Huawei Certified ICT Professional (HCIP) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **What is the typical time frame for reviewing and finalizing a risky operation solution before implementation?**
   - **A. One week**
   - **B. One month**
   - **C. One day**
   - **D. One hour**

2. **Which protocol can operate in both dense mode (DM) and sparse mode (SM)?**
   - **A. PIM**
   - **B. IGMP**
   - **C. DVMRP**
   - **D. OSPF**

3. **How does an IGMPv2 router recognize group membership on a local segment?**
   - **A. By maintaining a timer and deleting memberships that timeout**
   - **B. By sending a Query message after every membership change**
   - **C. By maintaining fixed membership regardless of traffic**
   - **D. By relying solely on Leave messages from hosts**

4. **Is using default routes between routers more resource-intensive than complete routing tables?**
   - **A. True**
   - **B. False**

5. **On a network operating with STP, how many types of RSTP BPDUs are defined?**
   - **A. One**
   - **B. Two**
   - **C. Three**
   - **D. Four**

6. What type of network does OSPF typically not recognize by default?

A. P2MP network

B. P2P network

C. Broadcast network

D. Hybrid network

7. Is it true that only MD5 authentication is supported between BGP peers?

A. True

B. False

8. The main difference between an OSPF NSSA area and a stub area is?

A. External routes can be imported into a NSSA area

B. Stub areas do not support external routes

C. NSSA areas allow for multiple ASBRs

D. Stub areas cannot be configured with ABRs

9. Which layer does DHCP typically operate at?

A. Transport layer

B. Application layer

C. Network layer

D. Data link layer

10. Which aspect does NOT contribute to network congestion issues?

A. High traffic volume on the network.

B. Slow processing speed of routers.

C. Unoptimized routing protocols.

D. Increased bandwidth availability.

Answers

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

Explanations

1. What is the typical time frame for reviewing and finalizing a risky operation solution before implementation?

A. One week

B. One month

C. One day

D. One hour

The typical time frame for reviewing and finalizing a risky operation solution before implementation is often a matter of urgency and thoroughness. In highly dynamic environments, such as IT and telecommunications, quick decision-making can be essential due to the fast-paced nature of technology and operations. A review period of one hour allows teams to quickly assess the risks, conduct necessary evaluations, and finalize solutions efficiently, particularly when time-sensitive operations must be addressed immediately. This short time frame is particularly realistic in scenarios where a quick evaluation of risks and a rapid response is necessary, such as in critical system adjustments or emergency situation protocols. The one-hour duration emphasizes the capacity for swift response while still maintaining a level of risk assessment, reflecting the capability of teams to make quick yet informed decisions based on their expertise and pre-existing protocols. While longer durations such as one day or one week may be appropriate for more complex or less urgent matters, the context of the operation in question influences the appropriateness of the one-hour timeframe, especially in environments where speed and rapid execution are key due to potential impacts on business continuity or service delivery. Thus, the choice of one hour aligns well with scenarios requiring urgent action and timeliness in risk management.

2. Which protocol can operate in both dense mode (DM) and sparse mode (SM)?

A. PIM

B. IGMP

C. DVMRP

D. OSPF

The chosen answer is PIM (Protocol Independent Multicast), which is indeed capable of operating in both dense mode (DM) and sparse mode (SM). PIM is a multicast routing protocol designed to efficiently route data to multiple recipients. Its flexibility allows it to adapt to different network environments—dense mode is often used in networks where multicast group members are concentrated in a small area, while sparse mode is used when members are distributed across a wider geographical area.   By using PIM, a network can effectively handle multicast traffic regardless of the distribution of the receivers. In dense mode, PIM uses a flood-and-prune mechanism to send multicast traffic to all potential recipients initially, then prunes back the branches where there are no group members. In sparse mode, it relies on explicit Join requests from receivers and uses a shared tree or source tree to manage traffic delivery, reducing unnecessary load on the network. In contrast, the other protocols listed do not share this dual-mode capability. IGMP (Internet Group Management Protocol) is primarily concerned with managing membership in multicast groups rather than routing. DVMRP (Distance Vector Multicast Routing Protocol) is designed mainly for dense mode environments and does not facilitate sparse mode operation effectively. OSPF (Open Shortest

