- ▶ Financial, Inventory applications based on the client server technology
- ▶ Tele communication based on Internet technologies.

**Q.No.38. What are the benefits of Client Server technology?
Discuss the impact of Client server technology to the users of mainframe systems. (RTP)**

Client/server systems bring tremendous benefits to new users, especially the users of mainframe systems. Many businesses are currently in the process of changing or in near future will change from mainframe (or PC) to client / server systems. Following are the benefits of client/server technology:

- a. People in the field of information systems can use client/server computing to make their jobs easier.
- b. Reduce the total cost of ownership.
- c. Increased Productivity i.e. End user productivity & Developer productivity
- d. Takes less people to maintain a client/server application than a mainframe.
- e. The expenses of hardware and network in the client/server environment are less than those in mainframe environment.
- f. Since applications can be easily divided among different users, efficiency will be high.
- g. **Reduce the cost of client's computer.** The server stores data for the clients. So, it is not necessary for clients to have large amounts of disk space. Therefore, less expensive network computers can be used.
- h. Reduce the cost of purchasing, installing, and upgrading software programs and applications on each client computer. Delivery and maintenance will be done from one central point i.e. server.
- i. The management control over the organisation will be increased.
- j. It is very easy to implement client/server system than any other systems.
- k. Leads to new technology and the move to rapid application development such as object oriented technology.
- l. Long term cost benefits for development and support.
- m. Easy to add new hardware to support new systems such as document imaging and video conferencing which are not feasible under mainframe environment.

Q.No.39. What are the characteristics of Client server technology?

There are 10 characteristics that reflect the key features of a client / server system. These ten characteristics are as follows:

- a. **Components:** Client/server architecture consists of a client process and a server process that can be distinguished from each other.
- b. **Separate platforms:** The client portion and the server portions can operate on separate computer platforms.
- c. **Individual upgradation:** Either the client platform or the server platform can be upgraded without upgrading the other platforms.
- d. **Concurrent service:** The server is able to service multiple clients concurrently. In some client/server systems, clients can access multiple servers.
- e. **Networking capability:** The client/server system includes some sort of networking capability.
- f. **Application logic:** A significant portion of the application logic resides at the client end.
- g. **Initiation of action:** Action is usually initiated at the client end, not at the server end.
- h. **GUI:** A user-friendly Graphical User Interface (GUI) generally resides at the client end.
- i. **SQL:** Structured Query Language (SQL) is a common characteristic of majority client/ server systems.
- j. **Security:** The database server will provide data protection and security.

Q.No.40. Discuss the components of a client server technology? (RTP)

Following are the components of C/S technology:

1. **Client: (M04 - 1M)** Generally clients are the personal computers. They are the “users” of the services offered by the servers. Basically, there are 3 types of clients.
 - ▶ **Non-Graphical User Interface (GUI) clients:** They require minimum amount of human interaction. E.g. ATMs, cell phones, fax machines, robots, etc.
 - ▶ **GUI-Clients:** They are human interaction models. They involve object/action models like pull-down menus in Windows.
 - ▶ **Object-Oriented User Interface (OOUI) Clients:** They have further expanded visual formats, multiple workplaces and object interaction rather than application interaction.
2. **Server:** Servers are the systems which provide required data to the clients. Servers receive requests from the client and regulate access to shared resources. Following are different types of servers
 - ▶ File servers help to share files across a network by maintaining a shared library of documents, data, and images.
 - ▶ Database servers can execute Structured Query Language (SQL) requests from clients.
 - ▶ Transaction servers execute a series of SQL commands,
 - ▶ Web servers allow clients and servers to communicate with a universal language called HTTP.
3. **Middleware:** The network system implemented within the client/server technology is known as middleware. Middleware is the software needed to allow clients and servers to interact. Middleware allows for communication, directory services, queuing, distributed file sharing and printing. Generally, middleware consists of four layers - Service, Back-end Processing, Network Operating System and Transport Stacks.
4. **Fat-client or Fat-server:** Fat-client and fat-server are popular terms in computer literature. In a fat-client system, most of the processing takes place in the client. **E.g.** file server or database server. Fat-servers place more emphasis on the server and try to minimize the processing done by clients. Examples of fat-servers are transaction, GroupWare, and web servers. Fat-clients are also known as “2-Tier” systems and fat-servers are known as “3-Tier” systems.
5. **Network hardware:** The network hardware is the communication cords and the devices that link the server and the clients. The communication and data flow over the network is managed and maintained by network software.

Q.No.41. Write about various types of servers?**1. Database Servers: ■**

- ▶ Database Management Systems (DBMS) can be divided into 3 primary components: development tools, user interface, and database engine.
- ▶ The database engine does all the selecting, sorting and updating.
- ▶ Currently, most DBMS combine the interface and engine on each user's computer.
- ▶ Database servers split these two functions, allowing the user interface software to run on each user's PC (the client), and running the database engine in a separate machine (the database server) shared by all users.
- ▶ This approach can increase database performance as well as overall LAN performance because only selected records are transmitted to the user's PC, not large blocks of files.
- ▶ The database engine must handle multiple requests. So, the database server itself is a bottleneck when a large number of requests are pending.
- ▶ Database servers offer real potential for remote database access and distributed databases.
- ▶ The database server sends only selected database record(s) to the client machine (instead of large blocks of data). So, remote access over relatively slow telephone lines can provide acceptable performance.
- ▶ In addition, a client computer can make requests to multiple servers regardless of physical location.

