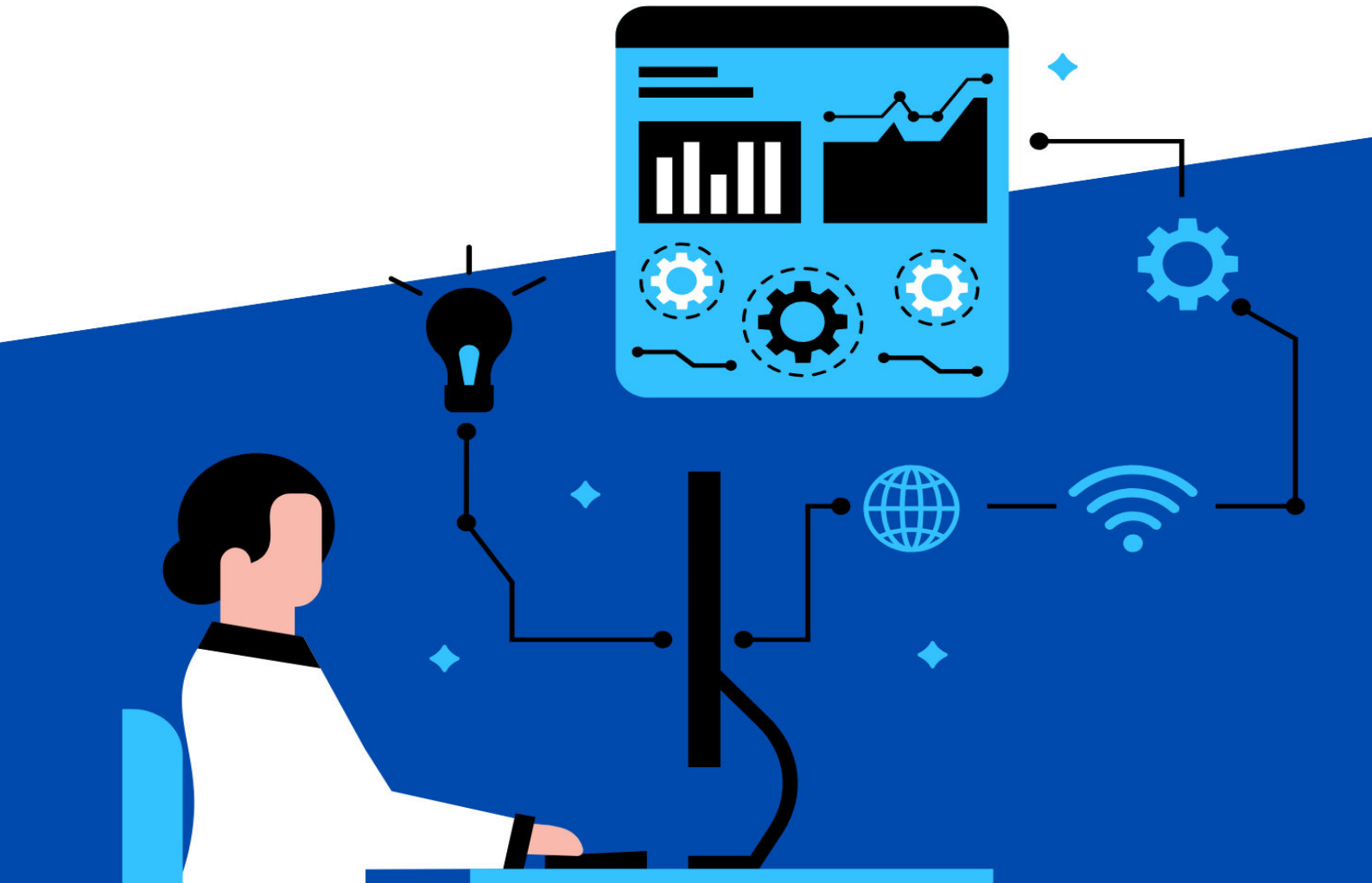
200+ CCNA Interview Q&A (Part – I)



Contents

Basic Networking Interview Questions & Answers

1. Define Network?

Network in general terms means a group of devices, connected with the help of some media in order to share some resources from a source to a destination and networking is a process of sharing the resources.

2. Differentiate User Mode from Privileged Mode.

Commands applied on user mode cannot effect the router while some commands of privilege mode can change the configurations. In user mode, no configuration can be made. We can only check the reachability and some basic commands in that mode. While in Privilege mode we can save, delete and modify the configuration files.

3. What is a Link?

Link is a physical or a logical component of a network to interconnect nodes or devices.

4. What is Bandwidth?

Ans - Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time -- usually one second.

5. What is the difference between broadcast domain and collision domain ?

Broadcast domain is a domain where if a broadcast frame is forwarded, every devices pays attention and receives the data.

While in Collision domain, chances of data collision is maximum. Like in Hub , if two or more send traffic at the same time, data will collide in between and none of the devices will receive the data.

6. Explain Flooding?

Ans- In a network, flooding is the forwarding by a router of a packet from any node to every other node attached to the router except the node from which the packet arrived. Flooding is a way to distribute routing information updates quickly to every node in a large network.

7. What is Telnet?

A network protocol that allows a user on one computer to log onto another computer .it uses TCP Port number 23

8. What is Sub Interface?

A sub interface is a virtual interface created by dividing one physical interface into multiple logical interfaces. A sub-interface in a Cisco Router uses the parent physical interface for sending and receiving data.

9. What is BootP?

Ans - The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server.

10. What is a Window in networking terms?

Ans - A Window refers to the number of segments that is allowed to be sent from source to destination before an acknowledgement is sent back.

11. What is a node?

Node is a connection point on network for data transmission. It can be a computer or printer or any type of device that is capable of sending and receiving the data over the network.

12. What is a gateway?

Gateway is a node of a network which can be used as an entrance for other network. It is a piece of hardware and different from default gateway.

13. What is WAN?

Ans - A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metro area networks (MANs). This ensures that computers and users in one location can communicate with computers and users in other locations..

14. How does cut-through LAN switching work?

In Cut-Through LAN switching, as soon as the router receives the data frame, it will immediately send it out again and forward it to the next network segment after reading the destination address.

15. What is point-point link?

A connection between two nodes of the network is referred as point to point network and that link which connects both nodes is point to point link. Point-to-point protocol is widely used for the heavier and faster connections necessary for broadband communications.

16. What is VPN?

Ans- A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may Therefore benefit from the functionality, security, and management of the private network.

17. what is latency ?

Ans- Network latency is an expression of how much time it takes for a packet of data to get from one designated point to another. In some environments latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the latency.

18. What's the benefit of subnetting?

With the help of subnetting we can break a large network into smaller networks and assign IP addresses to those networks without changing our major network. It helps in utilizing our IP addresses more efficiently.

19. What is BGP (Border Gateway Protocol)?

BGP is an exterior gateway protocol used to connect two or more different autonomous systems. It is widely being used to route the traffic of Internet. It can also work for internal AS but we have better protocols for internal connectivity. It has Administrative distance of 20 for external routes and 200 for internal routes.

20. Explain clustering support?

Ans -In a computer system, a cluster is a group of servers and other resources that act like a single system and enable high availability and, in some cases, load balancing and parallel processing.

21. What is DoS?

Ans - DOS (Disk Operating System) is an operating system that runs from a hard disk drive. The term can also refer to a particular family of disk operating systems, most commonly MSDOS (Microsoft Disk Operating System).

22. What is NOS?

Ans- A network operating system (NOS) is a computer operating system system that is designed primarily to support workstation, personal computer, and, in some instances, older terminal that are connected on a local area network (LAN).

23. What is Gateway-to-Gateway protocol?

Gateway-to-Gateway protocol is now obsolete. This was being used for routing datagrams between internet gateways. It uses Minimum hop Algorithm.

24. What are firewalls?

Ans- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A firewall can be hardware, software, or both.

25. What are some drawbacks of implementing a ring topology?

Ans- 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.

26. What is a Multi-homed Host?

Multi-homed host is defined as a node connected with more than one networks. Like a PC can be connected with both Home network and a VPN. These kind of hosts can be assigned with multiple addresses, one for each network.

27. What is OSPF?

OSPF stands for Open Shortest Path First. It is a link state routing protocol that can connect a large number of networks without having any limitation to number of hops. It uses Dijkstra Algorithm and considers Cost as its' metric. It has AD of 110 and uses the concepts of Areas, Router-id, Process-id and Virtual link for connectivity.

28. What is Routing?

Routing is a process of exchanging route information form one router to another. Without routing it is impossible to connect two or more networks located at different or same geographical areas.

29. What is a Protocol?

Protocol is set of rules on which a sender and a receiver agrees to transmit the data. Protocols are responsible for data communication in between networks

30. What is a Frame Relay?

Ans- Frame relay is a packet-switching telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between endpoints in wide area networks (WANs).

31. What is HDLC?

Ans- A high-level data link control (HDLC) is a protocol that is a bit-oriented synchronous data link layer. HDLC ensures the error-free transmission of data to the proper destinations and controls the data transmission speed. HDLCs can provide both connection-oriented and connectionless services.

32. What is DLCI?

Ans- A data link connection identifier (DLCI) is a Frame Relay 10-bit-wide link-local virtual circuit identifier used to assign frames to a specific PVC or SVC. Frame Relay networks use DLCIs to statistically multiplex frames. DLCIs are preloaded into each switch and act as road signs to the traveling frames.

33. Explain difference between Router,Switch and Hub ?

Ans- Following are the differences in Hub, Routers and Switches,

Hubs

- Hubs operate at Layer 1 of OSI model.
- Hubs cannot process layer-2 or layer-3 traffic. Layer-2 deals with hardware addresses and layer-3 deals with logical (IP) addresses. So, hubs cannot process information based on MAC or IP addresses.
- Hubs cannot even process data based on whether it is a unicast, broadcast or multi-cast data.
- Hub transfers data to every port excluding the port from where data was generated.
- Hubs work only in half duplex mode.
- Collisions can happen.
- In case of a collision, a hub rejects data from all the devices and signals them to send data again. Usually devices follow a random timer after which data is sent again to hub.
- Maximum 2-12 number of ports can be found on Hubs.

Switches

- Switches are network devices that operate on layer-2 of OSI model. Some switches operate at higher level too.
- Switches are also known as intelligent hubs.
- Switches operate on hardware addresses (MAC) to transfer data across devices connected to them.
- It performs broadcast at first, after that Unicast.
- Major difference between Bridge and Switch being that a switch forwards data at wire speed as it uses special hardware circuits known as ASICs.

- Switches support full duplex data transfer communication.
- As layer 2 protocols headers have no information about network of data packet so switches cannot forward data based or networks and that is the reason switches cannot be used with large networks that are divided in sub networks.
- Switches can avoid loops through the use of spanning tree protocol.
- Switches can have 24-48 ports and can be practically unlimited ports because they don't divide speed unlike Hubs.

