Cisco Learning Network Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **Which three statements accurately describe MAC Authentication Bypass (MAB)?**

   A. MAB uses a device's IP address for authentication

   B. MAB uses a MAC address for both the username and password

   C. MAB is more secure than other authentication methods

   D. MAB is often used to authenticate devices such as printers

2. **Which standard identifies a hop-by-hop technique for data path virtualization?**

   A. 802.1Q

   B. 802.1X

   C. 802.1P

   D. 802.1S

3. **Which protocol allows a receiver to register interest in multicast traffic at the first hop router?**

   A. IGMP

   B. RIP

   C. OSPF

   D. IGRP

4. **In the context of management tools, what is true about agents?**

   A. They are optional for Chef and Puppet

   B. They are essential for deployment

   C. They can run independently of the management system

   D. They are only needed for virtual machines

5. **Which of the following options is NOT a characteristic of the Orchestration Plane?**

   A. First point of Authentication

   B. Distributes vSmart controllers to vEdge routers

   C. Authorizes all control connections

   D. Monitors network performance data

6. Which inter-VLAN routing method involves a router with separate physical interfaces connected to access ports in different VLANs?

A. Router-on-a-stick

B. Traditional inter-VLAN routing

C. Layer 3 switching

D. Dynamic ARP Inspection

7. In which SD-WAN plane would you find vBond operating?

A. Control Plane

B. Data Plane

C. Management Plane

D. Orchestration Plane

8. Which protocol can be used in conjunction with Local EAP as a backup?

A. LDAP

B. RADIUS

C. NTLM

D. Kerberos

9. Which of the following SD-WAN components serves as the endpoint for data traffic?

A. vBond

B. vSmart

C. vEdge

D. vManage

10. Which of the following correctly characterizes Access Lists in routing configurations?

A. They are primarily used for policy-based routing adjustments.

B. They can only permit full prefixes, not sub-prefixes.

C. They are simpler to configure than route maps.

D. They utilize complex numbers to dictate matching criteria.

Answers

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

Explanations

1. Which three statements accurately describe MAC Authentication Bypass (MAB)?

A. MAB uses a device's IP address for authentication

B. MAB uses a MAC address for both the username and password

C. MAB is more secure than other authentication methods

D. MAB is often used to authenticate devices such as printers

MAC Authentication Bypass (MAB) is a network access control method that primarily relies on the MAC address of a device to facilitate authentication. In MAB, the MAC address of the device acts as both the username and the password during the authentication process. This simplicity allows MAB to quickly identify and grant access to devices that do not support more advanced authentication protocols, such as 802.1X. When a device attempts to connect to the network, its MAC address is sent to the authentication server. The server checks this MAC address against its database to determine if the device is authorized for network access. This makes the use of the MAC address crucial in MAB, validating the option that states MAB uses a MAC address for both the username and password. In the context of security, MAB does have its limitations compared to other authentication methods such as 802.1X, which provides robust security mechanisms. Therefore, claiming that MAB is more secure than other methods does not accurately reflect its comparative safety. While MAB can certainly authenticate devices such as printers, it is not limited to this type of equipment. Other devices not supporting standard authentication protocols might also rely on MAB for access. Thus, while commonly used for printers and similar equipment

2. Which standard identifies a hop-by-hop technique for data path virtualization?

A. 802.1Q

B. 802.1X

C. 802.1P

D. 802.1S

The correct choice is based on the fact that IEEE 802.1Q is the standard that specifies VLAN (Virtual Local Area Network) tagging for Ethernet frames, thereby providing a method for data path virtualization. This standard enables the creation of virtual networks over a single physical network infrastructure. The "hop-by-hop" technique refers to the process where data packets are tagged at each switch (hop) they traverse, ensuring that they remain associated with the correct VLAN throughout their journey across the network. By implementing 802.1Q, a network can efficiently separate different types of traffic and improve overall network management through virtualization. This is crucial for maintaining data integrity and network performance in environments that require multiple, isolated networks sharing the same physical resources. The other standards listed do not pertain specifically to the hop-by-hop technique for data path virtualization. For instance, 802.1X is focused on network access control and authentication, while 802.1P deals with traffic prioritization through QoS (Quality of Service). On the other hand, 802.1S addresses Multiple Spanning Tree Protocol (MSTP), which optimizes the spanning tree operation across multiple VLANs but does not directly relate to hop-by-hop data path virtualization.

