COMPUTER NETWORK QUESTION BANK

FAQ's with Answers from Computer Network Domain

Prof. Avadhoot Joshi
[Computer Department]
MAEER's MIT, College Of Engineering
Paud Road, Kothrud, Pune

Oral Question Bank

Define Network?

A network is a set of devices connected by physical media links. A network is recursively is a connection of two or more nodes by a physical link or two or more networks connected by one or more nodes.

What is a Link?

At the lowest level, a network can consist of two or more computers directly connected by some physical medium such as coaxial cable or optical fiber. Such a physical medium is called as Link.

What is a node?

A network can consist of two or more computers directly connected by some physical medium such as coaxial cable or optical fiber. Such a physical medium is called as Links and the computer it connects is called as Nodes.

What is a gateway or Router?

A node that is connected to two or more networks is commonly called as router or Gateway. It generally forwards message from one network to another.

What is point-point link?

If the physical links are limited to a pair of nodes it is said to be point-point link.

What is Multiple Access?

If the physical links are shared by more than two nodes, it is said to be Multiple Access.

What are the advantages of Distributed Processing?

a. Security/Encapsulation
b. Distributed database
c. Faster Problem solving
d. Security through redundancy
e. Collaborative Processing

What are the criteria necessary for an effective and efficient network?

a. Performance
It can be measured in many ways, including transmit time and response time.
b. Reliability
It is measured by frequency of failure, the time it takes a link to recover from a failure, and the network’s robustness.
c. Security
Security issues includes protecting data from unauthorized access and viruses.

Name the factors that affect the performance of the network?

a. Number of Users
b. Type of transmission medium
c. Hardware
d. Software

Name the factors that affect the reliability of the network?

a. Frequency of failure
b. Recovery time of a network after a failure

Name the factors that affect the security of the network?

a. Unauthorized Access
b. Viruses

What is Protocol?

A protocol is a set of rules that govern all aspects of information communication.

What are the key elements of protocols?

The key elements of protocols are
a. Syntax
It refers to the structure or format of the data, that is the order in which they are presented.
b. Semantics
It refers to the meaning of each section of bits.
c. Timing
Timing refers to two characteristics: When data should be sent and how fast they can be sent.

What are the key design issues of a computer Network?

a. Connectivity
b. Cost-effective Resource Sharing
c. Support for common Services
d. Performance

Define Bandwidth and Latency?

Network performance is measured in Bandwidth (throughput) and Latency (Delay). Bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time. Latency corresponds to how long it t5akes a message to travel from one end off a network to the other. It is strictly measured in terms of time.

Define Routing?

The process of determining systematically hoe to forward messages toward the destination nodes based on its address is called routing.

What is a peer-peer process?

The processes on each machine that communicate at a given layer are called peer-peer process.

When a switch is said to be congested?

It is possible that a switch receives packets faster than the shared link can accommodate and stores in its memory, for an extended period of time, then the switch will eventually run out of buffer space, and some packets will have to be dropped and in this state is said to congested state.

What is Round Trip Time?

The duration of time it takes to send a message from one end of a network to the other and back, is called RTT.

Define the terms Unicasting, Multicasting and Broadcasting?

If the message is sent from a source to a single destination node, it is called Unicasting.
If the message is sent to some subset of other nodes, it is called Multicasting.
If the message is sent to all the m nodes in the network it is called Broadcasting.

What is Multiplexing?

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

Name the categories of Multiplexing?

a. Frequency Division Multiplexing (FDM)
b. Time Division Multiplexing (TDM)
  i. Synchronous TDM
  ii. Asynchronous TDM or Statistical TDM.
c. Wave Division Multiplexing (WDM)

What is FDM?

FDM is an analog technique that can be applied when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted.

What is WDM?

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve light signals transmitted through fiber optics channel.

What is TDM?

TDM is a digital process that can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices.

What is Synchronous TDM?

In STDM, the multiplexer allocates exactly the same time slot to each device at all times, whether or not a device has anything to transmit.

List the layers of OSI

a. Physical Layer
b. Data Link Layer
c. Network Layer
d. Transport Layer
e. Session Layer
f. Presentation Layer
g. Application Layer

Which layers are network support layers?

a. Physical Layer
b. Data link Layer and
c. Network Layers

Which layers are user support layers?

a. Session Layer
b. Presentation Layer and
c. Application Layer

Which layer links the network support layers and user support layers?

The Transport layer links the network support layers and user support layers.

What are the concerns of the Physical Layer?

Physical layer coordinates the functions required to transmit a bit stream over a physical medium.
a. Physical characteristics of interfaces and media
b. Representation of bits
c. Data rate
d. Synchronization of bits
e. Line configuration
f. Physical topology
g. Transmission mode

What are the responsibilities of Data Link Layer?

The Data Link Layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-node delivery.

1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.

What are the responsibilities of Network Layer?

The Network Layer is responsible for the source-to-destination delivery of packet possibly across multiple networks (links).
a. Logical Addressing
b. Routing

What are the responsibilities of Transport Layer?

The Transport Layer is responsible for source-to-destination delivery of the entire message.
a. Service-point Addressing
b. Segmentation and reassembly
c. Connection Control
d. Flow Control
e. Error Control

What are the responsibilities of Session Layer?

The Session layer is the network dialog Controller. It establishes, maintains and synchronizes the interaction between the communicating systems.
a. Dialog control
b. Synchronization

What are the responsibilities of Presentation Layer?

The Presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
a. Translation
b. Encryption
c. Compression

What are the responsibilities of Application Layer?

The Application Layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as e-mail, shared database management and other types of distributed information services.
a. Network virtual Terminal
b. File transfer, access and Management (FTAM)
c. Mail services
d. Directory Services

What are the two classes of hardware building blocks?

Nodes and Links.

What are the different link types used to build a computer network?

a. Cables
b. Leased Lines
c. Last-Mile Links
d. Wireless Links

What are the categories of Transmission media?

a. Guided Media
  i. Twisted - Pair cable
    1. Shielded TP
    2. Unshielded TP
  ii. Coaxial Cable
  iii. Fiber-optic cable
b. Unguided Media
  i. Terrestrial microwave
  ii. Satellite Communication

What are the types of errors?

a. Single-Bit error
  In a single-bit error, only one bit in the data unit has changed
b. Burst Error
  A Burst error means that two or more bits in the data have changed.

What is CRC?

CRC, is the most powerful of the redundancy checking techniques, is based on binary division. CRC appends a sequence of redundant bits derived from binary division to the data unit. The divisor in the CRC generator is often represented as an algebraic polynomial.

What is Checksum?

Checksum is used by the higher layer protocols (TCP/IP) for error detection

What are the Data link protocols?

Data link protocols are sets of specifications used to implement the data link layer. The categories of Data Link protocols are

1. Asynchronous Protocols
2. Synchronous Protocols
   a. Character Oriented Protocols
   b. Bit Oriented protocols

Compare Error Detection and Error Correction:

The correction of errors is more difficult than the detection. In error detection, checks only any error has occurred. In error correction, the exact number of bits that are corrupted and location in the message are known. The number of the errors and the size of the message are important factors.