Routers

- Routers are the network devices that operate at Layer-3 of OSI model.
- As layer-3 protocols have access to logical address (IP addresses) so routers have the capability to forward data across networks.
- Routers are far more feature rich as compared to switches.
- Routers maintain routing table for data forwarding.
- Routers have lesser port densities as compared to switches.
- Routers are usually used as a forwarding network elements in Wide Area Networks.

34. What is Checksum?

A checksum is an error-detection method in a the transmitter computes a numerical value according to the number of set or unset bits in a message and sends it along with each message frame. At the receiver end, the same checksum function (formula) is applied to the message frame to retrieve the numerical value. If the received checksum value matches the sent value, the transmission is considered to be successful and error-free. A checksum may also be known as a hash sum

35. What is Redundancy ?

Redundancy is a method of insuring network availability in case of network or path failure. Generally referred as backup paths in a networks.

36. What is multicast routing?

Ans- Multicast IP Routing protocols are used to distribute data (for example, audio/video streaming broadcasts) to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

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

Ans-. 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 include protecting data from unauthorized access and virus

38. What is the key advantage of using switches?

Ans- Switch doesn't broadcast on all the ports. They can be managed and vlans cab be created. They are fast, can store MAC addresses. They also don't divide the speed on each ports.

The main advantage of using switches is that each switch port has its own collision domain which removes the occurance of collision of frames. It forwards the packets based on the destination address, thereby eleminating unnecessary forwarding of packets to all ports as in hubs.

39. When does network congestion occur?

Ans-Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity.

40. Does a bridge divide a network into smaller segments?

Ans-No, What a bridge actually does is to take the large network and filter it, without changing the size of the network.

41. What is the difference between OSI and TCP/IP Model?

OSI(Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)
OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
OSI model has a separate Presentation layer and Session layer.	TCP/IP does not have a separate Presentation layer or Session layer.
OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	TCP/IP model is, in a way implementation of the OSI model.
Network layer of OSI model provides both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
It has 7 layers	It has 4 layers

42. What is the size of IP Address?

Ans-The size of ipv4=32bit or 4byte and ipv6=128bit or 16bytes

43. What is the range of class C address?

Ans- 192.0.0.0 to 223.255.255.255 Supports 254 hosts

44. What is POE (Power over Ethernet)?

Ans-Power over Ethernet or PoE pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points, IP cameras, and VoIP phones. It minimizes the number of wires required to install the network.

45. What are the advantages of Distributed Processing?

Ans-Distributed data processing is a computer-networking method in which multiple computers across different locations share computer-processing capability. This is in contrast to a single, centralized server managing and providing processing capability to all connected systems. Computers that comprise the distributed data-processing network are located at different locations but interconnected by means of wireless or satellite

Advantage: Lower cost, reliability, improved performance, reduced processing time, flexibility are the advantages of Distributed processing.

46. When were OSI model developed and why its standard called 802.XX and so on?

Ans- OSI model was developed in February1980 that why these also known as802.XX Standard

80 means =1980 & 2means =February.

47. What is Full form of AD?

Administrative Distance or it can be Advertised Distance.

48. What is a peer-peer process?

Ans= Stands for "Peer to Peer." In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

49. What is ping? Why you use ping?

Ping is a utility used to test the connectivity in the network. It stands for Packet Internet Groper.it uses ICMP [internet Control message protocol]Protocol.

50. Explain difference between straight and crossover cable with examples ?

Ans- Straight cable is used to connect two different layer devices like router-switch, router-pc, and switch-pc while cross cable is used to connect two same layer devices like router-router, switch switch, and pc-pc. Color coding for both cable is different. If color coding on both ends of the cable is same, it is a straight cable, while if 1<–>3, 2<–>6 is being used, it is a cross cable for data transfer.

51. What is the difference between tracert and trace route?

Ans –Both Tracert and traceroute commands do similar purpose. On a router or switch you would use the command traceroute and on a pc you would use tracert .

Trace-route :

- You can find this utility in **LINUX/UNIX based operating Systems.**
- It rely over UDP Probe packet with destination PORT : 33434.
- It uses random Source PORT.

Tracert :

- You can find this utility in **Windows based operating systems as well as Servers.**
- It rely over ICMP Type 8(Echo Packet) & Type 0(Echo Request).

52. What is Round Trip Time?

Round-trip time (RTT), also called round-trip delay, is the time required for a packet to travel from a specific source to a specific destination and back again.Source is the computer sending the packet and the destination is a remote computer or system that receives the packet and retransmits it. A user can determine the RTT to and from an IP address by pinging that address

53. Define the terms Unicasting, Multicasting and Broadcasting and Any-casting?

Unicasting means “one on one” communication, Multicasting means “one to many” communication but there must be atleast one devices that is not receiving the traffic while broadcasting means “one to all” communication. Each device receives packets in case of broadcasting. Anycast works in IPv6 and it means to “one to nearest” communication

54. How many pins do serial ports of routers have?

Ans-In computer it's known as com port and could be available in 9pin or 25 pin. On router it have

60 pins.

55. What are the differences between static ip addressing and dynamic ip addressing?

Ans- When a device is assigned a static IP address, the address does not change. Most devices use dynamic IP addresses, which are assigned by the network when they connect and change over time.

56. Difference between CSMA/CD and CSMA/CA ?

CSMA/CD is responsible for detecting collision in wired media mainly, while CSMA/CA works on wireless media to completely avoid collision because detecting collision in wireless media is a bit hard.

57. What is DHCP scope?

Ans- A DHCP scope is a valid range of IP addresses that are available for assignment or lease to client computers on a particular subnet. In a DHCP server, a scope is configured to determine the address pool of IPs that the server can provide to DHCP clients. Scopes determine which IP addresses are provided to the clients.

58. What are the different memories used in a CISCO router?

- **ROM**

ROM is read-only memory available on a router's processor board. The initial bootstrap software that runs on a Cisco router is usually stored in ROM. ROM also maintains instructions for Power-on Self Test (POST) diagnostics.

- **Flash Memory**

Flash memory is an Electronically Erasable and Re-Programmable memory chip. The Flash memory contains the full Operating System Image (IOS, Internetwork Operating System).Flash memory retains content when router is powered down or restarted.

- **RAM**

RAM is very fast memory that loses its information when the router is shutdown or restarted. On a router, RAM is used to hold running Cisco IOS Operating System, IOS system tables and buffers RAM is also used to store routing tables,RAM Provides temporary memory for the router configuration file of the router while the router is powered on.

RAM Stores running Cisco IOS Operating System, Active program and operating system instructions, the Running Configuration File, ARP (Address Resolution Protocol) cache, routing tables and buffered IP Packets.

- **NVRAM (Non-volatile Random Access Memory)**

NVRAM is used to store the Startup Configuration File. This is the configuration file that IOS reads when the router boots up. It is extremely fast memory and retains its content when the router is restarted.

59. What are the different types of passwords used in securing a CISCO router?

Enable password, Secret Password, Line passwords (VTY, Console and Aux) are the passwords used in Router.

60. What are the different types of passwords used in securing a CISCO router?

Ans- Depending on Connection (Device) :

- Enable password
- Console password
- VTY password
- AUX password

61. What is the use of "Service Password Encryption" ?

Service Password Encryption command encrypts plain text password into type 7 password. These are not very much secure and can be easily decrypted.

62. Briefly explain the conversion steps in data encapsulation.?

Process of adding header and trailer information in data is called Data Encapsulation. Whenever a layer passes the data to next layer it adds some extra information in data. This is called header. Next layer then processes the data and adds its own header. This process continues until data is place on physical media. This process is called Encapsulation. Removing header and trailer information from the data is called Data Decapsulation.

Step	**Action**	**Layers Involved**	**Keyword**
Step 1	Alphanumeric input from user converted into Data	**Application/Presentation/Session**	DATA
Step 2	Data converted into segments	**Transport**	SEGMENTS
Step 3	Segments converted into Packets or Datagrams and Network Header is added	**Network**	PACKETS
Step 4	Packets or Datagrams are built into Frames	**Data Link**	FRAMES
Step 5	Frames are converted into bits(1s and 0s) for transmission	**Physical**	BITS

63. **In configuring a router, what command must be used if you want to delete the configuration data that is stored in the NVRAM?**

Ans- Erase startup-config is the command to delete preconfigured files on the router.

64. **IEEE standard for wireless networking?**

Ans- 802.11

65. **What is the range of class A address?**

Ans- From 0.0.0.0 – 127.255.255.255, but we cannot use 0 and 127, so actual range is from 1 to 127

66. **What is the range of class B address?**

Ans- From 128.0.0.0 – 191.255.255.255

67. **Differentiate Logical Topology from Physical Topology?**

Physical topology represents the physical structure i.e cabling of the network while logical topology deals with the data flow in the network.

68. **what is AS (Autonomous System) ?**

A group of devices under a single administration is called an AS. AS Number is assigned by IANA (The Internet Assigned Numbers Authority)

69. **What is the difference between Private IP and Public IP ?**

Public IP addresses are for global routing over internet. They are allocated to the websites and companies to access the internet. They are unique worldwide if connected to Internet. Private IP addresses are for local use and are not routable over internet. They can be same in different organization.

70. **Explain different cable types ?**

Straight, Cross, Serial, Console are some cable types used in networking. Serial cable is used to connect a router to another router. Console cable is used to access the router or switches from a PC.

71. **How does RIP differ from EIGRP?**

The major difference between both is that EIGRP is Cisco propriety and RIP is open standard

Some internal differences between them are:

- AD value of Rip is 120 and AD value for EIGRP is 90 internal / 170 external.
- RIP uses Bellmen ford algorithm to calculate the path while Eigrp use Dual method to calculate the routes paths
- Maximum hop count for RIP is 15 that is after 15 counts the packet is dropped while that of EIGRP is 100 by default and upto 255 by configuration.
- RIP(ver 1) is classfull protocol where as EIGRP is classless protocol
- In RIP full routing table exchanged, but in EIGRP missing routes are exchanged
- For RIP protocol, hello timers every 30 seconds but in EIGRP hello timer every 5 seconds
- RIP v1 sends updates as broadcast while EIGRP send updates as Multicast
- EIGRP uses an Autonomous number to determine which domain it belongs to which is not the case with RIP protocols.
- RIP is mostly used for smaller networks which EIGRP is used for larger networks.
- RIP is a distance vector routing protocol while EIGRP is an hybrid routing protocol.
- RIP sends full update whenever network change occurs whereas EIGRP sends triggered updates

72. Differentiate User Mode from Privileged Mode

Commands applied on user mode cannot effect the router while some commands of privilege mode can change the configurations. In user mode, no configuration can be made. We can only check the reachability and some basic commands in that mode. While in Privilege mode we can save, delete and modify the configuration files.

73. What is 100BaseFX?

100BASE-FX is a version of Fast Ethernet over optical fiber.

