NETWORK

Engineer's

Handbook

By PCB

www.gmfaruk.com

❖ OSI (Open system interconnect)

1.Explain OSI Layer?

- Open system interconnect (OSI) was developed by the international organization for standardization (ISO) and introduced in 1984.
- It's a consists of seven layers
- Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data link layer, Physical layer.

2.Which Layer is Responsible for Reliable Connection?

The **transport layer** guarantees a reliable end-to-end connection

3.What are Different protocol works at each of the Layer in OSI model?

Application layer

It's responsible for providing an interface for the user to interact with application services or network services. Ex-Web browser (HTTP), Telnet

Presentation layer

It's responsible for defining a standard format to the data.
The major functions described at this layer are: -
Encoding-Decoding Ex- AVI-(video), WAV-(voice), JPEG (graphite), ASCII (text)
Encryption-Decryption

Session layer

It's responsible for establishing, maintaining, and terminating the sessions.
Session ID is used to identify a session or interaction.
Ex-Remote procedural call, Apple talk session protocol

Transport Layer

It provides data delivery mechanism between applications in the network.
Transport layer is the major function layer In OSI layer
Identifying service
Multiplexing&De-multiplexing
Segmentation, Error correction, flow control
Transport layer protocols?
The protocols which takes care of data transport at transport layer are TCP/UDP

Different between TCP/UDP

TCP		UDP
Transmission Control Protocol	← →	User datagram protocol
Connection Oriented	← →	Connection less
Support acknowledgements	← →	No support for acknowledgements
Reliable communication	← →	Unreliable communication
Protocol no.6	← →	Protocol no.17
Ex-HTTP, FTP, SMTP	← →	DNS, DHCP, TFTP

Network Layer

It provides logical addressing path determination (routing)
The protocols that work in this layer are: -Routed Protocol, Routing Protocol
Routed Protocols→Used to carry user data between data.
Routing Protocols→used performs path determinisation routing.

Data link layer

It provides communication with network layer.
Mac (media access control) it provides reliable transit of data across a physical link.

Physical layer

It defines the electrical, mechanical functional specification for communication between the network devices.

5.What is the port number and give some example?

A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit.

- **FTP**-File Transfer Protocol (TCP-20,21)
- **SSH**-Secure Shell SSH Secure Login (TCP-22)
- **Telnet** remote login service, unencrypted text messages (23)
- **SMTP**-Simple Mail Transfer Protocol E-mail routing (TCP-25)
- **DNS**-Domain Name System (TCP/UDP-53)
- **DHCP**-Dynamic Host Configuration Protocol IP-(67server)-68(client).
- **HTTP**-Hypertext Transfer Protocol (TCP-80) used in the World Wide Web (TCP-80)
- **POP3**-Post Office Protocol POP3 (TCP-110)
- **NTP**-Network Time Protocol (UDP-123)
- **SNMP**-Simple Network Management Protocol (UDP-161/162)
- **HTTPS**- Secure (HTTPS) HTTP over TLS/SSL(TCP-443)

6.What is the range of port Number?

Well known Ports – 0 to 1023
Registered Ports-1024 to 49151
Open Poerts-49152 to 65535

7.What is a Protocol Number and give some examples?

The protocol number is a single byte in the third word of the datagram header. The value identifies the protocol in the layer above IP to which the data should be passed.

Protocol **Protocol Number**

- ICMP----------1
- IGMP----------2
- IPV4----------4
- TCP----------6
- EGP----------8
- IGP----------9
- UDP----------17
- IPV6----------41
- GRE----------47
- EIGRP----------88
- OSPF----------89
- BGP----------179

8.What is the Unicast, Multicast and Broadcast?

Unicast

In computer networking, unicast is a one-to-one transmission.

Multicast

In computer networking, multicast is group communication.

Broadcast

In computer networking, one-to-many

9.What is the different between Half-duplex and Full duplex?

Half Duplex-Data can flow in both direction but not simultaneously. At a time, Data can flow only in one directional Ex-HUB.

Full Duplex-Data can flow both directional simultaneously-Switch.

10.What is the MAC format?

It is a 12 Digits 48 Bit(6byte) Hardware address written in Hexadecimal format.

It consists of two parts: -

- The first 24 Bits OUI (Organizationally Unique Identifier) is assigned by IEEE.
- The last 24 Bits is Manufacturing-assigned Code.

11.What is a Frame?

The Data link layer formats the message into pieces, each called a data frame and adds a customized header containing the hardware source and destination address.

12.What is the TCP/IP Model?

TCP/IP is four-layer standard model.

The four layers of TCP/IP model are: -Application layer, Transport layer, internet layer, Network access layer.

13.What are the protocols that are include by each layer of the TCP/IP model?

- **Application layer**-DNS, DHCP, FTP, TFTP, SMTP, HTTP,Telnet,SSH.
- **Transport layer**-TCP, UDP
- **Internet layer**-IP, ICMP, IGMP
- **Network access layer-**Ethernet, Token Ring, FDDI,X.25,Frame Relay,ARP,RARP.

❖ ARP (Address Resolution Protocol)

14.What is the 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.

15.ARP work at Which layer and Why?

ARP work at the data link layer (layer 2) ARP Is implemented by the network protocol driver and its packets are encapsulated by ethernet headers and transmitted.

16.What is an ARP Table(cache)?

An ARP cache is a collection of Address Resolution Protocol entries (mostly dynamic) that are created when an IP address is resolved to a MAC address (so the computer can effectively communicate with the IP address)An ARP cache helps the attackers hide behind a fake IP address.

17.What is the size of an ARP request and ARP reply packet?

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

18.What is Proxy ARP?

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

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

21.What is Reverse ARP?

Reverse ARP is used to obtain the device's IP address when its MAC address is already known.

22.What is Inverse ARP?

Inverse ARP dynamically maps local DLCIs to remote IP address when frame Relay is configured.

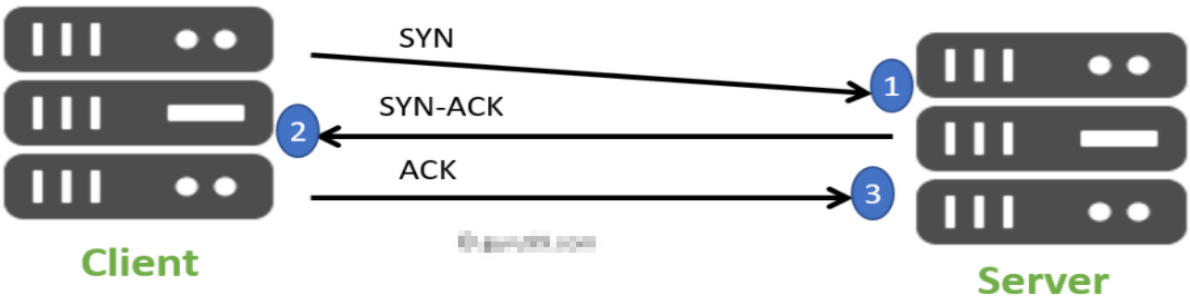
❖ TCP (Transmission Control Protocol)

23.What is (Transmission Control Protocol) TCP?

It is one of the most used protocols within digital network communications and ensures end-to-end data delivery. TCP organizes data so that it can be transmitted between a server and a client. It guarantees the integrity of the data being communicated over a network.

24.Explain TCP Three-Way handshake process?

TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.



3 way Handshake Diagram

25.What is the propose of RST bit?

When the connection is not allowed by destination connection is reset

26.What are the 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 receiver's application. If data is to be send on the immediate basic, we will push it.
- **2.Reset (RST)-** It Reset the connection.
- **3.Finish (FIN)-** It Finishes the session. It means No More Data form the sender.
- **4.Urgent (URG)-** It is used to set the priority to tell the receiver that this data is important for you.
- **5.Acknowlagement**- (ACK)-All packets after SYS packet sent by the 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 initiated a connection. It Synchronize sequence number.

28.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 send during a TCP session. By sequence number, the sender can be assured that the receiver received the data because the receiver uses this sequence number as the acknowledgement number in the next segment it sends to acknowledge the received data. When the TCP session starts, the initial sequences number can be any number in the range of 0-4294967295.
- Acknowledgement number is used to Acknowledge the received data and is equal to the received sequence number plus 1.