3. How does an IGMPv2 router recognize group membership on a local segment?

- A. By maintaining a timer and deleting memberships that timeout
- B. By sending a Query message after every membership change
- C. By maintaining fixed membership regardless of traffic
- D. By relying solely on Leave messages from hosts

An IGMPv2 router recognizes group membership on a local segment primarily by maintaining a timer that tracks each group's membership and deletes memberships that timeout. This process is fundamental to managing multicast group membership efficiently. In IGMPv2, hosts on a local network send Membership Reports to indicate their interest in receiving multicast traffic for specific groups. The router listens for these reports. If the router does not receive a Membership Report for a group within a specified time period (defined by the membership timeout), it assumes that no hosts want to receive the multicast traffic for that group anymore and removes that entry from its membership list. This timer mechanism helps ensure that group membership is current and reflects the active interest of hosts on the local segment. When considering the other options, sending Query messages does play a role in prompting hosts to report their membership but is not the primary method for recognizing group membership changes. Maintaining fixed membership regardless of traffic does not accurately reflect the dynamic nature of IGMP, as it would not account for hosts joining or leaving groups. Finally, relying solely on Leave messages would neglect the necessary communication of hosts joining the group, which could lead to incomplete or outdated membership information.

4. Is using default routes between routers more resource-intensive than complete routing tables?

- A. True
- B. False

Using default routes between routers involves directing traffic through a single, overarching path for packets destined for networks not included in the router's routing table. This method simplifies routing decisions because routers only need to reference the default route for unknown destinations rather than maintaining extensive routing tables with network-specific paths. When a router employs default routes, it can significantly conserve CPU and memory resources compared to managing complete routing tables that list all possible routes. Complete routing tables encompass detailed entries for each network, which can grow substantially in size, especially in larger networks or the Internet. Such extensive routing tables require more processing power and memory for lookups, updates, and maintenance. Hence, utilizing default routes is less resource-intensive because it reduces the complexity and size of routing information that routers need to manage. This efficiency is particularly beneficial in decreasing the overhead in environments where routing table management can become burdensome. In contrast, complete routing tables entail a higher demand on system resources, making the assertion that using default routes is more resource-intensive inaccurate.

5. On a network operating with STP, how many types of RSTP BPDUs are defined?

A. One

B. Two

C. Three

D. Four

In a network operating with Rapid Spanning Tree Protocol (RSTP), there are two types of Bridge Protocol Data Units (BPDUs) defined: the Configuration BPDU and the TCN (Topology Change Notification) BPDU. The Configuration BPDU is used to convey information about the network topology, including the bridge IDs and port roles, while the TCN BPDU is specifically utilized to inform other switches of topology changes, allowing the network to react accordingly. Understanding this distinction is crucial because it highlights how RSTP is designed to enhance the traditional Spanning Tree Protocol (STP) by allowing for rapid convergence and efficient handling of topology changes. In contrast to that, stating there is only one type of BPDU misses the complexity and functionality of RSTP in managing network changes and maintaining stability. The correct interpretation recognizes the two types, ensuring a deeper comprehension of RSTP's operational mechanisms.

6. What type of network does OSPF typically not recognize by default?

A. P2MP network

B. P2P network

C. Broadcast network

D. Hybrid network

The correct answer is that OSPF does not typically recognize a point-to-multipoint (P2MP) network by default. OSPF (Open Shortest Path First) is a link-state routing protocol used within a single AS (Autonomous System), and it is designed to work optimally with certain types of network topologies. In OSPF, the protocol is specifically optimized for point-to-point (P2P) networks, broadcast networks such as Ethernet, and non-broadcast multiple access (NBMA) networks. These types of networks have easily identifiable and manageable broadcast mechanisms that facilitate the OSPF's operations, such as sending Link State Advertisements (LSAs) efficiently. In contrast, a point-to-multipoint (P2MP) network topology introduces complexities because there is not a clear, single point that can handle all OSPF advertisement and communication, which can lead to challenges in how OSPF manages neighbor relationships and link-state information among multiple endpoints. As such, OSPF requires additional configuration to effectively operate in P2MP environments, which is why it does not recognize them by default.