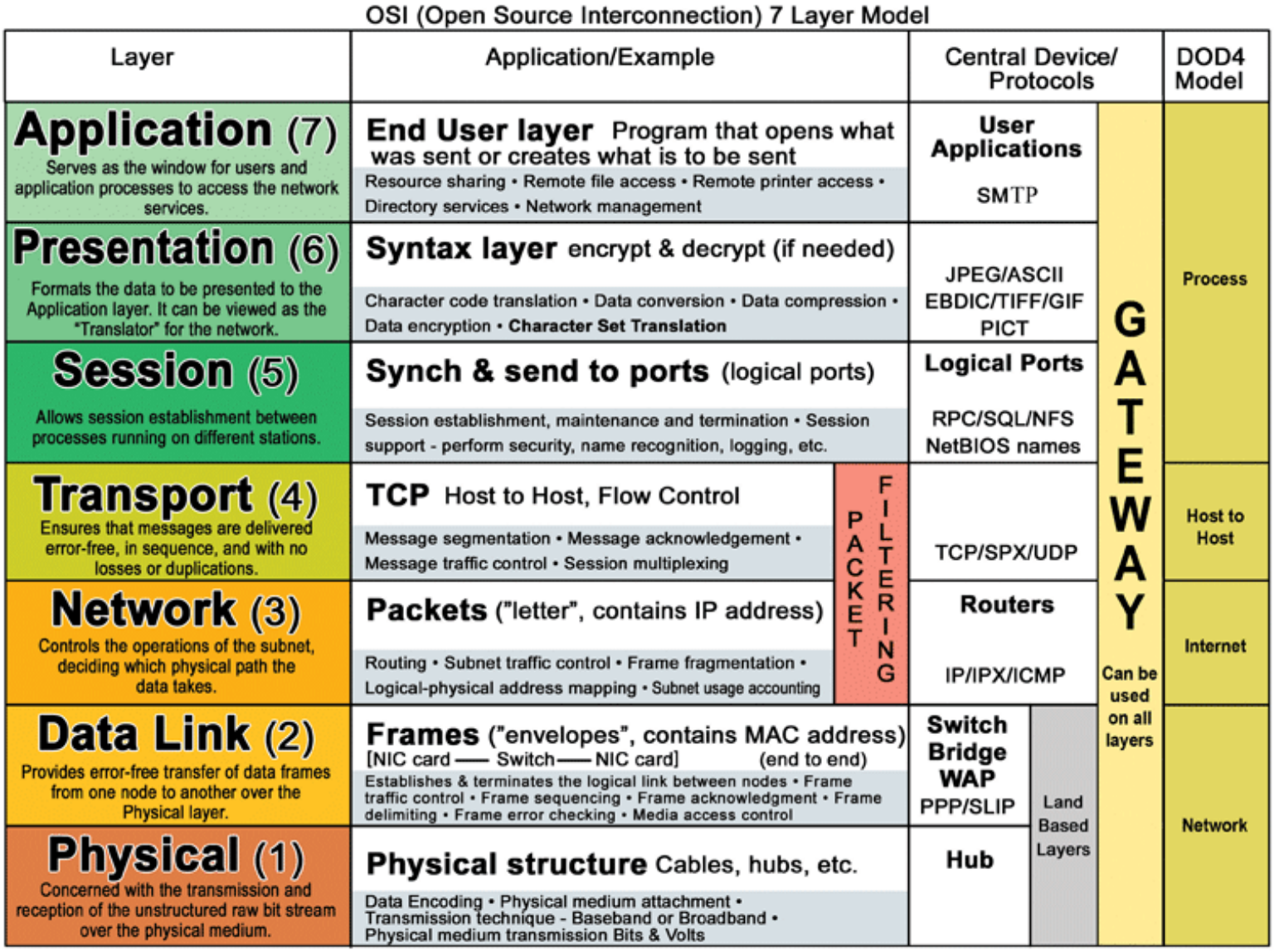
74. Differentiate full-duplex from half-duplex ?

In full duplex, user can send and receive data at the same time while in half duplex user can either receive or send the data at a time.

75. What does the show protocol display?

The show protocols command shows the global and interface-specific status of any configured Level 3 protocol.

OSI Model Interview Questions & Answers



76. **List the layers of OSI?**

From top to bottom, OSI layers are-

Application, Presentation, Session, Transport, Network, Data Link and Physical.

77. **What are the responsibilities of Data Link Layer?**

Framing, Error detection, CRC and Physical Addressing is the task of DLL.

78. **What are the responsibilities of Network Layer?**

Routing, IP Addressing and Path determination are the main responsibilities of Network Layer.

79. **What are the responsibilities of Transport Layer?**

Transport Layer has a lot of function. Most important being,

1. Multiplexing and De-Multiplexing
2. Segmentation and Re-assembly
3. Flow Control
4. Error Correction
5. Connection Establishment
6. Sequencing
7. Acknowledgement
8. 3 way Handshake

80. **Routers work at which OSI layer?**

Network Layer

81. **Switches work at which OSI layer?**

Layer 2 and Some Switches can operate at Layer 3 and above

82. **What is a Window in networking terms?**

Window is the amount of segments sent by TCP between two acknowledgements.

83. **What is the role of the LLC sublayer in** datalink **layer?**

Logical Link Control provides error detection, using Ethernet trailer field frame check sequence (FCS).

84. **What is the function of the Application Layer in networking?**

Application Layer is responsible for providing a user interface in between user and Network with the help of applications like web browsers.

85. **What is the difference between TCP and UDP?**

Following are differences in TCP and UDP,

- TCP stands for "Transmission Control Protocol" UDP stands for "User datagram Protocol".
- TCP is connection oriented protocol while UDP is connectionless protocol.
- TCP is more reliable than UDP.
- UDP is faster for data sending than TCP.
- UDP makes error checking but no reporting but TCP checks for errors and performs reporting.
- TCP provides guaranteed Delivery of Data but UDP has no guarantee.
- Header size of TCP is 20 bytes while that of UDP is 8 bytes.
- TCP has acknowledgement segments but UDP has no acknowledgement.
- TCP is used for application that require high reliability but less time critical whereas UDP is used for application that are time sensitive but require less reliability.

86. **What is the port no of DNS and Telnet?**

DNS = 53, Telnet = 23

87. **Which service use both TCP and UDP ?**

DNS uses both TCP and UDP

88. **What is the port no of SMTP and POP3?**

POP3 = 110; SMTP = 25

89. **In which layer term "Frames" is used ?**

Frames are PDU of Data Link Layer

90. **In which layer term "Packets" is used ?**

Packets are PDU of Network Layer

91. **In which layer term "Segments" is used ?**

Segments are used at Transport Layer

92. **Give some example for protocols work at Application layer ?**

Application Layer Protocols are HTTP, HTTPs, Telnet, SSH, DNS, FTP, TFTP, DHCP, RIP

93. **What is CRC? Which layer CRC works ?**

Cyclic Redundancy Check is used to detect the errors in network. It works at Data Link Layer (LLC Sub Layer).

94. **What is the purpose of the Data Link?**

Data Link Layer is responsible for Framing, Error Detection and Physical Addressing

95. **Which one is reliable – TCP or UDP ?**

TCP is reliable.

96. **What is the port number of** ftp **(data) and** ftp**?**

FTP port number 20 (Data); 21 for Control

97. **Which layer provides logical addressing that routers will use for path determination?**

Network Layer

98. **Which layer specifies voltage, wire speed, and pinout cables and moves bits between devices ?**

Physical

99. **Which layer combines bits into bytes and bytes into frames, uses MAC addressing, and provide error detection ?**

Data Link Layer

100. **Which layer is responsible for keeping the data from different applications separate on the network ?**

Session layer.

101. **Which layer segments and resembles data into a data stream ?**

Transport layer.

102. Which layer provides the physical transmission sof the data and handless error notification, network topology, and flow control ?

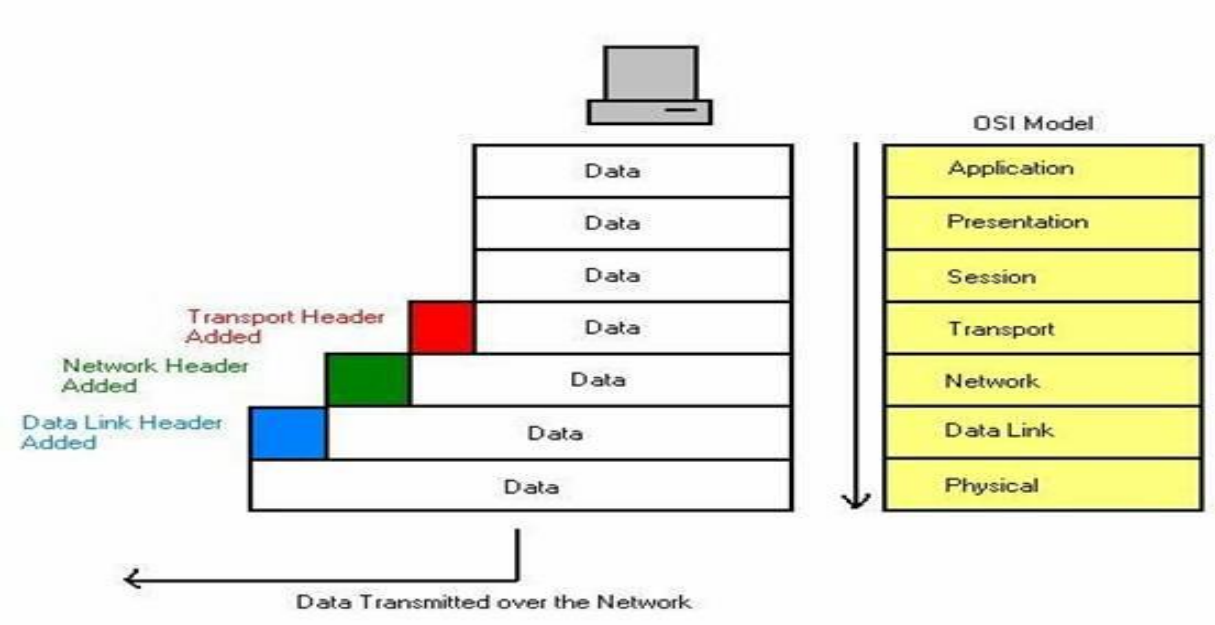
Data Link Layer

103. Which Layer manages device addressing, tracks the location of devices on the network, and determine the best way to move data ?

Network layer.

104. **How Data breaks down on each layer from top to bottom ?**

Encapsulation occurs in following format



105. MAC address works on which layer ? What are the differences of MAC sublayer and LLC sublayer?

MAC works at DATA LINK LAYER. Media Access Control provides physical addressing while Logical Link Control provides error detection, using Ethernet trailer field frame check sequence (FCS). It is 4 bytes field. When a sending device sends a data it put the data in a mathematical algorithm and it gets a product, sending device puts the product in FCS. When a receiving device receive a data it also put the data in same mathematical algorithm and get a product. If both products are same, Frame is accepted or else discarded.