2. Application Servers: ■

- ▶ An application server is a server program that resides in the server (computer) and provides the business logic for the application program.
- ▶ The server program is a program that provides its services to the client program.
- ▶ Application servers are mainly used in web-based applications that have 3-tier architecture.

First Tier: Front End - Browser (Thin Client) - a GUI interface lying at the client/workstation.

Second Tier: Middle Tier - Application Server - set of application programs.

Third Tier: Back End - Database Server.
- ▶ The application server is a second/middle tier of the three-tier architecture. In other words, application servers are now an integral part of 3 three-tier architecture.
- ▶ The application server syncs and combines with the web server for processing the request made by the client.
- ▶ If we look at the request-response flow, the client's request first goes to the web server, which then sends the required information to the application server. It then sends the response back to the web server after taking an appropriate action. The web server then sends the processed information back to the client.
- ▶ Web servers use different approaches or technology for forwarding or receiving back processed information.
- ▶ Some of the most common approaches are given below.

CGI (Common Gateway Interface): Can be written either in JAVA, C, C++, or Perl.

ASP (Active Server Pages): A Microsoft Technology

JSP (Java Server Pages): Java Servlets - Sun's Technology

Java Script (Server Side): Netscape technology which requires livewire for database connectivity.

Features of the Application Servers:

- a. **Component management:** It provides tools to managers for handling all the components and runtime services like session management, synchronous/asynchronous client notifications and executing server business logic.
- b. **Fault tolerance:** Ability of the application server with no single point of failure, defining policies for recovery and fail-over recovery in case of failure of one object or group of objects.
- c. **Load balancing:** Capability to send the request to different servers depending on the load and availability of the server.
- d. **Transaction Management.**
- e. **Management Console:** Single point graphical management console for remotely monitoring clients and server clusters.
- f. **Security:** There are security features for applications security.

Types of application servers:

- a. **Web Information Servers:** This type of server employs HTML templates and scripts to generate pages incorporating values from the database in them. These types of servers are stateless servers. Such servers include Netscape Server, HAHT, Allaire, Sybase, and Silver Stream.
- b. **Component Servers:** The main purpose of these servers is to provide database access and transaction processing services to software components including DLLs, CORBA, and JavaBeans. First, they provide environment for server-side components. Second, they provide access to database and other services to the component. These types of servers are stateless. Examples include MTS (which provides an interface for DLL), Sybase Jaguar, and IBM Component broker.
- c. **Active Application Server:** This type of server supports and provides a rich environment for server-side logic expressed as objects, rules and components. These types of servers are most suitable for dealing with based e-commerce and decision processing.

3. Print Servers:

- ▶ Print servers provide shared access to printers.
- ▶ Most LAN operating systems provide print service. Print service can run on a file server or on one or more separate print server machines.
- ▶ Non-file server print servers can be dedicated to the task of print service.

4. Transaction Servers:

- ▶ MTS or Microsoft Transaction Server is an integral part of Windows NT, and is installed by default as part of the operating system in NT 5.
- ▶ It is part of the system that is available in the background whenever one of our applications requires it.
- ▶ Control and configuration of MTS is via either a snap-in to the Microsoft Management Console, or through the HTML administration pages that are included with MTS.
- ▶ This is very similar to the interface provided for Internet Information Server 4, and gives an integrated management function that is useful when building and setting up distributed applications.

5. Internet Servers:**a. File server:**

- ▶ It is one of the simplest servers.
- ▶ It manages requests from clients for files stored in the server's local disk.
- ▶ A central file server permits groups and users to share and access data in multiple ways.
- ▶ Central file servers are backed up regularly and administrators may put disk space quotas for each user or group of users.

b. Mail server:

- ▶ A mail server is the most efficient way to receive and store electronic mail messages for a group of users.
- ▶ A central mail server can run for 24 hours a day.
- ▶ The mail server can also provide a global e-mail directory for all community and users.

E.g.: "Eudora" is a powerful cross-platform email client that receives incoming mail messages from and sends outgoing mail messages to a mail server.

- c. DNS server: (M08 - 1M)** Domain Name Service is an Internet-wide distributed database system that documents and distributes network-specific information, such as the associated IP address for a host name and vice versa. The host that stores this database is a name server.

- d. Gopher server:** Gopher is an Internet application that uses multiple Gopher servers to locate images, applications, and files stored on various servers on the Internet. For example, "Veronica" is a Gopher application that searches databases of the file contents of worldwide Gopher servers which help to locate Gopher resources.

- e. Web server:** The World Wide Web (WWW) is a very popular Internet source of information. Web browsers present information to the user in hypertext format.