What is Forward Error Correction?

Forward error correction is the process in which the receiver tries to guess the message by using redundant bits.

Define Retransmission?

Retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-freed.

What is Flow Control?

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

What is Error Control?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission.

What Automatic Repeat Request (ARQ)?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

What is Stop-and-Wait Protocol?

In Stop and wait protocol, sender sends one frame, waits until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.

What is Stop-and-Wait Automatic Repeat Request?

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

What is usage of Sequence Number in Reliable Transmission?

The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame. Since we want to minimize the frame size, the smallest range that provides unambiguous communication. The sequence numbers can wrap around.

What is Pipelining?

In networking and in other areas, a task is often begun before the previous task has ended. This is known as pipelining.

What is Sliding Window?

The sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, he sender and receiver need to deal with only part of the possible sequence numbers.

What are the two types of transmission technology available?

(i) Broadcast and (ii) point-to-point

What is subnet?

A generic term for section of a large networks usually separated by a bridge or router.

Difference between the communication and transmission.

Transmission is a physical movement of information and concern issues like bit polarity, synchronization, clock etc.

Communication means the meaning full exchange of information between two communication media.

What are the possible ways of data exchange?

(i) Simplex (ii) Half-duplex (iii) Full-duplex.

What is RAID?

A method for providing fault tolerance by using multiple hard disk drives.

What is passive topology?

When the computers on the network simply listen and receive the signal, they are referred to as passive because they don't amplify the signal in any way. Example for passive topology -linear bus.

What is point-to-point protocol?

A communications protocol used to connect computers to remote networking services including Internet service providers.

How Gateway is different from Routers?

A gateway operates at the upper levels of the OSI model and translates information between two completely different network architectures or data formats.

What is attenuation?

The degeneration of a signal over distance on a network cable is called attenuation.

What is MAC address?

The address for a device as it is identified at the Media Access Control (MAC) layer in the network architecture. MAC address is usually stored in ROM on the network adapter card and uniquely identifies a device on the network. It is also known as physical address or Ethernet address. A MAC address is made up of 6-bytes.

Difference between bit rate and baud rate.

Bit rate is the number of bits transmitted during one second whereas baud rate refers to the number of signal units per second that are required to represent those bits.
baud rate = (bit rate / N)
where, N is no-of-bits represented by each signal shift.

What is Bandwidth?

Every line has an upper limit and a lower limit on the frequency of signals it can carry. This limited range is called the bandwidth.

What are the types of Transmission media?

Signals are usually transmitted over some transmission media that are broadly classified in to two categories.

a.) **Guided Media**: These are those that provide a conduit from one device to another that include twisted-pair, coaxial cable and fiber-optic cable. A signal traveling along any of these media is directed and is contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic that accept and transport signals in the form of electrical current. Optical fiber is a glass or plastic cable that accepts and transports signals in the form of light.

b.) **Unguided Media**: This is the wireless media that transport electromagnetic waves without using a physical conductor. Signals are broadcast either through air. This is done through radio communication, satellite communication and cellular telephony.

What is Project 802?

It is a project started by IEEE to set standards to enable intercommunication between equipment from a variety of manufacturers. It is a way for specifying functions of the physical layer, the data link layer and to some extent the network layer to allow for interconnectivity of major LAN protocols.

It consists of the following:

1. 802.1 is an internetworking standard for compatibility of different LANs and MANs across protocols.
2. 802.2 Logical link control (LLC) is the upper sublayer of the data link layer which is non-architecture-specific, that is remains the same for all IEEE-defined LANs.
3. Media access control (MAC) is the lower sublayer of the data link layer that contains some distinct modules each carrying proprietary information specific to the LAN product being used. The modules are Ethernet LAN (802.3), Token ring LAN (802.4), Token bus LAN (802.5).
4. 802.6 is distributed queue dual bus (DQDB) designed to be used in MANs.

What are the different type of networking / internetworking devices?

1. **Repeater**: Also called a regenerator, it is an electronic device that operates only at physical layer. It receives the signal in the network before it becomes weak, regenerates the original bit pattern and puts the refreshed copy back in to the link.
2. **Bridges**: These operate both in the physical and data link layers of LANs of same type. They divide a larger network in to smaller segments. They contain logic that allow them to keep the traffic for each segment separate and thus are repeaters that relay a frame only the side of the segment containing the intended recipient and control congestion.
3. **Routers**: They relay packets among multiple interconnected networks (i.e. LANs of different type). They operate in the physical, data link and network layers. They contain software that enable them to determine which of the several possible paths is the best for a particular transmission.
4. **Gateways**: They relay packets among networks that have different protocols (e.g. between a LAN and a WAN). They accept a packet formatted for one protocol and convert it to a

packet formatted for another protocol before forwarding it. They operate in all seven layers of the OSI model.

What is ICMP?

ICMP is Internet Control Message Protocol, a network layer protocol of the TCP/IP suite used by hosts and gateways to send notification of datagram problems back to the sender. It provides messaging and communication for protocols within the TCP/IP stack. It uses the echo test / reply to test whether a destination is reachable and responding. It also handles both control and error messages that are used by network tools such as PING.

What are the data units at different layers of the TCP / IP protocol suite?

The data unit created at the application layer is called a message, at the transport layer the data unit created is called either a segment or an user datagram, at the network layer the data unit created is called the datagram, at the data link layer the datagram is encapsulated in to a frame and finally transmitted as signals along the transmission media.

What is difference between ARP and RARP?

The address resolution protocol (ARP) is used to associate the 32 bit IP address with the 48 bit physical address, used by a host or a router to find the physical address of another host on its network by sending a ARP query packet that includes the IP address of the receiver.

The reverse address resolution protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

What is the minimum and maximum length of the header in the TCP segment and IP datagram?

The header should have a minimum length of 20 bytes and can have a maximum length of 60 bytes.

What is the range of addresses in the classes of internet addresses?

Class A	-	0.0.0.0	-	127.255.255.255
Class B	-	128.0.0.0	-	191.255.255.255
Class C	-	192.0.0.0	-	223.255.255.255
Class D	-	224.0.0.0	-	239.255.255.255
Class E	-	240.0.0.0	-	247.255.255.255

What is the difference between TFTP and FTP application layer protocols?

The Trivial File Transfer Protocol (TFTP) allows a local host to obtain files from a remote host but does not provide reliability or security. It uses the fundamental packet delivery services offered by UDP.

The File Transfer Protocol (FTP) is the standard mechanism provided by TCP / IP for copying a file from one host to another. It uses the services offer by TCP and so is reliable and secure. It establishes two connections (virtual circuits) between the hosts, one for data transfer and another for control information.

What are major types of networks and explain?

1. **Server-based network**: provide centralized control of network resources and rely on server computers to provide security and network administration
2. **Peer-to-peer network**: computers can act as both servers sharing resources and as clients using the resources.

