Nokia Certified Network Routing Specialist I (NRS I) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Router R5 receives four route updates for the same prefix. Which of the four routes will be installed in R5's routing table?**

   A. Route learned from router R1

   B. Route learned from router R2

   C. Route learned from router R3

   D. Route learned from router R4

2. **How does OSPF identify the most up-to-date routing information?**

   A. By the priority value in the Hello packet.

   B. By the age in the Link State Advertisement.

   C. By master/slave status in the Database Description packet.

   D. By the sequence number in the Link State Advertisement.

3. **What is meant by the "next-hop" in routing?**

   A. The final destination IP address of a packet

   B. The last router that has processed the packet

   C. The IP address of the next router where a packet should be forwarded

   D. The address of the originating device

4. **Which of the following is the physical infrastructure that provides interconnections between ISPs?**

   A. A demarcation point

   B. An Internet exchange point

   C. A central office

   D. A point of presence

5. **Which of the following about an IP filter in a Nokia 7750 SR is FALSE?**

   A. It is also known as an Access Control List (ACL).

   B. It is applied to all interfaces by default.

   C. It can filter traffic based on IP addresses.

   D. It can be applied to egress traffic.

6. What is the main difference between TCP and UDP?

- **A. TCP is connectionless; UDP is connection-oriented**
- **B. TCP is faster; UDP is slower**
- **C. TCP is connection-oriented and reliable; UDP is connectionless and faster**
- **D. TCP prioritizes quality; UDP prioritizes speed**

7. What is the primary advantage of using ICMP?

- **A. To provide secure data transmission**
- **B. To manage bandwidth efficiently**
- **C. To provide error reporting and diagnostics of network communications**
- **D. To enhance signal strength in networks**

8. Which statement about the displayed IP filter on a Nokia 7750 SR is TRUE?

- **A. It discards traffic from network 1.2.3.0/24.**
- **B. It discards traffic to network 1.2.3.0/24.**
- **C. It discards all traffic except from network 1.2.3.0/24.**
- **D. It discards all traffic except to network 1.2.3.0/24.**

9. What operation does an iLER perform when it receives a packet?

- **A. It pushes a new MPLS label and forwards the packet to the next LSR.**
- **B. It swaps the MPLS label and forwards the packet to the next LSR.**
- **C. It forwards the packet to the next LSR without altering the MPLS label.**
- **D. It pops the MPLS label and forwards the packet to the next IP router.**

10. In the context of BGP, what does AS represent?

- **A. Automatic System**
- **B. Autonomous System**
- **C. Administered Segment**
- **D. Authorized Segment**

Answers

1. D
2. D
3. C
4. B
5. B
6. C
7. C
8. A
9. A
10. B

Explanations

1. Router R5 receives four route updates for the same prefix. Which of the four routes will be installed in R5's routing table?

A. Route learned from router R1

B. Route learned from router R2

C. Route learned from router R3

D. Route learned from router R4

In routing protocols, when a router receives multiple updates for the same prefix, it applies certain rules to determine which route to install in its routing table. The key factors typically include the administrative distance, metric values, and the specific routing protocol used. In this case, if route updates are being considered, one likely reason for D being the correct answer is that it has the most preferred administrative distance or the best metric among the received routes. Administrative distance is a value that routers use to determine the trustworthiness of the route source; lower values indicate more reliable sources. If the route from router R4 offers the best metric (e.g., shortest path) and a lower administrative distance than those from R1, R2, and R3, then it would be the route that gets installed in R5's routing table. In routing, the principle of using the best route applies heavily when multiple routes exist for the same destination. Therefore, if R4's route is the most efficient (with a better metric or lower administrative distance), it becomes the selected route installed in the routing table of R5.

2. How does OSPF identify the most up-to-date routing information?

A. By the priority value in the Hello packet.

B. By the age in the Link State Advertisement.

C. By master/slave status in the Database Description packet.

D. By the sequence number in the Link State Advertisement.

OSPF utilizes the sequence number in the Link State Advertisement (LSA) to identify the most up-to-date routing information. Each LSA generated by an OSPF router contains a unique sequence number. When routers exchange LSAs, they use this sequence number to determine which LSA is more recent. If a router receives an LSA with a higher sequence number than it already has in its database, it recognizes that the new LSA represents more current routing information and updates its local database accordingly. The sequence number mechanism allows OSPF to efficiently maintain and synchronize routing information across the network. This ensures that routers have the latest information to make optimal routing decisions, which is crucial for maintaining the overall performance and reliability of an OSPF network. This choice is key in OSPF's operation, as it avoids potential issues that could arise from older or duplicate routing information being used, thus maintaining a consistent and accurate view of the network topology among all OSPF routers.

