Question: Give some detail about "fault tolerance".

Answer: Fault tolerance means the system will not fail because any one component fails. The system also should provide recovery from multiple failures. Components are often over engineered or purposely underutilized to ensure that while performance may be affected during an outage the system will perform within predictable, acceptable bounds.

Question: What are regulatory Agencies?

Answer: All communication technology is subject to regulation and laws by government agencies. The purpose is to protect Public Interest by regulating Radio, Television and Cable Communications.

Question: What is the main problem with ASK (amplitude Shift Keying)?

Answer: The main problem with ASK is the noise. Noise usually affected the amplitude so it is most affected by Noise.

Question: What are the basic components of a data communication system ?

Answer: There are five basic components of a data communication. These are as follows:- 1) message 2) sender 3) receiver 4) medium 5) protocol

---

Question: How can I define Data communication?

Answer: Data communication is the name of a communication between computers. More specifically, the exchange of data in the form 0's and 1's between two devices (computers) via some form of the transmission medium. Nowadays, data communication between computers also supports digital speech telephone and videophone, thus following direct communication between people.

Question: What is PCMCIA?

Answer: PCMCIA (Personal Computer Memory Card International Association) is an international standards body and trade association with over 100 member companies that was founded in 1989 to establish standards for Integrated Circuit cards and to promote interchangeability among mobile computers where ruggedness, low power, and small size were critical. As the needs of mobile computer users has changed, so has PCMCIA. By 1991, PCMCIA had defined an I/O interface for the same 68 pin connector initially used for memory cards. At the same time, the Socket Services Specification was added and was soon followed by the Card Services Specifcation as developers realized that common software would be needed to enhance compatibility.

Question: Will VoIP work with DSL?

Answer: Yes, VoIP works with DSL. Many of the phone companies currently providing DSL and landline phone services are in the process of unbundling

DSL and phone services.

Question: What is attenuation?

Answer: Attenuation is signal loss due to the diminishing availability of signal energy, or signal power. As a analog or digital signal traverses across a medium, it fades. High attenuation may lead to the inability to recover the signal on the far end. Signal repeaters may be used on the transmission path to periodically boost the signal strength. Baseband transmission is extremely limited to attenuation. Broad-band much less so, In addition, wireless communications is much less susceptible to attenuation that is wire-line communications such as x-DSL or cable modems.

Question: What is difference between logical address and physical address?

Answer: The OSI model is a good place to start to learn more about the differences between physical and logical addressing. Think of the physical address as the 48-bit MAC address that manufacturers encode in their network interface cards (NICs). This type of address is unique, referred to as the Ethernet or hardware address, and cannot be changed. The MAC or Ethernet address is associated with Layer 2 (data Link) of the OSI Model. The logical address is a 32-bit IP address that is not embedded in the network card but it is assigned to it for the purpose of routing between networks. This type of address operates at Layer 3 (network) of the OSI Model.

Question: What is the differences between OSI and TCP/IP Model?

Answer: The ISO/OSI protocol is a 7 layer reference model that was designed after TCP/IP model, which only has 4 layers. That said, the differences between the two are only minor.
The 7 layers of the OSI Protocol Stack are as follows:
7. Application: end user services such as email
6. Presentation: data problems and data compression
5. Session: authentication and authorization
4. Transport: guarantee end-to-end delivery of packets
3. Network: packet routing
2. Data Link: transmit and receive packets
1. Physical: The physical connection or cable itself.
Of these 7 layers, the 4 layers the TCP/IP Protocol Stack use are as follows:
5. Application: authentication, compression, and end user services
4. Transport: handles the flow of data between systems and provides access to the network for applications via the BSD socket library
3. Network: packet routing
2. Link: Kernel OS/device driver interface to the network interface on the computer.
The main differences between OSI and TCP/IP are:
The application layer in TCP/IP handles the responsibilities of layers 5,6, and 7 in the OSI model. The transport layer in TCP/IP does not always