106. Which layer is responsible for converting data packets from the Data Link layer into electrical signals ?

Physical Layer

107. At which layer is routing implemented, enabling connections and path selection between two end systems. ?

Network Layer

108. Which layer defines how data is formatted, presented, encoded,and converted for use on the network ?

Presentation Layer

109. Which layer is responsible for creating, managing and terminating sessions between applications ?

Session Layer

110. DNS uses which protocol? Why?

DNS uses both TCP and UDP. It is necessary to maintain a consistent DNS database between DNS Servers This is achieved by the TCP protocol. A client computer will always send a DNS Query using UDP Protocol over Port 53. If a client computer does not get response from a DNS Server, it must re-transmit the DNS Query using the TCP after 3-5 seconds of interval.

111. Which layer is closer to the user?

From sender point of view, Application Layer is closest and from Receiver point of view Pgysical Layer is closest.

112. Differentiate between forward lookup and reverse lookup in DNS?

- Forward Lookup: Name to IP resolution
- Reverse Lookup: IP to Name resolution;

113. What is IPSec?

IPSec provides data security at the IP Packet Level.

114. What is the way to establish a TCP connection?

TCP Connection is established using three-way Handshake.

115. What is the difference between flow control and error control?

Error Controls the process of detecting and correcting both the bit and packet level error. While flow control is a mechanism to ensure the efficient delivery of Data. Flow control is agreeing on the minimum amount of data that a receiver can handle at a time.

RIP Interview Questions & Answers

116. What is RIP?

RIP is a Distance-Vector Routing protocol. It is a Classful routing protocol (Classful routing protocols do not send subnet mask information with their routing updates). It does not support VLSM (Variable Length Subnet Masking). RIP uses Hop count as its metric to determine the best path to a remote network and it supports maximum hop count of 15. Any router farther than 15 hops away is considered as unreachable. It sends its complete routing table out of all active interfaces every 30 seconds.

117. What is route poisoning?

With route poisoning, when a distance vector routing protocol notices that a route is no longer valid, the route is advertised with an infinite metric, signifying that the route is bad. In RIP, a metric of 16 is used to signify infinity.

118.What is Split Horizon ?

The Split Horizon feature prevents a route learned on one interface from being advertised back out of that same interface.

119. Utilizing RIP, what is the limit when it comes to number of hops?

Routing information protocol is one of the oldest distance vector routing protocols which employ the hop count as a routing metric.The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.

120. Which category is RIP belong to ?

RIP is a standard based, Distance Vector, Interior Gateway Protocol (IGP) used by router to exchange the routing information.

121. Why is RIP known as Distance Vector?

RIP is known as Routing Information Protocol an it is a Distance Vector because it uses hop count to determine the best path to remote network. It has two version 1 (Classful) and version 2 (Classless).

122. What is administrative distance of RIP ?

Administrative distance of RIP is 120

123. Which metric is used by RIP ?

Only Hop Count metric is used by RIP.

124. What is the limit of hop count in RIP ?

Limit of hop count in RIP is 15, mean if anything require 16 hop is deemed unreachable.

125. How is RIP select the best path to the remote network ?

RIP only uses hop count to determine the best path to the remote network, route with lowest hop count will be prefer as best path to remote network. If RIP finds more than one link with the same hop count to the same remote network, it will automatically perform a Round-Robin load balancing. RIP can perform load balancing for up to 6 equal cost link and by default is 4.

126. Why RIP causes overhead in network?

Routers which are configured with RIP, periodically exchange all of its routing table information with others in every 30 seconds. So if assuming a scenario has 100 RIP networks in one router and there are 15 routers , so there would be 15 routers exchanging the information with each other even if its same info. Therefore, it causes overhead. If its RIPv1- then it will broadcast so every other router will hear the info. For RIPv2 its multicast.

127. Which transport layer protocol used by RIP ?

RIP use UDP (User Datagram Protocol) as one of its Transport protocol, and assigned the reserved port number 520.

128. Which algorithm used by RIP ?

RIP uses Bellman Ford algorithm.

129. Why RIP is inefficient on large network ?

RIP is inefficient on large networks with slow wan link or on network with large number of router installed.

130. Explain RIP process.

In a RIP network, each router broadcast its entire RIP table to its neighboring routers every 30 second. When a router receives a neighbor's RIP table, it uses the information provided to update its own routing table and then sends the updated table to its neighbors.

131. Explain load balancing in RIP.

If RIP finds more than one link with the same hop count to the same remote network, it will automatically perform a Round-Robin load balancing. RIP can perform load balancing for up to 6 equal cost link (By default is 4).

132. What is the range of load balancing in RIP ?

Range of load balancing in RIP is 4 by default, but RIP can perform load balancing for up to 6 equal cost link.

133. What is differences between RIPv1 and RIPv2 ?

RIPv1 (Routing Information Protocol Version 1)

- It is Distance Vector Protocol.
- Interior Gateway Protocol.
- Maximum hop count limit is 15
- It is classful
- Broadcast Based
- Does not support VLSM (Variable Length Subnet Masking).
- There is no authentication.
- Does not support for Discontiguous Network
- Hello/Dead time - 30/180
- Broadcast based - RIPv1 sends routing update periodically every 30second as broadcast using destination IP address as limited broadcast IP address 255.255.255.255. Since the updates are sent using the destination IP address of limited broadcast IP address

255.255.255.255, every router need to process the routing update message (Whether they are running RIPv1 or not)

RIPv2 (Routing Information Protocol Version 2)

- It is Distance Vector Protocol.
- Interior Gateway Protocol.
- Maximum hop count limit is 15
- It is classless
- Use multicast 224.0.0.9
- Support VLSM (Variable Length Subnet Masking).
- Allow for MD5 authentication.
- Support for Discontiguous Network
- Hello/Dead time - 30/180
- RIPv2 routing updates are sent as multicast traffic at destination multicast address of 224.0.0.9. Multicast updates reduces the network traffic. The multicast routing updates also helps in reducing routing update message processing overhead in routers which are not running RIPv2. Only the routers running RIPv2 join to the multicast group 224.0.0.9. Other routers which are not running RIPv2 can simply filter the routing update packet at layer 2

134. What is pinhole congestion ?

When two routes for the same destination have the same hop count in the RIP, this situation is known as Pinhole Congestion.

135. What is passive interface in RIP ?

This command prevents RIP update broadcasts from being sent out a specified interface, yet that same interface can still receive RIP updates. Thus a RIP router with a passive interface will still learn about the network advertise by other router.

136. How to configure passive interface in RIP on particular interface ?

Router#config t
Router(config)#router rip

```
Router(config-router)#network 192.168.20.0
Router(config-router)#passive-interface serial 0/0
```

137. How to configure passive interface in RIP on all interface ?

We can configure all interfaces by using "passive-interface default" command and then individually ues the "no passive-interface" command on the interfaces we want updates to be sent out

```
Router#config t
Router(config)#router rip
Router(config-router)#network 192.168.20.0
Router(config-router)#network 192.168.30.0
Router(config-router)#passive-interface default
Router(config-router)#no passive-interface F0/0
```

138. How to configure passive interface in RIP when we used the neighbor command under the RIP process ?

If you used the neighbor command under the RIP process, the router will send unicast updates as well as multicast updates. The passive interface command must be used disable Multicast/broadcast updates and allowing only unicast.

```
Router#config t

Router(config)#router rip

Router(config-router)#passive-interface S0/0/0

Router(config-router)#passive-interface S0/1/0

Router(config-router)#neighbor 192.168.20.1

Router(config-router)#neighbor 192.168.30.1
```

139. Explain RIP timers ?

RIP uses four different type of timers-

Route update timer (30 Second)

- Sets the interval (typically 30 seconds) between periodic routing updates in which the router sends a complete copy of its routing table out to all neighbors.

Route invalid timer (180 Second)

- Determines the length of time that must elapse (180 seconds) before a router determines that a route has become invalid.If it hasn't heard any updates about a particular route for that period.
- When that happens, the router will send out updates to all its neighbors letting them know that the route is invalid.

Hold-down timer (180 Second)

- This sets the amount of time during which routing information is suppressed.
- Routes will enter into the holddown state
- when an update packet is received that indicates the route is unreachable.
- This continues either until an update packet is received with a better metric, the original route comes back up, or the holddown timer expires.
- The default is 180 seconds.

Route flush timer (240 Second)

- Sets the time between a route becoming invalid and its removal from the routing table (240 seconds).
- Before it's removed from the table, the router notifies its neighbors of that route's impending demise.
- The value of the route invalid timer must be less than that of the route flush timer.
- This gives the router enough time to tell its neighbors about the invalid route before the local routing table is updated.

140. How to configure RIPv1 ?

Router#config t

Router(config)#router rip

Router(config-router)#network 10.0.0.0

141. How to configure RIPv2 ?

Router(config)#router rip

Router(config-router)#network 10.0.0.0

Router(config-router)#version 2

142. Can we use RIP in inter-network having more than 15 routers ?

Yes, If connected with Broadcast Multi Access Network. In BMA (Broadcast Multi Access) more than two router connected via switch within a same network**.**

143. What is difference between RIP and RIPng ?

RIP is for IPv4 and RIPng for IPv6.

144. What is multicast address of RIPv2 ?

Multicast Address of RIPv2 is 224.0.0.9

145. How do you stop RIP updates from propagating out an interface on a router ?

Holding Down RIP Propagations

There are a few different ways to stop unwanted RIP updates from propagating across your LANs and WANs, and the easiest one is through the passive-interface command. This command prevents RIP update broadcasts from being sent out a specified interface, yet that same interface can still receive RIP updates.

Here's an example of how to configure a passive-interface on a router using the CLI:

Router#config t

Router(config)#router rip

Router(config-router)#network 192.168.20.0

Router(config-router)#passive-interface serial 0/0

This command will stop RIP updates from being propagated out serial interface 0/0, but serial interface 0/0 can still receive RIP updates.

146. If a RIPv2 router advertise it's route, would it be received by all the devices on the network ?

Rip v2 is multicast. So the route advertisement would be received only by devices which has Rip v2 enabled. If the advertisement was Rip v1, then it would be received by all devices on the network as Rip v1 is broadcast.

147. How can a Rip route advertisement be blocked on a specific interface ?

By using the passive interface command.

148. If a static route and a RIP learned route are available on a router which entry would be chosen by the router to forward the packet ?

Static route would be chosen since it has lower administrative distance than Rip

149. Can a subnet mask information be stored in a RIPv1 packet ?

Rip v1 is a classfull routing protocol. It does not understand classless concepts like Subnets. So it is not possible

150. Is a subnet mask field available in a RIPv2 packet ?

Ripv2 is classless routing protocol. A ripv2 packet has a field to include the subnet mask information.

151. How can we manipulate metrics in RIP ?

We can manipulate metrics in RIP through the Offset-Lists.

152. What is Offset-List ?

- An offset list is the process of Traffic Engineering.
- This technique used for increasing incoming and outgoing metrics to routes learned via EIGRP or RIP.
- The offset value is added to the routing metric.
- An offset list that specifies an interface type and interface number is considered to be an extended list and takes precedence over an offset list that is not extended.
- Therefore, if an entry passes the extended offset list and a normal offset list, the offset of the extended offset list is added to the metric.
- An Offset List Can Be Used to Prefer a Faster Path.