- f. FTP server:** File Transfer Protocol (FTP) is an Internet-wide standard for distribution of files from one computer to another. The computer that stores files and makes them available to others is a server. Client software is used to retrieve the files from the server.

g. News server:

- ▶ Usenet News is a world wide discussion system consisting of thousands of news groups organized into hierarchies by subject.
- ▶ Users read and post articles to these newsgroups using client software. The "news" is held for distribution and access on the news server.

h. Chat server:

- ▶ Some organizations choose to run a server that will allow multiple users to have "real-time" discussions, called "chats" on the Internet. Some chat groups are moderated.
- ▶ However, most of them are unmoderated public discussions.
- ▶ Further, most chat servers allow the creation of "private" chat rooms where participants can "meet" for private discussions.
- ▶ "Chat" is a graphical form of an Internet service called IRC, or Internet Relay Chat.

i. Caching server:

- ▶ A caching server is employed when we want to restrict our number of accesses to the Internet.
- ▶ Basically, a caching server sits between the client computer and the server that would normally fulfill a client's request.
- ▶ Once the client's request is sent, it is intercepted by the caching server.
- ▶ The caching server maintains a library of files that have been requested in the recent past by various users on the network. If the requested information is available in it then the caching server will send such information without going to the original Internet source.
- ▶ Storing the frequently used information locally is a good way to reduce overall traffic to and from the Internet.
- ▶ A caching server does not restrict information flow. Instead, it makes a copy of requested information, so that frequently requested items can be served locally, instead of original Internet source.
- ▶ Caching servers can also be connected in a hierarchy so if the local cache does not have the information, it can pass the request to nearby caching servers that might also contain the desired files.

j. Proxy server:

- ▶ A proxy server is designed to restrict access to information on the Internet.
- ▶ If we don't want our users to access certain material then a proxy server can be used to refuse the access to such material.
- ▶ A proxy server operates on a list of rules given to it by a System Administrator.
- ▶ Some proxy software uses list of specific forbidden sites, while other proxy software examines the content of a page before it is served to the requester. If certain keywords are found in the requested page, access to it is denied by the proxy server.
- ▶ Technologically, there's no substantial difference between a caching server and a proxy server. The difference comes in the desired outcome of such servers.
- ▶ If we want to reduce the overall amount of traffic between our network and the Internet then a caching server is the best choice.
- ▶ On the other hand, if we want to restrict or prohibit the flow of certain types of information to our network, a proxy server will serve that purpose.

Q.No.42. Write about Intrusion Detection System (IDS)?

Meaning: The goal of intrusion detection system is to monitor the network assets, to detect anomalous behavior and misuse. This concept is there for nearly twenty years. But in recent years there is a dramatic rise in its popularity and it is being incorporated into the overall information security infrastructure. Following are different components of IDS:

Components of IDS:**1. Network Intrusion Detection (NID): ■**

- ▶ Network intrusion detection deals with information passing in the wire between hosts.
- ▶ Typically referred to as "packet-sniffers,"
- ▶ Network intrusion detection devices intercept packets traveling in different communication channels. Once captured, the packets are analyzed in a number of different ways.

- ▶ Some NID devices will simply compare the packet with a database consisting of known attacks and malicious packet "fingerprints",
- ▶ While others will look for anomalous (= abnormal) packet activity that might indicate malicious behaviour.
- ▶ In either case, network intrusion detection should be treated as a perimeter defense.

2. Host-based Intrusion Detection (HID): ■

- ▶ Host-based intrusion detection systems are designed to monitor, detect and respond to user and system activity and attacks on a given host.
- ▶ Some more robust tools also offer audit policy management and centralization, supply data forensics, statistical analysis and evidentiary support, and in some cases provide some measure of access control.
- ▶ The difference between host-based and network-based intrusion detection is that NID deals with data transmitted from host to host while HID is concerned with what occurs on the hosts themselves.
- ▶ Host-based intrusion detection is best suited to combat (= fight against) internal threats.
- ▶ Majority of computer threats come from within organization. For example, disgruntled employees, corporate spies, etc.

3. Hybrid Intrusion Detection:

- ▶ Hybrid intrusion detection systems offer management of and alert notification from both network and host-based intrusion detection devices.
- ▶ Hybrid solutions provide the logical complement to NID and HID i.e. Central Intrusion Detection Management.

4. Network-Node Intrusion Detection (NNID): ■

- ▶ Network-node intrusion detection was developed to work around the inherent flaws in traditional NID.
- ▶ Network-node pulls the packet-intercepting technology from the wire and puts it on the host.
- ▶ With NNID, the "packet-sniffer" is positioned in such a way that it captures packets after they reach their final destination i.e. host.
- ▶ The packet is then analyzed just as if it were traveling along the network through a conventional "packet-sniffer."
- ▶ In this approach, network-node is simply another module that can attach to the HID agent. The major disadvantage is that it only evaluates packets addressed to the host on which it resides.
- ▶ On the other hand, traditional network intrusion detection can monitor packets on an entire subnet.
- ▶ "packet-sniffers" are also incapable of viewing a complete subnet when the network uses high-speed communications, encryption or switches since they are essentially "without a sense of smell".
- ▶ But NNID can defend the specific hosts against packet-based attacks in these complex environments where conventional NID is ineffective.

Q.No.43. Write about (a) 2 tier (b) 3 tier (c) N tier architecture.

1. 2-tier architecture: ■

Meaning:

- With the appearance of LAN, PC's are being connected to servers also.
- Servers are mainly database servers which offer data on the server.
- Thus the application intelligence is implemented on the client.
- Since there are only tiered data-server and client, this is called 2-tier architecture.
- This model is still predominant today,
- This is actually opposite to the terminal based system where the entire intelligence lies on the host system.

