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

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

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 ?

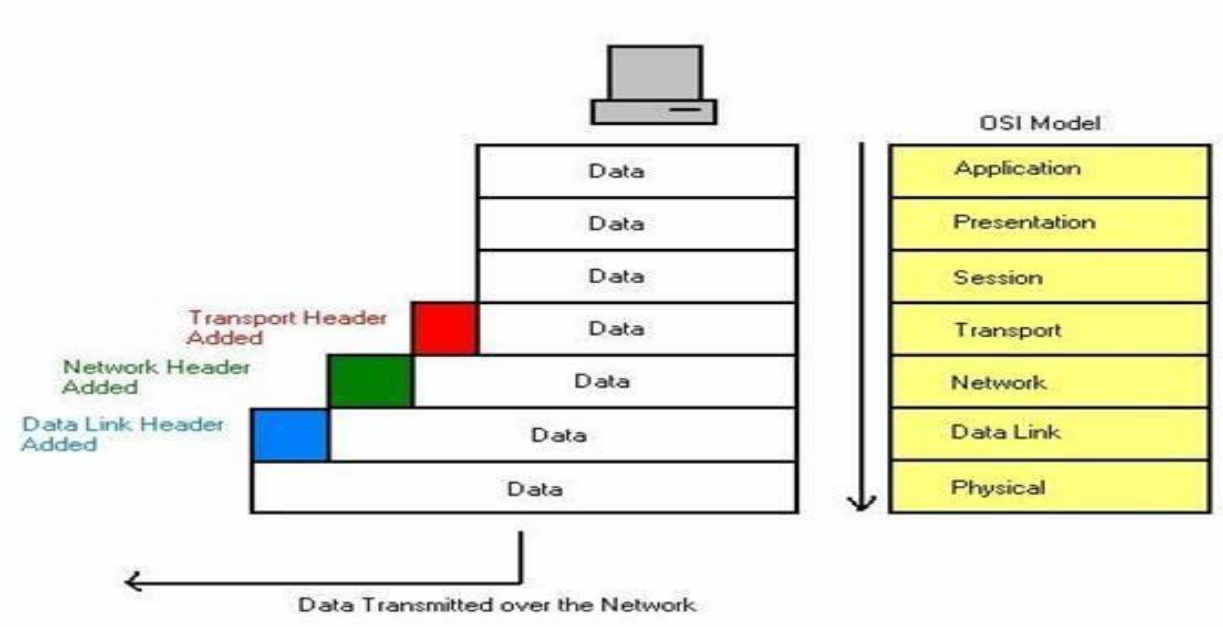
Data Link Layer

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.

266. What are the OSPF network types?

The four OSPF network types are:

- **Point-to-point networks**
- **Broadcast networks**
- **Non-broadcast**
- **Non-broadcast multi-access (NBMA) networks**

Point-to-multipoint networks configuration-

Note- To change network type we use "**Router(config-if)# ip ospf network point-to-multipoint** [non-broadcast]" command

267. What is a Designated Router?

A Designated Router is a router that represents a multiaccess network, and the routers connected to the network, to the rest of the OSFP domain.

268. How does a Cisco router calculate the outgoing cost of an interface?

Cisco IOS calculates the outgoing cost of an interface as 100/BW, where BW is the configured bandwidth of the interface.

269. What is the purpose of the variable IP-OSPF-Transmit-Delay?

This variable adds a specified time to the age field of an update. If the delay is not added before transmission over a link, the time in which the link-state advertisement (LSA) propagates over the link is not considered. The default value is 1 second. This parameter has more significance on very low-speed links.

270. What is a partitioned area?

An area is partitioned if one or more of its routers cannot send a packet to the area's other routers without sending the packet out of the area.

271. What is a virtual link?

A virtual link is a tunnel that extends an OSPF backbone connection through a non-backbone area.

272. What is the difference between OSPF network entries and OSPF router entries?

OSPF network entries are entries in the route table, describing IP destinations. OSPF router entries are entries in a separate route table that record only routes to ABRs and ASBRs.

273. Which three fields in the LSA header distinguish different LSAs? Which three fields in the LSA header distinguish different instances of the same LSA?

The three fields in the LSA header that distinguish different LSAs are the Type, Advertising Router, and the Link State ID fields. The three fields in the LSA header that distinguish different instances of the same LSA are the Sequence Number, Age, and Checksum fields

274. Is it true that only the static option of the virtual link in OSPF allows discontiguous networks, regardless of the mask propagation properties?

No, virtual links in OSPF maintain connectivity to the backbone from nonbackbone areas, but they are unnecessary for discontiguous addressing. OSPF provides support for discontiguous networks because every area has a collection of networks, and OSPF attaches a mask to each advertisement.

275. What does the clear ip ospf redistribution command do?

The clear ip ospf redistribution command flushes all the type 5 and type 7 link-state advertisements (LSAs) and scans the routing table for the redistributed routes. This causes a partial shortest path first algorithm (SPF) in all the routers on the network that receive the flushed/renewed LSAs. When the expected redistributed route is not in OSPF, this command may help to renew the LSA and get the route into OSPF.

276. Does OSPF form adjacencies with neighbors that are not on the same subnet?

The only time that OSPF forms adjacencies between neighbors that are not on the same subnet is when the neighbors are connected through point-to-point links. This may be desired when using the ip unnumbered command, but in all other cases, the neighbors must be on the same subnet.

277. How often does OSPF send out link-state advertisements (LSAs)?

OSPF sends out its self-originated LSAs when the LSA age reaches the link-state refresh time, which is 1800 seconds. For more information, refer toLink-State Advertisements.

278. 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.

In Internet service provider (ISP) and large enterprise networks, many of the distribution routers have more than 200 interfaces. Configuring passive-interface on each of the 200 interfaces can be difficult. The solution in such situations is to configure all the interfaces as passive by default using a single passive-interface default command. Then, configure individual interfaces where adjacencies are desired using the no passive-interfacecommand. For more information, refer to Default Passive Interface Feature.

There are some known problems with the passive-interface default command. Workarounds are listed in Cisco bug ID CSCdr09263 (registeredcustomers only) .

279. 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 IP 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.

280. Why is it that my Cisco 1600 router does not recognize the OSPF protocol?

Cisco 1600 routers require the Plus feature set image of Cisco IOS Software to run OSPF. Refer to Table 3: Cisco 1600 Series Routers Feature Sets in the Release Notes for Cisco IOS Release 11.2(11) Software Feature Packs for Cisco 1600 Series Routers for more information.

281. Why is it that my Cisco 800 router does not run OSPF?

Cisco 800 routers do not support OSPF. However, they do support Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP). You can use the Software Advisor (registered customers only) tool for more information on feature support.

282. 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. The only case in which the OSPF process number is taken into account is when OSPF is used as the routing protocol on a Provider Edge to Customer Edge (PE-CE) link in a Multiprotocol Label Switching (MPLS) VPN. PE routers mark OSPF routes with the domain attribute derived from the OSPF process number to indicate whether the route originated within the same OSPF domain or from outside it. If the OSPF process numbering is inconsistent on PE routers in the MPLS VPN, the domain-id OSPF mode

command should be used to mark that the OSPF processes with different numbers belong to the same OSPF domain.

This means that, in many practical cases, you can use different autonomous system numbers for the same OSPF domain in your network. However, it is best to use consistent OSPF-process numbering as much as possible. This consistency simplifies network maintenance and complies with the network designer intention to keep routers in the same OSPF domain.

283. I have a router that runs Cisco Express Forwarding (CEF) and OSPF, who does load-balancing when there are multiple links to a destination?

CEF works by performing the switching of the packet based on the routing table which is populated by the routing protocols such as OSPF. CEF does the load-balancing once the routing protocol table has been calculated. For more details on load balancing, refer to How does load-balancing work?

284. How does OSPF use two Multilink paths to transfer packets?

OSPF uses the metric aCost, which is related to the bandwidth. If there are equal cost paths (the same bandwidth on both multilinks), OSPF installs both routes in the routing table. The routing table tries to use both links equally, regardless of the interface utilization. If one of the links in the first multilink fails, OSPF does not send all the traffic down the second multilink. If the first multilink peaks 100%, OSPF does not send any traffic down the second multilink because OSPF tries to use both links equally, regardless of the interface utilization. The second is used fully only when the first multilink goes down.

285. How can you detect the topological changes rapidly?

In order to have a rapid fault detection of topology changes, the hello timer value needs to be set to 1 second. The hold timer value, which is is four times that of the hello timer, also needs to be configured. There is a possibility of more routing traffic if the hello and hold timer values are reduced from their default values.

Note: Tuning OSPF Timers might result in network as well device resource overhead. Cisco recommends to use Bidirectional Forwarding Detection (BFD) instead of tuning the routing protocol timers. BFD also gives sub-second convergence. Refer toOSPF Support for BFD over IPv4 for more information.

286. Does the 3825 Series Router support the OSPF Stub feature?

Yes, the 3800 Series Router that runs Advanced IPServices image supports the OSPF Stub feature.

287. What does the error message %OSPF-4-FLOOD_WAR: Process process-id re-originates LSA ID ip address type-2 adv-rtr ip address in area area id means?

The error message is due to the some router that is flushing the network LSA because the network LSA received by the router whose LSA ID conflicts with the IP address of one of the router's interfaces and flushes the LSA out of the network. For OSPF to function correctly the IP addresses of transit networks must be unique. If it is not unique the conflicting routers reports this error message. In the error message the router with the OSPF router ID reported as adv-rtr reports this message.

288. Can we have OSPF run over a GRE tunnel?

Yes, refer to Configuring a GRE Tunnel over IPSec with OSPF.

289. Is there a way to manipulate and prefer the Type 3 LSAs to originate from two different areas sent to the non-backbone area?

Type 3 LSA is originated by the Area Border Router (ABR) as a summary route. Manipulating the summary route is not possible in an ABR router.

290. Is there a drop/flap of an OSPF neighborship when changing an OSPF area type from nssa no-summary to nssa?

When the NSSA ABR is configured to move from nssa no-summary to nssa, the OSPF neighborship does not flap.

291. In the %OSPF-5-ADJCHG: Process ID, Nbr [ip-address] on Port-channel31 from FULL to EXSTART, SeqNumberMismatcherror message, what does SeqNumberMismatch signify?

The OSPF neighbor was changed state from FULL to EXSTART because of the receipt of a Database Description (DBD) packet from the neighbor with an unexpected sequence number.

Seq Number Mismatch means that a DBD packet during OSPF neighborship negotiation has been received that either:

has an unexpected DBD sequence number

unexpectedly has the Init bit set

has an Options field differing from the last Options field received in a Database Description packet.

What is the maximum number of OSPF processes (VRF aware) on 7600/6500 platforms?

