Huawei

H19-301_V3.0

HCSA-Presales-IP Network Certification V3.0

Latest Version: 9.0

Question: 1

Which of the following are characteristics of traditional IP routing and forwarding? (Select All that Apply)

A. All routers need to know the network-wide routes.
B. Each router needs to obtain the network layer information about the packet and selects routing entries for packet forwarding based on the longest match rule.
C. It is connectionless and cannot provide good end-to-end QoS guarantee.
D. It uses the hop-by-hop forwarding mode, in which a packet is decapsulated by all routers that receive the packet.

Answer: A,B,C,D

Explanation:
Option A:In traditional IP routing, each router in the network must maintain a routing table that contains network-wide routes or at least the routes relevant to its operation. This ensures that packets can be forwarded correctly to their destination.
Option B:Traditional IP routing operates on the principle of the "longest match rule." When a router receives a packet, it examines the destination IP address and matches it against the entries in its routing table. The longest prefix match determines the next hop for the packet.
Option C:Traditional IP networks are inherently connectionless, meaning there is no dedicated path established between the source and destination before data transmission. This lack of connectionoriented mechanisms makes it challenging to guarantee Quality of Service (QoS) across the entire network.
Option D:In traditional IP networks, packets are forwarded using a hop-by-hop mechanism. Each router along the path decapsulates the packet, inspects its headers, and forwards it to the next hop based on its routing table.
Reference:
HCSA-Presales-IP Network V3.0 Training Material, Chapter 2: IP Routing Fundamentals.
Huawei Networking Technology and Device (HNTD) Documentation.

Question: 2

Unlike managing a device through a console port, managing a device through Telnet does not require connecting to the device with a cable. The only requirement is that the Telnet client has a reachable address and can communicate with the Telnet service port of the device. Which kind of address should the client have?

A. VLAN
B. AS
C. MAC

D. IP

Answer: D

Explanation:
Understanding Telnet:Telnet is a protocol used for remote management of networkdevices. Unlike console port management, which requires a physical connection, Telnet operates over the network.
Address Requirement:For Telnet communication to occur, the client must have an IP address. This is because Telnet relies on the TCP/IP protocol suite, and communication is established using IP addresses.
Why Not Other Options?
VLAN:A VLAN (Virtual Local Area Network) is a logical segmentation of a network but does not directly represent an address for communication.
AS:An Autonomous System (AS) is a collection of IP networks under a single administrative domain, not an address type.
MAC:A MAC address is a hardware identifier used at Layer 2 of the OSI model. While important for local network communication, it is not sufficient for Telnet, which operates at Layer 3.
Conclusion:The correct answer is IP, as it is the fundamental addressing scheme required for Telnet communication.
Reference:
HCSA-Presales-IP Network V3.0 Training Material, Chapter 5: Network Management Protocols.
Huawei Enterprise Networking Product Documentation.

Question: 3

Depending on the geographical coverage, networks can be classified into local area networks (LANs), wide area networks (WANs), and metropolitan area networks (MANs) between LANs and WANs.

A. TRUE
B. FALSE

Answer: A

Explanation:
Network Classification Based on Geographical Coverage:
Networks are categorized based on their geographical scope into three primary types:
Local Area Network (LAN):Covers a small geographic area, such as a single building or campus.
Metropolitan Area Network (MAN):Covers a larger area than a LAN, typically spanning a city or metropolitan region. It serves as an intermediate between LANs and WANs.
Wide Area Network (WAN):Covers a large geographic area, often spanning multiple cities, countries, or continents.
Role of MANs:MANs act as a bridge between LANs and WANs, providing connectivity for organizations that need to connect multiple LANs within a city or region.
Conclusion:The statement is correct because networks are indeed classified into LANs, MANs, and WANs based on their geographical coverage.
Reference:

HCSA-Presales-IP Network V3.0 Training Material, Chapter 1: Network Fundamentals.
Huawei Networking Technology and Device (HNTD) Documentation.

Question: 4

Which of the following are dynamic routing protocols? (Select All that Apply)

A. OSPF
B. IS-IS
C. RIP
D. BGP

Answer: A,B,C,D

Explanation:
Dynamic Routing Protocols Overview:
Dynamic routing protocols enable routers to exchange routing information dynamically, allowing them to adapt to changes in the network topology automatically.
Explanation of Each Protocol:
OSPF (Open Shortest Path First):A link-state routing protocol that uses the Dijkstra algorithm to calculate the shortest path to destinations. It is widely used in enterprise networks.
IS-IS (Intermediate System to Intermediate System):Another link-state routing protocol, similar to OSPF, but primarily used in service provider networks.
RIP (Routing Information Protocol):A distance-vector routing protocol that uses hop count as its metric. It is simple but less scalable compared to OSPF and IS-IS.
BGP (Border Gateway Protocol):A path-vector routing protocol used for inter-domain routing (e.g., between autonomous systems). It is the backbone of the Internet.
Conclusion:All four options (OSPF, IS-IS, RIP, and BGP) are dynamic routing protocols.
Reference:
HCSA-Presales-IP Network V3.0 Training Material, Chapter 2: IP Routing Protocols.
Huawei Enterprise Networking Product Documentation.

Question: 5

What are the basic roles of devices in the typical MPLS VPN technical architecture? (Select All that Apply)

A. PE
B. Aggregation
C. P
D. Core
E. CE

Answer: A,C,E

Explanation:
MPLS VPN Architecture Overview:
MPLS (Multiprotocol Label Switching) VPN is a widely used technology for creating virtual private networks over a shared infrastructure. It involves specific roles for devices in the network.
Explanation of Each Role:
PE (Provider Edge):These devices sit at the edge of the service provider's network and connect to customer sites. They are responsible for assigning labels and managing VPN routes.
P (Provider):These devices are located in the core of the service provider's network.They perform label switching but do not participate in VPN-specific functions.
CE (Customer Edge):These devices belong to the customer and connect to the PE devices. They are unaware of the MPLS network and simply forward traffic to the PE.
Aggregation and Core:These terms are not specific to MPLS VPN architecture. "Aggregation" refers to a general networking concept, and "Core" is too broad to describe a specific role in MPLS VPNs.
Conclusion:The correct roles in MPLS VPN architecture are PE, P, and CE.
Reference:
HCSA-Presales-IP Network V3.0 Training Material, Chapter 7: MPLS and VPN Technologies.
Huawei MPLS Solution Guide.