Suitability: 2-tier architecture is suitable in the following situations –

- a. Tools and middleware implemented in client are –
 - ▶ Relatively inexpensive and well integrated PC-tools and
 - ▶ Good Rapid Application Development (RAD) qualities i.e. simple applications can be produced in a comparatively short time.
- b. Server side uses relatively expensive tools.

Limitations:

- a. Massive applications implemented on PC are expensive to maintain.
- b. Windows 3.X and Mac systems have tough resource restrictions. For this reason application programmers should be well trained in systems technology, so that they can optimize scarce resources.
- c. Since the application logic is executed on the PC, in case of a new software release, all personal computers have to be updated. This is very costly, time consuming, complicated and error prone.
- d. Once the software reaches users desktop it should be installed and then tested for correct execution. Due to distributed character of such a procedure, there is no guarantee that all clients work on the correct copy of the program.

2. 3-tier architecture: ■

In 3-tier architecture, application logic is transferred from the client back to the server.

Tiers: It has the following tiers -

- a. **Client – tier:**
 - ▶ It is responsible for the presentation of data, receiving user events and controlling the user interface.
 - ▶ The actual business logic is moved to application server.
 - ▶ Today, Java – applets offer an alternative to traditionally written PC – applications.
- b. **Application – Server – tier:**
 - ▶ This tier is new, i.e., it is not present in 2-tier architecture.
 - ▶ Business – objects that implement the business rules “live” here, and are available to the client-tier. This level is the central key to solve 2-tier problems.
 - ▶ It protects the data from direct access by the clients.
 - ▶ Furthermore, the term “component” is also found here. Today the term describes visual components on the client-side.
 - ▶ Components on the server-side can be defined as configurable objects, which can be put together to form new application processes.
- c. **Data-server-tier:**
 - ▶ This tier is responsible for data storage:
 - ▶ Besides the widespread relational database systems, existing legacy systems databases are also used here.

Advantages: It solves number of problems that are inherent in 2-tier architecture.

- a. **Clear separation of user-interface-control and data presentation from application-logic:** With this separation more clients are able to have access to a wide variety of server applications. The two main advantages for client-application are
 - ▶ Quicker development
 - ▶ Shorter test phase.
- b. **Dynamic load balancing:** If bottlenecks occur in terms of performance then the server process can be moved to other servers at runtime.
- c. **Change management:**
 - ▶ It is easy and faster to exchange components on the server than to provide number of PCs with new program versions.
 - ▶ In addition such components require high standard of quality control.

3. Multi tier (n tier) architecture: ■**Meaning:**

- ▶ The client program has only UI code.
- ▶ The UI code talks to the “middle tier” on which the business and database logic sits. In turn the middle tier talks to the database.
- ▶ If necessary the middle tier can be placed on the same machine as the database.
- ▶ In either case the data “traffic” is highest between database logic and database.
- ▶ So, the network infrastructure that connects the database logic with the database server needs have very high bandwidth i.e. expensive.

Advantages of Multi-tier architecture: The advantages of a multi-tier architecture are:

- ▶ Forced separation of UI and business logic.
- ▶ Low bandwidth network.
- ▶ Business logic sits on a small number of centralised machines.

Q.No.44. What is a data center and what are the different types of data centers?**Meaning:**

- ▶ A data center is a centralized repository ^(= warehouse) for the storage, management and dissemination _(=distribution) of data and information.
- ▶ Data center is a highly secure, fault-resistant facilities, hosting customer equipment that connects to telecommunications networks.
- ▶ The purpose of a data center is to provide space and bandwidth connectivity for servers in a reliable, secure and scaleable environment.
- ▶ Data centres are often referred to as Internet hotel, server farm, data farm, data warehouse, corporate data center, Internet Service Provide (ISP) or Wireless Application Service Provider (WASP).
- ▶ These facilities can accommodate thousands of servers, switches, routers and racks, storage arrays and other associated telecom equipment.
- ▶ This kind of data center may contain a Network Operations Center (NOC), which is a restricted access area, and contains automated systems which constantly monitor server activity, Web traffic, network performance and report even slight irregularities to engineers Thus engineers can spot potential problem before they happen.
- ▶ The primary 'goal' of a data center is to arrange the required state-of-the-art, redundant infrastructure ^(= additional, more than the required) and systems so as to maximize availability and prevent or mitigate ^(= minimize) any potential downtime for customers.

Different types of Data centers: Data centers serve variety of needs of different businesses. On this basis, data centers can be classified into following two main categories:

- a. **Private Data Centre:** A private data center (also called captive or enterprise data center) is managed by the organization's own IT department, and it provides the applications, storage, web-hosting, and e-business functions needed to maintain full operations. If an organisation wants to outsource these IT functions, then it turns in to a public data center.
- b. **Public data centers:** A public data center (also called internet data centers) provides services ranging from equipment collocation to managing web-hosting. Generally, clients access their data and applications through internet.

Features/Requisites of Data centers: Following are the requisites of data centers.