Cisco IOS has a limit of 32 routing processes. Two of these are saved for static and directly connected routes. The Cisco 7600 router supports 28 OSPF processes per VRF.

292. How does ISPF impact or improve the OSPF network?.

Incremental SPF is more efficient than the full SPF algorithm, thereby allowing OSPF to converge faster on a new routing topology in reaction to a network event. The incremental SPF is designed in such a way that it only updates the affected nodes without rebuilding the whole tree. This results in a faster convergence and saves CPU cycles because the unaffected nodes do not need to be processed. Concerning the best practice ISPF would make more of a difference for a large OSPF domain.

Incremental SPF provides greater improvements in convergence time for networks with a high number of nodes and links. Incremental SPF also provides a significant advantage when the changes in the network topology are further away from the root of the SPT; for example, the larger the network the more significant the impact. A segment of 400-1000 nodes should see improvements. However, it might be hard to verify in a deployed production network without some kind of facility or tool to measure the end-to-end delay. For more information, refer to OSPF Incremental SPF.

293. Is there a way to compare Cisco NX-OS/IOS OSPF commands?

Yes, refer to Cisco NX-OS/IOS OSPF Comparison.

294. Is there any feature of OSPF protocol for quick convergence and a slow re-convergence of routes?

The OSPF Shortest Path First Throttling feature makes it possible to configure SPF scheduling in millisecond intervals and to potentially delay SPF calculations during network instability. SPF is scheduled to calculate the Shortest Path Tree (SPT) when there is a change in topology.

Syntax of the command under OSPF:

timers throttle spf [spf-start] [spf-hold] [spf-max-wait]

Where:

spf-start—Initial delay to schedule an SPF calculation after a change, in milliseconds. Range is from 1 to 600000.

spf-hold—Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000.

spf-max-wait—Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is 1 to 600000.

For more information on the OSPF Throttling feature, refer to OSPF Shortest Path First Throttling.

295. What does BADSEQNUM in the %OSPF-5-NBRSTATE: ospf-101 [5330] Process 101, Nbr 10.253.5.108 on Vlan7 02 from FULL to EXSTART, BADSEQNUM OSPF log message mean?

This message is related to the DBD exchange process, which uses a sequence number for the synchronization of the database. For some reason a bad sequence number was reported in the DBD packet. This might occur because of transient conditions, which includes packet loss or packet corruption.

296. Are the multicast IP addresses mapped to MAC-level multicast addresses?

OSPF sends all advertisements using multicast addressing. Except for Token Ring, the multicast IP addresses are mapped to MAC-level multicast addresses. Cisco maps Token Ring to MAC-level broadcast addresses.

297. Does the Cisco OSPF implementation support IP TOS-based routing?

Cisco OSPF only supports TOS 0. This means that routers route all packets on the TOS 0 path, eliminating the need to calculate nonzero TOS paths.

298. Does the offset-list subcommand work for OSPF?

The offset-list command does not work for OSPF. It is used for distance vector protocols such as Interior Gateway Routing Protocol (IGRP), Routing Information Protocol (RIP), and RIP version 2.

299. Can an OSPF default be originated into the system based on external information on a router that does not itself have a default?

OSPF generates a default only if it is configured using the command default-information originate and if there is a default network in the box from a different process. The default route in OSPF is 0.0.0.0. If you want an OSPF-enabled router to generate a default route even if it does not have a default route itself, use the command default-information originate always.

300. When I issue the show ip ospf neighbor command, why do I only see FULL/DR and FULL/BDR, with all other neighbors showing 2-WAY/DROTHER?

To reduce the amount of flooding on broadcast media, such as Ethernet, FDDI, and Token Ring, the router becomes full with only designated router (DR) and backup designated router (BDR), and it shows 2-WAY for all other routers.

301. Why do I not see OSPF neighbors as FULL/DR or FULL/BDR on my serial link?

This is normal. On point-to-point and point-to-multipoint networks, there are no designated routers (DRs) or backup designated routers (BDRs).

302. Do I need any special commands to run OSPF over BRI/PRI links?

In addition to the normal OSPF configuration commands, you should use the dialer map command. When using the dialer map command, use thebroadcast keyword to indicate that broadcasts should be forwarded to the protocol address.

303. Do I need any special commands to run OSPF over asynchronous links?

A. In addition to the normal OSPF configuration commands, you should use the async default routing command on the asynchronous interface. This command enables the router to pass routing updates to other routers over the asynchronous interface. Also, when using the dialer map command, use the broadcast keyword to indicate that broadcasts should be forwarded to the protocol address.

304. Which Cisco IOS Software release began support for per-interface authentication type in OSPF?

Per-interface authentication type, as described in RFC 2178 Description: leavingcisco.com , was added in Cisco IOS Software Release 12.0(8).

305. Can I control the P-bit when importing external routes into a not-so-stubby area (NSSA)?

When external routing information is imported into an NSSA in a type 7 link-state advertisement (LSA), the type 7 LSA has only area flooding scope. To further distribute the external information,

type 7 LSAs are translated into type 5 LSAs at the NSSA border. The P-bit in the type 7 LSA Options field indicates whether the type 7 LSA should be translated. Only those LSAs with the P-bit set are translated. When you redistribute information into the NSSA, the P-bit is automatically set. A possible workaround applies when the Autonomous System Boundary Router (ASBR) is also an Area Border Router (ABR). The NSSA ASBR can then summarize with the not-advertise keyword, which results in not advertising the translated type 7 LSAs.

306. Why are OSPF show commands responding so slowly?

You may experience a slow response when issuing OSPF show commands, but not with other commands. The most common reason for this delay is that you have the ip ospf name-lookup configuration command configured on the router. This command causes the router to look up the device Domain Name System (DNS) names for all OSPF show commands, making it easier to identify devices, but resulting in a slowed response time for the commands. If you are experiencing slow response on commands other than just OSPF show commands, you may want to start looking at other possible causes, such as the CPU utilization

ACL Interview Questions and Answers

307. What is ACL?

Access Control List is a packet filtering method that filters the IP packets based on source and destination address. It is a set of rules and conditions that permit or deny IP packets to exercise control over network traffic.

308. What are different Types of ACL?

There are two main types of Access lists:-

1.Standard Access List.

2.Extended Access List.

309. Explain Standard Access List?

Standard Access List examines only the source IP address in an IP packet to permit or deny that packet. It cannot match other field in the IP packet. Standard Access List can be created using the access-list numbers 1-99 or in the expanded range of 1300-1999. Standard Access List must be

applied close to destination. As we are filtering based only on source address, if we put the standard access-list close to the source host or network than nothing would be forwarded from source.

Example:-

R1(config)# access-list 10 deny host 192.168.1.1

R1(config)# int fa0/0

R1(config-if)# ip access-group 10 in

310. Explain Extended Access List?

Extended Access List filters the network traffic based on the Source IP address, Destination IP address, Protocol Field in the Network layer, Port number field at the Transport layer. Extended Access List ranges from 100 to 199, In expanded range 2000-2699. Extended Access List should be placed as close to source as possible. Since extended access list filters the traffic based on specific addresses (Source IP, Destination IP) and protocols we don't want our traffic to traverse the entire network just to be denied wasting the bandwidth.

Example:-

R1(config)# access-list 110 deny tcp any host 192.168.1.1 eq 23

R1(config)# int fa0/0

R1(config-if)# ip access-group 110 in

311. Explain Named ACL and its advantages over Number ACL?

It is just another way of creating Standard and Extended ACL. In Named ACL names are given to identify access-list.

It has following advantage over Number ACL - In Name ACL we can give sequence number which means we can insert a new statement in middle of ACL.

Example:-

R1(config)# ip access-list extended CCNA

R1(config)# 15 permit tcp host 10.1.1.1 host 20.1.1.1 eq 23

R1(config)# exit

This will insert above statement at Line 15.

R1(config)# int fa0/0

R1(config-if)# ip access-group ccna in

312. What is Wildcard Mask?

Wildcard mask is used with ACL to specify an individual hosts, a network, or a range of network. Whenever a zero is present, it indicates that octet in the address must match the corresponding reference exactly. Whenever a 255 is present, it indicates that octet need not to be evaluated.

Wildcard Mask is completely opposite to subnet mask.

Example:- For /24

Subnet Mask - 255.255.255.0

Wildcard Mask - 0.0.0.255

313. How to permit or deny specific Host in ACL?

1. Using a wildcard mask "0.0.0.0"

Example:- 192.168.1.1 0.0.0.0 or

2. Using keyword "Host"

Example:- Host 192.168.1.1

314. In which directions we can apply an Access List?

We can apply access list in two direction:-

IN - ip access-group 10 in

OUT - ip access-group 10 out

315. Difference between Inbound Access-list and Outbound Access-list?

When an access-list is applied to inbound packets on interface, those packets are first processed through ACL and than routed. Any packets that are denied won't be routed. When an access-list is applied to outbound packets on interface, those packets are first routed to outbound interface and than processed through ACL.

316. Difference between #sh access-list command and #sh run access-list command?

#sh access-list shows number of Hit Counts.

#sh run access-list does not show number of Hit Counts.

317. How many Access Lists can be applied to an interface on a Cisco router?

We can assign only one access list per interface per protocol per direction which means that when creating an IP access lists, we can have only one inbound access list and one outbound access list per interface. Multiple access lists are permitted per interface, but they must be for a different protocol.

318. How Access Lists are processed?

Access lists are processed in sequential, logical order, evaluating packets from the top down, one statement at a time. As soon as a match is made, the permit or deny option is applied, and the packet is not evaluated against any more access list statements. Because of this, the order of the statements within any access list is significant. There is an implicit "deny" at the end of each access list which means that if a packet doesn't match the condition on any of the lines in the access list, the packet will be discarded.

319. What is at the end of each Access List?

At the end of each access list, there is an implicit deny statement denying any packet for which the match has not been found in the access list.

Key Information

- Any access list applied to an interface without an access list being created will not filter traffic.
- Access lists only filters traffic that is going through the router. They will not filter the traffic that has originated from the router.
- If we will remove one line from an access list, entire access-list will be removed.
- Every Access list should have at least one permit statement or it will deny all traffic

NAT Interview Questions and Answers

320. What is NAT?

Network Address Translation translates the private addresses into public addresses before packets are routed to public network. It allows a network device such as Router to translate addresses between the private and public network.

321. What are the Situations where NAT is required?

- When we need to connect to internet and our hosts doesn't have globally unique IP addresses.
- When we want to hide internal IP addresses from outside for security purpose.
- A company is going to merge in another company which uses same address space.

322. What are the advantages of Nat?

- It conserves legally registered IP addresses.
- It prevents address overlapping.
- Provides security by hiding internal (private) IP addresses.
- Eliminates address renumbering as a network evolves.