What are the important topologies for networks?

1. **BUS topology**: In this each computer is directly connected to primary network cable in a single line.
   Advantages: Inexpensive, easy to install, simple to understand, easy to extend.
2. **STAR topology**: In this all computers are connected using a central hub.
   Advantages: Can be inexpensive, easy to install and reconfigure and easy to trouble shoot physical problems.
3. **RING topology**: In this all computers are connected in loop. Advantages: All computers have equal access to network media, installation can be simple, and signal does not degrade as much as in other topologies because each computer regenerates it.

What is mesh network?

A network in which there are multiple network links between computers to provide multiple paths for data to travel.

What is difference between baseband and broadband transmission?

In a baseband transmission, the entire bandwidth of the cable is consumed by a single signal. In broadband transmission, signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.

What is the difference between routable and non- routable protocols?

Routable protocols can work with a router and can be used to build large networks. Non-Routable protocols are designed to work on small, local networks and cannot be used with a router.

Why should you care about the OSI Reference Model?

It provides a framework for discussing network operations and design.

What is logical link control?

One of two sublayers of the data link layer of OSI reference model, as defined by the IEEE 802 standard. This sublayer is responsible for maintaining the link between computers when they are sending data across the physical network connection.

What is virtual channel?

Virtual channel is normally a connection from one source to one destination, although multicast connections are also permitted. The other name for virtual channel is virtual circuit.

What is virtual path?

Along any transmission path from a given source to a given destination, a group of virtual circuits can be grouped together into what is called path.

What is multicast routing?

Sending a message to a group is called multicasting, and its routing algorithm is called multicast routing.

What is silly window syndrome?

It is a problem that can ruin TCP performance. This problem occurs when data are passed to the sending TCP entity in large blocks, but an interactive application on the receiving side reads 1 byte at a time.

What is BGP (Border Gateway Protocol)?

It is a protocol used to advertise the set of networks that can be reached with in an autonomous system. BGP enables this information to be shared with the autonomous system. This is newer than EGP (Exterior Gateway Protocol).

What are the basic differences between Internet, Intranet and Extranet?

The terms Internet, Intranet and Extranet are used to describe how a network application should be accessed. In Internet anyone can access the application from anywhere in world. In Intranet only the authorized users from the company for which the application was built can access the application. In Extranet selected external users are allowed to access the application which was built for Internet.

What does the term topology defines in computer network?

A topology is the physical layout which defines how computers are connected with each other's in a computer network.

Which topology uses a centralized device for connectivity?

Star topology uses a centralized device (HUB or Switch) for connectivity.

Which topology uses coaxial cable and terminators?

Bus topology uses coaxial cable and terminators.

A company has offices in Jaipur and Delhi. What type of computer network it will use to connect these offices?

WAN (Wide Area Network) network is used to connect the networks which are spread over the different geographical location.

Based on physical location what are the two most common network types?

LAN (Local Area Network) and WAN (Wide Area Network) are the two most common network types.

Does number of computers matter in LAN and WAN?

No, number of computers does not matter in LAN and WAN. This categorization is purely based on geographical location of network. For example we may have 1000 computers connected together in a network. If this network is located in a building or a campus, it will be considered as a LAN network. Just like this, we may have a network of only two computers. If one computer is located in one city and other computer is located in another city then this network will be considered as a WAN network.

What is the difference between physical topology and logical topology?

A physical topology describes how computers are connected with each other's physically. While a logical topology describes how data is being transmitted over the physical topology.

How will you consider a topology which uses HUB as a centralized device to connect all computers?

Physically it is a star topology but logically it is a bus topology. Since this topology satisfies the primary requirement of star topology, physically it can be considered as a star topology. But Hub cannot filter the data traffic, so all computers will receive data packets from all computers just like the bus topology. So physically it's a star topology but logically it's a bus topology.

Explain Collision domain?

Collision domain is a group of computers those share same collision. More computers you put in network, more collision you will experience. Collision seriously effect network performance. Collision should be less than one percent of total traffic. If it increases, we will have to implement collision removal devices. Bridges, switches, routers, multilayer switches can control the collision.

Define Collision?

Collision is the effect of two devices sending transmissions simultaneously in Ethernet. When they meet on the physical media, the signals from each device collide and damaged.

Explain types of Hub?

There are two types of HUB
Passive HUB: - It forwards the data signal from all ports except the port on which signal arrived. It doesn't interfere in data signal.
Active HUB: - It also forwards the data signal from all ports except the port on which signal arrived. But before forwarding, it improves quality of data signal by amplifying it. Due to this added features active HUB is also known as repeaters.

What is Brouter?

Brouters are the combination of router and bridge. It can be used as a bridge or router. Brouters are the earlier implementation of the routers. At layer two it's a fairly expensive device which cost more than other high end switches that work much faster than it. At layer three it has a lot of complexity. Due to these drawbacks it is rarely used. Gradually it has been replaced by high end switch at layer 2 and by router at layer three.

What do you mean by data communication?

It is the exchange of data between two devices via some form of transmission medium such as wire cable. The communicating system must be part of a communication system made up of a combination of hardware and software. The effectiveness of a data communication system depends on three fundamental characteristics: delivery, accuracy and timeliness.

What are the basic features of 10Base2 Ethernet architecture?

In This architecture 10 stands for speed, Base stands for Baseband transmission and 2 stands for 200 meters (Maximum distance it can span). Basic features of 10Base2 Ethernet architecture are following: -

- ✓ It is used in Bus Topology.
- ✓ It uses Thinnet coaxial cable.
- ✓ Maximum speed of this architecture is 10Mbps.
- ✓ It uses Baseband transmission.
- ✓ Theoretically it supports 200 meter but practically it will supports only 185 meter distance because this architecture uses Thinnet coaxial cable which supports only
- ✓ 185 meter.
- ✓ There can be 30 nodes in each segment.

There must be a distance of 0.5 meter between two hosts.

What are the advantages of OSI layer model?

- ✓ It prevents changes in one layer from affecting other layers.
- ✓ It describes what functions occur at each layer of the model that encourages industry standardization.
- ✓ Dividing network communication process in smaller component makes software development, design, and troubleshooting easier.
- ✓ Standardization of network components allows multiple-vendor development.
- ✓ It allows different types of network hardware and software to communicate.
- ✓ Dividing network in layers make network administrators life easier. They can troubleshoot issue more quickly and effectually by looking in layer that is causing issue rather than finding it entire network. It also makes learning easier.

List different application layer protocols with their purposes?

- ✓ **SNMP (Simple Network Management Protocol)** — Used to control the connected networking devices.
- ✓ **TFTP (Trivial File Transfer Protocol)** — Used to transfer the files rapidly.
- ✓ **DNS (Domain Naming System)** — Used to translate the name with IP address and vice versa.
- ✓ **DHCP (Dynamic Host Configuration Protocol)** — Used to assign IP address and DNS information automatically to hosts.
- ✓ **Telnet**— used to connect remote devices.
- ✓ **HTTP (Hypertext Transfer Protocol)** — Used to browse web pages.
- ✓ **FTP (File Transfer Protocol)** — Used to reliably sends/retrieves files.
- ✓ **SMTP (Simple Mail Transfer Protocol)** — Used to sends email.
- ✓ **POP3 (Post Office Protocol v.3)** — Used to retrieves email.
- ✓ **NTP (Network Time Protocol)** — Used to synchronizes clocks.

