Network Journey

A journey towards packet life !!!

50 MCQ Questions And Answers with Explanation CCNP

1.Question:Which routing protocol is considered a link-state routing protocol?

A) RIP (Routing Information Protocol)

B) EIGRP (Enhanced Interior Gateway Routing Protocol)

C) OSPF (Open Shortest Path First)

D) BGP (Border Gateway Protocol)

Answer:C) OSPF (Open Shortest Path First)

Explanation: OSPF is a link-state routing protocol that uses the Shortest Path First (SPF) algorithm to calculate the best path through the network.

2. Question: Which routing protocol uses a composite metric that includes bandwidth, delay, reliability, load, and MTU?

A) OSPF

B) RIP

C) EIGRP

D) BGP

Answer: C) EIGRP (Enhanced Interior Gateway Routing Protocol)

Explanation: EIGRP uses a composite metric known as the "metric" or "feasible distance" that takes into account various factors, including bandwidth, delay, reliability, load, and Maximum Transmission Unit (MTU).

3. Question: What is the administrative distance of OSPF?

A) 90
B) 100
C) 110
D) 120

Answer: C) 110

Explanation: OSPF has an administrative distance of 110 by default.

4. Question: In which type of OSPF area are ASBRs (Autonomous System Boundary Routers) typically located?

A) Backbone Area (Area 0)

B) Stub Area

C) Totally Stubby Area

D) Not-So-Stubby Area (NSSA)

Answer: A) Backbone Area (Area 0)

Explanation: ASBRs are often located in the Backbone Area (Area 0) of an OSPF network.

5. Question:Which routing protocol uses the concept of "split horizon" to prevent routing loops in distance-vector routing?

A) OSPF

B) RIP

C) EIGRP

D) BGP

Answer:B) RIP (Routing Information Protocol)

Explanation:RIP uses the split horizon mechanism to prevent routing loops by not advertising routes back out of the interface they were learned on.

6. Question:What is the default administrative distance of a directly connected network in Cisco routers?

A) 0

B) 90

C) 100

D) 120

Answer: A) 0

Explanation: A directly connected network has an administrative distance of 0, making it the most preferred route in the routing table.

7. Question: Which routing protocol is classified as a hybrid routing protocol, combining characteristics of both distance-vector and link-state protocols?

A) OSPF

B) RIP

C) EIGRP

D) BGP

Answer: C) EIGRP (Enhanced Interior Gateway Routing Protocol)

Explanation:EIGRP is considered a hybrid routing protocol because it incorporates elements of both distance-vector and link-state routing protocols.

8.Question: What is the administrative distance of an external BGP (eBGP) route?

A) 20

B) 90

C) 110

D) 120

Answer:D) 120

Explanation: External BGP (eBGP) routes have an administrative distance of 120 by default.

9. Question: Which routing protocol uses the concept of "hello packets" to establish neighbor adjacencies?

A) OSPF

B) RIP

C) EIGRP

D) BGP

Answer: A) OSPF (Open Shortest Path First)

Explanation:OSPF uses "hello packets" to discover and establish neighbor adjacencies with other OSPF routers.

10. Question: What is the purpose of the "feasible successor" concept in EIGRP?

A) It identifies the primary route to a destination network.

B) It identifies a backup route to a destination network.

C) It calculates the EIGRP metric.

D) It determines the administrative distance of EIGRP routes.

Answer:B) It identifies a backup route to a destination network.

Explanation:Feasible successors are backup routes in EIGRP that can be used if the primary route fails. They are precalculated to provide faster convergence in case of route changes.

11. Question: What is the purpose of the Spanning Tree Protocol (STP) in switched networks?

A) Load balancing traffic across multiple links

B) Preventing broadcast storms

C) Improving switch performance

D) Enabling VLAN communication

Answer: B) Preventing broadcast storms

Explanation: STP's primary purpose is to prevent broadcast storms and create a loop-free topology in switched networks.

12. Question: Which Spanning Tree Protocol (STP) variant is considered the most efficient and widely used?

A) STP (802.1D)

B) RSTP (802.1w)

C) MSTP (802.1s)

D) PVST+

Answer: B) RSTP (802.1w)

Explanation: Rapid Spanning Tree Protocol (RSTP or 802.1w) is an enhancement to the original STP, offering faster convergence times and improved efficiency.

13. Question: What is the primary benefit of using Virtual LANs (VLANs) in a switched network?

A) Reducing network latency

B) Enhancing network security

C) Increasing network bandwidth

D) Simplifying network management

Answer: B) Enhancing network security

Explanation:VLANs help enhance network security by isolating broadcast domains and controlling access between different network segments.