323. What are different types of NAT?

There are mainly three types of NAT:-

- Static NAT
- Dynamic NAT
- Port Address Translation (Overloading)

324. What is Static NAT?

Static NAT allows for one to one mapping that is it translates one Private IP address to one Public IP address.

R1(config)# ip nat inside source static 10.1.1.1 15.36.2.1

R1(config)# int fa0/0

R1(config-if)# ip nat inside (It identifies this interface as inside interface)

R1(config)# int fa0/1

R1(config-if)# ip nat outside (It identifies this interface as outside interface)

In ip nat inside source command we can see that the command is referencing the inside interface as source or starting point of the translation.

325. What is Dynamic NAT?

It maps an unregistred IP address to a registered IP address from out of a pool of registered Ip addresses.

R1(config)# ip nat pool CCNA 190.1.1.5 190.1.1.254 netmask 255.255.255.0

R1(config)# ip nat inside source list 10 pool CCNA

R1(config)# int fa0/0

R1(config-if)# ip nat inside (It identifies this interface as inside interface)

R1(config)# int fa0/1

R1(config-if)# ip nat outside (It identifies this interface as outside interface)

R1(config)# access-list 10 permit 192.168.1.0 0.0.0.255 (To specify which unregistered addresses needs to be translated)

326. What is Port Address Translation (Overloading)?

It maps multiple unregistred IP address to single registered IP address using different port numbers. PAT allows thousands of users to connect to internet using one pulic address only.

R1(config)# ip nat pool CCNA 190.1.1.5 190.1.1.254 netmask 255.255.255.0

R1(config)# ip nat inside source list 10 pool CCNA overload

R1(config)# int fa0/0

R1(config-if)# ip nat inside (It identifies this interface as inside interface)

R1(config)# int fa0/1

R1(config-if)# ip nat outside (It identifies this interface as outside interface)

R1(config)# access-list 10 permit 192.168.1.0 0.0.0.255 (To specify which unregistered addresses needs to be translated)

327. What are Inside Local, Inside Global, Outside Local, Outside Global address?

- Inside local address is an IP address of Host before translation.
- Inside Global address is the public IP address of Host after translation.
- Outside Local address is the address of router interface connected to ISP.
- Outside Global address is the address of outside destination (ultimate destination).

DHCP Interview Questions and Answers

328. What is DHCP?

Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to hosts dynamically. It allows easier administration and works well in small as well as very large network environments. All types of hardware can be used as a DHCP server including a Cisco router.

329. What information a DHCP server can provide to a host?

DHCP server can provide following information -

- IP address
- Subnet mask
- Default gateway
- Domain Name Server
- WINS information

330. How DHCP Works?

DHCP works on **DORA Process** (DISCOVER - OFFER - REQUEST - ACKNOWLEDGEMENT).

1. When a Client needs an IP configuration, it tries to locate a DHCP server by sending a broadcast called a DHCP DISCOVER. This message will have a Destination IP of 255.255.255.255 and Destination MAC of ff:ff:ff:ff:ff:ff.

[Source IP - 0.0.0.0 , Destination IP - 255.255.255.255, Source Mac - Mac address of Host, Destination Mac - FF:FF:FF:FF:FF:FF]

2. On Receiving DHCP Discover, Server sends a DHCP OFFER message to the client. The DHCPOFFER is a proposed configuration that may include IP address, DNS server address, and lease time. This message will be unicast and have the destination mac address of DHCP client's mac address. The source mac address will be that of the DHCP server.

[S.Mac - Mac address of Server , D.Mac - Mac address of Host]

3. If the Client finds the Offer agreeable, it sends DHCP REQUEST Message requesting those particular IP parameters. This message will be a Broadcast message.

[Source Mac - Mac address of Host, Destination Mac - FF:FF:FF:FF:FF:FF]

4. The Server on receiving the DHCP REQUEST makes the configuration official by sending a unicast DHCP ACK acknowledgment.

[Source Mac - Mac address of Server, Destination Mac - Mac address of Host]

331. What is the reason for getting APIPA address?

With APIPA, DHCP clients can automatically self-configure an IP address and subnetmask when a DHCP server is not available. When DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask.

A client uses the self-configured IP address until a DHCP server becomes available. The APIPA service also checks regularly for the presence of a DHCP server. If it detects a DHCP server on the network, APIPA stops and the DHCP server replaces the APIPA networking addresses with dynamically assigned addresses.

332. What is the range of APIPA address?

The IP address range is 169.254.0.1 through 169.254.255.254. The client also configures itself with a default Class B subnet mask of 255.255.0.0.

333. What is the purpose of relay agent?

A DHCP relay agent is any host that forwards DHCP packets between clients and servers if server is not on the same physical subnet. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet.

DHCP relay agent can be configured using the **ip helper-address** command.

334. What is DHCP decline message?

It is Sent by Client to server indicating network address is already in use (already assigned to another device).

335. What is DHCPNAK message?

If the Server is unable to satisfy the DHCPREQUEST message (The requested network address has been allocated) the Server Should sent DHCPNAK message to client. It can also be Sent if client's notion of network address is incorrect (Client has moved to new subnet) or client's lease expired.

TCP Interview Questions and Answers

336. What is TCP?

Transmission Control Protocol is a connection oriented protocol. This means that before any data transfer can take place , Certain Parameters has to be negotiated in order to establish the connection.

337. Explain TCP Three Way Handshake process?

For Reliable connection the Transmitting device first establishes a connection-oriented (reliable) session with its peer system, which is called three way handshake. Data is then transferred. When the Data transfer is finished, connection is terminated and virtual circuit is teared down.

1. In the First Part of Three way Handshake, Source sends a TCP SYN Segment with the initial sequence number X indicating the desire to open the connection.

2. In Second Part, When Destination receives TCP SYN, It acknowledges this with Ack (X+1) as well as its own SYN Y (It informs Source what sequence number it will start its data with and will use in further messages). This response is called SYN/ACK.

3. In Third Part, Source Sends an ACK (ACK = Y+1) Segment to the destination indicating that the connection is set up. Data transfer can then begin.

During this 3 way Handshake, Devices are negotiating parameters like Window Size etc.

338. What does Window Size indicate?

It is 16-bit Window field which indicates the number of bytes a sender will send before receiving an acknowledgment from the receiver.

339. What is the purpose of RST bit?

When the connection Is not allowed by destination connection is reset.

340. What are TCP Flags?

TCP Flags are used to influence the Flow of Data across a TCP Connection.

1. **PUSH (PSH) -** It Pushes the Buffered data to the receivers application. If data is to be send on immediate Basis we will push it.

2. **Reset (RST) -** It Resets the connection.

3. **Finish (FIN) -** It finishes the session. It means No More Data from the Sender.

4. **Urgent (URG) -** It is use to set the priority to tell the receiver that this data is important for you.

5. **Acknowledgement (ACK) -** All packets after SYN packet sent by Client should have this Flag Set. ACK=10 means Host has received 0 through 9 and is expecting Byte 10 Next.

6. **Synchronize (SYN) -** It Initiates a Connection. It Synchronizes the sequence number.

341. What is the difference between PUSH and URG flag?

The PSH flag in the TCP header informs the receiving host that the data should be pushed up to the receiving application immediately. The URG flag is used to inform a receiving station that certain data within a segment is urgent and should be prioritized.

342. What is the importance of Sequence Number and Acknowledgement Number?

Sequence Number is a 32-bit field which indicates the amount of data that is sent during a TCP session. By Sequence Number sender can be assured that the receiver received the data because the receiver uses this sequence number as the acknowledgment number in the next segment it sends to acknowledge the received data. When the TCP session starts, the initial sequence number can be any number in the range 0–4,294,967,295.

Acknowledgment number is used to acknowledge the received data and is equal to the received sequence number plus 1.

IP Header Interview Questions and Answers

343. Which is the importance of identification field in the IP packet?

This is used to identify each fragmented packet so that destination device can rearrange the whole communication in order.

344. Which device can reassemble the packet?

This is done only by the ultimate destination of the IP message.

345. What is IP datagram?

IP datagram can be used to describe a portion of IP data. Each IP datagram has set of fields arranged in order. IP datagram has following fields Version, Header length, Type of service, Total length, checksum, flag, protocol, Time to live, Identification, Source IP Address and Destination Ip Address, Padding, Options and Payload.

346. What is MTU (Maximum Transmission Unit) ?

The maximum transmission unit (MTU) of an interface tells Cisco IOS the largest IP packet that can be forwarded out on that interface.

347. What is Fragmentation ?

Fragmentation is a process of breaking the IP packets into smaller pieces (fragments). Fragmentation is required when the datagram is larger than the MTU. Each fragment than becomes a datagram in itself and transmitted independently from source. These datagrams are reassembled by the destination.

348. How the packet is reassembled?

1. When a host receives an IP fragment, it stores this fragment in a reassembly buffer based on its fragment offset field.

2. Once all the fragments of the original IP datagram are received, the datagram is processed.

3. On receiving the first fragment, a reassembly timer is started.

4. If this reassembly timer expires before all the fragments are received than datagram is discarded.

349. What is the importance of DF, MF flag?

Don't fragment bit

If DF bit is set, fragmentation is not allowed.

when a router needs to forward a packet larger than the outgoing interface's MTU, the router either fragments the packet or discards it. If the IP header's Do Not Fragment (DF) bit is set, means fragmentation is not allowed and the router discards the packet. If the DF bit is not set, means Fragmentation is allowed and the router can perform Layer 3 fragmentation on the packet.

More fragments bit

If MF Bit is set to 1 means more fragments are coming. If it is set to 0 means This is the Last Fragment.

All fragments that belong to an IP datagram will have more fragments bit set except for the final fragment. The final fragment does not have the more fragment bit set indicating that this is the last fragment. This is how the End hosts comes to know that it has collected all the fragments of the IP datagram.

350. What is the purpose of fragment offset?

It is used to define the Size of each Fragmented Packet.

351. What is the importance of TTL value?

It defines how long a packet can travel in the network. It is the number of hops that the IP datagram will go through before being discarded. At every hop TTL value is decremented by 1. When this field becomes zero, the data gram is discarded. This behavior helps prevent routing loops. The typical value for a TTL field is 32 or 64.

352. What does the protocol field determines in the IP packet?

The Protocol field is an 8-bit field that identifies the next level protocol. It Indicates to which upper-layer protocol this datagram should be delivered.

Example - TCP, UDP.

ICMP Interview Questions and Answers

353. What is the Internet Control Message Protocol?

ICMP is basically a management protocol and messaging service provider for IP. It can provide Hosts with information about network problems.

354. ICMP works at which layer?

It works at Network Layer.

355. Which two fields in the ICMP header is used to identify the intent of ICMP message?

Type and Code.

356. What are various ICMP messages?

1. Destination Unreachable.

2.Buffer Full.

3.Hops/Time Exceeded.

4.Ping.

5.Traceroute.