What is subnet mask?

A subnet mask is combined with an IP address in order to identify two parts: the extended network address and the host address. Like an IP address, a subnet mask is made up of 32 bits.

What is the backbone network?

The network which connects two or more networks together is considered as a backbone network. Usually backbone network contains high speed data transferring devices such as routers and switches. Backbone network should never be used for end user connectivity. The network which provides end user connectivity should be connected through the backbone network.

What is Gateway?

Gateway is used to forward the packets which are intended for remote network from local network. Till host is configured with default gateway address, every packet should have default gateway address. A default gateway address is the address of gateway device. If packet does not find its destination address in local network then it would take the help of gateway device to find the destination address in remote network. A gateway device knows the path of remote destination address. If require, it also change the encapsulation of packet so it can travel in other network to get its destination address.

What is simplex?

It is the mode of communication between two devices in which flow of data is unidirectional i.e. one can transmit and other can receive. E.g. keyboard and monitor.

What is half-duplex?

It is the mode of communication between two devices in which flow of data is bi-directional but not at the same time i.e. each station can transmit and receive but not at the same time. E.g walkie-talkies are half-duplex system.

What is full duplex?

It is the mode of communication between two devices in which flow of data is bi-directional and it occurs simultaneously. Here signals going in either direction share the capacity of the link. E.g. telephone.

What are the basic features of 10Base5 Ethernet architecture?

In this architecture 10 stands for speed, Base stands for Baseband transmission and 5 stands for 500 meters distance. This architecture can cover 500 meter distance per network segment. It uses Baseband technology for data transmission. It provides maximum 10Mbps speeds. It is used in Bus topology. It uses Thicknet coaxial cable.

Why 10Base2 and 10Base5 Ethernet architecture are no longer used in modern network?

Because both architectures are used in bus topology which is no longer used to build the networks.

What are the Services provided by OSI model?

To insure the data transmission over the network, OSI model provides several services including following:

- ✓ **Data Segmentation: -** In this process a large data file is divided into smaller segments sufficient enough to transmit over the network.
- ✓ **Packet acknowledgment: -** Every transferred segment is acknowledged with a return message from recipient which insures that segment is delivered successfully.
- ✓ **Flow control: -** This mechanism instructs sender computer to match its transmissions speed with receiver computer.
- ✓ **Error detection and correction: -** In this process receiving computer verify the content of data.
- ✓ If any segment is corrupted, it will inform the sender that specific piece of data was damaged and must be retransmitted
- ✓ **Data compression: -** To eliminate redundant, segments are compressed before transmission.
- ✓ **Data encryption: -** To increase the data safety, segments are encrypted with a key already known by receiving system.

What are the services provided by transport layer?

Transport layer provides following services: -

- ✓ It sets up and maintains the connection between two devices.
- ✓ It multiplexes connections that allow multiple applications to simultaneously send and receive data.
- ✓ According to requirement data transmission method can be connection oriented or connection less.
- ✓ For unreliable data delivery connection less method is used.
- ✓ Connection less method uses UDP protocol.
- ✓ For reliable data delivery connection oriented method is used.
- ✓ Connection oriented method uses TCP protocol.
- ✓ When implemented a reliable connection, sequence numbers and acknowledgments (ACKs) are used.
- ✓ Reliable connection controls flow through the uses of windowing or acknowledgements.

Briefly describe NAT?

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share single connection to the Internet. A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks (VPN), is Network Address Translation (NAT)

What is a private IP address?

Private IP addresses are assigned for use on intranets. These addresses are used for internal networks and are not routable on external public networks. These ensures that no conflicts are present among internal networks while at the same time the same range of private IP addresses are reusable for multiple intranets since they do not "see" each other.

What are the main advantages of star topology?

Main advantages of star topology are scalability, easy to troubleshoot and centralized network component. Adding and removing a device in this topology is much easier than the other topologies. Besides this if there is any break in cable then only the device which is connected with that cable will be down.

What are the main disadvantages of star topology?

Main disadvantages of star topology are cost and centralized network component. In positive side a centralized device makes administrator life easier but in downside if this device fails then the entire network will be down.

What are the different Guided Media?

The media which provides a conduct from one device to another is called a guided media. These include twisted pair cable, coaxial cable, and fibre-optic cable.

Describe about the different Guided Medias?

Twisted pair cable consists of two insulated cupper wires twisted together. It is used in telephone line for voice and data communications.
Coaxial cable has the following layers: a metallic rod-shaped inner conductor, an insulator covering the rod, a metallic outer conductor (shield), an insulator covering the shield, and a plastic cover. Coaxial cable can carry signals of higher frequency ranges than twisted-pair cable. Coaxial cable is used in cable TV networks and Ethernet LANs.
Fibre-optic cables are composed of a glass or plastic inner core surrounded by cladding, all encased in an outer jacket. Fibre-optic cables carry data signals in the form of light. The signal is propagated along the inner core by reflection. Its features are noise resistance, low attenuation, and high bandwidth capabilities. It is used in backbone networks, cable TV networks, and fast Ethernet networks.

What is the CSMA/CD?

This is mechanism of removing collision from network. When two or more nodes simultaneously sense the wire and found no frame and each device places its frame on the wire. These frame would be collide in wire and a collision will occur. If the NICs see a collision for their transmitted frames, they have to resend the frames. In this situation, each NIC that was transmitting a frame when a collision occurred creates a special signal, called a jam signal, on the wire, waits a small random time period and examine the wire again. If no frame is currently on the wire, NIC will retransmit its original frame again. This collision detection method is known as CSMA/CD.

What is UDP?

UDP is a connection less protocol. Connection-less transmission is said to be unreliable. Now, don’t get worried about the term "unreliable" this doesn’t mean that the data isn’t going to get its destination; its only means that it isn’t guaranteed to get its destination. Think of your options when you are sending a postcard, put it in the mailbox, and chances are good that it will get where it’s supposed to go but there is no guarantee. There is always a chance of missing in the way. On the other hand, it’s cheap.

What is TCP?

TCP is a connection oriented protocol. Connection-oriented transmission is said to be reliable. Think TCP as registry AD facility available in Indian post office. For this level of service, you have to buy extra ticket and put a bunch of extra labels on it to track where it is going and where it has been. You get a receipt when it is delivered. In this method you have a guaranteed delivery. All of this costs you more—but it is reliable!

What is the purpose of cables being shielded and having twisted pairs?

The main purpose of this is to prevent crosstalk. Crosstalks are electromagnetic interferences or noise that can affect data being transmitted across cables.

What is the hybrid topology?