guarantee reliable delivery of packets as the transport layer in the OSI model does.
So as you can see there is not too much difference between the models. In terms of software implementation TCP/IP looks like this:
Application Layer: some of the applications covered are SMTP (mail), Telnet, FTP, Rlogin, NFS, NIS, and LPD.
Transport Layer: the transport uses two protocols, UDP (User Datagram Protocol) and TCP, which does not guarantee packet delivery and applications which use this must provide their own means of verifying delivery. TCP guarantees delivery of packets to the applications that use it.
Network Layer: the network layer is concerned with packet routing and used low level protocols such as ICMP, IP, and IGMP.
Link Layer: the link layer is concerned with the actual transmittal of packets as well as IP to Ethernet address translation. This layer is concerned with Arp, the device driver and Rarp.

Question: What is Tx and Rx?

Answer: Tx is the abrivation used for transmission/ transmitor and Rx is reciever.

Question: What do we mean by wireless networking?

Answer: The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs.

Question: What is PDU in OSI Model?

Answer: Normally a communication request originates at the highest layer (Application Layer). The request is passed down through the lower layers in the form of a packet called a protocol data unit (PDU). Layers in the protocol stack communicate with their adjacent layers via one or more Service Access Points (SAP). Each succeeding layer in the stack adds its own information to the PDU that will be read by its counterpart (peer) layer on the receiving system. Once the data arrives at the lower layers, the PDU is encoded into data frames and placed onto the cable for transmission. The data frames make their way to the receiving system and the entire process is reversed as the PDU makes its way up the protocol stack. As it moves up the stack, each layer "unwrap" the PDU and receives the information from its peer layer on the sending system.

Question: What is the difference between WAP and GPRS?

Answer: Wireless Application Protocol, a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones. Wireless Application Protocol (or WAP) is envisioned as a comprehensive and scalable protocol designed to use with mobile phones

using Short Message Services (SMS), General Packet Radio Services (GPRS), CDMA and GSM.

Question: What are routers, repeaters and bridges?

Answer: Router: Routers relay packets among multiple interconnection networks. Router is device that determines the next network point to which a data packet should be forwarded enroute toward its destination. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet.

Question: What do we mean by capacity of the channel?

Answer: Channel capacity: The maximum possible information transfer rate through a channel, subject to specified constraints.

Question: What is remote data communication?

Answer: Data Communication is considered remote, if the devices are farther apart.

Question: Explain VPN (Virtual Private Network

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

Question: Define Protocols

Answer: Protocol is an agreed-upon format for transmitting data between two devices. The protocol determines the following: 1) The type of error checking to be used. 2) Data compression method, if any. 3) How the sending device will indicate that it has finished sending a message? 4) How the receiving device will indicate that it has received a message?

Question: Define encryption of data.

Answer: Encryption of data: The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

Question: Can we implement OSI in wireless networks?

Answer: Wireless Application Protocol (WAP), a secure specification that allows users to access information via handheld wireless devices, specifies

architecture based on layers that follow the OSI model fairly closely. WAP defines network architecture for content delivery over wireless networks. Central to the design of WAP is a network stack based on the OSI model. WAP implements several new networking protocols that perform functions similar to the well-known Web protocols HTTP, TCP, and SSL.

Question: What is distributed processing?

Answer: It refers to any of a variety of computer systems that use more than one computer, or processor, to run an application. This includes parallel processing, in which a single computer uses more than one CPU to execute programs. More often, however, distributed processing refers to local-area networks (LANs) designed so that a single program can run simultaneously at various sites. Most distributed processing systems contain sophisticated software that detects idle CPUs on the network and parcels out programs to utilize them. Another form of distributed processing involves distributed databases, databases in which the data is stored across two or more computer systems. The database system keeps track of where the data is so that the distributed nature of the database is not apparent to users.

Question: What is a sample?