- | | |
|---------------------------------|----------------------------------|
| ▶ Size, | ▶ Security, |
| ▶ Data Security, | ▶ System monitoring and support, |
| ▶ Availability of Data, | ▶ Storage, |
| ▶ Electrical and power systems, | |

Q.No.45. Write about different tiers in data centers?

- a. Typically, data centers can be classified in tiers, ranging from tier I to tier IV. Tier I being the most basic and inexpensive and tier 4 being the most robust ^(= very tough) and costly. If the application is more 'mission critical' then more redundancy, robustness and security are required for the data center.
- b. **A tier 1 data center:**
- ▶ Need not have redundant power and cooling infrastructures.
 - ▶ It only needs a lock for security and
 - ▶ Can tolerate upto **28.8 hours** of downtime per year.
- c. **A tier 4 data center:**
- ▶ must have redundant systems for power and cooling, with multiple distribution paths that are active and fault tolerant.
 - ▶ access should be controlled with biometric reader and single person entry ways;
 - ▶ gaseous fire suppression is required;
 - ▶ the cabling infrastructure should have a redundant backbone; and
 - ▶ the facility must permit no more than **0.4 hours** of downtime per year.
- d. Tier 1 or 2 is usually sufficient for enterprise data centers because they serve users within a corporation.
- e. Financial data centers are typically tier 3 or 4 because they are critical to our economic stability and therefore must meet the higher standards set by the government.

Q.No.46. Generally which type of organizations need data centers?

- ▶ Any large volume of data that needs to be centralized, monitored and managed centrally needs a data center.
- ▶ Of course, a data center is not mandatory for all organizations that have IT. Everything depends on the size and criticality of data.
- ▶ Data centers are extremely capital-intensive facilities.
- ▶ Commissioning costs amount to millions of dollars and operational costs involved in maintaining redundant connectivity, hardware and human resources, will also be very high.
- ▶ Only for few companies it is economical to commission and operate an enterprise data center.
- ▶ Majority of small, medium and large enterprises host their online and web-enabled applications with established public data centers because they can use the existing infrastructure services, round-the-clock support and monitoring infrastructure.
- ▶ Certain sectors like defence and banks prefer their own infrastructure i.e. private data centers.

Q.No.47. What are the features of data centers? (M06, N06 - 5M)

A data center is a centralized repository ^(= warehouse) for the storage, management and dissemination ^(=distribution) of data and information. Data center is a highly secure, fault-resistant facilities, hosting customer equipment that connects to telecommunications networks. Following are the features of data centers:

1. **Size:** The most distinguishing feature of data centers is their size of operations. A financially viable data center could contain several hundreds to several thousands of servers. This would require a minimum area of around 5,000 to 30,000 square meters. Apart from this, the physical structure of the data center should be able to withstand the weight of the servers. Thus, there is a need for high quality construction.
2. **Data Security:** Another critical issue of data centers is the need to provide maximum data security and 100% availability. Data centers should be protected from intruders through access controls and video surveillance ^(= observation through CCTV cameras, etc). They should be able to withstand natural disasters and calamities like fire, power failures, etc. Disaster Recovery sites must be well maintained.

3. **Availability of Data:** The goal of a data center is to maximize the availability of data and to minimize the downtime. To do this, redundancy should be maintained in case of all important infrastructure such as connectivity, electrical supply, security and surveillance, air conditioning, fire suppression, etc.
4. **Electrical and power systems:** A data center should provide highest power availability with Uninterrupted Power Systems (UPS).
5. **Security:** Physical security and systems security are critical to operations. Thus, it should provide both types of security measures to ensure the security of equipment and data placed at the data center.
 - a. **Physical security:** It can be achieved through
 - ▶ Security guards
 - ▶ Proximity card and PIN for door access
 - ▶ Biometrics devices
 - ▶ 24 x 365 CCTV surveillance and recording
 - b. **Data security:** Data security within a data center should be maintained at multiple levels.
 - ▶ **Perimeter security:** This is to manage both internal and external threats. This consists of firewalls, intrusion detection and content inspections, host security, anti-virus, access control, administrative tools, etc.
 - ▶ **Access management:** This is for both applications and operating systems that host these critical applications.
6. **System monitoring and support:** The data center should provide system monitoring and support so that one can be assured that the servers are being monitored round the clock.
 - a. 24x7x365 hours network monitoring
 - b. Proactive customer notification
 - c. Notification to customers for pre-determined events
 - d. Monitoring of power supply, precision air conditioning system, fire and smoke detection systems, water detection systems, generators and uninterruptible power supply (UPS) systems.

A data center will be considered as world-class only if there are no shortcuts in providing facilities. Connectivity, electrical supply and security are the three most important requirements of any data center.
7. **Storage:** In public data centers, data storage runs into multiple terabytes. As the customer requirements differ, data centers usually have hybrid storage and backup infrastructure. Primarily, data center storage can be differentiated into:
 - ▶ Primary storage (SAN, NAS, DAS)
 - ▶ Secondary storage (tape libraries)
 - ▶ Tertiary storage (offline tape storage, such as DAT drives, and magneto-optical drives)

Most data centers today operate in hands-off mode i.e. no individual enters the data center unless there is a genuine need. All the storage is operated and managed from remote consoles, located outside the data centers.