29.Which is the importance of the identification field in the IP Packets?

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

30.What is the MTU (Maximum Transmission Unit)?

A maximum transmission unit (MTU) is the largest packet or frame size, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network such as the internet. The internet's transmission control protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission.

31.What is the Fragmentation?

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

32.How the packet is reassembled?

IP fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size. The fragments are reassembled by the receiving host.

33.What is the Importance of DF, FM Flag?

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 fragment the packet or discards it.

34.What is the purpose of a fragment offset?

It is used to define the size of each fragmentation packet.

35.What is the important 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, the TTL value is decremented by 1. When this field become zero, the datagram is discarded. This behaviour helps prevent routing loops. The typical value for a TTL field is 32 or 64.

❖ Routing

37.What is the Routing?

The function of routing is to route packet between networks that are not locally attached.

38.What is the Router?

- It's is a device which enables communication between two or more different logical network.
- It's a network layer-3 device.

39.What are the different types of Memory in the router?

- **RAM**-Running configuration file: running -config is store in RAM.
- **NVRAM**-Start-up configuration file: start-up configuration is stored in NVRAM
- **Flash Memory**-IOS is stored in Flash memory
- **ROM**-Instruction for Post, Bootstrap, Mini-IOS is Stored in ROM

40.What are the possible location of IOS Image?

- FLASH and TFTP Server.

41.What are different modes in the router?

User mode: -

- Only some basic monitoring and limited show commands work in this mode.
- Ex-Enable, ping, traceroute, etc. Router>

Privilege mode: -

- Monitoring Troubleshooting and verification commands work in this mode.
- Ex-show, configure terminal, write, etc Router#

Global Configuration mode: -

- Global Configuration made in this mode affects the operation of the device.
- Ex-Hostname, etc. Router(config)#

42.What is the command to reboot a router?

- #reload

43.What is the command to backup IOS to TFTP server?

- #copy flash tftp

44.What is the command to copy running config to startup config?

- #copy running-config start-up-config

45.Define static routing?

- In static routing, route manually configured on the router by network administrator

Advantages	Disadvantages
Secured	←→No automatic updates
Reliable	←→Need of destination network ID for the Configuration
Faster	←→Administrative work is more
No wastage of bandwidth	←→Used in small network

46.What is a default route?

A default route specifies a path that the router should take if the destination is unknow. All the IP datagrams with unknow destination address are send to default route.

47.What is a Dynamic routing?

In Dynamic routing, route is learned by using a routing protocols will learn about routers from other neighbouring router running the same routing protocol Ex-OSPF, EIGRP, BGP.

48.What is the Routed protocol?

A routed protocol carries data from one network to another network. Routed protocol carries user traffic such as file transfer, web traffic, e-mail.

Ex-IP, IPX and apple talk.

49.What is the Routing Protocol?

Routing protocols learn the routes and provide the best route from one network to another network. **Ex**-EIGRP, OSPF, RIP.

50.What is IGP?

An Interior Gateway Protocol refer to a routing protocol that handles routing a single autonomous system. **Ex**-RIP, EIGRP, OSPF.

51.What is EGP?

An Exterior Gateway Protocol refer to a routing protocol that handles routing between different Autonomous System (AS) Ex-Border Gateway Protocol (BGP).

52.What is an Autonomous System?

An Autonomous System (AS) is a group of networks under a single administrative control.

53.What is Administrative Distance?

Administrative Distance is the trustworthiness of a routing protocol. Routers use AD value to select the best path when there are two or more different routes to the same destination learned two different routing protocols.

54.What is the Range of AD Values?

- 0-255, Where 0 is the best and 255 is the worst.

Routing Protocol	Administrative Distance
Direct connect	→0
Static route -	→1
EIGRP (summary route)	→5
eBGP route	→20
EIGRP route	→90
OSPF route	→110
RIP route	→120
Exterior EIGRP	→170
iBGP	→200

55.What is Distance-Vector Routing Protocol?

Distance vector routing protocol use the distance or hops as the metric to find path to destination.

- **Ex**-RIP, EIGRP

56.What is Link-State Routing Protocol?

Link state routing is a technique in which each router shares the knowledge of its neighbourhood with every other router in the internetwork. Every router that receives the packet sends the copies to all its neighbours. Finally, each router receives a copy of the same information

- **Ex**-OSPF

57.What is Hybrid Routing Protocol?

Hybrid Routing Protocol (HRP) is a network routing protocol that combines Distance Vector Routing Protocol (DVRP) and Link State Routing Protocol (LSRP) features.

- **Ex**-EIGRP

58.What is a Routing Metric?

Routing Protocol uses route metric value to find the best path when there are two or more different route to the same destination.
Different routing protocols use route metric to compute the destination.

- **Ex**-RIP-Hop count, OSPF-Cost, EIGRP-Bandwidth, Delay, Reliability, Load, MTU.

59.What is Hop Count?

Hop count is the number of routers from the sources though which data must pass to reach the destination network.

60.What is Bandwidth, Delay, Reliability, Load?

- **Bandwidth**- It is the Data capacity of a link in Kbps.
- **Delay**- It is the time takes to reach the destination.
- **Reliability**- The path with the least amount of errors or downtime.
- **Load**- It is the amount of utilization of a path
- **MTU**- maximum transmission unit (MTU) define the maximum size of the packet that can be sent over a medium.

61. Define Bandwidth and Latency?

Bandwidth looks at the amount of data being transferred while latency looks at the amount of time it takes data to transfer. These two terms come together as throughput, which refers to the amount of data that is being transferred over a set period.

62.What is Cost?

Cost is the inverse proportion of bandwidth of the links.

63.What is CDP?

Cisco Discovery Protocol is a Cisco proprietary protocol to help administrators in collection about information both locally attached and remote devices.

❖ EIGRP (Enhanced Interior Gateway Routing Protocol)

64.Explain EIGRP Routing Protocol?

- 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. Is also considered as a hybrid routing protocol because it has characteristic of both Distance vector & Link State Routing Protocol.
- EIGRP support classless routing & VLSM, route summarization, incremental updates, load balancing and other future.

65.What are the requirement Neighborship in EIGRP?

The following field in a hello packet must for routers to become neighbours: -

- Autonomous System number
- K-values.
- Authentication.
- Primary address should be used.
- If static neighborship them should be define on both sides.

66.What table do EIGRP routers maintain?

EIGRP router stores routing and topology information in Three tables: -

- **Neighbour Table**- Store information about EIGRP neighbours.
- **Topology Table**- Store routing information which is learn from neighbours' routers.
- **Routing Table**- Store the best path to all networks.

70.Why no auto-summary command used in EIGRP?

By default ,EIGRP behaves like a classful routing protocol which means it does not advertise the subnet mask information along with the routing information .No auto-summary command will ensure that EIGRP sent the subnet mask information along with the routing information.

71.What metric does EIGRP used?

EIGRP calculated its metric by using Bandwidth, Load, Delay, Reliability and MTU.

72.What are the EIGRP Hello & Hold Timer?

- **Hello Timer**- Router will send a hello to its neighbours every 5 seconds (hello time)
- **Hold Timer**- If Router does not receive hello for 15 seconds (hold timer) then it will assume that link down and it will drop neighborship.

73.What is a Successor?

A successor is the best path to reach a destination in the topology table.

74.What is the Feasible successor?

A Feasible successor is the second-best path to reach a destination after successor. It acts as a backup for the successor.

75.What is the Feasible distance?

Feasible distance is the distance (metric) to reach the destination network. The route with this metric will be in the routing table as it is the best route to reach a remote(destination) Network.

76.What is advertised Distance & Reported Distance?

Advertised distance is the distance (metric) of a neighbour router to reach the destination network. This is the metric of a destination network as reported by a neighbour.

77.What authentication does EIGRP support?

EIGRP support only MD5 authentication.

78.What is the Formula EIGRP used to Calculate Metric?

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

79.What is the Different Administrative Distance that EIGRP used?

- Internal-90
- Extranal-170
- Summary -5

80.What is the EIGRP packet types?

Hello — Used for discovery of EIGRP neighbours and for detecting when a neighbour is no longer available

Request— Used to get specific information from one or more neighbours

Update— Used to transmit routing and reachability information with other EIGRP neighbours

Query—Sent out to search for another path during convergence

Reply—Sent in response to a query packet

81.What is the EIGRP named mode?