3. Which protocol allows a receiver to register interest in multicast traffic at the first hop router?

A. IGMP

B. RIP

C. OSPF

D. IGRP

The correct choice is IGMP, which stands for Internet Group Management Protocol. This protocol is specifically designed to allow a host to express interest in receiving multicast traffic. When a device wants to join a multicast group, it sends an IGMP membership report to the local router (the first hop router), which then becomes responsible for managing the multicast traffic for that group. IGMP plays a crucial role in traditional IP multicast networks since it helps in managing the membership of multicast groups and provides a mechanism for routers to understand which hosts are interested in specific multicast traffic. By utilizing IGMP, the routers can manage bandwidth more efficiently and forward multicast traffic only to those segments of the network where there are interested receivers. Other protocols listed, such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and IGRP (Interior Gateway Routing Protocol), are routing protocols used for determining the best path for unicast traffic across a network rather than managing multicast group membership. They do not facilitate the registration of hosts' interest in multicast traffic, which is the specific function of IGMP.

4. In the context of management tools, what is true about agents?

A. They are optional for Chef and Puppet

B. They are essential for deployment

C. They can run independently of the management system

D. They are only needed for virtual machines

In the context of management tools such as Chef and Puppet, agents play a crucial role in the automation and management of infrastructure. They are essential for deployment because they act as the components that communicate directly with the central management server. Agents are responsible for executing the instructions and configurations sent from the management system to ensure that the desired state of the system is maintained. When using a configuration management tool, the agent takes care of applying configurations, enforcing policies, and reporting back the status to the management server. This interaction is vital for ensuring that changes are appropriately deployed across the infrastructure. Without agents, configuration management would lack the automation and responsiveness needed for effective deployment and management. Other options suggest alternative roles or usages of agents, but those do not reflect the fundamental purpose of agents in tools like Chef and Puppet, which is to facilitate deployment and management efficiently and effectively.

5. Which of the following options is NOT a characteristic of the Orchestration Plane?

A. First point of Authentication

B. Distributes vSmart controllers to vEdge routers

C. Authorizes all control connections

D. Monitors network performance data

The Orchestration Plane is primarily responsible for managing control plane data, which includes functions such as device authentication, distribution, and authorization. It serves as the central management component that performs critical tasks to maintain the overall health and organization of the network. The role of the Orchestration Plane includes authenticating devices before they can join the network, ensuring that vSmart controllers are properly distributed to vEdge routers, and authorizing connections between different components of the network. This functionality is vital for maintaining security and ensuring that the various elements of the network can communicate effectively. On the other hand, monitoring network performance data typically falls under the responsibilities of other components, such as the data plane or monitoring tools that analyze traffic and network behavior, rather than the Orchestration Plane itself. Therefore, the ability to monitor performance does not align with the primary characteristics of the Orchestration Plane, making it the correct choice for this question.

6. Which inter-VLAN routing method involves a router with separate physical interfaces connected to access ports in different VLANs?

A. Router-on-a-stick

B. Traditional inter-VLAN routing

C. Layer 3 switching

D. Dynamic ARP Inspection

Traditional inter-VLAN routing involves the use of a router with multiple physical interfaces, each one connected to a switch port that is assigned to a different VLAN. This setup requires that the router has a physical port for each VLAN so that it can route traffic between them. This method effectively allows the router to receive traffic from one VLAN, process it, and then forward it to another VLAN through its different physical interfaces. In this scenario, each interface on the router is assigned an IP address that corresponds to the subnet of the VLAN it is servicing. This means that devices within those VLANs can communicate with each other through the router by using the respective subnet IP addresses when sending packets. This method is distinct from the other options. In contrast, router-on-a-stick involves a single router interface that is configured with sub-interfaces for each VLAN and uses VLAN tagging to manage inter-VLAN traffic through a trunk link. Layer 3 switching refers to the capability of certain switches to perform routing functions without needing a separate router, whereas Dynamic ARP Inspection is a security feature that helps prevent ARP spoofing attacks. Each of these methods serves different purposes in network design and architecture.