A topology which consist more than one topology is considered as a hybrid topology for example a star-bus topology, in which multiple star topologies are connected through the central bus topology.

What do you mean by wireless communication?

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is referred as wireless communication. Here signals are broadcaster through air and thus available to anyone who has a device to receive it.

In which topology all nodes have a direct connection to every other node on the network?

In mesh topology all nodes have a direct connection with each node in network.

Which network topology uses terminators?

Bus topology uses terminators to absorb the signals at the end of the cable.

Explain Three Way Handshake Process?

Three way handshake process is as follows:

1) PC1 sends a SYN single to PC2 indicating that it wants to establish a reliable session.
2) P2 replies with ACK/SYN signal where ACK is the acknowledgment of PC1's SYN signal and SYN indicates that PC2 is ready to establish a reliable session.
3) PC1 replies with ACK signal indicating that is has received SYN signal and session is now fully established.

Once connection is established data transmission will be initiated. To provide maximum reliability it includes following functions:-

- ✓ Detect lost packets and resend them
- ✓ Detect packets that arrived out of order and reorder them
- ✓ Recognize duplicate packets and drop extra packets
- ✓ Avoid congestion by implementing flow control

What do you mean by switching?

It is a method in which communication devices are connected to one another efficiently. A switch is intermediary hardware or software that links devices together temporarily.

What are the switching methods?

There are three fundamental switching methods: circuit switching, packet switching, and message switching, cell switching.

In **circuit switching**, a direct physical connection between two devices is created by space division switches, time division switches or both.

In **packet switching** data is transmitted using a packet switched network. Packet switched network is a network in which data are transmitted in independent units called packets.

With **message switching** there is no need to establish a dedicated path between two stations. When a station sends a message, the destination address is appended to the message. The message is then transmitted through the network, in its entirety, from node to node. Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node. This type of network is called a store-and-forward network.

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

What are the types of errors?

Errors can be categorized as a single-bit error or burst error. A single bit error has one bit error per data unit. A burst error has two or more bits errors per data unit.

Briefly explain the IEEE standards?

Standard	Description
802.1	Standards for LAN/MAN bridging and management
802.2	Standards for Logical Link Control (LLC)
802.3	Ethernet Standards CSMA/CD

802.4	Standards for Token passing bus access
802.5	Standards for token ring access and for communications between LANs and MANs
802.6	Standards for information exchange between systems
802.7	Standards for broadband LAN cabling
802.8	Standards for fibre optical connection
802.9	Standards for integrated services, like voice and data
802.10	Standards for LAN/MAN security implementations
802.11	Standards for Wi-Fi (Wireless Networking)
802.12	Standards for demand priority access method
802.14	Standards for cable television broadband communications
802.15	Standards for Bluetooth network
802.15	Standards for ZigBee (Wireless Sensor/Control Networks)
802.16	Standards for WiMAX Wireless Networking

Briefly describe various network types?

Network	Description
LAN	Local Area Network (LAN) connects computers which reside in a small geographical area such as building or campus.
WAN	Wide Area Network (WAN) connects multiple LANs which are separated by a large geographical distance such as different continents
MAN	Metropolitan Area Networks (MAN) connects multiple LANs which are separated in a metro city.
CN	Content Network is used to cache and distribute the Internet traffic.
SAN	Storage Area Network provides high speed infrastructure between storage devices and file servers.
Intranet	This is a private network. Outsiders are not allowed to connect in this network.
Extranet	This network allows certain services from Intranet to known external users.
Internet	This network allows unknown external users to connect with internal resources of network such as web server.

VPN	This network provides secure connection across the public network such as Internet.

What is the equivalent layer or layers of the TCP/IP Application layer in terms of OSI reference model?

The TCP/IP Application layer actually has three counterparts on the OSI model: the Session layer, Presentation Layer and Application Layer.

How can you identify the IP class of a given IP address in binary representation?

By looking at the first octet of any given IP address, you can identify whether it's Class A, B or C. If the first octet begins with a 0 bit, that address is Class A. If it begins with bits 10 then that address is a Class B address. If it begins with 110, then it's a Class C network.

What is the main purpose of OSPF?

OSPF, or Open Shortest Path First, is a link-state routing protocol that uses routing tables to determine the best possible path for data exchange.

Give some examples of private IP addresses?

10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts)
172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts)
192.168.0.0 – 192.168.255.255/16 (65,536 hosts)

What is the number of network IDs in a Class C network?

For a Class C network, the number of usable Network ID bits is 21. The number of possible network IDs is 2 raised to 21 or 2,097,152. The number of host IDs per network ID is 2 raised to 8 minus 2, or 254.

What do you mean by redundancy?

Redundancy is the concept of sending extra bits for use in error detection. Three common redundancy methods are parity check, cyclic redundancy check (CRC), and checksum.

Define Parity Check?

In parity check, a parity bit is added to every data unit so that the total number of 1s is even (or odd for odd parity).Simple parity check can detect all single bit errors. It can detect burst errors only if the total number of errors in each data unit is odd. In two dimensional parity checks, a block of bits is divided into rows and a redundant row of bits is added to the whole block.

What is Hamming Code?

The hamming code is an error correction method using redundant bits. The number of bits is a function of the length of the data bits. In hamming code for a data unit of m bits, we use the formula $2^r >= m+r+1$ to determine the number of redundant bits needed. By rearranging the order of bit transmission of the data units, the hamming code can correct burst errors.

Define Hamming Distance? How to calculate the hamming distance?

The number of bit positions in which codewords differs is called the Hamming Distance (i. e. The hamming distance between two words [of same size] is number of differences between the corresponding bits). The hamming distance can easily be found if we apply XOR operation (□) on the two words and count the number of '1's in the result (Note that hamming distance is a value greater than or equal to zero).

What do you mean by flow control?

It is the regulation of sender's data rate so that the receiver buffer doesn't become overwhelmed i.e. flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.

Define Go-Back-N ARQ?

In Go-Back-N ARQ, multiple frames can be in transit at the same time. If there is an error, retransmission begins with the last unacknowledged frame even if subsequent frames arrived correctly. Duplicate frames are discarded.

What is ICMP?

ICMP is Internet Control Message Protocol. It provides messaging and communication for protocols within the TCP/IP stack. This is also the protocol that manages error messages that are used by network tools such as PING.

What is Ping?

Ping is a utility program that allows you to check connectivity between network devices on the network. You can ping a device by using its IP address or device name, such as a computer name.

What is DNS?

DNS is Domain Name System. The main function of this network service is to provide host names to TCP/IP address resolution.

What advantages does fibre optics have over other media?

One major advantage of fibre optics is that is it less susceptible to electrical interference. It also supports higher bandwidth, meaning more data can be transmitted and received. Signal degrading is also very minimal over long distances.

Define Selective Repeat ARQ?

In Selective Repeat ARQ, multiple frames can be in transit at the same time. If there is an error, only unacknowledged frame is retransmitted.

What is the difference between a hub and a switch?