14. Question:Which type of VLAN is typically used for carrying user-generated traffic?

A) Data VLAN

B) Native VLAN

C) Management VLAN

D) Voice VLAN

Answer: A) Data VLAN

Explanation: Data VLANs are used for user-generated traffic and are the most common type of VLAN in a network.

15. Question:In a redundant switch topology, what is the purpose of the EtherChannel or Link Aggregation Group (LAG) feature?

A) Load balancing traffic

B) Preventing broadcast storms

C) Isolating VLANs

D) Enforcing security policies

Answer: A) Load balancing traffic

Explanation: EtherChannel or LAG allows multiple physical links to be treated as a single logical link, enabling load balancing and fault tolerance.

16. Question: What is the purpose of the Dynamic Trunking Protocol (DTP) in Cisco switch configurations?

A) Enabling EtherChannel

B) Automatically negotiating trunking between switches

C) Assigning VLANs to switch ports

D) Blocking VLAN traffic

Answer:B) Automatically negotiating trunking between switches

Explanation: DTP is used to dynamically negotiate trunking between switches, making it easier to configure trunk links.

17. Question: Which switch port mode is used when connecting an end-user device like a computer or IP phone?

A) Access

B) Trunk

C) Dynamic

D) VLAN

Answer: A) Access

Explanation: Access port mode is used to connect end-user devices to a single VLAN.

18. Question:Which protocol is commonly used for automatically assigning IP addresses to devices in a switched network?

A) ARP (Address Resolution Protocol)

B) DHCP (Dynamic Host Configuration Protocol)

C) ICMP (Internet Control Message Protocol)

D) DNS (Domain Name System)

Answer:B) DHCP (Dynamic Host Configuration Protocol)

Explanation: DHCP is used to automatically assign IP addresses to devices in a network, including those in a switched environment.

19. Question: What is the purpose of the HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol) in a switched network?

A) Load balancing traffic

B) Providing redundant default gateways

C) Preventing broadcast storms

D) Enforcing VLAN segmentation

Answer: B) Providing redundant default gateways

Explanation:HSRP and VRRP are used to provide a redundant default gateway for devices in case of router failure.

20. Question:Which switch feature allows you to divide a physical switch into multiple logical switches with separate VLAN configurations?

A) Port Security

B) Virtual Switching System (VSS)

C) Virtual LAN Trunking Protocol (VTP)

D) Private VLANs

Answer:D) Private VLANs

Explanation: Private VLANs (PVLANs) allow you to segment a physical switch into multiple logical switches with separate VLAN configurations, enhancing security and isolation.

21. Question: What is the primary purpose of Network Address Translation (NAT)?

A) Load balancing incoming traffic

B) Concealing internal IP addresses from external networks

C) Enforcing Quality of Service (QoS) policies

D) Distributing IP addresses to devices on the network

Answer: B) Concealing internal IP addresses from external networks

Explanation: NAT is commonly used to hide internal/private IP addresses from external networks by translating them to a single public IP address.

22. Question: Which type of NAT allows multiple internal devices to share a single public IP address?

A) Dynamic NAT

B) Static NAT

C) PAT (Port Address Translation)

D) NAT64

Answer: C) PAT (Port Address Translation)

Explanation: PAT (also known as NAT overload) allows multiple internal devices to share a single public IP address by using unique source port numbers.

23. Question: In Quality of Service (QoS), what is the purpose of traffic policing?

A) Prioritizing traffic based on DSCP values

B) Marking packets with a different IP address

C) Dropping or remarking packets that exceed defined limits

D) Redirecting traffic to a different gateway

Answer: C) Dropping or remarking packets that exceed defined limits

Explanation: Traffic policing is used to control and potentially drop or remark packets that exceed specified rate limits.

24. Question: Which protocol is commonly used to assign IP addresses to devices dynamically, eliminating the need for manual configuration?

A) ARP (Address Resolution Protocol)

B) DNS (Domain Name System)

C) DHCP (Dynamic Host Configuration Protocol)

D) ICMP (Internet Control Message Protocol)

Answer: C) DHCP (Dynamic Host Configuration Protocol)

Explanation: DHCP is used for automatic IP address assignment to devices on a network.

25. Question: What is the purpose of an Access Control List (ACL) in networking?

A) Filtering network traffic based on MAC addresses

B) Prioritizing network traffic

C) Controlling access to network resources based on defined rules

D) Load balancing incoming traffic

Answer: C) Controlling access to network resources based on defined rules

Explanation: ACLs are used to control which network traffic is allowed or denied based on defined rules.

26. Question: Which protocol is commonly used for securely accessing network devices remotely, providing encrypted communication?

