Computer Network

1) What is a Link?
A link refers to the connectivity between two devices. It includes the type of cables and protocols used for one device to be able to communicate with the other.
2) What are the layers of the OSI reference model?
There are 7 OSI layers: 1) Physical Layer, 2) Data Link Layer, 3) Network Layer, 4) Transport Layer, 5) Session Layer, 6) Presentation Layer, and 7) Application Layer.
3) What is the backbone network?
A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles the management of bandwidth and multiple channels.
4) What is a LAN?
LAN stands for Local Area Network. It refers to the connection between computers and other network devices that are located within a small physical location.
5) What is a node?
A node refers to a point or joint where a connection takes place. It can be a computer or device that is part of a network. Two or more nodes are needed to form a network connection.
6) What are routers?
Routers can connect two or more network segments. These are intelligent network devices that store information in its routing tables, such as paths, hops, and bottlenecks. With this info, they can determine the best path for data transfer. Routers operate at the OSI Network Layer.
7) What is a point to point link?
It refers to a direct connection between two computers on a network. A point to point connection does not need any other network devices other than connecting a cable to the NIC cards of both computers.
8) What is anonymous FTP?
Anonymous FTP is a way of granting user access to files in public servers. Users that are allowed access to data in these servers do not need to identify themselves, but instead, log in as an anonymous guest.
9) What is a subnet mask?
A subnet mask is combined with an IP address 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.
10) What is the maximum length allowed for a UTP cable?
A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches.
11) What is data encapsulation?
Data encapsulation is the process of breaking down information into smaller, manageable chunks before it is transmitted across the network. In this process that the source and destination addresses are attached to the headers, along with parity checks.
12) Describe Network Topology
Network Topology refers to the layout of a computer network. It shows how devices and cables are physically laid out, as well as how they connect.
13) What is a VPN?
VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.
14) 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 a single connection to the Internet.
15) What is the job of the Network Layer under the OSI reference model?
The Network layer is responsible for data routing, packet switching, and control of network congestion. Routers operate under this layer.
16) How does a network topology affect your decision to set a network?
Network topology dictates what media you must use to interconnect devices. It also serves as a basis on what materials, connectors, and terminations that is applicable for the setup.
17) What is RIP?
RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.
18) What are the different ways of securing a computer network?
There are several ways to do this. Install a reliable and updated anti-virus program on all computers. Make sure firewalls are setup and configured correctly. User authentication will also help a lot. All these combined would make a highly secured network.
19) What is NIC?
NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.
20) What is WAN?
WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.
21) What is the importance of the OSI Physical Layer?
The physical layer does the conversion from data bits to the electrical signal, and vice versa. This is where network devices and cable types are considered and setup.

