Networking Interview Questions & Answer

1. 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.

2. 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.

3. 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.

4. 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.

5. What is point-point link?

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

6. What is Multiple Access?

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

7. What are the advantages of Distributed Processing?

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

8. 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 virues.

9. Name the factors that affect the performance of the network?

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

10. Name the factors that affect the reliability of the network?

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

11. Name the factors that affect the security of the network?

a. Unauthorized Access
b. Viruses

12. What is Protocol?

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

13. 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.

14. What are the key design issues of a computer Network?

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

15. 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.

16. Define Routing?

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

17. What is a peer-peer process?

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

18. 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.

19. What is semantic gap?

Defining a useful channel involves both understanding the applications requirements and recognizing the limitations of the underlying technology. The gap between what applications expects and what the underlying technology can provide is called semantic gap.

20. 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.

21. Define the terms Unicasting, Multiccasting 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.

22. What is Multiplexing?

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

23. 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)

24. 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.

25. What is WDM?

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

26. 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.

27. 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.

28. 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

29. Which layers are network support layers?

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

30. Which layers are user support layers?

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

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

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

32. 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

33. 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.
a. Framing
b. Physical Addressing
c. Flow Control
d. Error Control
e. Access Control

34. 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

35. 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

36. 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

37. 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

38. 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

39. What are the two classes of hardware building blocks?

Nodes and Links.

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

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

41. 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

42. 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.

43. What is Error Detection? What are its methods?

Data can be corrupted during transmission. For reliable communication errors must be deducted and Corrected. Error Detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination. The common Error Detection methods are

a. Vertical Redundancy Check (VRC)
b. Longitudinal Redundancy Check (VRC)
c. Cyclic Redundancy Check (VRC)
d. Checksum

44. What is Redundancy?

The concept of including extra information in the transmission solely for the purpose of comparison. This technique is called redundancy.

45. What is VRC?

It is the most common and least expensive mechanism for Error Detection. In VRC, a parity bit is added to every data unit so that the total number of 1s becomes even for even parity. It can detect all single-bit errors. It can detect burst errors only if the total number of errors in each data unit is odd.

46. What is LRC?

In LRC, a block of bits is divided into rows and a redundant row of bits is added to the whole block. It can detect burst errors. If two bits in one data unit are damaged and bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error. In LRC a redundant data unit follows n data units.

47. What is CRC?

CRC, is the most powerful of the redundancy checking techniques, is based on binary division.

48. What is Checksum?

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

49. List the steps involved in creating the checksum.

a. Divide the data into sections
b. Add the sections together using 1's complement arithmetic
c. Take the complement of the final sum, this is the checksum.

50. 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

51. 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.

52. What is Forward Error Correction?

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

53. 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.

54. What are Data Words?

In block coding, we divide our message into blocks, each of k bits, called datawords. The block coding process is one-to-one. The same dataword is always encoded as the same codeword.

55. What are Code Words?

"r" redundant bits are added to each block to make the length n = k + r. The resulting n-bit blocks are called codewords. 2^n - 2^k codewords that are not used. These codewords are invalid or illegal.

56. What is a Linear Block Code?

A linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword.

57. What are Cyclic Codes?

Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.

58. Define Encoder?

A device or program that uses predefined algorithms to encode, or compress audio or video data for storage or transmission use. A circuit that is used to convert between digital video and analog video.

59. Define Decoder?

A device or program that translates encoded data into its original format (e.g. it decodes the data). The term is often used in reference to MPEG-2 video and sound data, which must be decoded before it is output.

60. What is Framing?

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet has to go and the sender address helps the recipient acknowledge the receipt.

61. What is Fixed Size Framing?

In fixed-size framing, there is no need for defining the boundaries of the frames. The size itself can be used as a delimiter.

62. Define Character Stuffing?

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

63. What is Bit Stuffing?

Bit stuffing is the process of adding one extra 0 whenever five consecutive Is follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

64. 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.

65. 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.

66. 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).

67. 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.

68. 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.

69. What is usage of Sequence Number in Relaible 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.

70. 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.

71. 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.

72. What is Piggy Backing?

A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

73. What are the two types of transmission technology available?

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

74. What is subnet?

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

75. Difference between the communication and transmission.

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

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

76. What are the possible ways of data exchange?

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

77. What is SAP?

Series of interface points that allow other computers to communicate with the other layers of network protocol stack.

78. What do you meant by "triple X" in Networks?

The function of PAD (Packet Assembler Disassembler) is described in a document known as X.3. The standard protocol has been defined between the terminal and the PAD, called X.28; another standard protocol exists between hte PAD and the network, called X.29. Together, these three recommendations are often called "triple X".

