Free Cisco 300-110 WLSD Practice Questions

Shared by Craft on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An enterprise is using wireless as the main network connectivity for clients. To ensure wireless network availability, two standalone controllers are installed in the head office. APs are connected to the controllers using a round-robin approach to load balance the traffic. After a power cut, the wireless clients disconnect while roaming. An engineer tried eping from the controller but fails. Which protocol needs to be allowed between the networks that the controllers are installed?

Options:

A- IP Protocol 67
B- IP Protocol 77
C- IP Protocol 87
D- IP Protocol 97

Answer:

D

Explanation:

When eping (EoIP ping) fails between two Cisco Wireless LAN Controllers, it indicates that the data path of the mobility tunnel is blocked. In Cisco AireOS wireless networks, the mobility data path uses IP Protocol 97 (EtherIP --- Ethernet-over-IP encapsulation) for tunneling client traffic between the anchor and foreign controllers. This is distinct from the control path, which uses UDP port 16666. When the mobility data path (IP Protocol 97) is blocked by a firewall or ACL between the two controllers' networks, eping will fail because eping specifically tests the EoIP data encapsulation path. After a power cut, when clients disconnect and attempt to roam between APs on different controllers, the mobility tunnel must be operational for session continuity. If IP Protocol 97 is blocked, the mobility data plane cannot function, causing client disconnections during inter-controller roaming events. The other IP protocols listed (67, 77, 87) are not used for Cisco WLC mobility tunneling. Reference: WLSD Study Guide --- Mobility Tunnel Data Path, IP Protocol 97 (EtherIP), eping Command and Troubleshooting.

Question 2

Question Type: MultipleChoice

A customer purchases this Cisco equipment for a new branch office: * 20 Cisco Catalyst 9120 APs * five Catalyst 9130 APs * a single Catalyst 9300 Series Switch The customer wants to extend its existing wired and wireless fabric-enabled network to the branch office and manage all devices via a centrally deployed Cisco Catalyst Center (formerly DNA Center). Which Cisco Catalyst Center licenses are required for the branch office equipment?

Options:

A- Cisco Catalyst Advantage for the switch and all the APs
B- Cisco Catalyst Essentials on the APs and Cisco Catalyst Advantage on the switch
C- Cisco Catalyst Essentials on the switch and all the APs
D- Cisco Catalyst Advantage on the APs and Cisco Catalyst Center Premiere on the switch

Answer:

A

Explanation:

Cisco Catalyst Center uses a tiered licensing model --- Essentials and Advantage --- applied to both switching and wireless infrastructure. To enable a fully fabric-enabled (SD-Access) deployment with centralized management, the Cisco Catalyst Advantage license is required across all device types. The Advantage tier unlocks Software-Defined Access fabric capabilities including macro and micro-segmentation, integration with Cisco ISE for policy enforcement, AI/ML-driven analytics via DNA Spaces and Assurance, and automated provisioning. The Essentials license provides only basic device management, inventory, and software image management --- it does not unlock SD-Access fabric functionality. Since the branch design specifically extends an existing fabric-enabled network, the Essentials tier for either the switch or APs would create a licensing gap preventing full fabric participation. Options B, C, and D all create asymmetric licensing that would partially disable fabric capabilities. The correct design mandates Catalyst Advantage for the Catalyst 9300 switch and all 25 APs. Reference: WLSD Study Guide --- Cisco Catalyst Center Licensing, SD-Access Design, Fabric-Enabled Wireless Architecture.

Question 3

Question Type: MultipleChoice

A customer wants to provide wireless coverage in a parking lot outside of a building. An engineer determines that three APs are required. The APs can be mounted on the light poles in the parking lot because there are cable routes already in place for these locations. The closest wiring closet is approximately 200 meters away. Which setup powers and connects the APs back to the customer network?