153. Can we use Offset-list in Link State Routing Protocols ?

No, Offset lists are only used with distance vector routing protocols.

154. How to configure Offset-List ?

To configure an offset to incoming and outgoing metrics to routes learned via EIGRP or RIP, use **the offset-list {access-list-number | access-list-name} {in | out} offset [interface-type interface-number]**

Access-list-number | access-list-name ---Standard access list number or name to be applied. Access list number 0 indicates all access lists. If the offset value is 0, no action is taken.
in---Applies the access list to incoming metrics.

Out---Applies the access list to outgoing metrics.

offset---Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.

Interface-type interface-number---(Optional) Interface type and number to which the offset list is applied.

155. What is incoming metrics ?

- The incoming metric modifies the cost of an individual segment when a route across the segment is imported into the routing table.

- For example, if you set the incoming metric on the segment to 3, the individual segment cost along the link is changed from 1 to 3.
- The increased cost affects all route calculations through that link. Other routes that were previously excluded because of a high hop count might now be selected into the router's forwarding table.

156. What is outgoing metrics ?

- The outgoing metric modifies the path cost for all the routes advertised out a particular interface.
- Unlike the incoming metric, the outgoing metric modifies the routes that other routers are learning and thereby controls the way they send traffic.

157. What are limitations of RIP ?

- The hop count limit in RIP is 15, Without using RMTI, Hop count cannot exceed 15, in the case that it exceeds this limitation, it will be considered invalid or routes will be dropped.
- Most of RIP networks are flat. RIP has no any concept of areas or boundaries in RIP networks (but aggregation is possible).
- RIPv1 does not support VLSM (Variable Length Subnet Masking)
- RIP has slow convergence due to periodic routing update and count to infinity problems.

158. Explain loop avoidance mechanism in RIP.

Maximum Hop Count

- RIP permits a hop count of up to 15, so anything that requires 16 hops is deemed unreachable.
- In other words, after a loop of 15 hops, Network will be considered down.
- Thus, the maximum hop count will control how long it takes for a routing table entry to become invalid or questionable.

Split Horizon

- This reduces incorrect routing information and routing overhead in a distance vector network by enforcing the rule that routing information cannot be sent back in the direction from which it was received.

Route Poisoning

- When Network goes down, Router initiates route poisoning by advertising Network with a hop count of 16, or unreachable (sometimes referred to as infinite).

Hold-downs

- A hold-down prevents regular update messages from reinstating a route that is going up and down (called flapping). Typically, this happens on a serial link that's losing connectivity and then coming back up..

EIGRP Interview Questions & Answer

159. What is EIGRP?

Enhanced Interior Gateway Routing Protocol (EIGRP Protocol) is an enhanced distance vector routing protocol which Uses Diffused Update Algorithm (DUAL) to calculate the shortest path. It is also considered as a Hybrid Routing Protocol because it has characteristics of both Distance Vector and Link State Routing Protocols.

EIGRP supports classless routing and VLSM, route summarization, incremental updates, load balacing and other features.

160. What are the different tables in EIGRP?

EIGRP router stores routing and topology information in three tables:

1. Neighbor table - Stores information about EIGRP neighbors.

2. Topology table - Stores routing information which is learned from neighbor routers.

3. Routing table - Stores the best paths to all networks.

161. Why EIGRP is called hybrid protocol?

EIGRP is also called hybrid protocol because its metric is not just plain HOP COUNT (max-255, included in pure distance vector protocol) rather includes the links bandwidth, delay, reliability and Load parameter into the calculation. Thats why called Advanced or Hybrid protocol.

162.What are the different packets or message in EIGRP?

Ans-There are Six packets in EIGRP

1-Hello , 2-Update, 3-Query, 4-Reply, 5-Acknoladgment, 6.Request

EIGRP will use six different packet types when communicating with its neighboring EIGRP routers,

- **Hello Packets –** EIGRP sends Hello packets once it has been enabled on a router for a particular network. These messages are used to identify neighbors and once identified, serve or function as a keepalive mechanism between neighboring devices. EIGRP Hello packets are sent to the link local Multicast group address 224.0.0.10. Hello packets sent by EIGRP do not require an Acknowledgment to be sent confirming that they were received. Because they require no explicit acknowledgment, Hello packets are classified as unreliable EIGRP packets. EIGRP Hello packets have an **OPCode of 5.**

- **Update Packets** – EIGRP Update packets are used to convey reachability of destinations. Update packets contain EIGRP routing updates. When a new neighbor is discovered, Update packets are sent via Unicast to the neighbor which the can build up its EIGRP Topology Table. It is important to know that Update packets are always transmitted reliably and always require explicit acknowledgement. Update packets are assigned an **OPCode of 1.**

- **Query Packet** – EIGRP Query packets are Multicast and are used to reliably request routing information. EIGRP Query packets are sent to neighbors when a route is not available and the router needs to ask about the status of the route for fast convergence. If the router that sends out a Query does not receive a response from any of its neighbors, it resends the Query as a Unicast packet to the non-responsive neighbor(s). If no response is received in 16 attempts, the EIGRP neighbor relationship is reset. EIGRP Query packets are assigned an **OPCode of 3.**

- **Reply Packets** – EIGRP Reply packets are sent in response to Query packets. The Reply packets are used to reliably respond to a Query packet. Reply packets are Unicast to the originator of the Query. The EIGRP Reply packets are assigned an **OPCode of 4.**

- **Acknowledgement Packets** – An EIGRP Acknowledgment (ACK) packet is simply an EIGRP Hello packet that contains no data. Acknowledgement packets are used by EIGRP to confirm reliable delivery of EIGRP packets. ACKs are always sent to a Unicast address, which is the source address of the sender of the reliable packet, and not to the EIGRP Multicast group address. In addition, Acknowledgement packets will always contain a non-zero acknowledgment number. The ACK uses the same OPCode as the Hello Packet because it is essentially just a Hello that contains no information. **The OPCode is 5.**

- **Request Packets** – Request packets are used to get specific information from one or more neighbors and are used in route server applications. These packet types can be sent either via Multicast or Unicast, but are always transmitted unreliably.

- Refer the link for more info- https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html

163. Conditions for EIGRP neigbours.

Ans- 1. The routers must be able to send/receive IP packets to one another.

2-Interfaces' primary IP addresses must be in same subnet.

3-Must not be passive on the connected interface.

4-Must use the same ASN (EIGRP) in the router configuration command.

5-Must pass neighbor authentication (if configured).

6-K-values (used in metric calculation) must match

164. What is meant by active and passive states in EIGRP ?

Active State: Routes for which the successor route fails and no feasible successor routes exist moves to an active state forcing the EIGRP to send out query packets and reconverge.

Passive State: A route is in passive state for which the router has a successor route, and no failure has yet occurred. A stable EIGRP network will have all routes in a Passive state..

165. What are the different K-values used in EIGRP

- Bandwidth (K1=1)
- Load (K2=0)
- Delay (K3=1)
- Reliability (K4=0)
- Maximum Transmission Unit (K5=0)

By default, EIGRP only uses bandwidth (K1) and delay (K3) to calculate metric.

166.Does EIGRP require an ip default-network command to propagate a default route?

Although eigrp can propagate a default route using the default network method, it is not required. Eigrp redistributes default routes directly

167. Should I always use the EIGRP log-neighbor-changes command when I configure EIGRP?

Yes, this command makes it easy to determine why an EIGRP neighbor was reset. This Reduces troubleshooting time.

168. Does EIGRP support secondary addresses?

Ans- Yes, EIGRP supports secondary addresses. Since EIGRP always sources data packets from the primary address, Cisco recommends that you configure all routers on a particular subnet with primary addresses that belong to the same subnet. Routers do not form EIGRP neighbors over secondary networks.

169. What debugging capabilities does EIGRP have?

- show ip eigrp neighbors
- show ip eigrp interfaces
- show ip eigrp topology
- show ip eigrp traffic

170. What are the advantages of EIGRP other routing protocol ?

Ans- EIGRP is mix of distance vector and link state feature oriented routing protocol that uses DUAL for route calculation. It was Cisco proprietary but since it is been declared open source. It uses5 K values to calculate shortest path and is the only protocol that can provide unequal load balancing. Also provides encryption for security and can be used with iBGP for WAN routing.

171. What is Advertised distance ?

Ans- The Advertised Distance (AD) is the distance from a given neighbor to the destination router also known as **Reported Distance.**

172. What is successor ?

Ans- Successor is considered as the best path to distance from many paths.

173. What is the muticast address used by EIGRP to send Hello packets ?

Ans-224.0.0.10

174. What does stuck-in-active mean?

If a router does not receive a reply from a queried neighbor within the active time (3 minutes, by default), the route is declared stuck-in-active. A response with an infinite metric is entered on the neighbor's behalf to satisfy DUAL, and the neighbor is deleted from the neighbor table.

175.What is the feasibility condition?

The feasibility condition is the rule by which feasible successors are chosen for a destination. The feasibility condition is satisfied if a neighbor's advertised distance to a destination is lower than the current successors feasible distance to the destination.

176. What is Reliable Transport Protocol?

EIGRP uses RTP (Reliable Transport Protocol) to deliver EIGRP packets between neighbors in a reliable and ordered way. If the packet with RTP enable sent, gets lost in the transit it will be send again (resend).

177. What packets are RTP enabled?

1. Update Packet.

2.Query Packet.

3.Reply Packet.

178. Explain what will happen if the packet is not acknowledged?

If a packet is not acknowledged, EIGRP will retransmit the packet to the non responding neighbor as a unicast. No other traffic is sent to this neighbor until it responds. After 16 unacknowledged re-transmissions, the neighbor is removed from the neighbor table.

179.Explain EIGRP Router ID?

In EIGRP, duplicate RIDs do not prevent routers from becoming neighbors and two EIGRP routers with the same router ID will still form a neighbor relationship. The only time the value of EIGRP RIDs consider is when injecting external (redistributed) routes into EIGRP. In this case, the routers injecting the external routes should have unique RIDs to avoid confusion.

To manually configures the router ID

R1(config)# router eigrp 10

R1(config-router)# eigrp router-id 1.1.1.1

180.Explain Split Horizon?

The Split Horizon feature prevents a route learned on one interface from being advertised back out of that same interface. It is used to prevent loop in EIGRP.

181. Explain Null Zero?

It is a loop avoidance mechanism entry stored in routing table only in case of summarization (auto & manual). It terminates or flush unwanted packets, if any traffic goes towards null0 it will be drop by eigrp.