7. In which SD-WAN plane would you find vBond operating?

A. Control Plane

B. Data Plane

C. Management Plane

D. Orchestration Plane

In the context of SD-WAN architecture, vBond serves as a crucial component within the orchestration plane. This plane is responsible for the secure establishment of connections between various SD-WAN elements, such as vSmart controllers and branch devices. vBond facilitates the initial authentication and helps in the management of secure communication channels by ensuring trusted connections. While the control plane is involved in routing and policy management, and the data plane is focused on the actual transmission of user data across the network, the orchestration plane specifically handles the provisioning and management aspects, which is where vBond's functionality lies. The management plane, on the other hand, is more focused on network management functionalities that are typically external to the core SD-WAN components. Thus, recognizing that vBond operates at the orchestration layer highlights its role in establishing secure networking foundations essential for the overall SD-WAN infrastructure.

8. Which protocol can be used in conjunction with Local EAP as a backup?

A. LDAP

B. RADIUS

C. NTLM

D. Kerberos

The combination of Local EAP (Extensible Authentication Protocol) with RADIUS (Remote Authentication Dial-In User Service) serves as a robust solution for authentication processes. Using RADIUS as a backup protocol is particularly advantageous because RADIUS is widely supported and allows for centralized authentication, authorization, and accounting. In environments where Local EAP is implemented for authentication, RADIUS can provide an effective failover option in case Local EAP encounters issues or is unable to complete the authentication process. This ensures that users can still authenticate and maintain access to network resources without significant interruption. RADIUS operates effectively by providing a way for access points or network devices to communicate with an authentication server. This server can manage user credentials and facilitate different types of authentication methods, including EAP, for a more comprehensive security architecture. In contrast, while LDAP (Lightweight Directory Access Protocol), NTLM (NT LAN Manager), and Kerberos can be used for authentication, they do not serve the same purpose in the context of providing a backup solution specifically for Local EAP within network access scenarios. LDAP, for instance, is primarily used for directory services and isn't typically utilized as a direct backup for Local EAP authentication.

9. Which of the following SD-WAN components serves as the endpoint for data traffic?

A. vBond

B. vSmart

C. vEdge

D. vManage

The vEdge component in an SD-WAN architecture serves as the endpoint for data traffic. It operates at the edge of the enterprise network and is responsible for establishing secure tunnels to other vEdge devices and facilitating the transmission of data between different locations. The vEdge routers manage the actual data traffic, making intelligent forwarding decisions based on the SD-WAN policies defined in the controller. They handle tasks such as application optimization, WAN path selection, and real-time performance monitoring. Essentially, vEdge devices are what route the end-user data traffic over the WAN, leveraging various connectivity options to ensure reliable and efficient communication. Understanding the role of vEdge is crucial because it lies at the foundational level of an SD-WAN deployment, directly impacting how data flows between users and applications across the network.

10. Which of the following correctly characterizes Access Lists in routing configurations?

A. They are primarily used for policy-based routing adjustments.

B. They can only permit full prefixes, not sub-prefixes.

C. They are simpler to configure than route maps.

D. They utilize complex numbers to dictate matching criteria.

Access Lists are indeed simpler to configure compared to route maps, which makes this statement correct. Access Lists are designed to filter traffic based on defined criteria, such as source and destination IP addresses, protocols, and ports. This straightforward structure allows network administrators to quickly and easily set up access control rules without the added complexity that can come with route maps. Route maps provide more granular control and flexibility for routing decisions, but this complexity often translates into a steeper learning curve and longer configuration times. When comparing the two, Access Lists serve as a more straightforward method for filtering and controlling network traffic based on simple parameters. The other choices present different concepts about Access Lists that do not align with their fundamental purpose or capabilities. For example, policy-based routing also involves more complex rules and conditions that Access Lists alone cannot offer. Similarly, the ability to work with full prefixes versus sub-prefixes isn't a limitation of Access Lists; they can indeed handle subnets as well. Lastly, Access Lists use standard criteria for matching, rather than relying on complex numerical systems. Therefore, the simplicity of Access Lists makes them a valuable tool in a network engineer's toolkit, particularly for basic traffic filtering needs.