The named mode is the new way of configuring **EIGRP** this mode allows EIGRP configurations to be entered in a hierarchical manner under the router mode. Each named mode configuration can have multiple address families and autonomous system number combinations.

82.What is the EIGRP Passive interface?

With EIGRP running on a network, the passive-interface command stops both outgoing and incoming routing updates

83.What is EIGRP variance values?

EIGRP provides a mechanism to load balance over unequal cost paths through **Variance** Command. **Variance** is a number (1 to 128), multiplied by the local best metric then includes the routes with the lesser or equal metric. The default **Variance value** is 1, which means equal-cost load balancing.

84. What is the EIGRP Convergence?

Regarding convergence, EIGRP maintains a backup route. In case the current path to the destination network fails, it can immediately switch over to using the backup route, the feasible successor leading to faster convergence.

85. How do I fix EIGRP stuck in active?

EIGRP maintains a timer called “active timer” which has a default value of 3 minutes (180 seconds). EIGRP waits half of the active timer value (90 seconds) for a reply. If the router does not receive a response within 90 seconds, the originating router sends a stuck in active (SIA) query to EIGRP neighbours that did not respond

86. What is leak map in EIGRP?

The leak-map just allows you to advertise a specific prefix within the range of a summary advertisement, as well as the summary itself. Basically, all routers just have EIGRP 100 running & auto-summary disabled.

87. What is the EIGRP stub router?

Stub routing is an EIGRP feature primarily designed to conserve local router resources, such as memory and CPU, and improve network stability. The stub routing feature is most used in hub-and-spoke networks.

88.What is split horizon in EIGRP?

Split horizon is one of the methods used by distance vector routing protocols to avoid routing loops. The principle is simple – a router will not advertise a route back onto the interface from which it was learned. Split horizon is enabled on interfaces by default.

89.What multicast address does EIGRP used?

EIGRP router use the multicast address of 224.0.0.10

90.How Configure EIGRP?

- Router (Config)#router eigrp 100
- Router (Config-router) #network 172.16.1.0 0.0.0.255
- Router (Config-router) #network 10.16.1.0 0.0.0.255
- Router (Config-router) #no auto-summary

91.How to configuration EIGRP named mode?

- R1(Config)# router eigrp name IBM Hyd
- R1(Config-router) #address-family ipv4 autonomous-system 12
- R1(Config-router-af) # Network 192.168.12.0
- R1(Config-router-af)#af-interface Fastehternet 0/0

92.Tell me some commands to troubleshoot EIGRP?

- #show ip route → It Shows full Routing Table
- #show router ip eigrp → It Shows only EIGPR Routes
- #show ip eigrp neighbours → It Shows EIGPR Neighbours Table
- #show ip eigrp topology → It Shows EIGPR Topology Table

❖ OSPF (Open Shortest Path First)

93.What is the OSPF routing protocol?

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First (SPF). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/Backup Designated Router (BDR).

94.What is the area in OSPF?

An area is a logical collection of OSPF networks, routers, and links that have the same area identification. A router within an area must maintain a topological database for the area to which it belongs.

95.What is the Intra-area route?

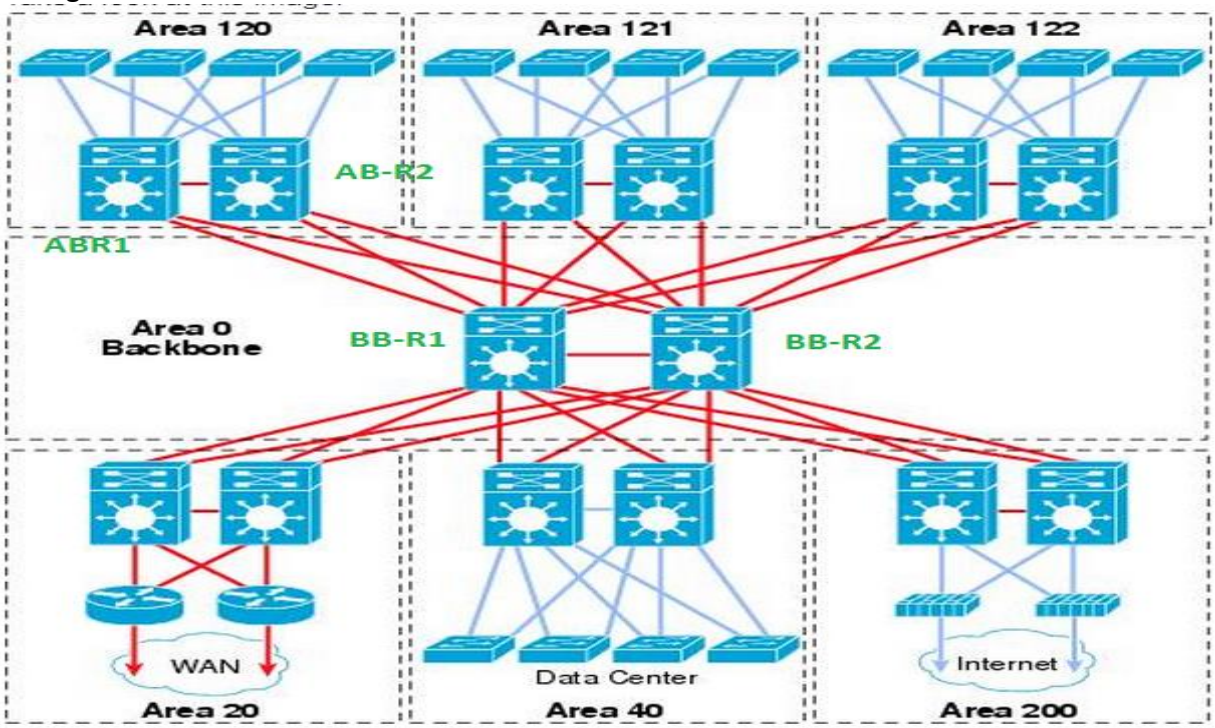
Intra-area routes refer to updates that are passed within the area.

96.What is an Area border router (ABR)?

An area border router is in the OSPF boundary between two areas. Both sides of any link always belong to the same OSPF area.

97.What is the Backbone area?

The backbone area (Area 0) is the core of an OSPF network. All other areas are connected to it and all traffic between areas must traverse it. All routing between areas is distributed through the backbone area



98.What is an Autonomous System Boundary Router ASBR?

An Autonomous System Boundary Router (ASBR) is a router that is running multiple protocols and serves as a gateway to routers outside the OSPF domain and those operating with different protocols. The ASBR can import and translate different protocol routes into OSPF through a process known as redistribution.

99.Why area is used in OSPF?

OSPF uses areas to simplify administration and optimize traffic and resource utilization.

100.What is the Router ID (RID)?

Every router running OSPF within a network must have a unique router ID (RID). This identification is a 32-bit number that identifies one router to another router within an AS.

101.What is OSPF Hello interval?

OSPF uses hello packets and two timers to check if a neighbour is still alive or not: Hello interval (10 sec)

102.What is OSPF Dead interval?

Dead interval: this defines how long we should wait for hello packets before we declare the neighbour dead. (40 Sec)

103.What is the OSPF interface priority?

Default priority for an OSPF interface is 1. The range is from 0 to 255. 0 means that the interface does not involve in the DR/BDR election.

104.What is the passive interface?

- Passive Interface is a feature used by routing protocol to stop sending updates on the interface.
- If an interface is configured as a passive interface, it does not participate in OSPF and does not establish adjacencies or send routing updates. However, the interface is announced as part of the routing network

105.What are the Requirements of neighbor adjacency?

Establish neighbour adjacencies: OSPF-enabled routers must form adjacencies with their neighbour before they can share information with that neighbour.

- The devices must be in the same area.
- The devices must have the same authentication configuration.
- The devices must be on the same subnet.
- The MTUs on the interfaces must match.
- The devices hello and dead intervals must match.
- The devices must have matching stub flags.

106.How do I reset my OSPF neighbour?

Use the clear ip ospf neighbour command to clear neighbour

107.What is Designated Router (DR)?

- **Designated Router (DR)** – It is elected to minimize the number of adjacencies formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.