Q.No.48. Explain the various types of services provided by data centers? (M05 - 5M) (N07 - 5M)

Some of the value added services that a data center provides are:

- a. **Database monitoring:** This is done through a database agent, which enables the high availability of database through comprehensive automated management.
- b. **Web monitoring:**
 - ▶ The main objective is to assess and monitor website performance, availability, integrity and the responsiveness from the visitor's point of view.
 - ▶ It also reports on HTTP, FTP service status, monitors URL availability, response times, verifies web content accuracy and changes.

c. Backup and restore:

- ▶ They provide centralized, multi-system management capabilities.
- ▶ They also provide an integrated management solution for enterprise data storage using specialised backup agents for operating system, database, open files and applications.

d. Intrusion detection system (IDS):

- ▶ ID stands for Intrusion Detection, which is the art of detecting inappropriate, incorrect, or anomalous (=irregular, strange) activity.
- ▶ The term intrusion is used to describe attacks from the outside. Whereas, misuse is used to describe an attack that originates from the internal network.
- ▶ ID systems that operate on a host computer to detect malicious activity on that computer are called host-based ID systems.
- ▶ ID systems that operate on network data flows are called network-based ID systems.
- ▶ The IDS is scalable.

e. Storage on demand:

- ▶ It provides back-end infrastructure as well as expertise, best practices and proven processes to give robust, easy and cost effective storage strategy.
- ▶ It provides data storage infrastructure that supports access to information at any given moment.
- ▶ It also gives security, reliability and availability needed to meet company demands.

Q.No.49. Constituents of a data center / Summarise the essential components of a data centre required for their smooth operation. (N05 - 5M)

To keep equipment running reliably, even under the worst circumstances, the data center is built with the following support infrastructure:

- ▶ Network connectivity with various levels of physical (optical fibre and copper) and service (both last mile and international bandwidth) provider redundancy
- ▶ Dual DG sets and dual UPS
- ▶ HVAC systems for temperature control
- ▶ Fire extinguishing systems
- ▶ Physical security systems - swipe card/ biometric entry systems, CCTV, guards and so on.
- ▶ Raised flooring
- ▶ Network equipment
- ▶ Network management software
- ▶ Multiple optical fiber connectivity
- ▶ Network security - segregating the public and private network, installing firewalls and Intrusion Detection Systems (IDS)

Q.No.50. What are the various alternative solutions available for eliminating or mitigating downtime in data centres? (M06 - 5M) (M08 - 5M)
Disaster Recovery Plans:

- ▶ Data centers need to be equipped with appropriate disaster recovery systems that minimize downtime for its customers.
- ▶ Downtime can be eliminated by having proper Disaster Recovery (DR) Plans for mission-critical types of organisations.
- ▶ Some of the larger IT organizations, which cannot tolerate too much downtime, will set up their DR site as a hot site.
- ▶ Here, both primary and DR sites are kept in real-time synchronisation.

Types of DR sites: Following are the different types of disaster recovery plans

- a. **Cold site:** It is an alternative facility which does not consist of any resources or equipment, except air conditioning and raised flooring. Equipment and resources must be installed to duplicate the critical business functions of an organisation. Cold sites may vary depending on the communication facilities.
- b. **Warm site:** This is an alternate processing site that is only partially equipped. It can be either shared (sharing servers, equipment) or dedicated (own servers). They are similar to cold sites with minimal equipment and resources which are required to start critical operations of a business.
- c. **Hot site:** Hot sites are fully equipped with the required facilities and resources needed to recover business functions that are affected by a disaster. Hot sites may vary in the type of facilities offered (such as data processing, communications or any other critical business functions needing duplication). The location and size of the hot site must be proportional to the equipment and resources needed.

Q.No.51. State the challenges faced by organisations in the management of data centres.

Following are challenges faced by organisations in the management of data centers:

- a. **Maintaining skilled staff and high infrastructure needed for daily data center operations:** A company needs to have staff that is expert in network management, has software and hardware skills. The company has to employ large number of such employees, as they have to work on shift basis.
- b. **Maximising uptime and performance:** While establishing sufficient redundancy and maintaining water tight security; data centers should maintain maximum uptime and system performance.
- c. **Technology selection:** The other challenges that enterprise data centers face is technology selection, which is very crucial for their operations. Another problem is compensating for obsolescence.
- d. **Resource balancing:** The enterprise needs to balance reduced operational budgets, increased demands on existing infrastructure, maximise availability, ensuring round-the-clock monitoring and management, periodic upgrades, etc. That is why even some of the largest enterprises in the world prefer public data centres.

Q.No.52. What are disaster events?

- ❖ Disasters are disruptions which make the entire facility inoperative for a long period of time (usually more than a day).
- ❖ There is a potential for significant interruption to normal business processing.
- ❖ All disruptions ^(=disturbances) are not disasters,
- ❖ In case of disaster there is a potential for significant interruption to normal business processing,
- ❖ Business is associated with natural disasters ^(=calamity) like earthquake, flood, tornadoes, thunderstorms, fire, etc.
- ❖ On the other hand catastrophes are disruptions resulting from disruption of processing facility.

Q.No.53. Write short notes on Business Continuity Plan (BCP)?