Answer: Sample is the amplitude of an analog signal at some specific interval. It is achieved in pulse amplitude modulation, which is the first step towards analog to digital conversion.

Question: What Is Line Discipline?

Answer: Whatever the system, no device in it should be allowed to transmit until that device has evidence that the intended receiver is able to receive and is prepared to accept the transmission. What if the receiver does not expect a transmission, is busy, or is out of commission? With no way to determine the status of intended receiver, the transmitting device may waste its time sending data to a nonfunctioning receiver or may interfere with signals already on the link. The line discipline function of the data link layer oversees the establishment of links and the right of a particular device to transmit at a given time. Line discipline answers the question. Who should send now?

Question: Is it possible for digital data to be transmitted via ordinary phone line?

Answer: The Digital Subscriber line (DSL) is a newer technology that uses the existing telecommunication networks such as the local loop telephone line (still an analog line) to accomplish high speed delivery of data, voice, video and multimedia.

Question: What is then difference between T-lines and E-Lines?

Answer: Europeans use a version of T lines called E lines. The two systems are conceptually identical, but their capacities differ.

Question: What do we mean by the term session?

Answer: Session is the period of time a user interfaces with an application. The user session begins when the user accesses the application and ends when the user quits the application.

Question: How can I define Data communication?

Answer: Data Communication is the exchange of data (in the form of 0's and 1's) between two devices (computers) via some form of the transmission medium. Data communication is communication between computers. Data communication concerns the exchange of digital data between computers. Nowadays, data communication between computers also supports digital speech telephone and videophone, thus supporting direct communication between people.

Question: How could it be more secure using distributed processing?

Answer: In this case security is achieved by providing the user with limited access. It means that user can only perform those tasks which are allowed by system designer. Its' simple example is bank's ATM. Where user can't perform operations on database other than provided.

Question: What does the terms transit and response time mean? Also tell me about the topic peak load periods.

Answer: Transit time is the time taken by the message to travel from source to destination. Response time is the time of response (acknowledgement) from destination to source. Peak load periods are those periods of time in which number of users on a network are more than normal time.

Question: What are the advantages of networking?

Answer: • Files can be stored on a central computer (the file server) allowing data to be shared throughout an organization. • Files can be backed up more easily when they are all on a central fileserver rather than when they are scattered across a number of independent workstations. • Networks also allow security to be established, ensuring that the network users may only have access to certain files and applications. • Software and resources can be centrally managed. • Network versions of software often allow for their speedy installation on workstations from the file server. • Expensive devices such as laser printers or scanners can be shared. • Users can access their files from any workstation

---

Question: What are different factors to choose a network topology?

Answer: Working conditions of network, working scenarios, arrangement of links and devices. Depending upon our network what actually we are dealing with and in which geographical area our devices are present, small area available

or have large area. All these factors are considered when choosing a Topology.

Question: What is the relative status of the devices to be linked?

Answer: The geographical area in which our devices are present is the relative status of devices.

Question: What is the definition of Hub?

Answer: Hub is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. A passive hub serves simply as a conduit for the data, enabling it to go from one device (or segment) to another. So-called intelligent hubs include additional features that enable an administrator to monitor the traffic passing through the hub and to configure each port in the hub. Intelligent hubs are also called manageable hubs. A third type of hub, called a switching hub, actually reads the destination address of each packet and then forwards the packet to the correct port.

Question: What do we mean by "TAP"?

Answer: A tap is a connection to a coaxial cable in which a hole is drilled through the outer shield of the cable so that a clamp can be connected to the inner conductor of the cable. Instead of cutting the cable and attaching connectors to both ends of the severed coaxial cable,

Question: Give some detail about "fault tolerance".

Answer: Fault tolerance means the system will not fail because any one component fails. The system also should provide recovery from multiple failures. Components are often over engineered or purposely underutilized to ensure that while performance may be affected during an outage the system will perform within predictable, acceptable bounds

---

Question: What is the difference between radio and microwave?