357. How Traceroute works?

1. Firstly, Traceroute creates a UDP packet from the source to destination with a TTL value of 1.

2. Packet reaches the first router where the router decrements the value of TTL by 1, making packet's TTL value 0 because of which the packet gets dropped.

3. As the packet gets dropped, it sends an ICMP message [Hop/Time exceeded] back to the source.

4. This is how Traceroute comes to know the first router's address and the time taken for the round-trip.

5. It sends two more packets in the same way to get average round-trip time. First round-trip takes longer than the other two due to the delay in ARP finding the physical address, the address stays in the ARP cache during the second and the third time and hence the process speeds up.

6. These steps Takes place again and again until the destination has been reached. The only change that happens is that the TTL is incremented by 1 when the UDP packet is to be sent to next router/host.

7. Once the destination is reached, Time exceeded ICMP message is NOT sent back this time because the destination has already been reached.

8. But, the UDP packet used by Traceroute specifies the destination port number that is not usually used for UDP. So, when the destination verifies the headers of the UDP packet, the packet gets dropped because of improper port being used and an ICMP message [Destination Unreachable] is sent back to the source.

9. When Traceroute encounters this message, it understands that the destination is reached. Also, The destination is reached 3 times to get the average round-trip time.

358. Why there are three columns in traceroute results?

Three probes (change with -q flag) are sent at each ttl setting and a line ***is printed showing the ttl, address of the gateway and round trip time of each probe(so three *).

359. Which ICMP message confirms the traceroute is completed?

Destination Unreachable Message

ARP Interview Question and Answers

360. What is ARP?

Address Resolution Protocol (ARP) is a network protocol, which is used to map a network layer protocol address (IP Address) to a data link layer hardware address (MAC Address). ARP basically resolves IP address to the corresponding MAC address.

361. ARP works at which layer and Why?

ARP works at data link layer (Layer 2). ARP is implemented by the network protocol driver and its packets are encapsulated by Ethernet headers and transmitted.

362. Explain the use of ARP?

If a host in an Ethernet network wants to communicate with another host, it can communicate only if it knows the MAC address of other host. ARP is used to get the Mac address of a host from its IP address.

363. What is an ARP Table (cache)?

ARP maintains a table that contains the mappings between IP address and MAC address. This Table is called ARP Table.

364. What is the Source & Destination IP address in ARP Request and ARP Reply packet?

ARP Request

Source - Mac Address of Host which transmitted the ARP Request packet. (Senders MAC address)

Destination - FF:FF:FF:FF:FF:FF Broadcast

ARP Reply

Source - Mac address of Host replying for ARP Request.

Destination - Mac Address of Host which generated the ARP Request packet.

365. What is the Size of an ARP Request and ARP Reply packet?

The size of an ARP request or ARP reply packet is 28 bytes.

366. How can we differentiate between a ARP Request packet and a ARP Reply packet?

We can differentiate ARP request packet from an ARP reply packet using the 'operation' field in the ARP packet. For ARP Request it is 1 and for ARP Reply it is 2.

367. What is Proxy ARP?

Proxy ARP is the process in which one system responds to the ARP request for the another system.

Example - Host A sends an ARP request to resolve the IP address of Host B. Instead of Host B, Host C responds to this ARP request.

367. What is Gratuitous ARP? Why it is used?

When a Host sends an ARP request to resolve its own IP address, it is called Gratuitous ARP. In the ARP request packet, the Source IP address and Destination IP address are filled with the Same Source IP address itself. The Destination MAC address is the Broadcast address (FF:FF:FF:FF:FF:FF).

Gratuitous ARP is used by the Host after it is assigned an IP address by DHCP Server to check whether another host in the network does not have the same IP address. If the Host does not get ARP reply for a gratuitous ARP request, It means there is no another host which is configured with the same IP address. If the Host gets ARP reply than it means another host is also configured with the same IP address.

368. What is Reverse ARP?

Reverse ARP is used to obtain Device's **IP address when its MAC address** is already Known.

369. What is Inverse ARP?

Inverse ARP dynamically maps local **DLCIs to remote IP addresses** when Frame Relay is configured.

Background Images Question and answers Answers Photo Driving Map Digital media player.

SNMP Interview Questions and Answers

370. What is SNMP?

The Simple Network Management Protocol (SNMP) enables a network device to share information about itself and its activities. It uses the User Datagram Protocol (UDP) as the transport protocol for passing data between managers and agents.

371. What are the Components of SNMP?

A complete SNMP system consists of the following parts:-

SNMP Manager - A network management system that uses SNMP to poll and receive data from any number of network devices. The SNMP manager usually is an application that runs in a central location.

SNMP Agent - A process that runs on the network device being monitored. All types of data are gathered by the device itself and stored in a local database. The agent can then respond to SNMP polls and queries with information from the database, and it can send unsolicited alerts or "traps" to an SNMP manager.

372. Which Ports are used in SNMP?

SNMP uses the UDP port 161 for sending and receiving requests, and port 162 for receiving traps from managed devices.

373. Explain MIB?

MIB is a hierarchical Database Structure for information on the device. Example - Serial numbers are in a specific location, NIC Statistics etc.

374. What are different SNMP versions?

There are different versions of SNMP - SNMP V1, SNMP V2c, and SNMP V3.

SNMP version 1 - It is the oldest flavor. It is Easy to set up – only requires a plaintext community.

SNMP version 2c - It is identical to Version 1, except that it adds support for 64 bit counters.

SNMP version 3 - It adds security to the 64 bit counters. SNMP version 3 adds both Encryption and Authentication, which can be used together or separately.

375. I can issue a Simple Network Management Protocol (SNMP) ping to the router asking it to ping all data-link connection identifier (DLCI) partners, and it is successful. What does this indicate?

This confirms that the protocol is configured and the protocol-to-DLCI mapping is correct at both ends.

Basic Layer 2 - Switching Interview Questions & Answer

376. What is Hub ?

hub is the simplest of these devices. Any data packet coming from one port is sent to all other ports. It is then up to the receiving computer to decide if the packet is for it. Imagine packets going through a hub as messages going into a mailing list. The mail is sent out to everyone and it is up to the receiving party to decide if it is of interest.

The biggest problem with hubs is their simplicity. Since every packet is sent out to every computer on the network, there is a lot of wasted transmission. This means that the network can easily become bogged down.

Hubs are typically used on small networks where the amount of data going across the network is never very high.

377. What are advantages of using switches in Network ?

Advantages of Switches:

- Switches increase available network bandwidth
- Switches reduce the workload on individual computers
- Switches increase network performance
- Networks that include switches experience fewer frame collisions because switches create collision domains for each connection (a process called micro segmentation)
- Switches connect directly to workstations.

378. Which type address used by layer 2 switching?

Layer 2 switching uses Hardware Address (MAC Address) of devices. Media Access Control (MAC) address burned into each and every Ethernet network interface card (NIC). The MAC, or hardware, address is a 48-bit (6-byte) address written in a hexadecimal format.

379. What is the use of Spanning Tree Protocol (STP)?

The function of Spanning Tree Protocol (STP) is to prevent Layer 2 switching loop and broadcast storms in a Local Area Network (LAN). The Spanning Tree Protocol (STP) allows redundant links in a network to prevent complete network failure if an active link fails, without the danger of Layer 2 Switching loops.

380. How to bridges and switches build and maintain the filter table ?

Bridges use software to create and manage a filter table, switches use application-specific integrated circuits (ASICs) to build and maintain their filter tables.

381. Why layer 2 switches and bridging are faster than router ?

Layer 2 switches and bridges are faster than routers because they don't take up time looking at the Network layer header information. Instead, they look at the frame's hardware addresses before deciding to either forward, flood, or drop the frame.

382. What are differences between Bridging and LAN switching ?

- Bridges are software based, while switches are hardware based because they use ASIC chips to help make filtering decisions.
- A switch can be viewed as a multiport bridge.
- There can be only one spanning-tree instance per bridge, while switches can have many.
- Most switches have a higher number of ports than most bridges.
- Both bridges and switches flood layer 2 broadcasts.
- Bridges and switches learn MAC addresses by examining the source address of each frame received.
- Both bridges and switches make forwarding decisions based on layer 2 addresses.

383. What is the difference between STP and RSTP?

The main difference between Rapid Spanning Tree Protocol (RSTP IEEE 802.1W) and Spanning Tree Protocol (STP IEEE 802.1D) is that Rapid Spanning Tree Protocol (RSTP) assumes the three Spanning Tree Protocol (STP) ports states Listening, Blocking, and Disabled are same (these states do not forward frames and they do not learn MAC addresses). Hence RSTP places them all into a new called Discarding state. Learning and forwarding ports remain more or less the same.

In Spanning Tree Protocol (STP IEEE 802.1D), bridges would only send out a BPDU when they received one on their root port. They only forward BPDUs that are generated by the Root Bridge. Rapid Spanning Tree Protocol (RSTP IEEE 802.1W) enabled switches send out BPDUs every hello time, containing current information.

Spanning Tree Protocol (STP IEEE 802.1D) includes two port types; Root Port and Designated Port. Rapid Spanning Tree Protocol (RSTP IEEE 802.1W) includes two additional port types called as alternate ports and backup ports. Analternate port is a port that has an alternative path or paths to the root but is currently in a discarding state (can be considered as an additional unused root port). A backup port is a port on a network segment that could be used to reach the root switch, but there

is already an active designated port for the segment (can be considered as an additional unused designated port).

384. Explain the function of layer 2 switching ?

Address learning -
Layer 2 switches and bridges remember the source hardware address of each frame received on an interface, and they enter this information into a MAC database called a forward/filter table.

Forward/filter decisions -
Step - 1 When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database. If the destination hardware address is known and listed in the database, the frame is only sent out the correct exit interface. The switch doesn't transmit the frame out any interface except for the destination interface. This preserves bandwidth on the other network segments and is called frame filtering.

Step - 2 But if the destination hardware address is not listed in the MAC database, then the frame is flooded out all active interfaces except the interface the frame was received on. If a device answers the flooded frame, the MAC database is updated with the device's location (interface). If a host or server sends a broadcast on the LAN, the switch will flood the frame out all active ports except the source port by default.

Loop avoidance -
If multiple connections between switches are created for redundancy purposes, network loops can occur. Spanning Tree Protocol (STP) is used to stop network loops while still permitting redundancy

385. How cab we see the mac address forward-filter table of switches ?

Show mac address-table - The command show mac address-table will show you the forward/filter table used on the LAN switch.

386. What is the advantage of redundant link between switches ?

Redundant links between switches are a good idea because they help prevent irrecoverable network failures in the event one link stops working.

387. What is UDLD and why it is required?

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and

disable unidirectional links. When UDLD detects a unidirectional link, it administratively shuts down the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

388. How do you stop someone from simply plugging a host into one of your switch ports—or worse, adding a hub, switch, or access point into the Ethernet jack in their office?