79. What is frame relay, in which layer it comes?

Frame relay is a packet switching technology. It will operate in the data link layer.

80. What is terminal emulation, in which layer it comes?

Telnet is also called as terminal emulation. It belongs to application layer.

81. What is Beaconing?

The process that allows a network to self-repair networks problems. The stations on the network notify the other stations on the ring when they are not receiving the transmissions. Beaconing is used in Token ring and FDDI networks.

82. What is redirector?

Redirector is software that intercepts file or prints I/O requests and translates them into network requests. This comes under presentation layer.

83. What is NETBIOS and NETBEUI?

NETBIOS is a programming interface that allows I/O requests to be sent to and received from a remote computer and it hides the networking hardware from applications.

NETBEUI is NetBIOS extended user interface. A transport protocol designed by microsoft and IBM for the use on small subnets.

84. What is RAID?

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

85. 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.

86. What is Brouter?

Hybrid devices that combine the features of both bridges and routers.

87. What is cladding?

A layer of a glass surrounding the center fiber of glass inside a fiber-optic cable.

88. What is point-to-point protocol?

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

89. 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.

90. What is attenuation?

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

91. 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 is unique.

92. 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.

93. 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.

94. 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.

95. 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.

96. What is Protocol Data Unit?

The data unit in the LLC level is called the protocol data unit (PDU). The PDU contains of four fields a destination service access point (DSAP), a source service access point (SSAP), a control field and an information field. DSAP, SSAP are addresses used by the LLC to identify the protocol stacks on the receiving and sending machines that are generating and using the data. The control field specifies whether the PDU frame is a information frame (I - frame) or a supervisory frame (S - frame) or a unnumbered frame (U - frame).

97. 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 recipent 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.

98. 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 uses the echo test / reply to test whether a destination is reachable and responding. It also handles both control and error messages.

99. 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.

100. 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.

101. 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.

102. 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

103. 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.

104. 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.

105. 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.

106. What is mesh network?

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

107. 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.

108. Explain 5-4-3 rule?

In a Ethernet network, between any two points on the network ,there can be no more than five network segments or four repeaters, and of those five segments only three of segments can be populated.

109. What MAU?

In token Ring , hub is called Multistation Access Unit(MAU).

110. 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.

111. Why should you care about the OSI Reference Model?

It provides a framework for discussing network operations and design.

112. 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.

113. 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.

114. 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.

115. What is packet filter?

Packet filter is a standard router equipped with some extra functionality. The extra functionality allows every incoming or outgoing packet to be inspected. Packets meeting some criterion are forwarded normally. Those that fail the test are dropped.

116. What is traffic shaping?

One of the main causes of congestion is that traffic is often busy. If hosts could be made to transmit at a uniform rate, congestion would be less common. Another open loop method to help manage congestion is forcing the packet to be transmitted at a more predictable rate. This is called traffic shaping.

117. What is multicast routing?

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

118. What is region?

When hierarchical routing is used, the routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

119. 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.

120. What are Digrams and Trigrams?

The most common two letter combinations are called as digrams. e.g. th, in, er, re and an. The most common three letter combinations are called as trigrams. e.g. the, ing, and, and ion.

121. Expand IDEA.

IDEA stands for International Data Encryption Algorithm.

122. What is wide-mouth frog?

Wide-mouth frog is the simplest known key distribution center (KDC) authentication protocol.

123. What is Mail Gateway?

It is a system that performs a protocol translation between different electronic mail delivery protocols.

124. What is IGP (Interior Gateway Protocol)?

It is any routing protocol used within an autonomous system.

125. What is EGP (Exterior Gateway Protocol)?

It is the protocol the routers in neighboring autonomous systems use to identify the set of networks that can be reached within or via each autonomous system.

126. What is autonomous system?

It is a collection of routers under the control of a single administrative authority and that uses a common Interior Gateway Protocol.

127. 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).

128. What is Gateway-to-Gateway protocol?

It is a protocol formerly used to exchange routing information between Internet core routers.

129. What is NVT (Network Virtual Terminal)?

It is a set of rules defining a very simple virtual terminal interaction. The NVT is used in the start of a Telnet session.

130. What is a Multi-homed Host?

It is a host that has a multiple network interfaces and that requires multiple IP addresses is called as a Multi-homed Host.

131. What is Kerberos?

It is an authentication service developed at the Massachusetts Institute of Technology. Kerberos uses encryption to prevent intruders from discovering passwords and gaining unauthorized access to files.

132. What is OSPF?

It is an Internet routing protocol that scales well, can route traffic along multiple paths, and uses knowledge of an Internet's topology to make accurate routing decisions.

133. What is Proxy ARP?

It is using a router to answer ARP requests. This will be done when the originating host believes that a destination is local, when in fact is lies beyond router.