22) How many layers are there under TCP/IP?
There are four layers: 1) The Network Layer, 2) Internet Layer, 3) Transport Layer, and 4) Application Layer.
23) What are proxy servers, and how do they protect computer networks?
Proxy servers primarily prevent external users who are identifying the IP addresses of an internal network. Without knowledge of the correct IP address, even the physical location of the network cannot be identified. Proxy servers can make a network virtually invisible to external users.
24) What is the function of the OSI Session Layer?
This layer provides the protocols and means for two devices on the network to communicate with each other by holding a session. This includes setting up the session, managing information exchange during the session, and tear-down process upon termination of the session.
25) What is the importance of implementing a Fault Tolerance System?
A fault tolerance system ensures continuous data availability. This is done by eliminating a single point of failure.
26) What does 10Base-T mean?
The 10 refers to the data transfer rate. In this case, it is 10Mbps. The word Base refers to baseband, as opposed to broadband.
27) 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 ensure that no conflicts are present among internal networks. At the same time, the same range of private IP addresses is reusable for multiple intranets since they do not "see" each other.
28) What is NOS?
NOS, or Network Operating System, is specialized software. The main task of this software is to provide network connectivity to a computer in order to communicate with other computers and connected devices.
29) What is DoS?
DoS, or Denial-of-Service attack, is an attempt to prevent users from being able to access the Internet or any other network services. Such attacks may come in different forms and are done by a group of perpetrators. One common method of doing this is to overload the system server so it cannot anymore process legitimate traffic and will be forced to reset.
30) What is OSI, and what role does it play in computer networks?
OSI (Open Systems Interconnect) serves as a reference model for data communication. It is made up of 7 layers, with each layer defining a particular aspect of how network devices connect and communicate with one another. One layer may deal with the physical media used, while another layer dictates how data is transmitted across the network.
31) What is the purpose of cables being shielded and having twisted pairs?
The primary purpose of this is to prevent crosstalk. Crosstalk's are electromagnetic interferences or noise that can affect data being transmitted across cables.
32) What is the advantage of address sharing?
By using address translation instead of routing, address sharing provides an inherent security benefit. That's because host PCs on the Internet can only see the public IP address of the external interface on the computer. Instead, it provides address translation and not the private IP addresses on the internal network.
33) What are MAC addresses?
MAC, or Media Access Control, uniquely identifies a device on the network. It is also known as a physical address or an Ethernet address. A MAC address is made up of 6-byte parts.
34) What is the equivalent layer or layers of the TCP/IP Application layer in terms of the OSI reference model?
The TCP/IP Application layer has three counterparts on the OSI model: 1) Session Layer, 2) Presentation Layer, and 3) Application Layer.
35) How can you identify the IP class of a given IP address?
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.
36) 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.
37) What are firewalls?
Firewalls serve to protect an internal network from external attacks. These external threats can be hackers who want to steal data or computer viruses that can wipe out data in an instant. It also prevents other users from external networks from gaining access to the private network.
38) Describe star topology
Star topology consists of a central hub that connects to nodes. This is one of the easiest to set up and maintain.
Advantages: Here are pros/benefits of start topology:

- Easy to troubleshoot, set up, and modify.
- Only those nodes are affected, that has failed. Other nodes still work.
- Fast performance with few nodes and very low network traffic.
- In Star topology, addition, deletion, and moving of the devices are easy.

Disadvantages: Here are cons/drawbacks of using Star:

- If the Hub or concentrator fails, attached nodes are disabled.
- The cost of installation of star topology is costly.
- Heavy network traffic can sometimes slow the bus considerably.
- Performance depends on the Hub's capacity
- A damaged cable or lack of proper termination may bring the network down.

39) What are gateways?
Gateways provide connectivity between two or more network segments. It is usually a computer that runs the gateway software and provides translation services. This translation is key in allowing different systems to communicate on the network.
40) What is the disadvantage of a star topology?
One major disadvantage of star topology is that once the central Hub or switch gets damaged, the entire network becomes unusable.
41) What is SLIP?
SLIP, or Serial Line Interface Protocol, is an old protocol developed during the early UNIX days. This is one of the protocols that are used for remote access.
42) Give some examples of private network addresses.
10.0.0.0 with a subnet mask of 255.0.0.0172.16.0.0 with subnet mask of 255.240.0.0192.168.0.0 with subnet mask of 255.255.0.0
43) What is tracert?
Tracert is a Windows utility program that can use to trace the route taken by data from the router to the destination network. It also shows the number of hops taken during the entire transmission route.
44) What are the functions of a network administrator?
A network administrator has many responsibilities that can be summarized into 3 key functions: installation of a network, a configuration of network settings, and maintenance/troubleshooting of networks.
45) What is the main disadvantage of a peer to peer network?
Accessing the resources that are shared by one of the workstations on the network takes a performance hit.
46) What is a Hybrid Network?
A hybrid network is a network setup that makes use of both client-server and peer-to-peer architecture.
47) What is DHCP?
DHCP is short for Dynamic Host Configuration Protocol. Its main task is to assign an IP address to devices across the network automatically. It first checks for the next available address not yet taken by any device, then assigns this to a network device.
48) What is the main job of the ARP?
The main task of the ARP or Address Resolution Protocol is to map a known IP address to a MAC layer address.
49) What is TCP/IP?
TCP/IP is short for Transmission Control Protocol / Internet Protocol. This is a set of protocol layers that is designed to make data exchange possible on different types of computer networks, also known as a heterogeneous network.
50) How can you manage a network using a router?
Routers have a 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.
51) What protocol can be applied when you want to transfer files between different platforms, such as 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.
52) What is the use of a default gateway?
Default gateways provide means for the local networks to connect to the external network. The default gateway for connecting to the external network is usually the address of the external router port.
53) What can be considered as good passwords?
Good passwords are made up of not just letters, but by combining letters and numbers. A password that combines uppercase and lowercase letters is favorable than one that uses all upper case or all lower-case letters. Passwords must be not words that can easily be guessed by hackers, such as dates, names, favorites, etc. Longer passwords are also better than short ones.
54) What is the proper termination rate for UTP cables?
The proper termination for unshielded twisted pair network cable is 100 ohms.
55) What is netstat?
Netstat is a command-line utility program. It provides useful information about the current TCP/IP settings of a connection.
56) 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.
57) What happens when you use cables longer than the prescribed length?
Cables that are too long would result in signal loss. It means that data transmission and reception would be affected because the signal degrades over length.
58) What common software problems can lead to network defects?
Software related problems can be any or a combination of the following:

- Client-server problems
- Application conflicts
- Error in configuration
- Protocol mismatch
- Security issues
- User policy and rights issues

59) What is ICMP?
ICMP is an 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.
60) 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.

61) What is peer to peer?

Peer to peer (P2P) are networks that do not rely on a server. All PCs on this network act as individual workstations.

62) What is DNS?

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

63) What advantages does fiber optics have over other media?

One major advantage of fiber optics is that it is 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.

64) What is the difference between a hub and a switch?

Here is the major difference between Hub and switch:

Hub	Switch
A hub operates on the physical layer.	A switch operates on the data link layer.
Hubs perform frame flooding that can be unicast, multicast, or broadcast.	It performs broadcast, then the unicast and multicast as needed.
Just a singular domain of collision is present in a hub.	Varied ports have separate collision domains.
The transmission mode is Half-duplex	The transmission mode is Full duplex
Hubs operate as a Layer 1 device per the OSI model.	Network switches help you to operate at Layer 2 of the OSI model.
To connect a network of personal computers should be joined through a central hub.	Allow connecting multiple devices and ports.
Uses electrical signal orbits	Uses frame & packet
Does not offer Spanning-Tree	Multiple Spanning-Tree is possible
Collisions occur mostly in setups using hubs.	No collisions occur in a full-duplex switch.
Hub is a passive device	A switch is an active device
A network hub can't store MAC addresses.	Switches use CAM (Content Accessible Memory) that can be accessed by ASIC (Application Specific Integrated Chips).
Not an intelligent device	Intelligent device
Its speed is up to 10 Mbps	10/100 Mbps, 1 Gbps, 10 Gbps
Does not use software	Has software for administration

65) What are the different network protocols that are supported by Windows RRAS services?

There are three main network protocols supported: NetBEUI, TCP/IP, and IPX.

66) What are the maximum networks and hosts in class A, B, and C network?

For Class A, there are 126 possible networks and 16,777,214 hosts. For Class B, there are 16,384 possible networks and 65,534 hosts. For Class C, there are 2,097,152 possible networks and 254 hosts

67) What is the standard color sequence of a straight-through cable?

Orange/white, orange, green/white, blue, blue/white, green, brown/white, brown.

68) What protocols fall under the Application layer of the TCP/IP stack?

The following are the protocols under the TCP/IP Application layer: FTP, TFTP, Telnet, and SMTP.

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

Yes, you can connect two computers, using only one cable. A crossover type cable can be used 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.

70) What is ipconfig?

Ipconfig is a utility program that is commonly used to identify the addresses information of a computer on a network. It can show the physical address as well as the IP address.

71) 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, such as a PC to PC or Hub, to the Hub.

72) What is the 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 refer to a workstation that accesses the server.

73) Describe networking.

Networking refers to the interconnection between computers and peripherals for data communication. Networking can be done using wired cabling or through a wireless link.