A) SNMP (Simple Network Management Protocol)

B) SSH (Secure Shell)

C) TFTP (Trivial File Transfer Protocol)

D) FTP (File Transfer Protocol)

Answer: B) SSH (Secure Shell)

Explanation: SSH is commonly used for secure remote access to network devices, providing encrypted communication.

27. Question: What is the primary purpose of a DNS (Domain Name System) server in a network?

A) Assigning IP addresses to devices

B) Translating domain names into IP addresses

C) Filtering network traffic based on domain names

D) Routing network traffic between different subnets

Answer: B) Translating domain names into IP addresses

Explanation: DNS servers resolve domain names to corresponding IP addresses.

28. Question: Which IP service is used for translating between IPv6 and IPv4 addresses, enabling communication between networks with different IP versions?

A) NAT (Network Address Translation)

B) DHCPv6 (Dynamic Host Configuration Protocol for IPv6)

C) DNS64

D) NAT64

Answer: D) NAT64

Explanation: NAT64 is used to facilitate communication between IPv6 and IPv4 networks by translating between their respective address formats.

29. Question: What is the primary purpose of a proxy server in a network?

A) Routing traffic between different subnets

B) Accelerating web content delivery

C) Providing network security

D) Load balancing incoming traffic

Answer: B) Accelerating web content delivery

Explanation: Proxy servers cache and accelerate web content delivery by serving cached content to clients.

30. Question: In IP services, what is the purpose of a Reverse Proxy?

A) Forwarding client requests to a web server

B) Accelerating web content delivery

C) Enhancing network security

D) Routing traffic between different subnets

Answer:A) Forwarding client requests to a web server

Explanation:A reverse proxy forwards client requests to appropriate web servers, often used for load balancing and security purposes.

31. Question: What is the primary goal of a Firewall in network security?

A) Load balancing network traffic

B) Providing secure remote access

C) Filtering and controlling network traffic

D) Assigning IP addresses to devices

Answer: C) Filtering and controlling network traffic

Explanation: Firewalls are primarily used to filter and control network traffic based on predefined security policies.

32. Question: Which type of firewall operates at the application layer of the OSI model and can make decisions based on application-specific content?

A) Stateful Firewall

B) Packet-Filtering Firewall

C) Proxy Firewall

D) IDS/IPS (Intrusion Detection System/Intrusion Prevention System)

Answer: C) Proxy Firewall

Explanation: A proxy firewall operates at the application layer and can inspect application-specific content.

33. Question: Which security protocol is commonly used for secure remote access to network resources and often utilizes certificates for authentication?

A) IPsec (Internet Protocol Security)

B) SSH (Secure Shell)

C) SSL/TLS (Secure Sockets Layer/Transport Layer Security)

D) PPTP (Point-to-Point Tunneling Protocol)

Answer: C) SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Explanation: SSL/TLS is commonly used for secure remote access and web encryption, often employing certificates for authentication.

34. Question: Which network security device is designed to detect and prevent unauthorized access or attacks in real-time?

A) Firewall

B) VPN Concentrator

C) IDS (Intrusion Detection System)

D) Proxy Server

Answer: C) IDS (Intrusion Detection System)

Explanation: IDS is designed to detect and alert on suspicious activities or security breaches in real-time.

35. Question: What is the primary purpose of a VPN (Virtual Private Network) Concentrator?

A) Filtering and controlling network traffic

B) Encrypting network traffic between remote sites or users

C) Load balancing incoming traffic

D) Assigning IP addresses to devices

Answer: B) Encrypting network traffic between remote sites or users

Explanation: VPN concentrators are used to establish secure, encrypted connections between remote sites or users.

36. Question: What is the primary function of an Authentication, Authorization, and Accounting (AAA) server in network security?

A) Detecting and preventing network attacks

B) Managing network traffic policies

C) Providing secure remote access

D) Handling user authentication, authorization, and accounting

Answer: D) Handling user authentication, authorization, and accounting

Explanation: AAA servers are responsible for verifying user identities, granting or denying access, and tracking user activities.

37. Question: Which security mechanism is commonly used for securing wireless networks by encrypting data traffic between wireless devices and access points?

A) WPA2 (Wi-Fi Protected Access 2)

B) MAC Filtering

C) VLAN Segmentation

D) IPsec

Answer: A) WPA2 (Wi-Fi Protected Access 2)

Explanation: WPA2 is a common protocol used to secure wireless networks by encrypting data traffic.

38. Question: What is the primary purpose of Network Address Translation (NAT) in network security?

A) Concealing internal IP addresses from external networks

B) Filtering network traffic based on application content

C) Enforcing Quality of Service (QoS) policies

D) Detecting and preventing network attacks

Answer: A) Concealing internal IP addresses from external networks

Explanation: NAT is commonly used to hide internal IP addresses from external networks.