3. What is meant by the "next-hop" in routing?

A. The final destination IP address of a packet

B. The last router that has processed the packet

C. The IP address of the next router where a packet should be forwarded

D. The address of the originating device

The term "next-hop" in routing refers to the IP address of the next router where a packet should be forwarded. In a network, when a packet is sent from a source to a destination, it may need to pass through one or more intermediate routers before reaching its final destination. The next-hop address is critical in determining the path that packets take through a network. It provides the information necessary for routers to make forwarding decisions based on the destination IP address of the packet. By identifying the next hop, routers can efficiently route packets toward their end destination, optimizing network performance and minimizing delays. In this context, the next-hop address is not the final destination of the packet, nor is it the last router that processed the packet or the address of the originating device. Instead, it is specifically focused on the immediate next step in the packet's journey through the network. This mechanism is fundamental to routing protocols, as they rely on next-hop information to construct efficient routing tables and ensure data reaches its intended endpoint.

4. Which of the following is the physical infrastructure that provides interconnections between ISPs?

A. A demarcation point

B. An Internet exchange point

C. A central office

D. A point of presence

The correct answer is an Internet exchange point, which plays a vital role in the internet's structure by serving as a physical infrastructure where different Internet Service Providers (ISPs) interconnect. This facility allows ISPs to exchange traffic directly with one another, thus enhancing the efficiency of data transfer. By bypassing the need for third-party networks for data transfers, ISPs can achieve lower latency, reduced costs, and improved speed for their customers. Internet exchange points are strategically located in various regions, and they often host multiple networks and service providers. This clustering facilitates easier and more effective peering arrangements, allowing for seamless data exchange without necessitating transits through other intermediaries. In contrast, a demarcation point typically refers to the point at which the ISP's network ends and the customer's connection begins, not necessarily a point of interconnection for ISPs themselves. A central office serves primarily as a facility for telecommunications equipment, focusing more on end-user connections than on ISP interconnectivity. Meanwhile, a point of presence represents a location where an ISP maintains a presence for connecting to the end users but does not specifically function as an interconnection point for multiple ISPs. Thus, the Internet exchange point is distinctly recognized for its critical role in facilitating

5. Which of the following about an IP filter in a Nokia 7750 SR is FALSE?

A. It is also known as an Access Control List (ACL).

B. It is applied to all interfaces by default.

C. It can filter traffic based on IP addresses.

D. It can be applied to egress traffic.

The assertion that the IP filter is applied to all interfaces by default is incorrect. IP filters, or Access Control Lists (ACLs), on the Nokia 7750 SR need to be explicitly applied to individual interfaces as per the configuration requirements. This design allows for more granular control over which filters are used on specific interfaces, enabling network administrators to manage and optimize traffic based on their unique needs and policies. The other statements hold true: IP filters are indeed referred to as Access Control Lists (ACLs), they can effectively filter traffic based on IP addresses, and they can be applied to egress traffic, which refers to traffic leaving the interface. By requiring explicit application of filters, the design promotes flexibility and precision in network traffic management.

6. What is the main difference between TCP and UDP?

A. TCP is connectionless; UDP is connection-oriented

B. TCP is faster; UDP is slower

C. TCP is connection-oriented and reliable; UDP is connectionless and faster

D. TCP prioritizes quality; UDP prioritizes speed

The correct choice highlights that TCP (Transmission Control Protocol) is connection-oriented and reliable, while UDP (User Datagram Protocol) is connectionless and typically faster in terms of data transmission. TCP establishes a connection before data can be sent, ensuring that packets are delivered in order and without errors. This is achieved through mechanisms like error checking, retransmission of lost packets, and flow control. As a result, applications that require reliable communication, such as file transfers or email, often use TCP. On the other hand, UDP does not set up a connection before sending data. It simply sends packets (datagrams) without guaranteeing their delivery, order, or integrity. This makes UDP much faster than TCP, as there is no need for the overhead of establishing a connection or checking for errors. It is often preferred for applications like video streaming or online gaming where speed is more critical than reliability. The other options reflect misunderstandings about the fundamental characteristics of these two protocols. For example, TCP being connectionless or UDP being slower contradicts the established definitions of both protocols. Additionally, while UDP does prioritize speed, it does not inherently prioritize quality; rather, it sacrifices some reliability to achieve this speed.