74) 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 another one replaced the NIC card.

75) Explain clustering support

Clustering support refers to the ability of a network operating system to connect multiple servers in a fault-tolerant group. The main purpose of this is the if one server fails, all processing will continue with the next server in the cluster.

76) Where is the best place to install an Anti-virus program?

An anti-virus program must be installed on all servers and workstations to ensure protection. That's because individual users can access any workstation and introduce a computer virus. You can plug in their removable hard drives or flash drives.

77) 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.

78) What are some 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 network, the entire network must be temporarily brought down.

79) 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.

80) What is SMTP?

SMTP is short for Simple Mail Transfer Protocol. This protocol deals with all internal mail and provides the necessary mail delivery services on the TCP/IP protocol stack.

81) What is multicast routing?

Multicast routing is a targeted form of broadcasting that sends a message to a selected group of the user instead of sending it to all users on a subnet.

82) What is the importance of Encryption on a network?

Encryption is the process of translating information into a code that is unreadable by the user. It is then translated back or decrypted back to its normal readable format using a secret key or password. Encryption ensures that information that is intercepted halfway would remain unreadable because the user must have the correct password or key for it.

83) How are IP addresses arranged and displayed?

IP addresses are displayed as a series of four decimal numbers that are separated by period or dots. Another term for this arrangement is the dotted-decimal format. An example is 192.168.101.2

84) Explain the importance of authentication.

Authentication is the process of verifying a user's credentials before he can log into the network. It is normally performed using a username and password. This provides a secure means of limiting access from unwanted intruders on the network.

85) What is meaning by tunnel mode?

This is a mode of data exchange wherein two communicating computers do not use IPsec themselves. Instead, the gateway that is connecting their LANs to the transit network creates a virtual tunnel. So, it uses the IPsec protocol to secure all communication that passes through it.

86) What are the different technologies involved in establishing WAN links?

- Analog connections - using conventional telephone lines
- Digital connections - using digital-grade telephone lines
- Switched connections - using multiple sets of links between the sender and receiver to move data.

87) Explain Mesh Topology

The mesh topology has a unique network design in which each computer on the network connects to every other. It is developing a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, data still has an alternative path to reach its destination.

Types of Mesh Topology:

Partial Mesh Topology: In this type of topology, most of the devices are connected almost similarly as full topology. The only difference is that few devices are connected with just two or three devices.

Full Mesh Topology: In this topology, every node or device are directly connected with each other.

88) When troubleshooting computer network problems, what common hardware-related problems can occur?

A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs, and even hardware startups. Incorrect hardware configuration is also one of those culprits to look into.

89) How can you fix signal attenuation problems?

A common way of dealing with such a problem is to use repeaters and hubs because it will help regenerate the signal and therefore prevent signal loss. Checking if cables are properly terminated is also a must.

90) How does dynamic host configuration protocol aid in network administration?

Instead of having to visit each client computer to configure a static IP address, the network administrator can apply dynamic host configuration protocol to create a pool of IP addresses known as scopes that can be dynamically assigned to clients.

91) Explain profile in terms of networking concepts

Profiles are the configuration settings made for each user. A profile may be created that puts a user in a group, for example.

92) What is sneakernet?

Sneakernet is believed to be the earliest form of networking wherein data is physically transported using removable media, such as disk, tapes.

93) What is the role of the IEEE in computer networking?

IEEE, or the Institute of Electrical and Electronics Engineers, is an organization composed of engineers that issues and manages standards for electrical and electronic devices. This includes networking devices, network interfaces, cablings, and connectors.

94) What protocols fall under the TCP/IP Internet Layer?

There are 4 protocols that are being managed by this layer. These are ICMP, IGMP, IP, and ARP.

95) When it comes to networking, what are rights?

Rights refer to the authorized permission to perform specific actions on the network. Each user on the network can be assigned individual rights, depending on what must be allowed for that user.

96) What is one basic requirement for establishing VLANs?

A VLAN is required because at the switch level. There is only one broadcast domain. It means whenever a new user is connected to switch. This information is spread throughout the network. VLAN on switch helps to create a separate broadcast domain at the switch level. It is used for security purposes.