134. What is SLIP (Serial Line Interface Protocol)?

It is a very simple protocol used for transmission of IP datagrams across a serial line.

135. What is RIP (Routing Information Protocol)?

It is a simple protocol used to exchange information between the routers.

136. What is source route?

It is a sequence of IP addresses identifying the route a datagram must follow. A source route may optionally be included in an IP datagram header.

137. What is a router? Or define the basic requirements of a router?

A router is a layer 3 network device used to establish communication between different networks. Basic roles performed by a router are:

- * Inter-network communication
- * Best path selection
- * Packet forwarding
- * Packet filtering

138. What is the use of routing? or Why we use routing?

By default, a router provides inter-network communication only for directly connected networks. To establish communication between indirectly connected networks, we require ROUTING. We can use static or dynamic (IGP or EGP) routing, according to topology requirement.

139. Define the criteria for best path selection of a router?

A router's routing table contains only best route. To select a route as best, a router considers the following parameters;

- * Longest prefix match
- * Minimum AD (administrative distance)
- * Lowest metric value

If all listed parameters are the same, then it would perform equal cost load balancing.

140. Define "stuck in active."

If a successor route (best route) fails, then the router sends a query message to its neighbor demanding a feasible successor (back-up route) and a query received by the router may be forwarded to other neighbors that could lead to a loop, as well. The wait for the response of query message is called "stuck in active" (SIA).

140-A. Can we use OSPF without backbone area?

Yes, but it will be limited to intra-area (same area) communication. By default, Inter-area communication is not possible without backbone area.

141. What do you mean by OSPF transit area ?

A transit area is the area that has a virtual link connecting two or more ABRs attached to this area.

142. What is the difference between an OPPF neighbor and an adjacent neighbor?

Neighbors are the routers that are in the same area and exchange hello packets, but not LSA information. Adjacent routers are routers that have fully exchanged their LSA information and are stable.

If OSPF state is in 2WAY/DROTHER, it means a neighbor relationship and, if the state is FULL/DR or FULL/BDR, it means that the adjacency is formed.

143. BGP neighborship is not coming up. Please define the various steps to troubleshoot it.

To troubleshoot BGP, first we need to check neighbor state using “show ip bgp summary.” If the state is **Idle,** it means that the peer address or AS is not defined properly; if the state is **Active,** it means that TCP port 179 is not open, the peer is not reachable, network congestion, or BGP misconfiguration.

Common neighbor stability problems of BGP

- * Misconfigured neighbor’s IP address and AS number
- * Reachability issues when interfaces other than directly connected interfaces are used while peering (update-source issue).
- * Authentication must be properly implemented (if configured)
- * Router-ID must be unique

144. What is route reflector and why it is required?

Route reflector is a solution for BGP split horizon. The rule says “prefix learned from an iBGP neighbor will not be advertised to another iBGP neighbor.”
To overcome this situation, we have multiple options:

1. Make your network a full mesh
2. Route confederation
3. Confederation

Route reflector is something like a central point acting as a route reflector server: Rather than peering with every iBGP router in a full mesh, it makes IBGP neighbors as route reflector clients to overcome the split horizon issue.

145. What is the difference between standard and extended ACL?

Standard ACLs are source-based, whereas extended ACLs are source- and destination-based. Standard ACLs can only filter layer 3 network traffic, while extended ACLs can be used to filter layer 3 and layer 4, as well.

146. What is the use of distribute-list?

To filter a routing database, we use distribute-list, which can be applied over most routing protocols. This means that, If you don’t want any specific network in your routing table, then you can use distribute-list.

147. MPLS works on which layer?

MPLS operates between layer 2 and layer 3, so it is sometimes called layer 2.5.

148. What is penultimate hop popping (PHP) and what is its use?

PHP is the technique for removing the (POP) MPLS label before the egress router. The MPLS label on a switched packet is popped by either the egress router or the penultimate router, depending on your configuration. If you decide to use penultimate hop popping, you essentially terminate the LSP one hop earlier. The MPLS labels are popped by the routers that connect to the egress router, rather than all of them being popped by the same egress router.

149. What is the difference between layer 2 and layer 3 QoS?

L2-QoS is at the MAC layer and can be applied by using CoS (class of service) filed in the VLAN header. This will be used to prioritize traffic. Later, a QOS scheduler can use the COS filed to qualify the traffic into different QOS queues.

L3 QOS is required for IP level classification; it can be achieved through ToS (type of service) priority values—IPP (3-bit), DSCP (6-bit), which can be set in the TOS field of the IP header. This TOS will later be used by scheduling process to achieve QOS.

L2 queues are hardware-based, while L3 queues are software-based. That’s why we can modify L3 queues to meet our requirements.