108.What is Backup-Designated Router (BDR)?

Backup Designated Router (BDR) – BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

109.How OSPF DR and BDR are elected?

DR and BDR election – DR and BDR election takes place in broadcast network or multi-access network. Here are the criteria for the election:

- Router having the highest router priority will be declared as DR.
- If there is a tie in router priority, then highest router I'd will be considered. First, the highest loopback address is considered. If no loopback is configured, then the highest active IP address on the interface of the router is considered.

110.What is the OSPF packet types?

OSPF uses the assigned IPv4 protocol 89 and multicast addresses 224.0.0.5 (All routers) and 224.0.0.6 (DR routers) where possible to reduce unnecessary traffic.

- **Hello**- neighbour discovery, build neighbour adjacencies and maintain them.
- **DBD (Database description)**-This packet is used to check if the LSDB between 2 routers is the same. The DBD is a summary of the LSDB.
- **LSR (Link-state request)** -Requests specific link-state records from an OSPF neighbour.
- **LSU (Link-state update)**- Sends specific link-state records that were requested. This packet is like an envelope with multiple LSAs in it.
- **LSAck (Link-state acknowledgments)**- OSPF is a reliable protocol so we have a packet to acknowledge the others.

111.What is the OSPF neighbor states?

OSPF must get through 7 states to become neighbour here they are:

- **Down** – In this state, no hello packet has been received on the interface.
  Note – The Down state doesn't mean that the interface is physically down. Here, it means that OSPF adjacency process has not started yet.
- **INIT** – In this state, hello packet has been received from the other router.
- **2WAY** – In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.
  Note – In between the 2WAY state and Exstart state, the DR and BDR election takes place.
- **Exstart** – In this state, NULL DBD are exchanged. In this state, master and slave election take place. The router having the higher router I'd becomes the master while other becomes the slave. This election decides Which router will send it's DBD first (routers who have formed neighborship will take part in this election).
- **Exchange** – In this state, the actual DBDs are exchanged.
- **Loading** – In this state, LSR, LSU and LSA (Link State Acknowledgement) are exchanged.
  Important – When a router receives DBD from another router, it compares its own DBD with the other router DBD. If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed. The other router replies with the LSU containing the updates that are needed. In return to this, the router replies with the Link State Acknowledgement.
- **Full** – In this state, synchronization of all the information takes place. OSPF routing can begin only after the Full state.

113.What is the OSPF network types?

The default OSPF network type is based on media used for the connection. Can be changed independently of media used. Cisco provides five OSPF network types, as listed in Table 8

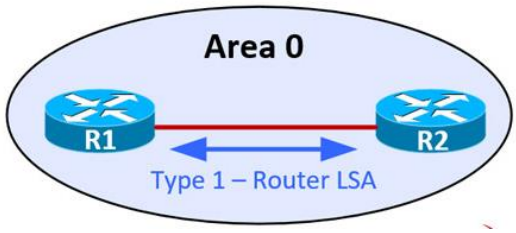
Type	Description	DR/BDR Field in OSPF Hellos	Timers
Broadcast	Default setting on OSPF-enabled Ethernet links	Yes	Hello: 10, Wait: 40, Dead: 40
Non-broadcast	Default setting on OSPF-enabled Frame Relay main interface or Frame Relay multipoint subinterfaces	Yes	Hello: 30, Wait: 120, Dead: 120
Point-to-point	Default setting on OSPF-enabled Frame Relay point-to-point subinterfaces.	No	Hello: 10, Wait: 40, Dead: 40
Point-to-multipoint	Not enabled by default on any interface type. Interface advertised as a host route. Sets the next-hop address to the outbound interface.	No	Hello: 30, Wait: 120, Dead: 120
Loopback	Default setting on OSPF-enabled loopback interfaces. Interface is advertised as a host route (/32).	N/A	N/A

114.What is the OSPF Authentication?

OSPF supports three types of authentication: null, simple password authentication and MD5 authentication. OSPF MD5 authentication can be configured globally or by interface. OSPF authentication is for security purpose.

115.What is the Router LSA (link-state advertisement)?

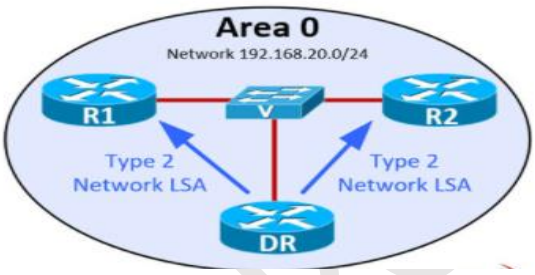
LSA Type 1 (**Router LSA**) packets are sent between routers within the same area of origin and do not leave the area. An OSPF router uses **LSA Type 1** packets to describe its own interfaces but also carries information about its neighbours to adjacent routers in the same area.



LSA Type 1 Packets exchanged between OSPF routers within the same area

116.What is the Network LSA?

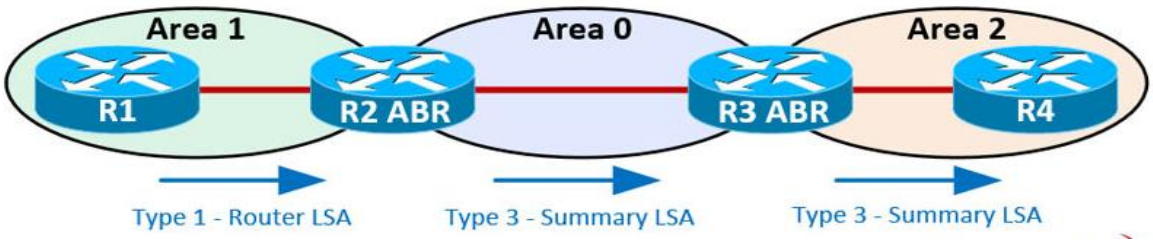
LSA Type 2 (**Network LSA**) packets are generated by the **Designated Router** (**DR**) to describe all routers connected to its segment directly. **LSA Type 2** packets are flooded between neighbours in the same area of origin and remain within that area.



LSA Type 2 Packets exchanged between OSPF DR and neighbour routers

117.What is the Summary LSA?

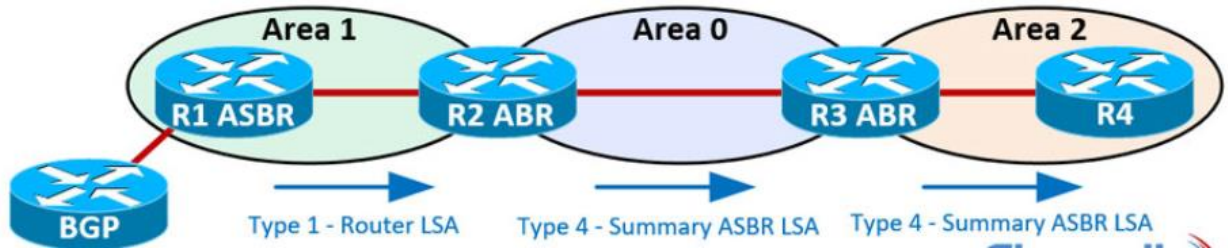
LSA Type 3 (**Summary LSA**) packets are generated by Area Border Routers (**ABR**) to summarize its directly connected area, and advertise inter-area router information to other areas the **ABR** is connected to, with the use of a summary prefix . (e.g. 192.168.0.0/22) **LSA Type 3** packets are flooded to multiple areas throughout the network and help with OSPF's scalability with the use of summary prefixes.



LSA Type 3 - An OSPF ABR router advertises the summarized route 192.168.2.0/24 to Area 0

118.What is the ASBR Summary LSA?