182. How Passive Interface command works in EIGRP?

With EIGRP running on a network, the passive-interface command stops sending outgoing hello packets, hence the router cannot form any neighbor relationship via the passive interface. This

behavior stops both outgoing and incoming routing updates. However, EIGRP still advertises the connected subnets if matched with an EIGRP network command.

router eigrp 1
passive-interface fastethernet0/0
Command to see list of passive-interfaces
show ip protocols

183. How can we change Hello and Hold time in EIGRP?

interface Fa0/0

ip hello-interval eigrp 100 3

ip hold-time eigrp 100 12

These commands will make hello interval 3 seconds and hold time 12 seconds.

show ip eigrp interfaces detail (To verify)

184. What types of Authentication is supported by EIGRP ?

Ans- 1. Null , 2.Plain text , 3. MD5

185. What is the use of "variance" Command in EIGRP?

EIGRP provides a mechanism to load balance over unequal cost paths throungh Variance Command. Variance is a number (1 to 128).

186. Internal and external Administrative distance in EIGRP ?

1.Internal - 90
2.External - 170
3.Summary – 5

187. Give the Formula EIGRP uses to calculate Metric?

((10^7/least bandwidth of link) + cumulative delay)*256

188. What is Feasible successor ?

A feasible successor to a destination is a neighbor that satisfies the feasibility condition for that destination.

189. What is Graceful Shutdown and GoodBye message in EIGRP?

When an EIGRP process is shut down, router sends out "goodbye" messages to its neighbors. The neighbors can then immediately begin recalculating paths to all the destinations that went through that shutdown router without having to wait for the hold timer to expire.

190.Maximum path load balanced by EIGRP ?

up to 32 equal-cost entries can be in the routing table for the same destination. The default is 4. We can also set the **maximum-path** to 1 disables load balancing.

Router(config)#router eigrp 100
Router(config-router)#maximum-paths 6
Set the maximum number of parallel routes that EIGRP will support to 6

191. How EIGRP support unequal load balancing ?

EIGRP also support unequal cost path load balancing. Use the variance n command in order to instruct the router to include routes with a metric of less than n times the minimum metric route for that destination. The variable n can take a value between 1 and 128.

192. What does the word serno mean on the end of an EIGRP topology entry when you issue the show ip eigrp topology command?

For example:

#show ip eigrp topology
P 172.22.71.208/29, 2 successors, FD is 46163456
via 172.30.1.42 (46163456/45651456), Serial0.2, **serno** 7539273
via 172.30.2.49 (46163456/45651456), Serial2.6, **serno** 7539266

Ans- Serno stands for serial number. When DRDBs are threaded to be sent, they are assigned a serial number. If you display the topology table at the time an entry is threaded, it shows you the serial number associated with the DRDB.

Threading is the technique used inside the router to queue items up for transmission to neighbors. The updates are not created until it is time for them to go out the interface. Before that, a linked list of pointers to items to send is created (for example, the thread).

These sernos are local to the router and are not passed with the routing update.

193.What percent of bandwidth and processor resources does eigrp use?

Eigrp version 1 introduced a feature that prevents any single eigrp process from using more than fifty percent of the configured bandwidth on any link during periods of network convergence. Each as or protocol (for instance, ip, ipx, or appletalk) serviced by eigrp is a separate process. You can use the ip bandwidth-percent eigrp interface configuration command in order to properly configure the bandwidth percentage on each wan interface. Refer to the eigrp white paper for more information on how this feature works.

In addition, the implementation of partial and incremental updates means that eigrp sends routing information only when a topology change occurs. This feature significantly reduces bandwidth use.

The feasible successor feature of eigrp reduces the amount of processor resources used by an autonomous system (as). It requires only the routers affected by a topology change to perform route re-computation. The route re-computation only occurs for routes that were affected, which reduces search time in complex data structures.

194. Does eigrp support aggregation and variable length subnet masks?

Yes, eigrp supports aggregation and variable length subnet masks (vlsm). Unlike open shortest path first (ospf), eigrp allows summarization and aggregation at any point in the network. Eigrp supports aggregation to any bit. This allows properly designed eigrp networks to scale exceptionally well without the use of areas. Eigrp also supports automatic summarization of network addresses at major network borders.

195. Can i configure more than one eigrp autonomous system on the same router?

Yes, you can configure more than one eigrp autonomous system on the same router. This is typically done at a redistribution point where two eigrp autonomous systems are interconnected. Individual router interfaces should only be included within a single eigrp autonomous system.

Cisco does not recommend running multiple eigrp autonomous systems on the same set of interfaces on the router. If multiple eigrp autonomous systems are used with multiple points of mutual redistribution, it can cause discrepancies in the eigrp topology table if correct filtering is not performed at the redistribution points. If possible, cisco recommends you configure only one eigrp autonomous system in any single autonomous system. You can also use another protocol, such as border gateway protocol (bgp), in order to connect the two eigrp autonomous systems.

196. If there are two eigrp processes that run and two equal paths are learned, one by each eigrp process, do both routes get installed?

No, only one route is installed. The router installs the route that was learned through the eigrp process with the lower autonomous system (as) number. In cisco ios software releases earlier than 12.2(7)t, the router installed the path with the latest timestamp received from either of the eigrp processes. The change in behavior is tracked by cisco bug id cscdm47037.

197. When i configure eigrp, how can i configure a network statement with a mask?

The optional network-mask argument was first added to the network statement in cisco ios software release 12.0(4)t. The mask argument can be configured in any format (such as in a network mask or in wild card bits). For example, you can use network 10.10.10.0 255.255.255.252 or network 10.10.10.0 0.0.0.3.

198. What is "goodbye" message received in eigrp?

Goodbye message-

The goodbye message is a feature designed to improve eigrp network convergence. The goodbye message is broadcast when an eigrp routing process is shut down to inform adjacent peers about the impending topology change. This feature allows supporting eigrp peers to synchronize and recalculate neighbor relationships more efficiently than would occur if the peers discovered the topology change after the hold timer expired.

The following message is displayed by routers that run a supported release when a goodbye message is received: **Apr 26 13:48:42.523: %dual-5-nbrchange: ip-eigrp(0) 1: neighbor 10.1.1.1 (ethernet0/0) is down: interface goodbye received**

A cisco router that runs a software release that does not support the goodbye message can misinterpret the message as a k-value mismatch and display the following message:-

Apr 26 13:48:41.811: %dual-5-nbrchange: ip-eigrp(0) 1: neighbor 10.1.1.1 (ethernet0/0) is down: k-value mismatch Obviously, the signalling to a neighbor that a protocol has been gracefully shutdown means good things for protocol convergence and loop prevention in a distance vector protocol. The point that i think is important is that a network that has some ios 15.1m and more mainstream sofware might see error messages about k-value mismatch and think that something is broken. In this case, the error message is exactly correct, and can be safely ignored.

As always, it depends™ on your exact configuration, its possible that someone has actually configured k-values (but it's unlikely these days) and the message is telling you.

199. Who does load-balancing when there are multiple links to a destination?

Load balancing is a standard functionality of the cisco ios® router software, and is available across all router platforms. It is inherent to the forwarding process in the router and is automatically activated if the routing table has multiple paths to a destination. It is based on standard routing protocols, such as routing information protocol (rip), ripv2, enhanced interior gateway routing protocol (eigrp), open shortest path first (ospf), and interior gateway routing protocol (igrp), or

derived from statically configured routes and packet forwarding mechanisms. It allows a router to use multiple paths to a destination when forwarding packets.

200. How can i use only one path when a router has two equal cost paths?

Configure the bandwidth value on the interfaces to default, and increase the delay on the backup interface so that the router does not see two equal cost paths.

Or you can also limit Max-path to 1 for load balancing.

201. What is the difference in metric calculation between eigrp and igrp?

Eigrp has totally replaced the obsolete igrp

2. Eigrp is a classless routing protocol while igrp is a classful routing protocol

3. Eigrp uses the dual while igrp does not

4. Eigrp consumes much less bandwidth compared to igrp

5. Eigrp expresses the metric as a 32 bit value while igrp uses a 24 bit value

202. What is the eigrp stub routing feature?

The enhanced interior gateway routing protocol (eigrp) stub routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration. Stub routing is commonly used in a hub and spoke network topology.

203. How can i send a default route to the stub router from the hub?

Do this under the outbound interface on the hub router with the ip summary-address eigrp x 0.0.0.0 0.0.0.0command. This command suppresses all the more specific routes and only sends the summary route. In the case of the 0.0.0.0 0.0.0.0, it means it suppresses everything, and the only route that is in the outbound update is 0.0.0.0/0. One drawback to this method is that eigrp installs a 0.0.0.0/0 route to null0 is the local routing table with an admin distance of 5.

204. What are different route types in eigrp?

Internal route—routes that are originated within the autonomous system (as).

Summary route—routes that are summarized in the router (for example, internal paths that have been summarized).

External route—routes that are redistributed to eigrp.

205. What is an offset-list, and how is it useful?

The offset-list is an feature used to modify the composite metrics in eigrp. The value configured in the offset-list command is added to the delay value calculated by the router for the route matched by an access-list. An offset-list is the preferred method to influence a particular path that is advertised and/or chosen.

206. What does the neighbor statement in the eigrp configuration section do?

The neighbor command is used in eigrp in order to define a neighboring router with which to exchange routing information. Due to the current behavior of this command, eigrp exchanges routing information with the neighbors in the form of unicast packets whenever the neighbor command is configured for an interface.

207. Why does the eigrp passive-interface command remove all neighbors for an interface?

The passive-interface command disables the transmission and receipt of eigrp hello packets on an interface. Unlike igrp or rip, eigrp sends hello packets in order to form and sustain neighbor adjacencies. Without a neighbor adjacency, eigrp cannot exchange routes with a neighbor. Therefore, the passive-interface command prevents the exchange of routes on the interface. Although eigrp does not send or receive routing updates on an interface configured with the passive-interface command, it still includes the address of the interface in routing updates sent out of other non-passive interfaces.

208. Why are routes received from one neighbor on a point-to-multipoint interface that runs eigrp not propagated to another neighbor on the same point-to-multipoint interface?

The split horizon rule prohibits a router from advertising a route through an interface that the router itself uses to reach the destination. In order to disable the split horizon behavior, use the no ip split-horizon eigrp as-numberinterface command. Some important points to remember about eigrp split horizon are:

Split horizon behavior is turned on by default.

When you change the eigrp split horizon setting on an interface, it resets all adjacencies with eigrp neighbors reachable over that interface.

Split horizon should only be disabled on a hub site in a hub-and-spoke network.

Disabling split horizon on the spokes radically increases eigrp memory consumption on the hub router, as well as the amount of traffic generated on the spoke routers.

The eigrp split horizon behavior is not controlled or influenced by the ip split-horizon command.

209. What are the primary functions of the pdm?

Eigrp supports 3 protocol suites: ip, ipv6, and ipx. Each of them has its own pdm. These are the primary functions of pdm:

Maintaining the neighbor and topology tables of eigrp routers that belong to that protocol suite Building and translating protocol specific packets for dual Interfacing dual to the protocol specific routing table Computing the metric and passing this information to dual; dual handles only the picking of the feasible successors (fss) Implement filtering and access lists.

Perform redistribution functions to/from other routing protocols.