97) What is IPv6?

IPv6, or Internet Protocol version 6, was developed to replace IPv4. At present, IPv4 is being used to control internet traffic but is expected to get saturated in the near future. IPv6 was designed to overcome this limitation.

98) What is the RSA algorithm?

RSA is short for the Rivest-Shamir-Adleman algorithm. It is the most commonly used public-key encryption algorithm in use today.

99) What is mesh topology?

Mesh topology is a setup wherein each device is connected directly to every other device on the network. Consequently, it requires that each device has at least two network connections.

100) what is the maximum segment length of a 100Base-FX network?

The maximum allowable length for a network segment using 100Base-FX is 412 meters. The maximum length for the entire network is 5 kilometers.

101) What is the 5-4-3 rule, and in which architecture is it used?

The 5-4-3 rule is used in 10Base2 and 10Base5 Ethernet architectures. In this rule, there can be a maximum of five segments in a network connected with four repeaters. Out of these five segments, only three segments can be populated with nodes.

102) What is the difference between TCP and UDP?

Here are some major differences between TCP and UDP protocols:

TCP	UDP
It is a connection-oriented protocol.	It is a connectionless protocol.
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the Internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.
The speed for TCP is slower.	UDP is faster as error recovery is not attempted.
Header size is 20 bytes	The header size is 8 bytes.
TCP is heavy-weight. TCP needs three packets to set up a socket connection before any user data can be sent.	UDP is lightweight. There are no tracking connections, ordering of messages, etc.
TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.
Acknowledgment segments	No Acknowledgment segments
Using handshake protocol like SYN, SYN-ACK, ACK	No handshake (so connectionless protocol)
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can't be guaranteed in UDP.
TCP offers extensive error checking mechanisms because it provides flow control and acknowledgment of data.	UDP has just a single error checking mechanism that is used for checksums.

103) What are the important elements of the protocol?
Here, are three most important elements of the protocol:

- **Syntax:** It is the format of the data. It is an order the data is displayed.
- **Semantics:** It describes the meaning of the bits in each section.
- **Timing:** What time the data is to be sent and how fast it is to be sent.

104) What is the maximum segment length of a 100Base-FX network?
The maximum length for a network segment using 100Base-FX is 412 meters.
105) What is a Decoder?
The decoder is a type of circuit that converts the encoded data to its original format. It also converts the digital signal into an analog signal.
106) What is Brouter?
Brouter is also known as Bridge Router. It is a device that acts as both a bridge and a router. As a bridge can forwards data between the networks. It also routes the data to specified systems within a network.
107) How to use VPN?
By using a Virtual Private Network (VPN), users can connect to the organization's network. Corporate companies, educational institutions, government offices.
108) Why the standard OSI model is known as 802.xx?
The OSI model was started in February 1980. In 802.XX, '80' stands for the year 1980, and '2' represents the month of February.
109) What is NVT (Network Virtual Terminal)?
NVT is a set of pre-defined rules to very simple virtual terminal interaction. This terminal helps you to start a Telnet session.
110) What is the source route?
The source route is a sequence of IP addresses that helps you to identify the route a datagram. You can include the source route in the IP datagram header.
111) Explain the term Pipelining
Pipelining describes the sequencing of processes. When any new task begins before an ongoing task is finished, it is called sequencing.
112) Which measurement unit is used to measure the transmission speed of Ethernet?
The transmission speed of Ethernet is mostly measured in Mbps.
113) What is the maximum length of Thinnet cable?
The length of the Thinnet cable is 185 meters.
114) Which cable is also called as the RG8 cable?
Thicknet cable is also called as the RG8 cable.
115) Is coaxial cable still used in the computer network?
No, Nowadays, coaxial cable no longer used in a computer network.
116) Which cable uses the RJ11 connector?
Most of the telephone cable uses the RJ11 connector.
117) Explain Multi-homed Host
It is a host that has multiple network interfaces that multiple IP addresses is called a Multi-homed Host.
118) Explain EGP
The full form of EGP is Exterior Gateway Protocol. It is the protocol of the routers. It is the neighboring autonomous systems that help you to identify the set of networks that you will able to reach within or via each independent system.
119) Explain the term Passive Topology
When a computer in the network listen and receive the signal, they are called passive topology.
120) What is the use of a Pseudo TTY?
It is a false terminal which allows you external machines to connect through Telnet or log in. Without this, no connection can take place.
121) Explain Redirector
Redirector is a kind of software which intercepts file or prints I/O requests and translates them into network requests. This component comes under the presentation layer.
122) What Is TCP Three-Way Handshake?
HREE-WAY handshake or a TCP 3-way handshake is a process that is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.
123) What is a Hamming code?
Hamming code is a liner code that is useful for error detection up to two immediate bit errors. It is capable of single-bit errors. In Hamming code, the source encodes the message by adding redundant bits in the message. These redundant bits are mostly inserted and generated at certain positions in the message to accomplish the error detection and correction process.
124) What is the Application of Hamming code?
Here are some common applications of using Hemming code:

- Satellites
- Computer Memory
- Modems
- PlasmaCAM
- Open connectors
- Shielding wire
- Embedded Processor

125) What are the benefits of the Hamming code?

Here, are important benefits of Hamming code

- The Hamming code method is effective on networks where the data streams are given for the single-bit errors.
- Hamming code not only provides the detection of a bit error but also helps you to indent bit containing error so that it can be corrected.
- The ease of use of hamming codes makes it suitable for use in computer memory and single-error correction.

126) What is a MAC Address?

MAC address is a unique identifier that is assigned to a NIC (Network Interface Controller/ Card). It consists of a 48 bit or 64-bit address, which is associated with the network adapter. MAC address can be in hexadecimal format. The full form of MAC address is Media Access Control address.

127) Why Use MAC Address?

Here are the important reasons for using MAC address:

- It provides a secure way to find senders or receivers in the network.
- MAC address helps you to prevent unwanted network access.
- MAC address is a unique number. Hence it can be used to track the device.
- Wi-Fi networks at the airport use the MAC address of a specific device in order to identify it.

128) What are the types of MAC Addresses?

Here are the important types of MAC addresses:

- Universally Administered Address
  UAA(Universally Administered Address) is the most used type of MAC address. It is given to the network adapter at the time of manufacturing.
- Locally Administered Address
  LAA (Locally Administered Address) is an address that changes the MAC address of the adapter. You may assign this address to a device used by network administrator.

129) What are the important differences between MAC address and IP address

Here, are some difference between MAC and IP address:

MAC	IP address
The MAC address stands for Media Access Control Address.	IP address stands for Internet Protocol Address.
It consists of a 48-bit address.	It consists of a 32-bit address.
MAC address works at the link layer of the OSI model.	IP address works at the network layer of OSI model.
It is referred to as a physical address.	It is referred to as a logical address.
You can retrieve the MAC address of any device using ARP protocol.	You can retrieve the MAC address of any device RARP protocol.
Classes are not used in MAC address.	In IP, IPv4 uses A, B, C, D, and E classes.

130) What is an Analog Signal?

Analog signal is a continuous signal in which one time-varying quantity represents another time-based variable. These kind of signals works with physical values and natural phenomena such as earthquake, frequency, volcano, speed of wind, weight, lighting, etc.

131) What is a Digital Signal?

A digital signal is a signal that is used to represent data as a sequence of separate values at any point in time. It can only take on one of a fixed number of values. This type of signal represents a real number within a constant range of values.

132) What are the differences between analog and digital signal?

Here are the main differences between Analog and Digital Signal:

Analog	Digital
An analog signal is a continuous signal that represents physical measurements.	Digital signals are time separated signals which are generated using digital modulation.
It is denoted by sine waves	It is denoted by square waves.
It uses a continuous range of values that help you to represent information.	The Digital signal uses discrete 0 and 1 to represent information.
The analog signal bandwidth is low	The digital signal bandwidth is high.
Analog hardware never offers flexible implementation.	Digital hardware offers flexibility in implementation.