39. Question: Which type of attack involves an attacker sending a large number of malicious requests to overwhelm and disrupt a network or service?

A) Phishing

B) DDoS (Distributed Denial of Service)

C) SQL Injection

D) Spoofing

Answer: B) DDoS (Distributed Denial of Service)

Explanation: DDoS attacks aim to overwhelm a network or service with a flood of malicious traffic.

40. Question: What is the primary function of a Network Intrusion Prevention System (IPS) in network security?

A) Detecting and alerting on network attacks

B) Filtering and controlling network traffic

C) Providing secure remote access

D) Encrypting data traffic between devices

Answer: A) Detecting and alerting on network attacks

Explanation: IPS is designed to detect and prevent network attacks by actively blocking or alerting on suspicious traffic.

41. Question: What does QoS (Quality of Service) primarily aim to improve in a network?

A) Network security

B) Network availability

C) Network performance and reliability

D) Network scalability

Answer: C) Network performance and reliability

Explanation: QoS is primarily focused on enhancing network performance and ensuring reliable delivery of services.

42. Question: Which field in an IP packet header is commonly used for classifying and marking traffic for QoS treatment?

A) Source IP address

B) Destination IP address

C) DSCP (Differentiated Services Code Point) field

D) Time-to-Live (TTL) field

Answer: C) DSCP (Differentiated Services Code Point) field

Explanation: The DSCP field in an IP header is used for marking and classifying traffic for QoS purposes.

43. Question: What is the primary function of a traffic shaper in a QoS-enabled network?

A) Prioritizing traffic

B) Dropping packets that exceed defined limits

C) Controlling the rate at which traffic is sent

D) Encrypting data traffic

Answer: C) Controlling the rate at which traffic is sent

Explanation: Traffic shapers control the rate at which traffic is sent to ensure it adheres to specified limits.

44. Question: What is the purpose of traffic policing in QoS?

A) Prioritizing traffic

B) Controlling the rate of incoming traffic

C) Encrypting data traffic

D) Ensuring high network availability

Answer: B) Controlling the rate of incoming traffic

Explanation: Traffic policing is used to control the rate of incoming traffic and potentially drop or remark packets that exceed defined limits.

45. Question: Which QoS mechanism is used to ensure that a certain amount of bandwidth is guaranteed for a specific type of traffic?

A) Traffic shaping

B) Traffic policing

C) Weighted Fair Queuing (WFQ)

D) Class-Based Weighted Fair Queuing (CBWFQ)

Answer: D) Class-Based Weighted Fair Queuing (CBWFQ)

Explanation: CBWFQ allows you to allocate a minimum bandwidth guarantee for specific traffic classes.

46. Question: What is the primary purpose of a priority queue in QoS?

A) Dropping packets that exceed defined limits

B) Ensuring high network availability

C) Prioritizing certain types of traffic

D) Controlling the rate of incoming traffic

Answer: C) Prioritizing certain types of traffic

Explanation: A priority queue is used to give higher priority to specific types of traffic.

47. Question: In a QoS-enabled network, what is the purpose of the "Best Effort" class?

A) Guaranteeing a minimum bandwidth for all traffic

B) Prioritizing mission-critical traffic

C) Treating all traffic equally without any special QoS treatment

D) Preventing traffic from exceeding defined limits

Answer: C) Treating all traffic equally without any special QoS treatment

Explanation: The "Best Effort" class does not receive any special QoS treatment and treats all traffic equally.

48. Question: Which QoS mechanism is used to allocate bandwidth fairly among different traffic flows or applications?

A) Traffic shaping

B) Traffic policing

C) Weighted Fair Queuing (WFQ)

D) Class-Based Weighted Fair Queuing (CBWFQ)

Answer: C) Weighted Fair Queuing (WFQ)

Explanation: WFQ allocates bandwidth fairly among different traffic flows based on weightings.

49. Question: What is the primary benefit of using Differentiated Services (DiffServ) for QoS?

A) It provides per-flow queuing and shaping

B) It offers fine-grained control over traffic

C) It simplifies QoS implementation by using a small number of code points

D) It guarantees minimum bandwidth for all traffic

Answer: C) It simplifies QoS implementation by using a small number of code points

Explanation: DiffServ simplifies QoS by using a small set of code points to classify and prioritize traffic.

50. Question: Which QoS tool is commonly used for reducing delay and jitter in real-time applications like VoIP and video conferencing?

A) Traffic shaping

B) Traffic policing

C) LLQ (Low Latency Queuing)

D) RED (Random Early Detection)

Answer: C) LLQ (Low Latency Queuing)

Explanation: LLQ is designed to reduce delay and jitter for real-time traffic by giving it higher priority in the queue.