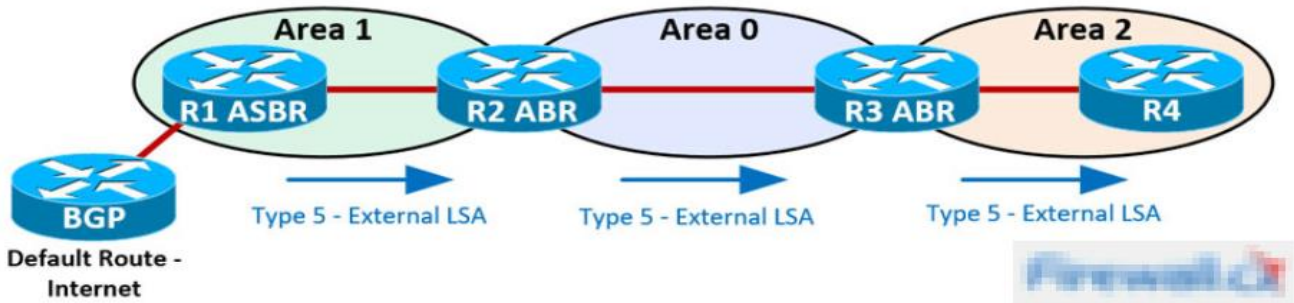
LSA Type 4 (**ASBR Summary LSA**) packets are the LSAs that advertise the presence of an Autonomous System Border Router (**ASBR**) to other areas. In the example below when **R2** (**ABR**) receives the **LSA Type 1** packet from **R1** it will create a **LSA Type 4** (**Summary ASBR LSA**) packet, which advertises the **ASBR** route received from **Area 1**, and inject it into **Area 0**.



While **LSA Type 4** packets are used by **ABRs** to advertise the **ASBR** route through their areas, it will not be used by the **ASBR** itself within its local area (**Area 1**); **ASBR** uses **LSA Type 1** to inform its neighbours (**R2** in this case) within its networks.

119.What is the ASBR External LSA?

LSA Type 5 (**ASBR External LSA**) packets are generated by the **ASBR** to advertise external redistributed routes into the OSPF's **AS**. A typical example of an **LSA Type 5** would be an **external prefix** e.g. **192.168.10.0/24** or **default route** (internet) as shown below:



LSA Type 5 packets advertise the default route to all OSPF routers

This external route/prefix is redistributed in to the OSPF network by the **ASBR** (**R1**) and seen as **O E1** or **E2** entries in other OSPF routers routing tables.

120.What is the NSSA external LSA?

LSA Type 7 (**NSSA External LSA**) packets are used for some special area types that do not allow external distributed routes to go through and thus block **LSA Type 5** packets from flooding through them, **LSA Type 7** packets act as a mask for **LSA Type 5** packets to allow them to move through these special areas and reach the **ABR** that is able to translate **LSA Type 7** packets back to **LSA Type 5** packets.

121.What does the Table maintain by OSPF?

OSPF router stores routing and topology information in three tables:

- **Neighbour table** – stores information about OSPF neighbours
- **Topology table** – stores the topology structure of a network
- **Routing table** – stores the best routes

122.Explain OSPF Virtual Link?

A virtual link is not a physical link. It is a logical link using the least cost path between the ABR of the non-backbone connected area and the backbone ABR of the transit area.
A virtual adjacency across the virtual link is formed, and routing information is exchanged.

123.Explain Stub Area and different types of Stub area?

Stub Area

Sometimes we need to control the advertisement of external routes into an area. This area is called stub area. Stub area 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.

Three restriction apply to OSPF stub area: -

- 1.No virtual links are allowed in the stub area.
- 2.Stub area cannot be a backbone area.
- 3.No Autonomous System Boundary Router are allowed

Totally Stubby Area

Like stub areas, totally stubby area does not receive type4 and type5 LSA from their ABRs. However, they also do not receive type 3 LSAs. It allows advertisement of internal router in that area.

Not-So-Stubby Areas

The motivation behind NSSA is to allow OSPF stub area to carry external routes. External router is 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.

Totally NSSA

Along with Type4 & Type5, Type3 LSA will also be filtered in Totally NSSA

124.Can we have OSPF run over a GRE Tunnel?

Yes, we can have OSPF run over a GRE tunnel.

125.How do we configure the OSPF Routing Protocol?

- Router (Config)#router ospf 100
- Router (Config-router) #network 172.16.1.0 0.0.0.255 area 0
- Router (Config-router) #network 10.16.1.0 0.0.0.255 area 1
- Router (Config-router) #exit

❖ BGP (Border Gateway Protocol)

126.Explain the Border Gateway Protocol (BGP)?

- Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. BGP is classified as a path-vector routing protocol, and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator.
- BGP used for routing within an autonomous system is called Interior Border Gateway Protocol, Internal BGP (iBGP). In contrast, the Internet application of the protocol is called Exterior Border Gateway Protocol, External BGP (eBGP).

127. What are the BGP features?

- Path vector protocol
- Open standard protocol.
- Classless routing protocol.
- Used the Path vector algorithm.
- Administrative distance for eBGP is 20, iBGP-200
- BGP exchange router information between autonomous system.
- Hello timer is 60 sec; hold on timer is 180 sec.
- BGP used TCP port number 179.

128.Can Router on different subnet become BGP Neighbors?

Can does not require neighbours to be attached to the same subnet. Instead, BGP routers use a TCP connection between the routers to pass BGP message allowing neighbouring routers to be on the same or different subnet.

129.Different between eBGP & iBGP neighbors?

- **IBGP-** neighborship is formed between routers within the same AS (autonomous system)
- **EBGP**-neighborship is formed between routers different AS (autonomous system)

130.Explain Loop prevention mechanism in BGP?

BGP used two mechanisms to prevent loops: -

- When a router learns route from an iBGP peer, that router does not advertise the same routes to another iBGP peer.
- By using AS_PATH- When advertising to an eBGP peer, a BGP router adds its own ASN to the AS_PATH. If a BGP router receives an Update and the route advertisement lists an_AS_PATH with its own ASN, the router ignores that route.

Note:- A BGP router does not add its ASN when advertising to an iBGP Peer.

131.What is different between the hard reset and soft rest in BGP?

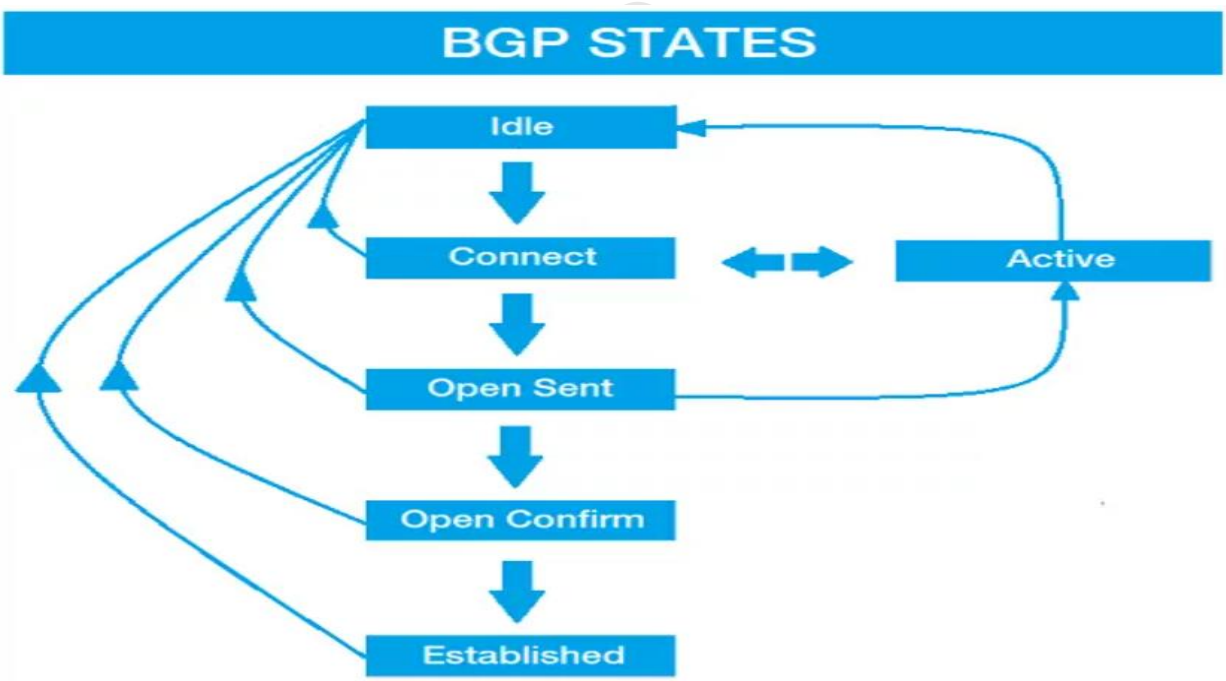
- **Hard Reset**-In case of hard reset the local router brings down the neighborship, brings down the underlying TCP connection and all the BGP table entire learning from neighbour are removed **#clear ip bgp** command used for hard reset.
- **Soft Reset**-In case of a soft reset the router does not bring down the BGP neighborship or the underlying TCP connection.
- However, the local router resends outgoing Updates and reprocesses incoming Update adjusting the BGP table base on the current configuration **#clear ip bgp * soft** command used for soft reset.