Answer: Although there is no clear-cut demarcation between radio and microwave, electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 GHz and 300 GHz are called microwaves. Radio waves are used for multicast communications, such as radio and television systems.

Question: What is the difference between internet and intranet?

Answer: Internet The Internet is a system of linked networks that are worldwide in scope and facilitate data communication services such as remote login, file transfer, electronic mail, the World Wide Web and newsgroups. With the meteoric rise in demand for connectivity, the Internet has become a

communications highway for millions of users. The Internet was initially restricted to military and academic institutions, but now it is a full-fledged conduit for any and all forms of information and commerce. Internet websites now provide personal, educational, political and economic resources to every corner of the planet. Intranet A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access. Like the Internet itself, intranets are used to share information. Secure intranets are now the fastest-growing segment of the Internet because they are much less expensive to build and manage than private networks based on proprietary protocols.

Question: What is the difference between hub and switch?

Answer: On the outside, hubs and switches appear very similar in that they both have a number of RJ-45 jacks for connecting devices. Inside, however, they work very differently. To understand why switches provide so much more functionality than hubs, you must understand a fundamental limitation of (non-switched) Ethernet: there can only be one device transmitting on a segment at any given time. If two or more devices attempt to transmit at the same time, a collision occurs. (In fact, an Ethernet segment where only one conversation can occur is called a collision domain.) After a collision, all devices must retransmit. As you can imagine, as the number of devices on an Ethernet segment increases, the probability for collisions increase. Because devices must spend more time retransmitting data, the network is perceived to be slow. Before the advent of switches, a network could be divided into segments with a device called a bridge. Bridges have two Ethernet ports. As traffic flows through a network, a bridge learns which devices (identified by the MAC or "hardware" address) are on each side. The bridge then makes decisions to forward or not forward each packet to the other side based on where the destination device is located. A bridge thus divides a network into two collision domains, allowing two independent "conversations" to occur. If a bridge is placed intelligently (e.g., separating two departments and their respective file servers), they can improve network efficiency. Hubs do no processing on network traffic--they simply repeat the incoming signal to all available ports. On a switch, every port acts as a bridge. If each switch port is connected to a single device, each device can, in principle, act independently of every other device. For example, consider a switch with the following devices attached: computer 1 computer 2 computer 3 printer file server uplink to the Internet In this case, computer 1 could be printing a document, while computer 2 connects to a files server, while computer 3 accesses the Internet. Because the switch intelligently forwards traffic only to the devices involved, there can be multiple independent simultaneous conversations.

Question: How different layers of OSI model are implemented?

Answer: The OSI 7 layers model has clear characteristics. Layers 7 through 4 deal with end to end communications between data source and destinations. Layers 3 to 1 deal with communications between network devices. On the other hand, the seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium.

Question: How can we define networking?

Answer: In information technology, networking is the construction, design, and use of network, including the physical (cabling, hub, bridge, switch, router, and so forth), the selection and use of telecommunication protocol and computer software for using and managing the network, and the establishment of operation policies and procedures related to the network

---

Question: What is walkie talkie?

Answer: A handie talkie, often referred to by its abbreviation, HT, is a handheld, portable two-way radio transceiver. This type of radio is sometimes called a "walkie talkie" or a "handheld." Handie talkies are popular among amateur radio operators, especially on their VHF and UHF bands at 144 and 432 MHz. Handie talkies are widely used by security personnel, military personnel, and police officers. Most HTs are used in conjunction with repeaters for extended range. Some HTs are designed for the 27-MHz Citizens Band (CB) radio service. A typical HT is a rectangular box about the size and weight of an old-fashioned telephone handset. The antenna protrudes from the top end, and consists of a coiled-up element encased in rubber and wound around a flexible rod. This type of antenna, known as a "rubber duck," is not particularly efficient, but is convenient and rugged. Volume and squelch controls are usually placed next to the antenna. The frequency control knob or buttons are on the top end or the front.