You can stop them in their tracks by using port security.

Switch#config t
Switch(config)#int f0/1
Switch(config-if)#switchport mode access →**[Change the port from desirable mode to access port]**

Switch(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addresses
violation Security violation mode
Switch(config-if)#switchport port-security maximum 1 → **[Allow only one host per port means only one mac address can be used on that port]**
Switch(config-if)#switchport port-security violation shutdown →**[Shutdown the port if rule is violated or user try to add another host on that segment]**

Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security violation shutdown

389. What are difference between Protect Mode and Restrict Mode in Security Violation ?

Switch(config-if)#switchport port-security violation ?

protect Security violation protect mode

restrict Security violation restrict mode

shutdown Security violation shutdown mode

Protect Mode - Protect mode means that another host can connect but its frames will just be dropped. , no notification action is taken when traffic is dropped.
Restrict Mode - a syslog message is logged, a Simple Network Management Protocol (SNMP) trap is sent, and a violation counter is incremented when traffic is dropped.

390. What is Switching?

The function of Switching is to Switch data packets between devices on the same network.

391. What is the difference between a HUB, Switch & Router?

Hub is designed to connect hosts to each other with no understanding of what it is transferring. When a Hub receives a packet of data from a connected device, it broadcasts that data packet to all other ports regardless of destination port. HUB operates at Layer 1 (Physical Layer).

Switch also connects hosts to each other like a hub. Switch differs from a hub in the way it handles packets. When a switch receives a packet, it determines what hosts the packet is intended for and sends it to that hosts only. It does not broadcast the packet to all the hosts as a hub does which means bandwidth is not shared and makes the network more efficient. Switch operates at Layer 2 (Data Link Layer).

Router is different from a switch or hub since its function is to route data packets to other networks, instead of just the local network. Routers operates at Layer 3 (Network Layer).

392. What is Sub Interface?

To support ISL or 802.1Q routing on a Fast Ethernet interface, the router's interface is divided into logical interfaces—one for each VLAN. These are called subinterfaces.

What is a MAC address Table and how a Switch will build a MAC table?

To switch frames between LAN ports efficiently, the switch maintains an address table called MAC address Table or CAM Table (Content Addressable Memory Table). When the switch receives a frame, source MAC address is learned and recorded in the CAM table along with the port of arrival, VLAN and time stamp. The switch dynamically builds the MAC address table by using the Source MAC address of the frames received. Than this table is used by switch to determine where to forward traffic on a LAN.

393. How Switch Learns Mac Address?

When a frame reaches to the port of a switch, the switch reads the MAC address of the source device from Ethernet frame and compares it to its MAC address table (also known as CAM (Content Addressable Memory) table). If the switch does not find a corresponding entry in MAC address table, the switch will add the address to the table with the port number at which the Ethernet frame is received.

If the MAC address is already available in the MAC address table, the switch compares the incoming port with the port already available in the MAC table. If the port numbers are different, the switch updates the MAC address table with the new port number.

394. How does Switch performs Forwarding function?

When a Layer2 Ethernet frame reaches a port on the Switch, it not only reads the source MAC address of the Ethernet frame as a part of learning function, but also reads the destination MAC address as a part of forwarding function. The destination MAC address is important to determine the port which the destination device is connected to.

As the destination MAC address is found on the MAC address table, the switch forwards the Ethernet frame via the corresponding port of the MAC address.

395. Explain Flooding?

If the destination MAC address is not found in the MAC address table, the switch forwards the frame out all of its ports except the port on which the frame was received. This is known as flooding.

396. Explain Dynamic Trunking Protocol (DTP) ?

Dynamic Trunking Protocol (DTP) is a Cisco proprietary trunking protocol used for negotiating trunking on a link between two Cisco Switches. Dynamic Trunking Protocol (DTP) can also be used for negotiating the encapsulation type of either 802.1q or Cisco ISL (Inter-Switch Link).

397. Explain dynamic desirable & dynamic auto?

Dynamic Desirable - It Initiates negotiation. Switch port configured as DTP dynamic desirable mode will actively try to convert the link to a trunk link if the port connected to other port is capable to form a trunk.

Dynamic Auto - It does not Initiates negotiation but can respond to negotiation. Switch port configured as DTP dynamic auto is capable to form trunk link if the other side switch interface is configured to form a trunk interface and can negotiate with trunk using DTP.

STP Interview Questions

398. What is STP?

- The function of Spanning Tree Protocol (STP) is to prevent Layer 2 switching loops and broadcast storms in a Local Area Network (LAN) because of redundant links.
- STP allows redundant links in a network to prevent complete network failure if an active link fails.

399. Who developed STP?

- Spanning Tree Protocol (STP) is based on an algorithm, which was developed by Radia Perlman at DEC (Digital Equipment Corporation, now part of HP).
- The Spanning Tree Protocol (STP) was then standardized by IEEE as IEEE 802.1D.

400. How does STP maintain a loop-free network?

STP chooses a Reference point (Root Bridge) in the network and calculates all the redundant paths to that reference point. Than it picks one path which to forward frames and blocks other redundant paths. When blocking hapeens, Loops are prevented.

401. What is Bridge Protocol Data Unit (BPDU) frame?

• The Spanning Tree Protocol (STP) enabled switches in a redundant Local Area Network (LAN) need to exchange information between each other for Spanning Tree Protocol (STP) to work properly.

• Bridge Protocol Data Units (BPDUs) are messages exchanged between the switches inside an interconnected redundant Local Area Network (LAN).

• Bridge Protocol Data Units (BPDUs) frames contain information regarding the Switch ID, originating switch port, MAC address, switch port priority, switch port cost etc.

• When Bridge Protocol Data Units (BPDUs) are received, the Switch uses a mathematical formula called the Spanning Tree Algorithm (STA) to know when there is a Layer2 Switch loop in network and determines which of the redundant ports needs to be shut down.

402. What is the destination MAC address used by Bridge Protocol Data Units (BPDUs)?

Bridge Protocol Data Units (BPDUs) frames are sent out as multicast messages regularly at multicast destination MAC address 01:80:c2:00:00:00.

403. What are the different types of BPDUs?

Three types of Bridge Protocol Data Units (BPDUs) are

1. Configuration BPDU (CBPDU),
2. Topology Change Notification (TCN) BPDU
3. Topology Change Notification Acknowledgment (TCA) BPDU

404. What is the basic purpose of the BPDUs and STA?

The basic purpose of the Bridge Protocol Data Units (BPDUs) and the Spanning Tree Algorithm (STA) is to avoid Layer2 Switching loops and Broadcast storms.

405. What is Switch Priority Value (Bridge Priority)?

• Every Switch Participating in a Spanning Tree Protocol network is assigned with a numerical value called Switch Priority Value.

• Switch Priority Value is a 16-bit binary number.

• The Switch Priority, which is a numerical value defined by IEEE 802.1D, which is equal to 32,768 by default.

• Switch Priority value decides which Switch can become Root Bridge (Root Switch).

• The Switch Priority value is used to find the Switch ID.

406. What is Switch ID (Bridge ID)?

• Switch ID decides which Switch can become Root Switch. A Switch with lowest Switch ID will become the Root Switch.

The Switch ID (Bridge ID) is made from two values.

• The Switch Priority which is a numerical value defined by IEEE 802.1D, which is equal to 32,768 by default.

• The MAC Address of the Switch.

407. What is Root Switch (Root Bridge)?

The main function of the root switch is to broadcast network topology changes to all the switches in the network.

• When a switch detects a topology change (i.e., a trunk goes down) it sends a topology change notification (TCN) BPDU to the root switch. The root switch then broadcasts that topology change out to the other switches.

408. How Root bridge is elected?

The bridge ID is used to elect the root bridge in the STP domain. This ID is 8 bytes long and includes both the priority and the MAC address of the device.

Switch with the lowest Bridge ID is elected as the Root bridge which means Switch with the lowest priority will become Root Bridge if two or more switches have same priority than switch with lowest mac address will become Root Bridge.

409. What are STP Timers and Explain different types of STP Timers?

STP uses three timers to make sure that a network converges properly before a bridging loop can form.

Hello timer - The time interval between Configuration BPDUs sent by the root bridge. It is 2 seconds by default.

Forward Delay timer - The time interval that a switch port spends in both the Listening and Learning states. The default value is 15 seconds.

Max (Maximum) Age timer - Maximum length of time a BPDU can be stored without receiving an update. It can also be define as a time interval that a switch stores a BPDU before discarding it. It is 20 seconds by default.

410. What are the different port states?

1. **Disabled -** A port in the disabled state does not participate in the STP.

2. **Blocking -** A blocked port does not forward frames. It only listens to BPDUs. The purpose of the blocking state is to prevent the use of looped paths.

3. **Listening -** A port in listening state prepares to forward data frames without populating the MAC address table. The port also sends and listens to BPDUs to make sure no loops occur on the network.

4. **Learning -** A port in learning state populates the MAC address table but doesn't forward data frames. The port still sends and receives BPDUs as before.

5. **Forwarding -** The port now can send and receive data frames, collect MAC addresses in its address table, send and receive BPDUs. The port is now a fully functioning switch port within the spanning-tree topology.

411. Explain types of STP Port Roles?

Root port - The root port is always the link directly connected to the root bridge, or the shortest path to the root bridge. It is always on Non-Root Bridge.

Designated port - A designated port is one that has been determined as having the best (lowest) cost. A designated port will be marked as a forwarding port. It can be on both Root Bridge & Non Root Bridge. All ports of Root Bridge are Designated Port.

Alternate port - A blocked port is the port that is used to prevent loops. It only listens to BPDUs. Any port other than Root port & designated port is a Block Port.

412. What is Extended System ID?

The Extended System ID is utilized by spanning-tree to include the VLAN ID information inside 16-bit STP Bridge Priority value. Extended System ID is the least significant 12-bits in 16-bit STP Bridge Priority value.

413. What is Path Cost or Spanning Tree Path Cost value?

The Spanning Tree Cost Value is inversely proportional to the bandwidth of the link and therefore a path with a low cost value is more preferable than a path with high cost value.

Link Bandwidth	Cost Value
10 Gbps	2
1 Gbps	4
100 Mbps	19
10 Mbps	100

414. Why spanning tree BPDU filter is used?

BPDU filter is a feature used to filter sending or receiving BPDUs on a switchport.....Enabling BPDU filtering in the interface level stops sending or receiving BPDU on this interface.

415. Explain store and forward Layer 2 Forwarding.

Store-and-forward switching is one of three primary types of LAN switching. With the store-and-forward switching method, the LAN switch copies the entire frame onto its onboard buffers and computes the cyclic redundancy check (CRC). Because it copies the entire frame, latency through the switch varies with frame length.