BCP: A Business Continuity Plan (BCP) is a documented description of

- ▶ action, resources and procedures to be followed before, during and after an event,
- ▶ vital functions to business operations are recovered,
- ▶ operational in an acceptable time frame.

Steps in the development of BCP:

Phase 1: Define requirements based on business needs

This involves risk analysis in critical, vital, sensitive and non critical areas, determining critical time period, applications to be recovered in critical recovery time period and coverage of insurance.

Phase 2: Statements of critical resources needed

It involves determination of minimum resources necessary, review of operations between current practices and backup procedures (whether they are adequate to support a business resumption plan).

Phase 3: Detailed planning on use of critical resources

This involves:

- ▶ Identification of most appropriate recovery solutions including information processing and telecommunication recovery,
- ▶ Hot sites which are fully configured and ready to operate within several hours.
- ▶ Warm sites are partially configured with network connections and selected peripheral equipments but without the main computer.
- ▶ Cold sites are ready to receive equipment but do not offer any equipment at the site in advance. It only provides basic environment to operate an information processing facilities.
- ▶ Duplicate information processing facilities.
- ▶ Reciprocal agreements.
- ▶ Preparing a list of alternatives,
- ▶ Visits and reviews

Phase 4: Define responsibilities of trained personnel

This involves:

- ▶ Plan preparation
- ▶ Provision for requirement of manual process,
- ▶ Document revised work flow,
- ▶ Plan development,
- ▶ Team building,
- ▶ Developing general plan.

Phase 5: Written documentations and procedures to cover all operations

This involves testing BCP in various phases like –

- ▶ Pre-test,
- ▶ Test,
- ▶ Post-test,
- ▶ Paper test,
- ▶ Preparedness test,
- ▶ Review test,
- ▶ Review test results

Phase 6: Commitment to maintain plan as per the changing needs

This involves Maintenance by BCP Coordinator who has to arrange for

- ▶ scheduled and unscheduled tests,
- ▶ develop a scheduled training,
- ▶ maintain records of test,
- ▶ training and review,
- ▶ update notification directory.

Q.No.54. What is a security program. What are the steps involved in security program?

Meaning: Network security consists of provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network accessible resources from unauthorized access and the effectiveness of these measures together.

Need for security: The basic objective of providing network security is two fold:

(a) to safeguard assets and (b) to ensure and maintain data integrity.

Types of security: There are two types of systems security

a) Physical security is implemented to protect the physical assets of an organization like personnel, hardware, facilities, supplies and documentation.

b) Logical security is intended to control (i) malicious and non-malicious threats to physical security and (ii) malicious threats to logical security itself.

Security program: The task of Security Administration in an organization is to conduct a security program which involves the following eight steps:

Step 1: Preparing project plan for enforcing security

In a sequence, the components of project plan are

- ▶ outlining the objectives of the review
- ▶ determining the scope of the review and tasks to be accomplished,
- ▶ assigning tasks to the project team
- ▶ preparing resources budget which will be determined by the volume and complexity of the review and
- ▶ fixing a target / schedule for task completion.

Step 2: Assets identification

Assets which need to be safeguarded are identified and subdivided into Personnel, Hardware, Facilities, Documentation, Supplies, Data, Application Software and System Software.

Step 3: Assets valuation

This is a very difficult job. The valuation can differ depending on

- ▶ age of assets
- ▶ the person doing the valuation,
- ▶ the way in which the asset can be lost
- ▶ the period for which it is lost and
- ▶ how old is the asset.

Valuation of assets include valuation of logical assets also. For example, the replacement value of the contents in a hard disk may be several times more than the replacement value of the hard disk itself.

Step 4: Threats Identification

The source of a threat can be external or internal and the nature of a threat can be non-deliberate (accidental) or deliberate.

Examples: non-deliberate external threat - act of God.
 non-deliberate internal threat – pollution.
 deliberate external threat – hackers
 deliberate internal threat - employees.

In other words, the sources of threat are the Nature or acts of God like earthquake, flood, fire, extreme temperatures and electromagnetic radiations followed by other sources like Hardware / Software Suppliers, Competitors, Contractors, Shareholders / Debenture holders, Unions, Governmental Regulations, Environmentalists, Criminals / Hackers, Management, Employees and Unreliable Systems.

Step 5: Assessment of probability of occurrence of threats

The fifth step is assessment of the probability of occurrence of threats over a given time period. This exercise is not so difficult if prior period statistical data is available. If prior period data is not available, it has to be extracted from the associated stakeholders like end users (providing the data aspect) and the management (providing the control aspect)

Step 6: Exposure analysis

It is done in the following order

- ▶ identify the controls in the place,
- ▶ assess the reliability of the existing controls,
- ▶ evaluate the probability that a threat can be successful and
- ▶ assess the resulting loss if the threat is successful.

For each asset and each threat the expected loss can be estimated as the product of

- ▶ the probability of threat occurrence,
- ▶ probability of control failure and
- ▶ the resulting loss if the threat is successful.

Step 7: Controls adjustment

The controls should be adjusted in such a way that the cost of control is lower than the reduction in the expected losses. The reduction in the expected losses is the difference between expected losses with the (i) existing set of controls and (ii) improved set of controls.