132.What are different BGP Message Types?

- **Open**-It is Used to establish a neighbour relationship and exchange parameters, including autonomous system number and authentication values.
- **Keepalive-** are sent periodically (every 60 seconds by default) to ensure that the remote peer is still available. If a router does not receive a KEEPALIVE from a peer for a Hold-time period (by default, 180 seconds), the router declares that peer dead.
- **Update**- It exchange Path Attributes and the associated prefix/length (NLRI) that use those attributes.
- **Notification**- It is used to report BGP error. It results in a reset of neighbour relationship.

133.Explain various state of BGP?

- **Idle**- the initial BGP state.
- **Connect**- The BGP process is waiting for the TCP Connection to be completed. If it is successful, it will be continuing to the Open Sent State. In case it fails, it will be continuing to active state.
- **Active** -BGP will try another TCP three-way handshake to establish a connection with the remote BGP neighbour. If it successful, it will be move to the Open Sent State.
- **Open sent**- BGP has both established the TCP connection and sent an OPEN Message and is awaiting a reply OPEN Message. Once it receives a reply OPEN Message, the BGP peer will send a KEEPALIVE message.
- **Open confirm**- BGP listens for a reply KEEPALIVE message
- **Established**- All neighbour parameters matched, the neighbour relationship has been established and the peers can now exchange update message.



134.Explain BGP Path Attributes?

BGP utilizes several attributes to determine the best path to a destination.

- **Next Hop**- It lists the next-hop IP address used to reach a prefix. If next hop is reachable? If no route to reach Next hop, the router cannot use this route.

- **Weight**- The Weight attribute is applied to inbound routes, dictating the best outbound path. It is a Cisco-proprietary attribute, and is only locally significant (and thus, is never passed on to BGP neighbours). The weight value can range from 0 – 65535, and the highest weight is preferred. By default, a route originated on the local router will be assigned a weight of 32768. All other routes will be assigned a weight of 0, by default.
- **Local Preference**- The Local Preference attribute is applied to inbound external routes, dictating the best outbound path. Unlike the Weight attribute, Local Preference is passed on to iBGP peers when sending updates. Local Preference informs iBGP routers how to exit the AS if multiple paths exist. Local Preference is a 32-bit number and can range from 0 to 4294967295. The highest Local Preference is preferred, and the default preference is 100.

- **Locally injected routes**- Locally injected routes (routes injected using network command) are better than iBGP/eBGP learned.

- **AS Path**- The AS-Path attribute is applied to outbound routes, dictating the best inbound path. Two things can be accomplished with the AS-Path attribute, prepend or filter. Smaller is preferred.

- **Origin**- The Origin attribute identifies the originating source of the route. The origin codes are as follows (listed in order of preference for route selection): • i (IGP) – Originated from an interior gateway protocol, such as OSPF. This usually indicates the route was injected into BGP via the network command under the BGP process. An origin code of "i" is most preferred. • e (EGP) – Originated from an external gateway protocol. • ? (incomplete) - Unknown origin. This usually indicates the route was redistributed into BGP (from either connected, static, or IGP routes). An origin code of "?" is the least preferred.

- **Multi-Exit Discriminator (MED)**- The MED (MultiExit Discriminator) attribute is applied to outbound routes, dictating the best inbound path into the AS (assuming multiple paths exist). The MED is identified as the BGP metric when viewing the BGP routing table. A lower metric is preferred, and the default MED value is 0. Smaller is preferred.

- **Neighbour type**- eBGP is preferred over iBGP
- **IGP metric**- Route with nearest IGP neighbour (lowest IGP metric) is preferred.
- **eBGP route**- Oldest (longest known) route is preferred.
- **Neighbour Router ID**- Lowest is preferred.
- **Neighbour IP Address**- Lowest is preferred.

135.Explain BGP Local preference?

The local preference BGP attribute is the second attribute and used to choose the exit path to an autonomous system from a local perspective. It is not exchanged between routers; its default value is 100 and the path with the highest local preference is preferred.

136.Explain BGP MED?

MED is an optional nontransitive attribute. MED is a hint to external neighbours about the preferred path into an autonomous system (AS) that has multiple entry points. The MED is also known as the external metric of a route. A lower MED value is preferred over a higher value.

137.Explain BGP local preference?

The local preference BGP attribute is the second attribute and used to choose the exit path to an autonomous system from a local perspective. It is not exchanged between routers, it's default value is 100 and the path with the highest local preference is preferred.

138.What is Recursive Lookup?

A Recursive lookup refers to routes for which the router must look up the connected route to a next-hop gateway to route the packet to its ultimate destination.

139.What is router reflector and why it is required?

In BGP, route learned from an iBGP neighbour will not be advertised to another iBGP neighbour. To overcome this situation route reflector is used. It is acts as a route reflector server and makes iBGP neighbours as route reflector client enabling route advertisements between them.

140.What is the command to administratively disable BGP neighborship?

#neighbor neighbor-ip shutdown
no neighbor neighbor-ip shutdown (to enable to again)

❖ Switching

141.What is switching?

The function of switching is to switch data packets between devices on the same network.

142.What is switching?

A switch is a device which is used to connect multiple devices inside Local Area Network (LAN). Unlike hubs, a switch examines each packet and process it accordingly rather than simply repeating the signal to all port. Switches operate at Layer Two (Data Link layer) of the OSI model.

143.What is the different between a HUB, Switch & Router?

144.What are functions of the switch?

The Switch performs three major function: -

- Address learning
- Packet forwarding.
- Loop avoidance by Spanning Tree Protocol

145.What is Sub interface?

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

146.What is a Broadcast Domain & Collision Domain?

Broadcast Domain- Broadcast is a type of communication, where the sending device sends a single copy of data and that copy of data will be delivered to every other device in the network segment.

Collision Domain- It is a network scenario where one device sends a packet on a network segment forcing every other device on that same segment to pay attention to it. At the same time, if a different device on that same segment to pay attention to it.

147.What is a MAC address table and how a switch will build a MAC table?

The switch maintains an address table called MAC address table to efficiently switch frames between interfaces. When the switch receives a frame, it associates the MAC address of the sending device with the switch port on which it was received.

148.How does switch learn Mac address?

A switch can learn MAC address in two ways; statically or dynamically. In the static option, we must add the MAC addresses in the CAM table manually. In the dynamic option, the switch learns and adds the MAC addresses in the CAM table automatically. The switch stores the CAM table in the RAM.

149.Explain Flooding?

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

❖ VLAN (Virtual LAN)

150.What is a VLAN and How does it reduce the broadcast traffic?

A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch. VLAN divides the broadcast domain so, the frames that will be broadcasted onto the network are only switched between the ports logically grouped within the same VLAN.

151.What is the deference between an access port and a trunk port?

- **Access Port**- Access port belongs to and carries the traffic of only one VLAN. Anything arriving on an access port is simply assumed to belong to the VLAN assigned to the port. Any device attached to an access link is unaware of a VLAN membership as switches remove any VLAN information from the frame before its forwarded out to an access-link device. Access-link device can't communicate with devices outside their VLAN unless the packet is routed.

- **Trunk Port**- Trunk port can carry the traffic of multiple VLANs from 1-4094 VLANs at a time. Normally Trunk link is used to connect switches to other switches or to routers. Trunk ports support tagged and untagged traffic simultaneously.

152.What is Frame Tagging and Different types of Tagging?

Frame tagging method uniquely assigns a VLAN ID to each frame. It is used to identify the VLAN that the Frame belongs to.

There are mainly two types of Frame Tagging Method: -

- Inter-Switch Link (ISL) cisco
- 802.1Q Open Standard

153.Explain the different between 802.1Q and ISL?