A hub acts as a multiport repeater. However, as more and more devices connect to it, it would not be able to efficiently manage the volume of traffic that passes through it. A switch provides a better alternative that can improve the performance especially when high traffic volume is expected across all ports.

What is HDLC?

It is a bit oriented data link protocol designed to support both half duplex and full duplex communication over point to point and multi point links. HDLC is characterized by their station type, configuration and their response modes.

You need to connect two computers for file sharing. Is it possible to do this without using a hub or router?

Yes, you can connect two computers together using only one cable. A crossover type cable can be use in this scenario. In this setup, the data transmit pin of one cable is connected to the data receive pin of the other cable, and vice versa.

What do you mean by CSMA?

To reduce the possibility of collision CSMA method was developed. In CSMA each station first listen to the medium (Or check the state of the medium) before sending. It can't eliminate collision.

What is the difference between a straight-through and crossover cable?

A straight-through cable is used to connect computers to a switch, hub or router. A crossover cable is used to connect two similar devices together, such as a PC to PC or Hub to hub.

What is client/server?

Client/server is a type of network wherein one or more computers act as servers. Servers provide a centralized repository of resources such as printers and files. Clients refers to workstation that access the server.

What do you mean by Bluetooth?

It is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers and so on. Bluetooth LAN Is an adhoc network that is the network is formed spontaneously? It is the implementation of protocol defined by the IEEE 802.15 standard.

When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when the NIC card was replace by another one.

What is IP address?

The internet address (IP address) is 32bits that uniquely and universally defines a host or router on the internet. The portion of the IP address that identifies the network is called netid. The portion of the IP address that identifies the host or router on the network is called hostid. Every host and router on the Internet has an IP address that can be used in the Source address and Destination address fields of IP packets. A host typically has only a single link into the network; when IP in the host wants to send a datagram, it does so over this link. The boundary between the host and the physical link is called an interface. It is important to note that an IP address does not actually refer to a host. It really refers to a network interface, so if a host is on two networks, it must have two IP addresses. (Most hosts are on one network and thus have one IP address. In contrast, routers have multiple interfaces and thus multiple IP addresses.)

What is subnetting?

Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets).

Discuss main features of IPv6?

Main Features of IPv6 are as follows:

- ✓ **First** and foremost, IPv6 has **longer addresses** than IPv4. They are 128 bits long, which solves the problem that IPv6 set out to solve: providing an effectively unlimited supply of Internet addresses.
- ✓ The **second** major improvement of IPv6 is the **simplification of the header**. It contains only seven fields (versus 13 in IPv4). This change allows routers to process packets faster and thus improves throughput and delay.
- ✓ The **third** major improvement is **better support for options**. This change was essential with the new header because fields that previously were required are now optional (because they are not used so often). In addition, the way options are represented is different, making it simple for routers to skip over options not intended for them. This feature speeds up packet processing time.
- ✓ A **fourth** area in which IPv6 represents a **big advance** is **in security**. Authentication and privacy are key features of the new IP.
- ✓ **Finally**, more attention has been paid to **quality of service (QoS)**.

What are the advantages of fibre optics cable?

The advantages of fibre optics cable over twisted pair cable are:
Noise resistance-As they use light so external noise is not a factor.
Less signal attenuation-fibre optics transmission distance is significantly greater than that of other guided media.
Higher bandwidth-It can support higher bandwidth.

What are the disadvantages of fibre optics cable?

The disadvantages of fibre optics cable over twisted pair cable are:
Cost-It is expensive.
Installation/maintenance-Any roughness or cracking defuses light and alters the signal.
Fragility-It is more fragile.

What do you mean by medium access control (MAC) sublayer?

The protocols used to determine who goes next on a multi-access channel belong to a sublayer of the data link layer is called the multi-access channel (MAC) sublayer. It is the bottom part of data link layer.

Describe Ethernet?

Ethernet is one of the popular networking technologies used these days. It was developed during the early 1970s and is based on specifications as stated in the IEEE. Ethernet is used in local area networks.

What are the drawbacks of implementing a ring topology?

In case one workstation on the network suffers a malfunction, it can bring down the entire network. Another drawback is that when there are adjustments and reconfigurations needed to be performed on a particular part of the network, the entire network has to be temporarily brought down as well.

What is the difference between CSMA/CD and CSMA/CA?

CSMA/CD, or Collision Detect, retransmits data frames whenever a collision occurred. CSMA/CA, or Collision Avoidance, will first broadcast intent to send prior to data transmission.

What do you mean by ALOHA?

It is the method used to solve the channel allocation problem. It is used for: i) ground based radio broadcasting ii) In a network in which uncoordinated users are competing for the use of single channel. It is of two types: 1.Pure aloha 2.Slotted aloha.

What is pure ALOHA?

It lets users transmit whenever they have data to send. Collision may occur but due to feedback property sender can know the status of message. Conflict occur when at one time more bits are transmitted. The assumptions are:

i. All frame size is same for all user.
ii. Collision occur when frames are transmitted simultaneously.
iii. Indefinite population of no. of user.
iv. N=number of frames/frame time.
v. It obeys Poisson's distribution if N>1 there will be collision 0<1.

What is slotted ALOHA?

In this method time is divided into discrete intervals, each interval corresponding to one frame. It requires user to agree on slot boundaries. Here data is not send at any time instead it wait for beginning of the next slot. Thus pure ALOHA is tuned into discrete one.

What do you mean by persistent CSMA (carrier sense multiple access)?

When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment. If channel is busy it waits until the station becomes idle. When collision occurs it waits and then sends. It sends frame with probability 1 when channel is idle.

What is SMTP?

SMTP is short for Simple Mail Transfer Protocol. The TCP/IP protocol that supports electronic mail on the internet is called Simple Mail Transfer Protocol. SMTP provides for mail exchange between users on the same or different computer and supports Sending a single message to one or more recipient Sending message that include text, voice, video, or graphics. Sending message to users on network outside the internet. This protocol deals with all Internal mail, and provides the necessary mail delivery services on the TCP/IP protocol stack.

What do you mean by non-persistent CSMA (carrier sense multiple access)?

Here if no one else is sending the station begins doing so itself. However if the channel is already in use, the station doesn't continuously sense it rather it waits for a random period of time and then repeats. It leads better channel utilization but longer delay.

What do you mean by p persistent CSMA (carrier sense multiple access)?

It applies to slotted channels. When a station becomes ready to send, it senses the channel. If it is idle it transmits with a probability P, with a probability Q=P-1 It defers until the next slot. If that slot is also idle, it either transmits or defers again with probability P and Q. The process is repeated until either the frame has been transmitted or another station begins transmitting.

What are Repeaters?

A receiver receives a signal before it becomes too weak or corrupted, regenerates the original bit pattern, and puts the refreshed copy back onto the link. It operates on physical layer of OSI model.

What are Bridges?

They divide large network into smaller components. They can relay frames between two originally separated LANs. They provide security through partitioning traffic. They operate on physical and data link layer of OSI model.