210. What are the various load-balancing options available in eigrp?

The offset-list can be used to modify the metrics of routes that eigrp learns through a particular interface, or pbr can be used.

211. What does the %dual-5-nbrchange: ip-eigrp(0) 100: neighbor 10.254.0.3 (tunnel0) is down: holding time expired error message mean?

This message indicates that the router has not heard any eigrp packets from the neighbor within the hold-time limit. Because this is a packet-loss issue, check for a layer 2 problem.

212. From the 16:29:14.262 poison squashed: 10.x.x.x/24 reverse message, what does poison squashed mean?

The router threads a topology table entry as a poison in reply to an update received (the router sets up for poison reverse). While the router is building the packet that contains the poison reverse, the router realizes that it does not need to send it. For example, if the router receives a query for the route from the neighbor, it is currently threaded to poison. Thus, it sends the poison squashed message.

OSPF Interview Questions & Answers

213. What is OSPF Routing Protocol?

Open shortest path first is an Open Standard Link State routing protocol which works by using Dijkastra algorithm to initially construct the shortest paths and follows that by populating the routing table with resulting best paths.

214. What are the steps required to change Neighborship into adjacency?

1.Two-way communication (using Hello Protocol).

2.Database Synchronization which means exchange of Database Description (DD) packets, Link State Request (LSR) packets, Link State Update (LSU) packets.

After Database synchronization is complete, the two routers are considered adjacent.

215. Explain LSA (Link-State Advertisement), LSU (Link State Update) and LSR (Link State Request)?

The LSAs (Link-State Advertisements) are used by OSPF routers to exchange routing and topology information. When two neighbors decide to exchange routes, they send each other a list of all LSAs in their respective topology database. Each router then checks its topology database and sends Link State Request (LSR) message requesting all LSAs that was not found in its topology table. Other router responds with the Link State Update (LSU) that contains all LSAs requested by the neighbor.

216. Explain OSPF Router ID?

Router Id is used to identify the Router. Highest IP address of the router's loopback interfaces is chosen as the Router ID, If no loopback is present than highest IP address of the router's physical interfaces will be chosen as Router ID. OSPF prevents neighborships between routers with duplicate RIDs. All OSPF RIDs in a domain should be unique. OSPF Router ID should not be changed after the OSPF process is started and the OSPF neighborships are established. If you change the OSPF router ID, we need to either reload the IOS or use "clear ip ospf process" command (restart the OSPF process) for changed RID to take effect.

To manually configure the router ID

R1(config)# router ospf 5

R1(config-router)# router-id 5.5.5.5

217. Can we use OSPF without backbone area?

Yes, but than only intra-area communication is possible. Inter-area communication is not possible without backbone area.

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

LSAs are exchanged only among adjacent routers not among neighbor routers.

219. What are different neighbour states in OSPF ?

OSPF routers need to go through several state before establishing a neighbor relationship -

1. Down - No Hello packets have been received on the interface.

2. Attempt - In Attempt state neighbors must be configured manually. It applies only to non-broadcast multi-access (NBMA) networks.

3. Init - Router has received a Hello message from the other OSFP router.

4. 2way - the neighbor has received the Hello message and replied with a Hello message of his own. Bidirectional Communication has been established. In Broadcast network DR-BDR election can occur after this point.

5. Exstart - DR & BDR establish adjacencies with each router in the network. Master-slave election will takes place (Master will send its DBD first).

6. Exchange - Routing information is exchanged using DBD (Database Descriptor) packets, Link-State Request (LSR) and Link-State Update packets may also be sent.

7. Loading - LSRs (Link State Requests) are send to neighbors for every network it doesn't know about. The Neighbor replies with the LSUs (Link State Updates) which contain information about requested networks. After all the requested information have been received, other neighbor goes through the same process.

8. Full - All neighbor routers have the synchronized database and adjacencies has been established.

220. What is an LSA? How does an LSA differ from an OSPF Update packet?

A router originates a link state advertisement to describe one or more destinations. An OSPF Update packet transports LSAs from one neighbor to another. Although LSAs are flooded throughout an area or OSPF domain, Update packets never leave a data link.

221. Explain different OSPF LSA Types?

1. **Router LSA (Type1)** - Each router geLSA Types?nerates a Type 1 LSA that lists its active interfaces, IP addresses, neighbors and the cost. LSA Type 1 is flooded only within an area.

2. **Network LSA (Type2)** - Type2 LSA is sent out by the designated router (DR) and lists all the routers on the segment it is adjacent to. Type 2 LSA are flooded only within an area.

3. **Summary LSA (Type3) -** Type 3 LSAs are generated by Area Border Routers (ABRs) to advertise networks from one area to the rest of the areas in Autonomous System.

4. **Summary ASBR LSA (Type4) -** Generated by the ABR. It contain routes to ASBRs.

5. **External LSA (Type5)** - External LSAs are generated by ASBRs and contain routes to networks that are external to the current Autonomous System.

6. **Not-So-Stubby Area LSA (Type7)** - Stub areas do not allow Type 5 LSAs. A Not So Stubby Area (NSSA) allows advertisement of Type 5 LSA as Type 7 LSAs. Type LSA is generated by an ASBR inside a Not So Stubby Area (NSSA) to describe routes redistributed into the NSSA.

222. Can I use the distribute-list in/out command with OSPF to filter routes?

The **distribute-list** commands are supported in OSPF but work differently than distance-vector routing protocols such as Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP).

OSPF routes cannot be filtered from entering the OSPF database. **The distribute-list in** command only filters routes from entering the routing table; it does not prevent link-state packets from being propagated. Therefore, this command does not help conserve router memory, and it does not prohibit a router from propagating filtered routes to other routers.

Caution: Use of the **distribute-list in** command in OSPF may lead to routing loops in the network if not implemented carefully.

The **command distribute-list out** works only on the routes being redistributed by the Autonomous System Boundary Routers (ASBRs) into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and inter-area routes.

Refer to configuration example of distribute-list in OSPF,

223. How can I give preference to OSPF inter-area routes over intra-area routes?

According to section 11 of RFC 2328 Description: learingcisco.com, the order of preference for OSPF routes is:

intra-area routes, O

interarea routes, O IA

external routes type 1, O E1

external routes type 2, O E2

This rule of preference cannot be changed. However, it applies only within a single OSPF process. If a router is running more than one OSPF process, route comparison occurs. With route comparison, the metrics and administrative distances (if they have been changed) of the OSPF processes are compared. Route types are disregarded when routes supplied by two different OSPF processes are compared.

224. Do I need to manually set up adjacencies for routers on the Switched Multimegabit Data Service (SMDS) cloud with the OSPF neighbor subcommand?

In Cisco IOS Software releases earlier than Cisco IOS Software Release 10.0, the neighbor command was required to establish adjacencies over nonbroadcast multiaccess (NBMA) networks (such as Frame Relay, X.25, and SMDS). With Cisco IOS Software Release 10.0 and later, you can use the ip ospf network broadcast command to define the network as a broadcast network, eliminating the need for the neighbor command. If you are not using a fully meshed SMDS cloud, you must use the ip ospf network point-to-multipoint command.

225. When routes are redistributed between OSPF processes, are all shortest path first algorithm (SPF) metrics preserved, or is the default metric value used?

The SPF metrics are preserved. The redistribution between them is like redistribution between any two IP routing processes.

226. How does Cisco accommodate OSPF routing on partial-mesh Frame Relay networks?

You can configure OSPF to understand whether it should attempt to use multicast facilities on a multi-access interface. Also, if multicast is available, OSPF uses it for its normal multicasts.

Cisco IOS Software Release 10.0 includes a feature called subinterfaces. You can use subinterfaces with Frame Relay to tie together a set of virtual circuits (VCs) to form a virtual interface, which acts as a single IP subnet. All systems within the subnet should be fully meshed. With Cisco IOS Software Releases 10.3, 11.0 and later, the ip ospf point-to-multipoint command is also available.

227. Which address-wild-mask pair should I use for assigning an unnumbered interface to an area?

When an unnumbered interface is configured, it references another interface on the router. When enabling OSPF on the unnumbered interface, use the address-wild-mask pair of interfaces to which the unnumbered interface is pointing.

228. Can I have one numbered side and leave the other side unnumbered in OSPF?

No, OSPF does not work if you have one side numbered and the other side unnumbered. This creates a discrepancy in the OSPF database that prevents routes from being installed in the routing table.

229. Why do I receive the "cannot allocate router id" error message when I configure Router OSPF One?

OSPF picks up the highest IP address as a router ID. If there are no interfaces in up/up mode with an IP address, it returns this error message. To correct the problem, configure a loopback interface.

230. Why do I receive the "unknown routing protocol" error message when I configure Router OSPF One?

Your software may not support OSPF. This error message occurs most frequently with the Cisco 1600 series routers. If you are using a 1600 router, you need a Plus image to run OSPF.

231. What do the states DR, BDR, and DROTHER mean in show ip ospf interface command output?

DR means designated router. BDR means backup designated router. DROTHER indicates a router that is neither the DR or the BDR. The DR generates a Network Link-State Advertisement, which lists all the routers on that network.

232. Why master slave needs to be elected between two neighbour interface?

Master sends its DBD (Database Description) First.

233. What is the requirement of doing summarization?

1. Reduces the amount of information stored in routing tables.

2. Allocates an existing pool of addresses more economically.

3. Lessens the load on router processor and memory resources.

4. Less number of update messages.

5. Less bandwidth.

234. How routes are selected in OSPF according to preference?

Intra-Area routes(0)> Inter-Area routes(0-IA)> External-Type-1(E1)> External-Type-2(E2)> NSSA-1(N1)> NSSA-2(N2).

235. What is Route Redistribution?

Route redistribution is the process of taking routes learned via one routing protocol and injecting those routes into another routing protocol domain.

For example two companies might merge, one company is using Enhanced Interior Gateway Routing Protocol (EIGRP) and the other is using Open Shortest Path First (OSPF). Route redistribution allows exchanging of routes between the two routing domains with a minimal amount of configuration and with little disruption to the existing networks.

236. Why are loopbacks advertised as /32 host routes in OSPF?

Loopbacks are considered host routes in OSPF, and they are advertised as /32. For more information, refer to section 9.1 of RFC 2328 Description: leavingcisco.com. In Cisco IOS Software Releases 11.3T and 12.0, if the ip ospf network point-to-point command is configured under loopbacks, OSPF advertises the loopback subnet as the actual subnet configured on loopbacks. ISDN dialer interface advertises /32 subnet instead of its configured subnet mask. This is an expected behavior if ip ospf network point-to-multipoint is configured.