7. Is it true that only MD5 authentication is supported between BGP peers?

A. True

B. False

The statement that only MD5 authentication is supported between BGP peers is not accurate. BGP (Border Gateway Protocol) can indeed utilize MD5 for authentication, but it is not limited to this method alone. The purpose of using MD5 is to secure BGP sessions by ensuring that the peers can authenticate each other and prevent unauthorized access to the BGP sessions. Many implementations of BGP support additional security measures and protocols, which can also include other forms of authentication beyond MD5, though MD5 is a commonly used option. Hence, MD5 is not the only method for authenticating BGP peers, making the assertion that only MD5 is supported incorrect. The flexibility in authentication mechanisms allows network administrators to choose the method that best fits their security requirements and the specific capabilities of their network hardware and software. Given this understanding, the correct answer to the question is that it is false that only MD5 authentication is supported between BGP peers.

8. The main difference between an OSPF NSSA area and a stub area is?

A. External routes can be imported into a NSSA area

B. Stub areas do not support external routes

C. NSSA areas allow for multiple ASBRs

D. Stub areas cannot be configured with ABRs

An NSSA (Not-So-Stubby Area) is designed to allow the importation of external routes, specifically from an Autonomous System Boundary Router (ASBR). This characteristic differentiates it significantly from a stub area, which does not permit external routes to be introduced. In an NSSA, external routes can be injected into the routing table, but they are treated differently than they would be in a normal area. This means that while NSSA areas can utilize the benefits of summarized routing and reduced overhead associated with stub areas, they still allow for a controlled method of bringing in external routing information. Having this capability enables better flexibility and connectivity for complex networking scenarios where both OSPF and external routing protocols are in play. The other options highlight characteristics that do not align with the definitions and functionality of NSSA and stub areas. Stub areas prevent external routes altogether, ensuring that their routing table remains simpler and focused solely on internal OSPF routes. The constraints on the use of ABRs (Area Border Routers) and the number of ASBRs in each type of area also support this fundamental difference in design purpose and operational capacity between these two OSPF area types.

9. Which layer does DHCP typically operate at?

A. Transport layer

B. Application layer

C. Network layer

D. Data link layer

Dynamic Host Configuration Protocol (DHCP) operates at the application layer of the OSI model. This layer is responsible for providing network services to applications and enables protocols to manage communication sessions between endpoints. Specifically, DHCP is designed to automate the process of IP address assignment and configuration settings for devices on a network. It enables devices to request and obtain IP addresses and other network parameters, simplifying network administration and management. The application layer encompasses protocols that facilitate software applications to interact with the underlying network, which is precisely what DHCP does. It uses protocols like UDP (User Datagram Protocol) at the transport layer to transmit its messages, but its core functionality and purpose align with the application layer. By operating here, DHCP communicates the necessary network information to clients without dealing directly with lower-layer functionalities like data transportation or network routing.

10. Which aspect does NOT contribute to network congestion issues?

A. High traffic volume on the network.

B. Slow processing speed of routers.

C. Unoptimized routing protocols.

D. Increased bandwidth availability.

Increased bandwidth availability does not contribute to network congestion issues because it directly enhances the capacity of the network to handle data traffic. When bandwidth is available in greater quantities, it allows more data to be transmitted simultaneously, effectively easing the flow of traffic and reducing the likelihood of congestion. In contrast, high traffic volume on the network, slow processing speed of routers, and unoptimized routing protocols can lead to congestion. High traffic volume increases the demand for bandwidth, potentially exceeding available resources and causing delays. Slow processing speeds in routers can lead to bottlenecks as packets are queued waiting for processing. Unoptimized routing protocols may result in inefficient paths being taken by data, adding unnecessary hops and increasing overall latency. Each of these issues can exacerbate network congestion, making increased bandwidth a vital solution rather than a contributing factor.