The frame is discarded if it contains a CRC error, if it's too short (less than 64 bytes including the CRC), or if it's too long (more than 1,518 bytes including the CRC). If the frame doesn't contain any errors, the LAN switch looks up the destination hardware address in its forwarding or switching table and determines the outgoing interface. It then forwards the frame toward its destination.

416. What is PVST or PVST+?

Per-VLAN spanning tree protocol plus (PVST+) is a Cisco proprietary protocol that expands on the Spanning Tree Protocol (STP) by allowing a separate spanning tree for each VLAN.

Cisco first developed this protocol as PVST, which worked with the Cisco ISL trunking protocol, andthen later developed PVST+ which utilizes the 802.1Q trunking protocol.

417. What is the working of PVST or PVST+?

By creating a separate spanning tree for each VLAN, data traffic from the different VLANs can take different paths across the network, as opposed to all switched traffic taking the same path. This can effectively create a load balancing situation and improve network efficiency.

By default the Cisco switches in Packet Tracer appear to be using PVST+ as the default implementation of spanning tree protocol.

418. What is RSTP?

Rapid Spanning Tree Protocol (RSTP) is an enhancement of the original STP 802.1D protocol. The RSTP 802.1w protocol is an IEEE open implementation.

419. What is Rapid-PVST+?

Cisco has its own proprietary implementation of RSTP, that includes the benefits of its Per-VLAN spanning tree protocols, called Rapid-PVST+.

420. What is the working of RSTP and Rapid-PVST+?

Rapid-PVST+ and RSTP are important enhancements to the original STP protocol because they can switch ports from blocking to forwarding without relying on timers, execute spanning tree calculations and converge the network faster than STP.

In STP, network convergence can take up to 50 seconds, with RSTP and Rapid-PVST+ network convergence can happen in just over 6 seconds.

Points to remember-

- STP is also called IEEE 802.1D
- STP is used to avoid loops
- Ethernet has no capacity for detecting loops.If a loop exist,broadcast storm will appear
- STP prevents loop formation by detecting redundant links and disabling them until needed.
- STP is enabled by default in switches
- STP works by selecting a switch in the network as a root bridge
- A STP network must select
    - One root bridge
    - One root port per non-root bridge
    - One designated port per network segment
- **Designated port (DP) :** All ports in root bridge must be DP.All designated ports will be in forwarding state
- **Root Port (RP) :** Root port is the port in the non-root bridge that connects the best path to root bridge
- **Blocked port (BP) :** Such ports will be in blocked state.it will receive informations from Designated ports but will not send any information through it
- One end of every link must be designated port.Other end may be Blocked Port OR Root Port

421. What is Loop Guard?

Loop Guard keeps track of the BPDU activity on non-designated ports. It does not allow non-designated ports to become designated ports in case of sudden loss of BPDUs. While BPDUs are received, the port is allowed to behave normally. When BPDUs go missing, Loop Guard moves the port into the loop-inconsistent state (port is effectively blocking at this point to prevent a loop from forming and to keep it in the non-designated role). When BPDUs are received on the port again, Loop Guard allows the port to move through the normal STP states and become active.

It can be enabled on both interface & global level. It affects per vlan basis.

Switch(config)# spanning-tree loopguard default

Switch(config-if)# spanning-tree guard loop

VLAN Interview Questions and Answer

422. What is SVI ?

A Switched Virtual Interface (SVI) is a virtual LAN (VLAN) of switch ports represented by one interface to a routing or bridging system. There is no physical interface for the VLAN and the SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN.

423. Which switching technology reduces the size of a broadcast domain?

VLAN's [virtual LAN's]

424. what is meant by "router on stick" ?

Router-on-a-stick is a term frequently used to describe a setup up that consists of a router and switch connected using one Ethernet link configured as an 802.1q trunk link. In this setup, the switch is configured with multiple VLANs and the router performs all routing between the different networks/VLANs.

425. which is the default mode in switch ports ?

Dynamic Auto

426. On a multilayer Catalyst switch, which interface command is used to convert a Layer 3 interface to a Layer 2 interface?

Switch (config-if)# switchport

427. Which protocols are used to configure trunking on a switch?

DTP [Dynamic Trunking Protocol

428. Explain difference between 802.1Q and ISL ?

single communication link called trunk is used between devices to carry traffic which may belong to multiple VLANS. We can configure the device to allow or deny particular VLAN through the trunk by its VLAN identifier.

VLAN identifier is a special tag that is encapsulated in a Ethernet frame. There are two main types of encapsulation protocols called ISL (Inter Switch Link) which is Cisco proprietary protocol and 802.1q which is an IEEE Standard.

ISL

- ISL is an Cisco proprietary protocol.

- Supports up to 1000 Vlans
- Original frame is encapsulated and a new header is inserted during encapsulation process.
- A 26 byte header and a 4 byte FCS (frame check sequence) are inserted. Hence a total of 30 Bytes of overhead.
- ISL tags frames from native Vlans.
- ISL is less preferred in networks because of its high overhead value which is added to each Ethernet frame.

802.1 q

- It is an IEEE Standard.
- 802.1q supports 4096 Vlans.
- IN 802.1q encapsulation process, a 4 byte tag is inserted into original frame and FCS (Frame Check Sequence) is re-calculated.
- 802.1q does not tag frames from native Vlans.

429. What is a Native VLAN and What type of traffic will go through Native VLAN?

The native VLAN is the only VLAN which is not tagged in a trunk, in other words, native VLAN frames are transmitted unchanged. Per default the native VLAN is VLAN 1 but you can change

430. What is Inter-Vlan Routing?

Layer 2 switches cannot forward traffic between VLANs without the assistance of a router. Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.

431. Two Switches are in VTP Server mode with different VLAN's. Revision Number of both the switches is 0. Which switch will overwrite his own VLAN Database onto other, if both switches are in the same VTP Domain?

The one where you make a change first; Both switches do nothing until you add or remove any vlans so that revision number goes up; then that switch will push vlans onto the other one.

432. If a Switch is in Client mode, Can we enter into the configuration mode ?

Yes

VTP Interview Questions and Answers

433. What is VTP?

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used by Cisco switches to exchange VLAN information. VTP is used to synchronize VLAN information (Example:-VLAN ID or VLAN Name) with switches inside the same VTP domain.

435. What are different VTP modes?

VTP Server mode - By default every switch is in server mode. Switch in VTP Server Mode can create, delete VLANs and will propagate VLAN changes.

VTP Client mode - Switch in VTP client mode cannot create or delete VLANs. VLAN Trunking Protocol (VTP) client mode switches listen to VTP advertisements from other switches and modify their VLAN configurations accordingly. It listens and forwards updates.

VTP Transparent mode - Switch in VTP Transparent mode does not share its VLAN database but it forwards received VTP advertisements. we can create and delete VLANs on a VTP transparent switch but these changes are not sent to other switches.

436. What are the requirements to exchange VTP messages between two switches?

- Switch should be configured as either a VTP server or VTP client.
- .VTP domain name must be same on both switches.
- VTP versions must match.
- link between the switches should be a trunk link.

437. What is VTP Pruning ?

VLAN Trunking Protocol (VTP) pruning is a feature in Cisco switches, which stops VLAN update information traffic from being sent down trunk links if the updates are not needed. Broadcast frames, multicast frames or unicast frames for which the destination MAC address is unknown are forwarded over a trunk link only if the switch on the receiving end of the trunk link has ports in the source VLAN. This avoids unnecessary flooding. VLAN 1 can never prune because it's an administrative VLAN.

Wan Interview Question and Answer

438. what is the difference between PPP and HDLC ?

HDLC	PPP
Operates at layer-2 (i.e. Data link layer)	Operates at layer-2 and layer-3 (i.e. network layer)
bit oriented protocol	byte oriented protocol
It does not have method to detect the errors.	It uses FCS to detect the errors while transmitting the data.
HDLC protocols have two types viz. ISO HDLC and Cisco HDLC	It uses HDLC format as defined by ISO.
It supports both synchronous and asynchronous links.	Supports synchronous, asynchronous, HSSI(high speed serial interface), ISDN links
It used to perform encapsulation of data without using other encapsulation protocols.	PPP can not encapsulate data without the help of other encapsulation protocols such as HDLC, SDLC(synchronous data link control)
It does not support authentication i.e. it fails to provide authentication between two nodes.	It supports authentication using protocols such as PAP and CHAP
It provides a frame format which contains a proprietary field. The other 6 fields are similar to PPP protocol frame fields. ISO HDLC do not have proprietary field and hence has only 6 fields.	It provides a frame format which contains a protocol field. The other 6 fields are similar to HDLC frame field.

It fails to check for quality of a link established.	**It uses link control protocol(LCP) to check for quality of the established link.**
HDLC frame format	**PPP , SLIP**

439. What is The Difference between PAP & Chap ?

Password Authentication Protocol -
PAPauthentication involves a two-way handshake where the username and password are sent across the link in clear text; hence, PAP authentication does not provide any protection against playback and line sniffing.

Challenge Handshake Protocol-
CHAP authentication, on the other hand, periodically verifies the identity of the remote node using a three-way handshake. After the PPP link is established, the host sends a "challenge" message to the remote node. The remote node responds with a value calculated using a one-way hash function. The host checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is terminated.

440. What is Virtual Circuit ?

As a WAN protocol, Frame Relay is most commonly implemented at Layer 2 (data link layer) of the Open Systems Interconnection (OSI) seven layer model. Two types of circuits exist: permanent virtual circuits (PVCs) which are used to form logical end-to-end links mapped over a physical network, and switched virtual circuits (SVCs). The latter are analogous to the circuit-switching concepts of the public switched telephone network (PSTN), the global phone network.

441. Can I use IP unnumbered with Frame Relay?

If you do not have the IP address space to use many subinterfaces, you can use IP unnumbered on each subinterface. You need to use static routes or dynamic routing for your traffic to get routed. And you must use point-to-point subinterfaces. For more information, refer to the Unnumbered IP over a Point-to-Point Subinterface Example section of Configuring Frame Relay.

442. Can I configure a Cisco router to act as a Frame Relay switch?

Yes. You can configure Cisco routers to function as Frame Relay data communication equipment (DCE) or network-to-network interface (NNI) devices (Frame Relay switches). A router can also be configured to support hybrid data terminal equipment/data communication equipment/permanent virtual circuit (DTE/DCE/PVC) switching. . For more information, refer to the Configuring Frame Relay section of the Cisco IOS Wide-Area Networking Configuration Guide, Release 12.1.

443. Can I bridge traffic over a Frame Relay link?

Yes. On multipoint interfaces, Frame Relay map statements must be configured using the frame-relay map bridge command to identify permanent virtual circuits (PVCs) for bridged traffic. Spanning(remove hyphen)Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) are passed at regular intervals depending on the bridging protocol configured.