Step 8: Report generation

Report generation includes

- ▶ documenting the findings of the review
- ▶ recommending new asset safeguarding techniques
- ▶ recommending the existing assets safeguarding mechanisms that should be eliminated / rectified,
- ▶ and also recommending the levels of security to be followed for individual end users and systems.

Q.No.55. Explain the threats and vulnerabilities involved in system security and state the measures to overcome them? (M08 - 5M)

The threats to the security of systems assets can be broadly divided into nine categories. Following table shows the threats and vulnerabilities involved in system security and the measures to be taken to overcome them.

1.	Fire,	Use of fire detection and fire avoiding equipment like automatic fire extinguishers.
2.	Water	Well designed water protection system.
3.	Energy variations like voltage fluctuations, circuit breakage, etc.	Use voltage stabilizers, circuit breakers, etc.
4.	Structural damages	Insurance.
5.	Pollution	Use dust proof material at the time of construction of computer room and ensure dust free environment.
6.	Intrusion like physical intrusion and eavesdropping	- Physical access controls, - prevention of electromagnetic emission,
7.	Viruses and Worms	Use preventive, detective and corrective controls.
8.	Misuse of software, data and services	Prepare employee's code of conduct.
9.	Hackers	Through robust logical access controls and/or Cyber laws of the land.

Abuse of software, Data and Services can arise in any of the following ways:

- a. Without any authority, employees may take away the copies of generalized software and proprietary databases of the organization. They may keep it for their own purposes or they may hand it over to competitors,
- b. Organizations fail to protect the privacy of individuals whose data is stored in databases,
- c. Employees use system services for their own personal gains and activities,

Q.No.56. Write about the following threats (a) Virus (b) Worms (c) Hackers

Virus: ■

- ▶ A virus is a malicious program that attaches itself to a legitimate program and penetrates into the operating system.
- ▶ A virus is a program that instructs the operating system to append it to other programs and thus propagates to other programs via files containing macros.

- ▶ A virus can replicate itself over and over and the replicated modules can grow independent of the initial virus.
- ▶ Sometimes a virus can be benevolent and it may cause minor disruptions by printing laughing message and sometimes a virus can be malignant and it may delete files or corrupt other programs.

Following are the controls to safeguard against the viruses:

a. Preventive controls like:

- ▶ using only clean and licensed copies of software,
- ▶ cutting the use of public domain software / shareware,
- ▶ downloading files or software only from reliable websites,
- ▶ implementing read-only access to software.
- ▶ checking new files / software with anti-virus software before installation,
- ▶ imparting education and training programs to end users

b. Detective controls like:

- ▶ regularly running antivirus software,
- ▶ file size comparison to observe whether the size of programs has changed,
- ▶ date / time comparisons to detect any unauthorized modifications.

c. Corrective controls like:

- ▶ maintaining a clean backup,
- ▶ having a recovery plan from virus infections,
- ▶ regularly running antivirus software (which is useful for both detection & removal of virus)

Worms: ■

- ▶ A computer worm is a self-replicating computer program.
- ▶ Worms are similar to viruses but they exist as separate and independent programs.
- ▶ It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention.
- ▶ Unlike a virus, worms do not need to attach itself to an existing program.
- ▶ Worms may cause harm to the network. For e.g. they may consume bandwidth.
- ▶ They exploit security weaknesses / bugs in the operating system to penetrate into other systems.
- ▶ Exposures that arise from worms are more difficult to control than that arise from virus.
- ▶ Generally anti virus / anti spyware software can prevent the attacks from Worms.

Hackers: ■

- ▶ Hackers attempt to gain unauthorized entry into a system by circumventing the access control mechanism of the system. They can do this either with good or bad intention.
- ▶ Some hackers may just trespass and read the files without making any changes to them.
- ▶ Some hackers may cause destruction by deleting critical files, disrupting / suspending operations, stealing sensitive data and / or programs.
- ▶ They can be avoided only through robust logical access controls and / or Cyber Laws of the Land.

Classification of Questions (Based on PCC exams)

A category questions : Q.No. 5, 6, 11, 12, 15, 16, 17, 18, 19, 20, 25, 27, 28, 29, 30, 31, 32, 35, 37, 40, 41(only Caching server & proxy server are imp.), 42, 43, 44, 45, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56.

B Category Questions : Q.No.4, 8, 13, 22, 23, 33, 34, 36, 38, 39, 41, 46,

C Category Questions : Q.No.1, 2, 3, 7, 10, 14, 21, 26,

1 mark questions:

LAN	File Server	Workstation	Network Interface Card	Twisted pair cables
Co-axial cables	Fiber optic cables	MAN	VPN	MODEM
Multiplexer	Front end communication processor	Protocol converters	Hub	Switches
Repeaters	Bridges	Gateways	Routers	Remote Access Devices
Serial Transmission	Parallel transmission	Circuit switching	Message switching	Packet switching
Bandwidth	Communication protocols	TCP/IP	Database servers	Application servers
Print servers	Transaction server	Mail server	DNS server	Gopher server
Web server	FTP server	News server	Chat server	Caching server
Proxy server	2 tier architecture	3 tier architecture	Data center	Virus
Worms	Hackers			

Note: This classification is made keeping in mind NOV 2008 exams of PCC.

The classification may change for May 2009 exams (minor modifications).

For latest updates keep in touch with our website.

The End