What are Routers?

Router relay packets among multiple interconnected networks. They receive packet from one connected network and pass it to another network. They have access to network layer addresses and certain software that enables them to determine which path is best for transmission among several paths. They operate on physical, data link and network layer of OSI model.

What do you mean by broadcasting?

Broadcast system allow addressing a packet to all destination by using a special code in address field. When packet is transmitted it is received and processed by every machine on the network.

Define IP?

Internetwork protocol (IP) is the transmission mechanism used by TCP/IP protocol. It is an unreliable and connectionless datagram protocol. It provides no error checking and tracking.

What is TELNET?

TELNET is a client –server application that allows a user to log on to a remote machine, giving the user access to the remote system. TELNET is an abbreviation of terminal Network.

What is Hypertext Transfer Protocol (HTTP)?

It is the main protocol used to access data on the World Wide Web .the protocol transfers data in the form of plain text, hypertext, audio, video, and so on. It is so called because its efficiency allows its use in a hypertext environment where there are rapid jumps from one document to another.

What is address mask?

An address mask determines which portion of an IP address identifies the network and which portion identifies the host.

Who decides the IP addresses?

Local level	-	ISP
Global level	-	Internet Assigned Number Authority (IANA)

List the types of categories of addresses in IPv6?

IPv6 defines 3 types of addresses:

1. Unicast
2. Multicast
3. Anycast

What is Bit Stuffing?

Bit stuffing is the process of adding one extra zero whenever there are 5 consecutive ones in the data. So that the receiver does not mistake it to be a flag bit as 01111110.

How can you manage a network using a router?

Routers have built in console that lets you configure different settings, like security and data logging. You can assign restrictions to computers, such as what resources it is allowed access, or what particular time of the day they can browse the internet. You can even put restrictions on what websites are not viewable across the entire network.

What protocol can be applied when you want to transfer files between different platforms, such between UNIX systems and Windows servers?

Use FTP (File Transfer Protocol) for file transfers between such different servers. This is possible because FTP is platform independent.

What does Ad Hoc Network mean?

An ad hoc network is a network that is composed of individual devices communicating with each other directly. The term implies spontaneous or impromptu construction because these networks often bypass the gatekeeping hardware or central access point such as a router. Many ad hoc networks are local area networks where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

What does Direct Sequence Spread Spectrum (DSSS) mean?

Direct sequence spread spectrum (DSSS) is a transmission technology used in local area wireless network transmissions. In this technology, a data signal at the sending station is combined with a high data rate bit sequence, which divides user data based on a spreading ratio. The benefits of using DSSS are resistance to jamming, sharing single channels among multiple users, less background noise and relative timing between transmitter and receivers. This term is also known as direct sequence code division multiple access.

Wireless LAN requirements?

The following are among the most important requirements for wireless LANs:

- ✓ **Throughput:** The medium access-control (MAC) protocol should make as efficient use as possible of the wireless medium to maximize capacity.
- ✓ **Number of nodes:** Wireless LANs may need to support hundreds of nodes across multiple cells.
- ✓ **Connection to backbone LAN:** In most cases, interconnection with stations on a wired backbone LAN is required. For infrastructure wireless LANs, this is easily accomplished through the use of control modules that connect to both types of LANs. There may also need to be accommodation for mobile users and ad hoc wireless networks.
- ✓ **Service area:** A typical coverage area for a wireless LAN has a diameter of 100 to 300 m.
- ✓ **Battery power consumption:** Mobile workers use battery-powered workstations that need to have a long battery life when used with wireless adapters. This suggests that a MAC protocol that requires mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station is inappropriate. Typical wireless LAN implementations have features to reduce power consumption while not using the network, such as a sleep mode.
- ✓ **Transmission robustness and security:** Unless properly designed, a wireless LAN may be interference-prone and easily eavesdropped. The design of a wireless LAN must permit reliable transmission even in a noisy environment and should provide some level of security from eavesdropping.
- ✓ **Collocated network operation:** As wireless LANs become more popular, it's quite likely that two or more wireless LANs will operate in the same area or in some area where interference between the LANs is possible. Such interference may thwart the normal operation of a MAC algorithm and may allow unauthorized access to a particular LAN.
- ✓ **License-free operation:** Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.
- ✓ **Handoff/roaming:** The MAC protocol used in the wireless LAN should enable mobile stations to move from one cell to another.
- ✓ **Dynamic configuration:** The MAC addressing and network management aspects of the LAN should permit dynamic and automated addition, deletion, and relocation of end systems without disruption to other users.

What id framing? Explain in detail?

A frame is a digital data transmission unit in computer networking and telecommunication. A frame typically includes frame synchronization features consisting of a sequence of bits or symbols that indicate to the receiver, the beginning, and end of the payload data within the stream of symbols or bits it receives. If a receiver is connected to the system in the middle of a frame transmission, it ignores the data until it detects a new frame synchronization sequence.

What are the different framing methods?

Character Count

This method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow, and hence where the end of the frame is. The disadvantage is that if the count is garbled by a transmission error, the destination will lose synchronization and will be unable to locate the start of the next frame. So, this method is rarely used.

Character stuffing

In the second method, each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX.(where DLE is Data Link Escape, STX is Start of text and ETX is End of text.) This method overcomes the drawbacks of the character count method. If the destination ever loses synchronization, it only has to look for DLE STX and DLE ETX characters. If however, binary data is being transmitted then there exists a possibility of the characters DLE STX and DLE ETX occurring in the data. Since this can interfere with the framing, a technique called character stuffing is used. The sender's data link layer inserts an ASCII DLE character just before the DLE character in the data. The receiver's data link layer removes this DLE before this data is given to the network layer. However character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitrary sized characters.

Bit stuffing

The third method allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. At the start and end of each frame is a flag byte consisting of the special bit pattern 01111110. Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream. This technique is called bit stuffing. When the receiver sees five consecutive 1s in the incoming data stream, followed by a zero bit, it automatically destuffs the 0 bit. The boundary between two frames can be determined by locating the flag pattern.

What is piggybacking?

In two-way communication, whenever a data frame is received, the receiver waits and does not send the control frame (acknowledgement or ACK) back to the sender immediately. The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame. This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.

Whenever party A wants to send data to party B, it will send the data along with this ACK field. Considering the sliding window here of size 8 bits, if A has send frames up to 5 correctly (from B), and wants to send frames starting from frame 6, it will send ACK6 with the data.

Three rules govern the piggybacking data transfer.

I. If station A wants to send both data and an acknowledgment, it keeps both fields there.
II. If station A wants to send just the acknowledgment, then a separate ACK frame is sent.
III. If station A wants to send just the data, then the last acknowledgment field is sent along with the data. Station B simply ignores this duplicate ACK frame upon receiving.

Distinguish between attenuation distortion and delay distortion?

Attenuation distortion arises because the attenuation of the signal in the transmitting media. Attenuation distortion is predominant in case of analog signals. Delay distortion arises because different frequency components of the signal suffer different delay as the signal passes through the media. This happens because the velocity of the signal varies with frequency and it is predominant in case of digital signals.