Options:

A- category 6 UTP cabling and Cisco UPOE
B- fiber connectivity with 802.3af
C- fiber connectivity with an AC/DC power module
D- Category 6 UTP cabling and PoE+

Answer:

C

Explanation:

This question hinges on a fundamental network engineering constraint: the maximum transmission distance of copper Ethernet cabling. IEEE 802.3 standards specify a maximum segment length of 100 meters for all standard PoE and Ethernet over Category 5e, 6, or 6A UTP copper cabling. The parking lot light poles are approximately 200 meters from the closest wiring closet --- more than double the maximum copper distance. This immediately eliminates Options A and D (Category 6 UTP): at 200 meters, UTP copper cannot reliably carry Ethernet at any supported speed. The correct solution is fiber optic connectivity between the wiring closet and the parking lot poles, combined with a local AC/DC power module at each pole location. Fiber optic cabling supports runs of hundreds of meters to kilometers --- easily spanning 200 meters. At the AP mounting location on the light pole, an AC/DC power module (powered from the pole's existing electrical supply) converts AC power to the DC power the AP requires. Option B (fiber with 802.3af) is incorrect because PoE cannot be delivered over fiber --- 802.3af requires copper cabling for simultaneous power and data delivery. The AC/DC power module at the remote end is the correct power solution when fiber is required. Reference: WLSD Study Guide --- Outdoor AP Deployment, Fiber vs. Copper Distance Limitations, Outdoor Power Solutions.

Question 4

Question Type: MultipleChoice

An educational organization recently deployed an anchored WLAN and has a high number of client connections at any given time that stream video. The wireless infrastructure includes two Cisco 9800 WLCs. To prevent web traffic being slow, an engineer must configure the deployment to prevent excessive fragmentation of the client dat

a. Which configuration must the engineer apply?

Options:

A- Set the MTU on both controllers to match.
B- Increase the MTU on both controllers.
C- Adjust the TCP MSS value below the fragmentation point.
D- Set the do not fragment bit on the mobility tunnel.

Answer:

C

Explanation:

In an anchored WLAN deployment, client traffic is encapsulated within CAPWAP mobility tunnels between the foreign WLC (where the AP joins) and the anchor WLC (in the DMZ or designated network segment). This tunneling adds encapsulation overhead --- CAPWAP/mobility tunnel headers consume a portion of the available MTU on the transport path. When video streaming clients generate large TCP segments, these segments may exceed the effective MTU of the mobility tunnel path, causing IP fragmentation at the WLC or along the path to the anchor. Fragmentation significantly degrades throughput and increases CPU overhead for high-volume video traffic. The correct solution is TCP MSS Clamping --- reducing the Maximum Segment Size value advertised in TCP SYN packets so that TCP endpoints negotiate a segment size remaining below the fragmentation threshold. The Cisco 9800 WLC supports TCP MSS adjustment, which intercepts TCP handshake packets and rewrites the MSS option to a value accounting for CAPWAP tunnel overhead. Setting matching MTUs (Option A) does not prevent fragmentation if the effective tunnel MTU is lower than the client segment size. Increasing the MTU (Option B) is often constrained by physical infrastructure. Setting the DF bit (Option D) would cause packets to be dropped rather than fragmented. Reference: WLSD Study Guide --- Anchored WLAN Design, CAPWAP Mobility Tunnel MTU, TCP MSS Clamping.

Question 5

Question Type: MultipleChoice

A customer wants a network engineer to design a Cisco wireless solution that will have redundancy through SSO and LAG. APs in the executive office must reassociate to the WLC as soon as possible in the event of a failure. The WLCs are located in a remote data center. The head office uses a WAN for connectivity with the data center. Which priority must be incorporated in the design to be assigned to the executive APs?

Options:

A- high

B- medium
C- low
D- critical

Answer:

D

Explanation:

Cisco WLC AP Failover Priority governs the order in which APs are processed when a WLC recovers and APs begin re-associating. The priority levels are: Critical, High, Medium, and Low. During recovery situations, the WLC will accept and process AP join requests in order of priority --- Critical priority APs are processed first, before all other priority levels. In a deployment where the WLC is located in a remote data center connected via WAN, the join process for all APs is slower due to WAN latency and potential bandwidth constraints. Under these conditions, assigning Critical priority to executive office APs ensures they are at the front of the processing queue and restore service before lower-priority APs. The executive office designation implies business-critical operations requiring the fastest possible wireless restoration --- a requirement that directly maps to the Critical priority level. High priority (Option A) would position the executive APs second in the queue behind any Critical priority APs. Medium (Option B) and Low (Option C) would place them further down the processing order. Reference: WLSD Study Guide --- AP Failover Priority Configuration, N+1 and SSO Redundancy Design, WAN-Linked Controller Deployments.