444. Is a special configuration necessary to connect Cisco routers to other vendor devices over Frame Relay?

Cisco routers use proprietary Frame Relay encapsulation by default. The Internet Engineering Task Force (IETF) encapsulation format must be specified to interact with other vendor devices. The IETF encapsulation can be specified on an interface or per data-link connection identifier (DLCI) basis. For more information, refer to the Frame Relay Configuration Examples section of Configuring Frame Relay, in the Cisco IOS Wide-Area Networking Configuration Guide, Release 12.1.

445. What is Frame Relay AutoInstall and how does it work? Is an additional configuration required?

AutoInstall allows you to configure a new router automatically and dynamically. The AutoInstall procedure involves connecting a new router to a network in which an existing router is preconfigured, turning on the new router, and enabling it with a configuration file that is downloaded from a TFTP server. For more information, refer to Using Configuration Tools.

To support AutoInstall over a link on which the existing router is configured with a point-to-point subinterface, the frame-relay interface-dlci command requires additions. The additional information provided with the frame-relay interface-dlci command is used to respond to the Bootstrap Protocol (BOOTP) request of the remote router. The addition of protocol ipip-address to the command indicates the IP address of the main interface of a new router or access server onto which a router configuration file is to be installed over a Frame Relay network. Use this option only when the device acts as the BOOTP server for automatic installation over Frame Relay.

To support AutoInstall over a link on which the existing router is configured with a multipoint (sub) interface, the frame-relay map command should be configured on the existing router, mapping the IP address of the new router to the local data-link connection identifier (DLCI) used for connecting to the new router.

Apart from this, the Frame Relay (sub) interface of the existing router should be configured with the ip helper-address command pointing to the IP address of the TFTP server.

445. Is Frame Relay Inverse Address Resolution Protocol (IARP) on by default? The inverse-arp command does not show up in the configuration.

Yes.

446 Can Frame Relay Inverse Address Resolution Protocol (IARP) work without Local Management Interface (LMI)?

No. It uses LMI to determine which permanent virtual circuits (PVCs) to map.

447. Under what Local Management Interface (LMI) conditions does a Cisco router not send packets over the data-link connection identifier (DLCI)?

When the permanent virtual circuit (PVC) is listed as inactive or deleted.

448. Will a Cisco router process and map an Inverse Address Resolution Protocol (IARP) if it comes across while a data-link connection identifier (DLCI) is down?

Yes, but the router will not use it until the DLCI is active.

449. When implementing a show frame map command, data-link connection identifiers (DLCIs) are defined and active. This can occur when the DLCIs are not working. What does defined and active mean?

The message defined and active tells you that the DLCI can carry data and that the router at the far end is active.

450. Can I change subinterfaces from point-to-point to multipoint or the reverse?

No, after a specific type of subinterface is created, it cannot be changed without a reload. For example, you cannot create a multipoint subinterface Serial0.2, and change it to point-to-point. To change it, delete the existing subinterface and reload the router or create another subinterface. When a subinterface is configured, an interface descriptor block (IDB) is defined by the Cisco IOS® Software. IDBs defined for subinterfaces cannot be changed without a reload. Subinterfaces that are deleted with the no interface command are shown as deleted by issuing the show ip interface brief command.

451. What does illegal serial line type xxx mean?

This message is displayed if the encapsulation for the interface is Frame Relay (or High-Level Data Link Control [HDLC]) and the router attempts to send a packet containing an unknown packet type.

452. What are Forward Explicit Congestion Notification (FECN) and Backward Explicit Congestion Notification (BECN) packets? How do they affect performance?

This congestion notification is accomplished by changing a bit in the address field of a frame as it traverses the Frame Relay network. Network DCE devices (switches) change the value of the FECN bit to one on packets traveling in the same direction as the data flow. This notifies an interface device (DTE) that congestion avoidance procedures should be initiated by the receiving device. BECN bits are set in frames that travel the opposite direction of the data flow to inform the transmitting DTE device of network congestion.

Frame Relay DTE devices may choose to ignore FECN and BECN information or may modify their traffic rates based on FECN and BECN packets received. The frame-relay adaptive-shaping command is used when Frame Relay traffic shaping is configured to allow the router to react to

BECN packets. For information on how the router adjusts traffic rates in response to BECNs, refer to Traffic Shaping.

453.How can I improve performance over a slow Frame Relay link?

Poor performance over a Frame Relay link is generally caused by congestion on the Frame Relay network and from packets that are discarded while in transit. Many service providers only provide best effort delivery on traffic that exceeds the guaranteed rate. This means that when the network becomes congested, it discards traffic over the guaranteed rate. That action can cause poor performance.

Frame Relay traffic shaping allows traffic to be shaped to the available bandwidth. Traffic shaping is frequently used to avoid performance degradation caused by congestion packet loss. For a description of Frame Relay traffic shaping and configuration examples, refer to Frame Relay Traffic Shaping or the Frame Relay Traffic Shaping section of the Comprehensive Guide to Configuring and Troubleshooting Frame Relay.

To improve performance, refer to theConfiguring Payload Compression or Configuring TCP/IP Header Compression sections of Comprehensive Guide to Configuring and Troubleshooting Frame Relay.

454. What is Enhanced Local Management Interface (ELMI) and how is it used for dynamic traffic shaping?

ELMI enables automated exchange of Frame Relay Quality of Service (QoS) parameter information between the Cisco router and the Cisco switch. Routers can base congestion management and prioritization decisions on known QoS values such as committed information rate (CIR), committed burst (Bc), and excess burst (Be). The router reads QoS values from the switch and can be configured to use those values in shaping traffic. This enhancement works between Cisco routers and Cisco switches (BPX/MGX and IGX platforms). Enable ELMI support on the router by issuing the frame-relay qos-autosense command. For information and configuration examples, refer to the Enabling Enhanced Local Management Interface section of the Configuring Frame Relay and Frame Relay Traffic Shaping.

455. Can I reserve bandwidth for certain applications?

A recently developed Cisco feature called Class-Based Weighted Fair Queuing (CBWFQ) allows reserved bandwidth for different applications of flows depending on Access Control List (ACL) or incoming interfaces. For configuration details, refer to Configuring Weighted Fair Queueing.

456. Can I use priority queuing with Transmission Control Protocol (TCP) header compression over Frame Relay?

For the TCP header compression algorithm to function, packets must arrive in order. If packets arrive out of order, the reconstruction will appear to create regular TCP/IP packets but the packets

will not match the original. Because priority queuing changes the order in which packets are transmitted, enabling priority queuing on the interface is not recommended.

457. Can Frame Relay prioritize voice traffic carried in IP packets over non-voice packets?

Yes. The Frame Relay IP RTP Priority feature provides a strict priority queueing scheme on a Frame Relay private virtual circuit (PVC) for delay-sensitive data, such as voice, which is identified by its Real-Time Transport Protocol (RTP) port numbers. This feature makes sure that voice traffic is given strict priority over other non-voice traffic.

458. What is Frame Relay private virtual circuit (PVC) Interface Priority Queueing (PIPQ)?

The Frame Relay PVC Interface Priority Queueing (PIPQ) feature provides interface level prioritization by giving priority to one PVC over another PVC on the same interface. This feature can also be used to prioritize voice traffic over non-voice traffic when they are carried on separate PVCs on the same interface.

459. How is IP split horizon handled on Frame Relay interfaces?

IP split horizon checking is disabled by default for Frame Relay encapsulation to allow routing updates to go in and out of the same interface. An exception is the Enhanced Interior Gateway Routing Protocol (EIGRP) for which split horizon must be explicitly disabled.

Certain protocols such as AppleTalk, transparent bridging, and Internetwork Packet Exchange (IPX) cannot be supported on partially meshed networks because they require split horizon to be enabled (a packet received on an interface cannot be transmitted over the same interface, even if the packet is received and transmitted on different virtual circuits).

Configuring Frame Relay subinterfaces ensures that a single physical interface is treated as multiple virtual interfaces. This capability allows you to overcome split horizon rules so packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface.

460. Does Open Shortest Path First (OSPF) require additional configuration to run over Frame Relay?

OSPF treats multipoint Frame Relay interfaces as NON_BROADCAST by default. This requires that neighbors be explicitly configured. There are various methods for handling OSPF over Frame Relay. The one that is implemented depends upon whether the network is fully meshed. For more information, refer to the following documents:

Initial Configurations for OSPF over Non-Broadcast Links

Initial Configurations for OSPF over Frame Relay Subinterfaces

Problems with Running OSPF in Mode over Frame Relay

461. How can the bandwidth consumed by routing updates over Frame Relay be calculated?

Reliable estimates can only be calculated for distance vector protocols that send periodic updates. This includes Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP) for IP, RIP for Internetwork Packet Exchange (IPX), and Routing Table Maintenance Protocol (RTMP) for AppleTalk. A discussion of the bandwidth consumed by these protocols over Frame Relay can be found in the RIP and IGRP section of Configuring and Troubleshooting Frame Relay.

462. Why am I unable to ping my own interface address?

You cannot ping your own IP address on a multipoint Frame Relay interface. To make a ping successful on a serial interface, an Internet Control Message Protocol (ICMP) echo request packet must be sent, and an ICMP echo reply packet must be received. Pings to your own interface address are successful on point-to-point subinterfaces or high-level data link control (HDLC) links because the router on the other side of the link returns the ICMP echo and echo reply packets.

The same principle also applies with multipoint (sub) interfaces. To successfully ping your own interface address, another router must send back the ICMP echo request and the echo reply packets. Because multipoint interfaces can have multiple destinations, the router must have Layer 2 (L2) to Layer 3 (L3) mapping for every destination. Because mapping is not configured for our own interface address, the router does not have any L2 to L3 mapping for its own address and does not know how to encapsulate the packet. That is, the router does not know which data-link connection identifier (DLCI) to use to send echo request packets to its own IP address resulting in encapsulation failure. To be able to ping its own interface address, a static mapping must be configured pointing towards another router over the Frame Relay link which can send back the ICMP echo request and reply packets.

463. Why am I unable to ping from one spoke to another spoke in a hub and spoke configuration using multipoint (sub) interfaces?

You cannot ping from one spoke to another spoke in a hub and spoke configuration using multipoint interfaces because the mapping for the other spoke's IP address is not done automatically. Only the hub's address is automatically learned by way of Inverse Address Resolution Protocol (INARP). If you configure a static map using the frame-relay map command for the IP address of another spoke to use the local data-link connection identifier (DLCI), you can ping the address of the other spoke.

464. What is the Frame Relay broadcast queue?

The Frame Relay broadcast queue is a major feature used in medium to large IP or Internet Package Exchange (IPX) networks in which routing and Service Advertising Protocol (SAP) broadcasts must flow across the Frame Relay network. The broadcast queue is managed independently of the normal interface queue, has its own buffers, and a configurable size and service rate. Due to timing

sensitivities, Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) are not transmitted using the broadcast queue.