802.1Q- It's an open standard created by the Institute of Electrical and Electronics Engineers (IEEE). To identify to which VLAN a frame belongs to, a field is inserted into the frame's header. It is a light weighted protocol & adds only 4 Byte within Frame's Header.

ISL (Inter-Switch Link)- This protocol is Cisco proprietary which means unlike 802.1Q, it can be used only between Cisco switches' works by adding Header (26 Bytes) and Trailer(4Bytes) with Original Ethernet Frame.

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

The trunk port is assigned a default VLAN ID for a VLAN that all untagged traffic will travel on. This VLAN is called the Native VLAN and is always VLAN 1 by default (but can be changed to any VLAN number). Similarly, any untagged or tagged traffic with unassigned VLAN ID is assumed to belong to the Native VLAN.

155.What is Inter-VLAN Routing?

VLANs divide broadcast domain in a LAN environment So, by default only Hosts that are members of the same VLAN can communicate. Whenever host in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as Inter-VLAN routing.

This can be done by two methods – Router-On-Stick & switch Virtual Interface (SVI)

156.Tell me the commands to create VLAN?

- Switch(config)#Vlan 10
- Switch(config-vlan) #name sale
- Switch(config-vlan) #exit

157.How can we add an interface to a VLAN?

- Switch(config)#interface fast Ethernet 0/0
- Switch(config-if) #switchport mode access
- Switch(config-if) #switchport access vlan 10

158.How to configure trunk link?

- Switch(config)#interface fast Ethernet 0/24
- Switch(config-if) #switchport trunk encapsulation <dot1q/isl>
- Switch(config-if) #switchport mode trunk

159.How can we change Native Vlan?

- Switch(config)#interface fast Ethernet f0/0
- Switch(config-if) switchport trunk native vlan 100

160.Which command used to trunk interface?

- Switch(config)#show interface trunk

161.Which command is used to see all VLANs

- Switch(config)#show vlan

❖ VTP (Vlan Trunking Protocol)

162.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. Ex- (VLAN ID or VLAN Name) with switches inside the same VTP domain.

163.What are different VTP mode?

- **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 switch listen to VTP advertisements from other switches and modify their VLAN configuration 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.

164.What are requirement to exchange VTP message between two switches?

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

165.Explain Dynamic Trucking Protocol (DTP)?

Dynamic Trunking Protocol (DTP) is a Cisco proprietary trunking protocol used for negotiating trunking on a look between two cisco switches. Dynamic Trunking Protocol (DTP) can also be used for negotiating the encapsulation type of either 802.18 or Cisco ISL (inter-switch-link)

166.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 initiate 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 (Spanning Tree Protocol)

167.What is STP and Redundant Links?

Spanning Tree protocol (STP) is a protocol which prevents layer2 loops. STP enables switches to become aware of each other so that they can negotiate a Loop-Free path through the network.

In practical Scenario, Redundant links are created to avoid completed network failure in an event of failure of one link.

168.How STP works?

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

169.What are the different port states?

- **Disabled**- A port in the disabled state does not participate in the STP.
- **Blocking**- A blocking port does not forward frames. It only listens to BPDUs. The purpose of the blocking state is to prevent the use of looped paths.
- **Listening**- 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.
- **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.

170.What is STP timer and explain different types of STP timer?

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

- **Hello timer-** The timer interval between configuration BPDUs send by the root bridge. Its 2 seconds by default.
- **Forward Delay timer**- The time interval that a switch port spends in both the Listening and Leaning 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 defined as a time interval that a switch stores a BPDU before discarding it. It is 20 seconds by default.

171.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 the root Bridge & non-root Bridge. All ports of root bridge are designated port.

- **Forwarding port**- A forwarding port forwarding frames.

- **Blocked port**- A blocked port is the port that is used to prevent loops. It only listens to BPDUs. Any port other than root port and designated port is a blocked port.

172.What is BPDU?

All the switches exchange information to select root bridge as well as for configuration of the network. This is done through the Bridge Protocol Data Unit (BPDU). Each switch compares the parameters in the BPDU that it sends to one neighbor with the one that it receives from another neighbor.

173.What is the destination MAC address used by Bridge Protocol data Unites (BPDUs)?

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

174.How Root Bridge is elected?

The bridge ID 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 devices.

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 then switch with lowest mac address will become root Bridge

175.What is the Root Port?

Once the Root switch is elected, every other switch in the network must select a single port on itself to reach the Root Switch. The port with the lowest root path cost (lowest cumulative cost to reach the root switch) is elected as the root port and is placed in the forwarding state. Root bridge will never have a root port.

❖ DHCP (Dynamic Host Configuration Protocol)

176.What is DHCP?

Dynamic Host Configuration Protocol (DHCP) assigns IP address 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. (Server port 66/client port 67)

177.What information can a DHCP provide to Host?

A DHCP server can provide the following information: -

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

178.How DHCP works?
DHCP works on DORA Process (DISCOVER – OFFER – REQUEST -ACKNOWLEDGEMENT)

179.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

180.What is the purpose of a relay agent?
A DHCP relay agent is any host that forwards DHCP packets between clients and servers if they are not on the same physical subnet. Relay agents are used to forwarding requests and replies between clients and servers when they are not on the same physical subnet.

181.What is DHCP decline message?
It is sent by a client to the server indicating network address is already in use (already assigned to another device).

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

183.Which port are used in SNMP?
SNMP uses the UDP port 161 for sending and receiving request, and port 162 for receiving traps from managed devices.

❖ VPN (Virtual Private Network)

184.What is VPN?
Virtual Private Network (VPN) create a secure network connection over a public network such as the internet. It allows devices to exchange data through a secure virtual tunnel. It uses a combination of security features like encryption, authentication, tunnelling protocols, and data integrity to provide secure communication between participating peers.

185.What is IPsec VPN?
IP Security Protocol VPN means VPN over IP security. It allows two or more users to communication in a secure manner by authentication and encryption each IP Packet of a communication session. IPsec provides data confidentiality, data integrity and data authentication between participating peers.

186.At which layer IPsec works?
- IPsec secures IP traffic at the Layer-3 (Network Layer) of OSI model.

187.Name a major drawback of IPsec?
- IPsec only supports unicast IP traffic.

188.What is the different between Transport & Tunnel mode?

- **Tunnel mode**- Protects data in network-to-network or site-to-site scenarios. It encapsulates and protects the entire IP packet-the payload including the original IP header and a new IP header (protects the entire IP payload including user data).

- **Transport mode**-Protects data in host-to-host or end-to-end scenarios. In transport mode, IPsec protects the payload of the original IP datagram by excluding the IP header (only protects the upper-layer protocols of IP payload (user data)

189.What are the three main security services that IPsec VPN provide?

IPsec offers the following security services: -

- Peer Authentication.
- Data confidentiality.
- Data integrity.

190.Define Digital Signature?

A digital signature is an attachment to an electronic message used for security purposes. It is used to verify the authenticity of the sender.

191.What is Site to Site and Remote access VPN?

A site-to-site VPN allows offices in multiple location to establish secure connections with each other over a public network such as the internet.
Remote Access VPN allows Remote users to connect to the Headquarters through a secure tunnel that is established over the internet. The remote user can access internal, private web pages and perform various IP-based network tasks.

There are two primary methods of deploying Remote Access VPN.

- Remote Access IPsec VPN.
- Remote Access Secure Sockets layer(SSL) VPN.

192.What are the 3-protocol used in IPsec?

- Authentication Header (AH).
- Encapsulation Security Payload (ESP).
- Internet Key Exchange (IKE).

193.How ESP & AH provide anti-replay protection?

Both ESP and AH protocols provide anti-replay protection based on sequence numbers. The sender increments the sequences number after each transmission, and the receiver checks the sequences number after sequence number and rejects the packet if it is out of sequence.

194.What is IKE?

It is a hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. It defines the mechanism for creating and exchanging keys. IKE derives authenticated keying material and negotiates SAs that are used for ESP and AH protocols.

195.Which protocol does IKE use?

IKE uses UDP port 500.

196.Explain how IKE/ISAKMP Works?

IKE is a two-phase protocol: -

Phase1

IKE phase 1 negotiates the following: -

- It protects the phase 1 communication itself (using cryto and hash algorithms).
- It generates session key using Diffie-Hellman groups.
- Peer will authenticate each other using pre-shared, public key encryption, or digital signature.
- It also protects the negotiation of phase 2 communication.