Why do you need encoding of data before sending over a medium?

Suitable encoding of data is required in order to transmit signal with minimum attenuation and optimize the use of transmission media in terms of data rate and error rate.

What are the four possible encoding techniques? Give examples.

The four possible encoding techniques are

i. Digital Data to Digital Signal; Example - Transmitter
ii. Analog Data to Digital Signal; Example - Codec (Coder-Decoder)
iii. Digital Data to Analog Signal; Example - Modem
iv. Analog Data to Digital Signal; Example – Telephone

Between RZ and NRZ encoding techniques, which requires higher bandwidth and why?

RZ encoding requires more bandwidth, as it requires two signal changes to encode one bit.

How does Manchester encoding differ from differential Manchester encoding?

In the **Manchester encoding**, a low-to-high transition represents a 1, and a high-to-low transition represents a 0. There is a transition at the middle of each bit period, which serves the purpose of synchronization and encoding of data.
In **Differential Manchester**, the encoding of a 0 is represented by the presence of a transition at the beginning of a bit period, and a 1 is represented by the absence of a transition at the beginning of a bit period. In this case, the midbit transition is only used for synchronization.

How Manchester encoding helps in achieving better synchronization?

In Manchester encoding, there is a transition in the middle of each bit period and the receiver can synchronize on that transition. Hence better synchronization is achieved.

List advantages and disadvantages of Direct Sequence Spread Spectrum (DSSS)?

Advantages of DSSS:

- ✓ More resistance to fading and multi-path effects.
- ✓ More efficient use of channel bandwidth.
- ✓ Short latency time.
- ✓ Constant processing gain - a better signal to noise ratio.
- ✓ Quick Lock-In as radio synchronize.
- ✓ No resynchronization with other radio necessary.
- ✓ Long outdoor range.
- ✓ Greater overall data throughput.

Disadvantage of DSSS:

- ✓ Complex design.

What is Frequency Hopping Spread Spectrum?

Frequency Hopping Spread Spectrum (FHSS) is a transmission technology used in wireless transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. The signal energy is spread in time domain rather than chopping each bit into small pieces in the frequency domain. This technique reduces interference because a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the same time. If synchronized properly, a single logical channel is maintained.

List advantages and disadvantages of Frequency Hopping Spread Spectrum (FHSS)?

Advantage of FHSS:

- ✓ Fundamentally much simpler to implement.
- ✓ Better range, due to lower receiver sensitivity.
- ✓ Good rejection of in band interference.
- ✓ Good performance in multipath environments.
- ✓ No "near/far" problems

Disadvantages of FHSS:

- ✓ Long latency time.
- ✓ Slow Lock-In, must search a channel.
- ✓ No processing gain.
- ✓ Must resynchronization with other after every hop.
- ✓ Short outdoor range.
- ✓ Lower overall data throughput.

Give an example system which uses DSSS or FHSS respectively?

Example for DSSS: CDMA, Wireless LAN
Example for FHSS: GSM, Bluetooth

Describe the problems when CSMA/CD is applied to wireless networks?

Two problems occur:
Hidden and exposed terminals - Carrier sensing may fail to detect another terminal or detect a terminal outside the interference range.
Near and far terminals - The local signal might drown out the remote transmission.

Describe how MACA solve the Hidden and exposed terminals, Near and far terminals problems?

When a station is ready for transmission, it sends a request to send (RTS) frame to the receiver and waits to receive a clear to send (CTS) frame from the receiver. As a result, all stations within the range will refrain from transmitting a data frame. Once CTS is received, the sender can send packets. In this way, the CTS frame can be heard by the hidden terminals and the medium for future use by other sending terminal is reserved. The exposed terminal won’t react to RTS and doesn’t receive CTS because the exposed terminal is not the receiver. The near and far terminals could be solved in the similar way.

Describe mobile IP operation?

1) A mobile node has a home agent which is the proxy of the mobile node during its absence from the home network. It acquires a care-of address that identifies its location in the current network from the foreign agent.
2) Each time a user moves the device to a different network, it acquires a care-of address and notify its home agent. The home agent then associates its home address with its care-of address.
3) Traffic for the mobile node is sent to the home network and forwarded by the home agent via tunnelling mechanisms to the appropriate care-of address.

Compare between IPv4 and IPv6?

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPsec support is only optional.	Inbuilt IPsec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to configure IPv4 addresses.	Auto-configuration of addresses is available.

What is spread spectrum?

Spread spectrum techniques involve spreading the bandwidth needed to transmit data – which does not make sense at first sight. Spreading the bandwidth has several advantages. The main advantage is the resistance to narrowband interference.

Define Mobile IP?

Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address

Compare between RIP, OSPF and BGP?

RIP	OSPF	BGP
RIP is intradomain routing protocol used with in the autonomous system	OSPF is also intradomain routing protocol used with in the autonomous system	BGP is interdomain routing protocol used between the autonomous system
RIP is used for small networks with maximum number of hops 15	OSPF is used in large autonomous system with no limitation	The BGP protocol is used for very large-scale networks
RIP uses distance vector	OSPF uses Link State	BGP uses path vector
RIP send entire routing update to all directly connected interfaces	OSPF send multicast Hello Packet to the neighbours, to create session	BGP send open packet to the neighbours to create session
RIP use Bellman Ford Algorithm	OSPF use Dijkstra Algorithm	BGP uses Path Vector Routing

Explain what is the difference between flow control and error control?

Flow control: adjust and confirm data flow rate for successful transmission.
Error Control: a way to recover corrupted data.

What is sockets?

A socket is an abstraction that represents an endpoint of communication. Most applications that consciously use TCP and UDP do so by creating a socket of the appropriate type and then performing a series of operations on that socket. The operations that can be performed on a socket include control operations (such as associating a port number with the socket, initiating or accepting a connection on the socket, or destroying the socket) data transfer operations (such as writing data through the socket to some other application, or reading data from some other application through the socket) and status operations (such as finding the IP address associated with the socket).

Explain how does TCP try to avoid network meltdown?

TCP includes several mechanisms that attempt to sustain good data transfer rates while avoiding placing excessive load on the network. TCP's "Slow Start", "Congestion Avoidance", "Fast Retransmit" and "Fast Recovery" algorithms are summarised in RFC 2001. TCP also mandates an algorithm that avoids "Silly Window Syndrome" (SWS), an undesirable condition that results in very small chunks of data being transferred between sender and receiver. SWS Avoidance is discussed in RFC 813. The "Nagle Algorithm", which prevents the sending side of TCP from flooding the network with a train of small frames, is described in RFC 896.

Which is the faster protocol either UDP or TCP?

UDP is the faster protocol as it doesn't wait for acknowledgement so it is not at all having reliability as compared to TCP.

Is the IP address of computer and modems is same or not?

No. The IP address of a system is the logical address whereas the address of the MODEM is the MAC (Media Access Control) address, it is the physical address provided by the vendor.