7. What is the primary advantage of using ICMP?

A. To provide secure data transmission

B. To manage bandwidth efficiently

C. To provide error reporting and diagnostics of network communications

D. To enhance signal strength in networks

The primary advantage of using ICMP (Internet Control Message Protocol) lies in its ability to provide error reporting and diagnostics for network communications. ICMP is an integral part of the Internet Protocol suite and serves several key functions, primarily focused on ensuring that the communication between devices across a network remains effective and efficient. One of the critical roles of ICMP is to send error messages when there are issues with the transmission of data packets. For instance, if a router cannot deliver a packet, it can send an ICMP message back to the source to inform it about the problem, such as "destination unreachable" or "time exceeded." This helps network administrators and engineers quickly identify and resolve issues. Additionally, ICMP facilitates diagnostic tools like "ping" and "traceroute," which are commonly used to assess the reachability of devices and to trace the path packets take through the network. This functionality is essential for troubleshooting connectivity problems and optimizing network performance. In contrast, the other options do not accurately reflect the primary functions of ICMP. Security features are not inherently a part of ICMP, as it does not provide encryption or secure data transmission. Likewise, ICMP does not manage bandwidth; it does not enhance or control the allocation of bandwidth across a network

8. Which statement about the displayed IP filter on a Nokia 7750 SR is TRUE?

A. It discards traffic from network 1.2.3.0/24.

B. It discards traffic to network 1.2.3.0/24.

C. It discards all traffic except from network 1.2.3.0/24.

D. It discards all traffic except to network 1.2.3.0/24.

The statement that traffic from network 1.2.3.0/24 is discarded is true because IP filters on devices like the Nokia 7750 SR typically control the flow of packets based on specified criteria, which may include source or destination IP addresses, among others. If the filter is configured to specifically discard traffic originating from a certain IP range, such as 1.2.3.0/24, then it will not allow packets from that source to pass through, thereby effectively preventing any traffic from that network from being transmitted. Understanding the structure of IP filtering helps clarify why this statement holds true. Filters often define rules based on source or destination, so if the rule in question explicitly specifies a discard action for the source network, it aligns with the observed behavior towards data packets originating from that address block.

9. What operation does an iLER perform when it receives a packet?

A. It pushes a new MPLS label and forwards the packet to the next LSR.

B. It swaps the MPLS label and forwards the packet to the next LSR.

C. It forwards the packet to the next LSR without altering the MPLS label.

D. It pops the MPLS label and forwards the packet to the next IP router.

The operation performed by an iLER (Ingress Label Edge Router) upon receiving a packet that is labeled involves pushing a new MPLS label onto the packet before forwarding it to the next Label Switching Router (LSR). This is a key part of the MPLS (Multiprotocol Label Switching) protocol, where the ingress router adds (or "pushes") a label to outbound packets to facilitate efficient and fast forwarding through the network. The iLER is responsible for determining the appropriate label based on its forwarding table, which typically takes into account the destination of the packet as well as other criteria. By pushing a new MPLS label, the data packet gets a new identity that allows subsequent LSRs in the MPLS path to forward the packet based on this label, rather than requiring a deeper examination of the packet contents itself. This process enhances network efficiency by reducing the need for every router along the path to perform complex route look-ups for each packet. Instead, they can simply read the MPLS labels to determine how to route the packets. Other operations like swapping, forwarding unchanged, or popping the label are performed by different types of MPLS routers along the path, which is why they do not align with what an iLER does. The i

10. In the context of BGP, what does AS represent?

A. Automatic System

B. Autonomous System

C. Administered Segment

D. Authorized Segment

In the context of Border Gateway Protocol (BGP), AS stands for Autonomous System. An Autonomous System is a collection of IP networks and routing policies that operates under a single technical administration. Each AS is assigned a unique Autonomous System Number (ASN) which is used in BGP to facilitate routing decisions between different networks on the internet. The concept of an Autonomous System is fundamental to understanding BGP as it helps in the identification of the paths that data can take across the vast network of interconnected systems. BGP uses this concept to maintain and share routing information effectively, allowing for efficient routing decisions that adhere to the policies defined by each AS. Understanding this terminology is crucial for networking professionals, particularly those involved in routing and internet connectivity, as it directly affects how data is managed and directed between different networks globally.