For example, consider two routers (R1 and R2) connected via FastEthernet interface. R1 has the loopback configured with the ip ospf network point-to-point command and advertises the loopback in OSPF.

interface Loopback0

ip address 1.1.1.1 255.255.255.0

ip ospf network point-to-point

When checked in router R2 with the show ip route ospf command, the route 1.1.1.1 is seen as:

!..output truncated

1.0.0.0/24 is subnetted, 1 subnets

O 1.1.1.0 [110/11] via 10.1.1.1, 00:00:02, FastEthernet0/0

However, when the ip ospf network point-to-point command is removed from R1 to 0 interface, the route 1.1.1.1 on R2 is seen as:

1.0.0.0/32 is subnetted, 1 subnets

O 1.1.1.1 [110/11] via 10.1.1.1, 00:00:01, FastEthernet0/0

237. What is the default redistribution OSPF cost ?

Redistribution into OSPF uses the following defaults:-

1. When taking from BGP, use a default metric of 1.

2. When taking from another OSPF process, take the source route's metric.

3. When taking from all other sources, use a default metric of 20.

238. What is the difference between Type-1 (E1) & Type-2 (E2) redistribution?

Type-2 is the default route type for routes learned via redistribution. The key with E2 routes is that the cost of these routes reflects only the redistributed cost. E2 = only redistributed cost.

Type-1 redistributed routes reflects cost to reach ASBR + redistributed cost. E1 = cost to reach ASBR + redistributed cost

239. Explain OSPF Virtual Link?

OSPF requires the use of a backbone area (area 0) with each area connecting to area 0 through an ABR. However in some cases, regular area might not have a convenient point of connection to the backbone area. In this case, OSPF uses virtual link to connect that regular area to backbone area virtually. An OSPF virtual link allows two ABRs that connect to the same non-backbone area to form a neighbor relationship through that non-backbone area, even when separated by many other routers and subnets. This virtual link acts like a virtual point-to-point connection between the two routers, with that link inside area 0. The routers form a neighbor relationship, inside area 0, and flood LSAs over that link.

240. Explain OSPF Stub Area and different types of Stub Areas?

Stub Area Sometimes we need to control the advertisement of external routes into an area. This area is called Stub area. Stub areas are not capable of importing routes external to ospf.Type 4 & Type 5 LSA are filtered from Stub areas and a default route is injected into that area by ABR in place of external routes.

To make area stub we have to give **# area 1 stub** command on all routers of that area.

Three restrictions apply to OSPF stub areas

1.No virtual links are allowed in stub area.

2.Stub area cannot be a backbone area.

3.No Autonomous System Boundary Routers are allowed.

Totally Stubby Area

Like stub areas, totally stubby areas do not receive type 4 or 5 LSAs from their ABRs. However, they also do not receive type 3 LSAs. It only allows advertisement of internal routes in that area.

To make area totally stubby area we have to give **# area 1 stub no-summary** command on ABR.

Not-So-Stubby Areas

The motivation behind NSSA is to allow OSPF stub areas to carry external routes. External routes are imported into OSPF NSSA as Type 7 LSA by ASBR. Type 7 LSA cannot go into area 0 so it is converted back into Type 5 LSA by ABR and injected into area 0.

To make area Not-So-Stubby Area we have to give **# area 1 NSSA** command on all routers of that area.

Totally NSSA

Along with Type 4 & Type 5 LSA, Type 3 LSA will also be filtered in Totally NSSA.

To make area Totally Not-So-Stubby Area we have to give **# area 1 nssa no-summary** command on ABR of that area.

Lsa information area vise

241. How do I change the reference bandwidth in OSPF?

We can change the reference bandwidth using the ospf auto-cost reference-bandwidth command under router ospf. By default, reference bandwidth is 100 Mbps.

242. How does OSPF calculate its metric or cost?

OSPF uses Cost as its metric. The formula to calculate the OSPF cost is reference bandwidth divided by interface bandwidth. For example, in the case of Ethernet, it is 100 Mbps / 10 Mbps = 10.

If # ip ospf cost _ command is used on the interface, it overrides this formulated cost.

243. What algorithm is used by OSPF if equal cost routes exist?

If equal cost routes exist, OSPF uses CEF load balancing. For more information, refer to Troubleshooting Load Balancing Over Parallel Links Using Cisco Express Forwarding.

244. Explain OSPF Authentication?

These are the three different types of authentication supported by OSPF to secure routing updates.

1.**Null Authentication -** also called Type 0. It means no authentication information is included in the packet header. It is the default.

2.**Plain Text Authentication -** also called Type 1. It uses simple clear-text passwords.

3.**MD5 Authentication -** also called Type 2. It uses MD5 cryptographic passwords.

Plain Text Authentication

Step1 - To configure plain text authentication, first we have to enable authentication. Authentication can be enabled either under area or for specific interface.

To enable authentication for area

Router(config)# router ospf 100

Router(config-router)# network 192.168.1.0 0.0.0.255 area 0

Router(config-router)# area 0 authentication

This will enable authentication for all the interfaces of the router in area 0.

OR

If we dont want to enable authentication for an area, we can enable it for the specific interface. This is useful if different interfaces that belong to the same area need to use different authentication methods..

Router(config)# interface fa0/1

Router(config-if)# ip ospf authentication

Step2 - Next, We have to configure authentication key on the interface

Router(config)# interface fa0/1

Router(config-if)# ip ospf authentication-key Cisco123

Here Cisco123 is the password value.

MD5 Authentication

Step1 - To configure MD5 authentication, first we have to enable authentication.

Router(config)# router ospf 1

Router(config-router)# network 192.168.1.0 0.0.0.255 area 0

Router(config-router)# area 0 authentication message-digest

OR

Router(config)# interface fa0/1

Router(config-router)# ip ospf authentication message-digest

Step2 - Next, We have to configure authentication key on the interface

Router(config)# interface fa0/1

Router(config-router)# ip ospf message-digest-key 10 md5 Cisco123

Here Cisco123 is the password value and 10 is the Key ID (number). It doesn't matter which key ID you choose but it has to be the same on both ends.

Authentication passwords do not have to be the same throughout an area. However, they must be same between neighbors.

245. How do I change the reference bandwidth in OSPF?

You can change the reference bandwidth in Cisco IOS Software Release 11.2 and later using the ospf auto-cost reference-bandwidth command under router ospf. By default, reference bandwidth is 100 Mbps. The ospf link-cost is a 16-bit number. Therefore, the maximum value supported is 65,535.

246. How does OSPF calculate its metric or cost?

OSPF uses a reference bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is reference bandwidth divided by interface bandwidth. For example, in the case of Ethernet, it is 100 Mbps / 10 Mbps = 10.

Note: If ip ospf cost cost is used on the interface, it overrides this formulated cost. For more information, refer to OSPF Cost.

Which command enables OSPF for IPv6 on a router?

ipv6 router ospf process-id

247. What is the link-state retransmit interval, and what is the command to set it?

OSPF must send acknowledgment of each newly received link-state advertisement (LSA). LSAs are retransmitted until they are acknowledged. The link-state retransmit interval defines the time between retransmissions. We can use the command ip ospf retransmit-interval to set the retransmit interval. The default value is 5 seconds.

248. When routes are redistributed between OSPF processes, are all shortest path first algorithm (SPF) metrics preserved or is the default metric value used?

The SPF metrics are preserved. The redistribution between them is like redistribution between any two IP routing processes.

249. How do I stop individual interfaces from developing adjacencies in an OSPF network?

To stop routers from becoming OSPF neighbors on a particular interface, issue the passive-interface command at the interface.

250. When I have two type 5 link-state advertisements (LSAs) for the same external network in the OSPF database, which path should be installed in the routing table?

When you have two type 5 LSAs for the same external network in the OSPF database, prefer the external LSA that has the shortest path to the Autonomous System Boundary Router (ASBR) and install that into the IP routing table. Use the show ip ospf border-routers command to check the cost to the ASBR.

251. Should I use the same process number while configuring OSPF on multiple routers within the same network?

OSPF, unlike Border Gateway Protocol (BGP) or Enhanced Interior Gateway Routing Protocol (EIGRP) does not check the process number (or autonomous system number) when adjacencies are formed between neighboring routers and routing information is exchanged.

Can we have OSPF run over a GRE tunnel?

Yes we can have OSPF run over a GRE tunnel.

252. What is an OSPF adjacency?

An OSPF adjacency is a conceptual link to a neighbor over which LSAs can be sent.

253. What are the five OSPF packet types? What is the purpose of each type?

The five OSPF packet types, and their purposes, are:

Hellos - which are used to discover neighbors, and to establish and maintain adjacencies

Updates - which are used to send LSAs between neighbors

Database Description packets - which a router uses to describe its link state database to a neighbor during database synchronization

Link State Requests - which a router uses to request one or more LSAs from a neighbor's link state database

Link State Acknowledgments - used to ensure reliable delivery of LSAs

254. What is a link state database? What is link state database synchronization?

The link state database is where a router stores all the OSPF LSAs it knows of, including its own. Database synchronization is the process of ensuring that all routers within an area have identical link state databases.

255. What is the default HelloInterval?

The default OSPF HelloInterval is 10 seconds.

256. What is the default Router Dead Interval?

The default Router DeadInterval is four times the HelloInterval.

257. What is a Router ID? How is a Router ID determined?

A Router ID is an address by which an OSPF router identifies itself. It is either the numerically highest IP address of all the router's loopback interfaces, or if no loopback interfaces are configured, it is the numerically highest IP address of all the router's LAN interfaces.

258. What is an area?

An area is an OSPF sub-domain, within which all routers have an identical link state database.

259. What is the significance of area 0?

Area 0 is the backbone area. All other areas must send their inter-area traffic through the backbone.

260. What is Max-Age?

MaxAge, 1 hour, is the age at which an LSA is considered to be obsolete.

261. Are OSPF routing protocol exchanges authenticated?

Yes, OSPF can authenticate all packets exchanged between neighbors. Authentication may be through simple passwords or through MD5 cryptographic checksums. To configure simple password authentication for an area, use the command ip ospf authentication-key to assign a password of up to eight octets to each interface attached to the area. Then, issue the area x authentication command to the OSPF router configuration to enable authentication. (In the command, x is the area number.)

Cisco IOS Software Release 12.x also supports the enabling of authentication on a per-interface basis. If you want to enable authentication on some interfaces only, or if you want different authentication methods on different interfaces that belong to the same area, use the ip ospf authenticationinterface mode command.

262. What is the link-state retransmit interval, and what is the command to set it?

OSPF must send acknowledgment of each newly received link-state advertisement (LSA). It does this by sending LSA packets. LSAs are retransmitted until they are acknowledged. The link-state retransmit interval defines the time between retransmissions. You can use the command ip ospf retransmit-interval to set the retransmit interval. The default value is 5 seconds.

263. What are the four OSPF router types?

The four OSPF router types are:

Internal Routers = whose OSPF interfaces all belong to the same area

Backbone Routers = which are Internal Routers in Area 0

Area Border Routers = which have OSPF interfaces in more than one area

Autonomous System Boundary Routers = which advertise external routes into the OSPF Domain

264. What are the four OSPF path types?

The four OSPF path types are:

Intra-area paths

Inter-area paths

Type 1 external paths

Type 2 external paths

265. What is the purpose of the subnets keyword when redistributing OSPF?

Without the Subnets keyword, only major network addresses that are not directly connected to the router will be redistributed.