Wireless Interview Questions and Answers

465. What is Wi-Fi?

Wi-Fi is a technology that uses radio waves to provide network connectivity. A wi-fi connection is established using a wireless adapter to create hotspots - areas in the vicinity of a wireless router that are connected to the network and allow users to access internet services. Once configured, wifi provides wireless connectivity to your devices by emitting frequencies between 2.4 GHz - 5 GHz, based on the amount of data on the network.

466. What is a Wi-Fi hotspot?

A hotspot is a physical location where people may obtain internet access, typically using wi-fi technology, via a wireless local area network (Wlan) using a router connected to an internet service provider.

467. What are IBSS and BSS?

Independent Basic Service Set (IBSS) allows two or more devices to communicate directly with each other without a need for a central device.

Basic Service Set (BSS) wireless LAN is established using a central device called an Access Point that centralizes access and control over a group of wireless devices.

468. Why WPA encryption is preferred over WEP?

A) Encryption is preferred over WEP.

B) The access point and the client are manually configured with different WPA key values.

C) Wep Key values remain the same until the client configuration is changed.

D) The values of WPA keys can change dynamically while the system is used.

469. What is 802.1x and EAP?

IEEE 802.1x is an IEEE standard for port-based network access control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or Wlan.

470. Name two devices can interfere with the operation of a wireless network because they operate on similar frequencies?

1. Microwave oven
2. Cordless phone

471. What are three basic parameters to configure on a wireless access point?

1. SSID
2. RF
3. Channel authentication method

472. What is the maximum data rate specified for IEEE 802.11b wlan?

11 mbps

473. Which encryption type does wpa2 uses?

WPA uses Tkip and wpa2 uses AES, but in summary Tkip is an older encryption standard used by the old WPA standard. AES is a newer wi-fi encryption solution used by the new-and-secure wpa2 standard. In theory, that's the end of it 317 and 802.1b is being utilized in the wireless network.

474. How does DHCP work with the Wireless?

The wireless is designed to act as a dhcp relay agent to the external dhcp server and acts like a dhcp server to the client. This is the sequence of events that occurs: Generally, wlan is tied to an interface which is configured with a dhcp server. When the wireless receives a dhcp request from the client on a wlan, it relays the Request to the dhcp server with its management ip address. The wireless shows its virtual ip address, which must be a non−routable address, usually configured as 192.168.0.1, as the dhcp server to the client.

475. Which two wireless encryption method are based on RC4 encryption algorithm?

1. Wep
2. Tkip

476. Which Spread spectrum technology does the 802.11b standard define for operation ?

DSSS

477. Which is the minimum parameter need on the access point in order to allow a wireless client to operate on it ?

SSID ,RF channel ,authentication method

478. What is the function of wlan on wireless?

Wlan is similar to that of ssid in the access point. It is required for a client to associate with its wireless network.

479. What is sneakernet?

Sneakernet is an informal term describing the transfer of electronic information by physically moving media such as magnetic tape, floppy disks, compact discs, USB flash drives or external hard drives from one computer to another; rather than transmitting the information over a computer network.

480. How do WLCs support oversized access points?

Controller software release 5.0 or later allows you to upgrade to an oversized access point image by automatically deleting the recovery image to create sufficient space. This feature affects only access points with 8 MB of flash (the 1100, 1200, and 1310 series access points). All newer access points have a larger flash size than 8 MB. As of August 2007, there are no oversized access point images, but as new features are added, the access point image size will continue to grow.

481. Does Layer 3 mobility work with an access point (AP) Group VLAN configuration?

Yes, Layer 3 mobility works with an AP Group VLAN configuration. Currently, traffic sources from a Layer 3 roamed wireless client is put on the dynamic interface assigned on the WLAN or the interface of the AP Group VLAN..

482. Why are our access points (APs) that are registered to other WLCs that are in the same RF group shown as rogues?

A. This can be due to Cisco bug ID CSCse87066 (registered customers only) . LWAPP APs in the same RF group are seen as rogue APs by another WLC for one of these reasons:

- The AP sees more than 24 neighbors. The neighbor list size is 24, so the 25th AP is reported as a rogue.
- AP1 can hear the client that communicates to AP2, but AP2 cannot be heard. Therefore, it cannot be validated as a neighbor.

The workaround is to manually set the APs to known internal on the WLC and/or WCS. Complete these steps on the WLC in order to manually set the APs to known internal:

1. Go to the WLC GUI and choose **Wireless**.
2. Click **Rogue Aps** in the left side menu.
3. From the Rogue-AP list, choose the specific access point and click**Edit**.
4. From the Update Status menu, choose **Known internal**.
5. Click **Apply**. This bug is fixed in version 4.0.179.11.

483. Wireless LAN Clients associated with the lightweight access points are not able to get IP addresses from the DHCP server. How do I proceed?

A. The DHCP server for a client is usually marked on the interface, which maps to the WLAN to which the client. Check if the interface is configured appropriately.

484. Is there any way to recover my password for WLC?

A. If you forget your password in WLC version 5.1 and later, you can use the CLI from the controller's serial console in order to configure a new user name and password. Complete these steps in order to configure a new user name and password.

1. After the controller boots up, enter **Restore-Password** at the user prompt.

Note: For security reasons, the text that you enter does not appear on the controller console.

2. At the Enter User Name prompt, enter a new user name.
3. At the Enter Password prompt, enter a new password.
4. At the Re-enter Password prompt, re-enter the new password.

The controller validates and stores your entries in the database.

5. When the User prompt reappears, enter your new username.
6. When the Password prompt appears, enter your new password.

The controller logs you in with your new username and password.

Note: For WLCs that run earlier versions of firmware (prior to 5.1), there is no way to recover the password. If you use the Cisco Wireless Control System (WCS) in order to manage the WLC, wireless LAN controller Module (WLCM) or Wireless Services Module (WiSM), you should be able to access the WLC from the WCS and create a new administrative user without logging into the WLC itself. Or, if you did not save the configuration on the WLC after you deleted the user, then a reboot (power cycling) of the WLC should bring it back up with the deleted user still in the system. If you do not have the default admin account or another user account with which you can log in, your only option is to default the WLC to factory settings and reconfigure it from scratch.

For mre wireless Interview Question please refer - https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/69561-wlc-faq.html

FHRP Interview Questions And Answer

485. What is the use of HSRP?

A: HSRP[Hot Standby Routing Protocol] is used to provide default gateway redundancy.

486. What is the maximum number of HSRP groups can be created in the router?

A: Maximum 16 groups.

487. What is the HSRP virtual MAC address

A: 0000.0c07.acxx

488. What are the maximum number of routers can be present in a group?

A: Maximum 16 routers can be present in a group.

489. HSRP uses TCP or UDP?

HSRP uses UDP port number 1985

490. What is the Source IP & Destination IP address of HSRP Hello message?

Source IP address = IP address of the Primary Interface

Destination IP address = 224.0.0.2

491. Is it possible to configure HSRP on Multi Layer Switch (MLS) ?

A: Yes it is possible to configure HSRP on MLS (3560) switches...

492. What are the HSRP default Hello and Hold Down Timers?

A: Hello Timer = 3 seconds

Hold Down Timer = 10 seconds

493. What is the difference between Active and Standby router in HSRP?

A: Active Router: Router which is responsible to forward the data

Standby Router: Router which is the backup to active router.

494. What is the difference between HSRP version 1 and HSRP version 2?

A: 1) HSRP version 1 supports 256 groups ranging from 0 to 255, HSRP version 2 supports 4096 groups ranging from 0 to 4095

2) HSRP vesion 1 uses multicast address for sending hello messages is 224.0.0.2, HSRP version 2 uses multicast address for sending hello messages is 224.0.0.102

3) HSRP version 1 and Version 2 are having different virtual mac addresses.

4) HSRP version 2 allows support for IPV6 whereas HSRP version 1 does not support.

495. If active router LAN interface is up but line protocol is down, In this case whether standby router will become active router?

A: Yes standby router will become as Active router if the interface is up but line protocol is down..

496. What is the default priority and default group number for HSRP?

A: Default Priority: 100
Default Group number: 0

497. If you perform traceroute, which ip address you will see in the reply (Physical or virtual IP)?

A: Physical IP address.

498. How many states present in HSRP?

A: 6 states present in HSRP

- Initial
- Learn
- Listen
- Speak
- Standby
- Active

499. What are Differencs betwenn HSRP VRRP & GLBP ?

Feature	VRRP	HSRP	GLBP
Router Role	1 master1 (or more) backup	1 active1 standby 1 or more listening	1 AVG2 (or more) AVF
IP Address	Real	Virtual	Virtual
Election	1 – highest priority 2 – highest IP (tiebreaker)	1 – highest priority 2 – highest IP (tiebreaker)	1 – highest priority 2 – highest IP (tiebreaker)
Load Balancing	No	No	Yes
Cisco proprietary	No (IEEE standard)	Yes	Yes

500. What Is GLBP ?

GLBP stands for Gateway Load Balancing Protocol and just like HSRP / VRRP it is used to create a virtual gateway that you can use for hosts. One of the key differences of GLBP is that it can do load balancing without the group configuration that HSRP/VRRP use .

501. What is the Difference Between AVG & AVF ?

All devices running GLBP will elect an AVG (Active Virtual Gateway). There will be only one AVG for a single group running GLBP but other devices can take over this rule if the AVG fails. The role of the AVG is to assign a virtual MAC address to all other devices running GLBP. All devices will become an AVF (Active Virtual Forwarder) including the AVG. Whenever a computer sends an ARP Request the AVG will respond with one of the virtual MAC addresses of the available AVFs. Because of this mechanism all devices running GLBP will be used to forward IP packets.

502. What are methods of GLBP Load Balancing?

There are multiple methods for load balancing:

- **Round-robin:** the AVG will hand out the virtual MAC address of AVF1, then AVF2, AVF3 and gets back to AVF1 etc.
- **Host-dependent**: A host will be able to use the same virtual MAC address of an AVF as long as it is reachable.
- **Weighted**: If you want some AVFs to forward more traffic than others you can assign them a different weight.

503. What address Does GLBP Messages Uses ?

GLBP routers use the local multicast address 224.0.0.102 to send hello packets to their peers every 3 seconds over UDP 3222.

504. What address does VRRP messages Uses?

Multicast IP address 224.0.0.18 and IP protocol number 112.

505. What is the VRRP virtual MAC address.

It uses 00-00-5E-00-01-XX as its Media Access Control (MAC) address. The last byte of the address (XX) is the Virtual Router IDentifier (VRID), which is different for each virtual router in the network. This address is used by only one physical router at a time, and it will reply with this MAC address when an ARP request is sent for the virtual router's IP address.