There are also two modes in IKE phase 1:

- **Main mode**- Total Six message is exchanged in the main mode for establishing phase 1SA.

- **Aggressive mode**- It is faster than the main mode as only Three message are exchanged in this mode to established phase 1 SA. It is faster but less secure.

At the end of phase 1, a bidirectional ISAKMP/IKE SA (phase 2 SA) is established for IKE communication.

Phase-2

IKE phase 2 protects the user data and establishes SA for IPsec.

There is one mode in IKE phase 2:

- **Quick mode**- In this mode, three messages are exchanged to establish the phase 2 IPsec SA.

At the end of phase 2 negotiation, two unidirectional IPsec SAs (Phase 2 SA) are established for used data – one for sending and another for receiving encrypted data.

197.Explain the message exchange between the peers in IKE/ISAKMP?

Phase-1 – Main mode

- MESSAGE 1- Initiator offers policy proposal which includes encryption, authentication, hashing algorithms (like AES, or 3DES, PAK or PKI, MD5 or RSA).
- MESSAGE-2- Responder presents policy acceptance (or not).
- MESSAGE-3- Initiator sends the Diffie-Helman key and nonce.
- MESSAGE-4 Responder sends the Diffie-Helman key and nonce.
- MESSAGE-5 Initiator sends ID, preshare key or certificate exchange for authentication.
- MESSAGE-6 Responder sends ID, preshare key or certificate exchange for authentication.

Only first four messages were exchanged in clear text. After all message are encrypted.

Phase-2-Quick mode

- MESSAGE-7 Initiator sends Hash, IPsec Proposal, ID, nonce.
- MESSAGE-8 Responder sends Hash, IPsec Proposal, ID, nonce.
- MESSAGE-9 Initiator sends signature, hash, ID.

All messages in Quick mode are encrypted.

198.What is Diffie-Hellman?

DH is a public-key cryptography protocol which allows two parties to establish a shared secret over an insecure communications channel. Diffie-Hellman is used within IKE to establish session keys and is a component of Oakley.

199.What are Security Associations?

The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (AH or ESP).

200.What is Transform set?

An IKE transform set is a combination of security protocols and algorithms. During yhe IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

201.What are Crypto access lists?

Crypto access lists specify which IP traffic is protected by Crypto and which traffic is not protected by crypto. To protect IP traffic "permit" keyword is used in an access list. If the traffic is not to be protected, then "deny" keyword is used in the access list.

202.How to Check the status of the tunnel's phase 1 & 2?

Use following commands to check the status of tunnel phases.

- Phase-1 #show crypto isakmp sa
- Phase-2 #show crypto ipsec sa

203.What is IPsec Virtual Tunnel Interface?

IPsec VTI is the concept of using a dedicated IPsec interface called IPsec Virtual Tunnel interface for highly scalable IPsec-based VPNs. IPsec VTI provides a routable interface for terminating IPsec tunnels. VTI also allows the encrypting of multicast traffic with IPsec.

204.What is the DMVPN?

DMVPN allows IPsec VPN networks to better scale hub-to-spok and spok-to-spok topologies optimizing the performance and reducing latency for communications between sites.

It offers the following benefits:

- It Optimizes network performance.
- It reduces router configuration on the hub.
- Support for dynamic routing protocols running over the DMVPN tunnels.
- Support for multicast traffic from hub to spokes.
- The capability of establishing direct spoke-to-spoke IPsec tunnel for communication between sites without having the traffic to go through the hub.

205.What is GRE?

Generic Routing Encapsulation Protocol is a tunnelling protocol developed by Cisco designed to encapsulate IP unicast, multicast and broadcast packets. It uses IP protocol number 47.

206.Name a major drawback of both GRE & L2TP?

No encryption.

207.What is SSL VPN? How it is different from IPsec VPN?

SSL VPN provides remote access connectivity from any internet enabled device though a standard web browser and its native SSL encryption. It does not require any special client software at a remote site. In IPsec VPN connection is initiated using a pre-installed VPN client software, only a web browser is required.

208.What is a firewall?

Firewall is a device that is placed between a trusted and untrusted network. It denies or permits traffic that enters or leaves network based on pre-configured policies.
Firewalls protect inside networks from unauthorized access by users on an outside network. A firewall can also protect inside networks from each other. For Ex-By keeping a Management network separate from a user network.

209.What is the difference between Gateway and Firewall?

A Gateway join two networks together and a network firewall protects a network against unauthorized incoming or outgoing access. Network firewalls may be hardware devices or software programs.

210.At which Layers does Firewall work?

Firewall works at layer 3,4 & 7.

211.What is the difference between Stateful & Stateless Firewall?

Stateful- A stateful firewall is aware of the connections that pass through it. It adds and maintains information about user's connection in the state table, referred to as a connection table. It then uses this connection table to implement the security policies for users connection. Example of the stateful firewall is PIX,ASA,Checkpoint.

Stateless firewall- (Packet Filtering) Stateless firewalls, on the other hand, does not look at the state of connections but just at the packets themselves.
Example of a packet filtering firewall is the Extended Access Control Lists on Cisco IOS Routers.

212.What information does Stateful firewall maintain?

Stateful firewall maintains the following information in its State table:-

- Source IP address.
- Destination IP address
- IP protocol loke TCP, UDP.
- IP protocol information such as TCP/UDP Port Numbers, TCP Sequence Numbers, and TCP Flags.

213.How can we allow packets from a lower security level to a higher security level (Override security Levels)?

We use ACLs to allow packets from the lower security level to a higher security level.

214.What is the security level of inside and outside interface by default?

The security level of the inside interface by default is 100. The security level of the outside interface by default is 0.

215.What protocols are inspected by ASA?
By default, TCP and UDP are inspected by ASA.

216.Does ASA inspect ICMP?
No. ASA does not inspect ICMP by default.

217.Explain DMZ (Demilitarized Zone) Server?
If we need some network resources such as a Web server or FTP server to be available to outside users, we place these resources on a separate network behind the firewall called a demilitarized zone (DMZ). The firewall allows limited access to the DMZ, but because the DMZ only includes the public servers, an attack there only affects the servers and does not affect the inside network.

218.What are the values for timeout of the TCP session, UDP session, ICMP session?
TCP session- 60 mints
UDP session- 2 mints
ICMP session- 2 sec

219.What is the difference in ACL on ASA than on Router?
In the router if we delete one access-control entry whole ACL will be deleted. In ASA if we will delete one access-control entry whole ACL will not be deleted.

220.What are the different types of ACL in the Firewall?
Standard ACL
Extended ACL
Ether type ACL (Transparent Firewall)
Web type ACL (SSL VPN)

221.What is Transparent Firewall?
In Transparent Mode, ASA acts as a Layer 2 device like a bridge or switch and forwards ethernet frames based on destination MAC-address.

222.What is the need for a Transparent Firewall?
If we want to deploy a new firewall into an existing network it can be a complicated process due to various issues like IP address reconfiguration, network topology changes, current firewall etc. We can easily insert a transparent firewall in an existing segment and control traffic between two sides without having to readdress or reconfigure the devices.

223.What are the different between a switch and ASA (in transparent mode)?
ASA does not flood unknown unicast frames that are not found in the MAC-Address Table.
ASA does not participate in STP.
Switch process traffic at layer 1 & layer 2 while ASA can process traffic from layer 1 to layer 7.

224.What information is exchanged between ASAs over a Failover link?
State- Active or standby.
Hello Messages
Network Link Status.
Mac Addresses.
Configuration Replication and Synchronization.

225.Explain Active/Standby Failover?

In Active/Standby Failover, one unit is the active unit which passe traffic. The standby unit does not actively pass traffic. When failover occurs, the active unit fails over to the standby unit, which then becomes active. We can use Active/Standby Failover for ASAs in both single and multiple context mode.

226. What is Policy NAT?

Policy NAT allows you to NAT by specifying both the source and destination addresses in an extended access list. We can also optionally specify the source and destination ports. Regular NAT can only consider the source addresses, not the destination address.

- In static NAT it is called as Static Policy NAT.
- In Dynamic NAT it is called Dynamic Policy NAT.