Question 6

Question Type: MultipleChoice

A customer has two Cisco 5520 WLCs that manage all APs throughout the network. The WLCs are in different locations to provide geographical redundancy. A mobility group has been configured on both WLCs and has an UP status on both controllers. The APs in location A are statically configured to use controller A as the primary and controller B as the secondary. If the WLC in location A goes offline, the APs successfully join the WLC in location B, but they do not fail over to their primary configured controller when it recovers. Which configuration task fixes the issue?

Options:

A- Configure the WLC in location A as primary using the CAPWAP AP Controller IP Address command on all the location A access points.
B- Use DHCP Option 43 and specify WLC in location A as primary.
C- Enable AP fallback globally on the WLC.

D- Change the AP Failover Priority to critical.

Answer:

C

Explanation:

Enabling AP fallback globally on the WLC allows access points to reconnect to their primary controller after they have connected to a secondary controller due to the primary being offline. This is the exact behavior described in the scenario --- APs successfully fail over to the secondary WLC but do not return to the primary WLC when it recovers. AP Fallback is a WLC-level setting that monitors the availability of each AP's configured primary controller and initiates a reconnection when the primary becomes reachable again. Without AP Fallback enabled, APs remain on whatever controller they most recently joined --- in this case, the secondary --- even after the primary recovers. The CAPWAP AP Controller IP Address command (Option A) permanently changes the primary controller configuration on the AP, which is not the intended solution --- the AP already has the correct primary configured. DHCP Option 43 (Option B) is used for initial AP discovery, not fallback. AP Failover Priority (Option D) controls which APs are processed first during a failover event, not whether APs return to their primary controller. Reference: WLSD Study Guide --- AP Fallback Configuration, N+1 Redundancy Recovery, Controller Primary/Secondary Hierarchy.

Question 7

Question Type: MultipleChoice

A community bank has three campus locations and one HQ with the data center. Each campus has four Cisco Catalyst 9120 APs. Poor WAN uplinks cause impacted connectivity back to HQ, and each campus is planned to have its own EWC controller based on C9120 AP to keep traffic local. Guest WLAN will be routed locally. Employee WLAN must be authenticated 802.1x PEAP via HQ ISE but can pass traffic locally once authenticated. HQ WLC will be the primary backup WLC for each WLC. Which design approach should the consulting engineer take?

Options:

A- One C9120 AP in each campus must be converted to EWC mode, and the preferred controller is set to that AP with HQ WLC set as N+1 backup. The campus guest WLAN will use local web auth on guest VLAN, and employee WLAN will need the HQ AAA server to be added to EWC.
B- Two C9120 campus APs must be converted to EWC mode, one for the active controller and the other for standby set as N+1 backup. The campus guest WLAN will use local web auth on guest VLAN, and employee WLAN will need the HQ AAA server added to EWC.
C- Two C9120 campus APs must be converted to EWC mode, one for the active controller and

the other for standby with HQ WLC as N+1 backup. The campus guest WLAN will use the guest anchor to HQ WLC for guest VLAN access, and employee WLAN will need the HQ AAA server added to EWC.
D- One C9120 campus AP must be converted to EWC mode, and the preferred controller is set to that AP with HQ WLC paired as mobility peer and configured as N+1 backup. The campus guest WLAN will use local web auth on guest VLAN. The campus employee WLAN will need the guest anchor back to the HQ employee WLAN.

Answer:

A

Explanation:

This community bank design scenario requires precise alignment of EWC deployment scale, AAA integration, and traffic routing decisions with the stated constraints. With four APs per campus and a goal of local traffic handling, converting a single C9120 to EWC mode is optimal --- converting two APs to EWC (Options B and C) on a four-AP campus wastes 50% of campus AP infrastructure for controller functions rather than client service. The single EWC AP serves as the active local controller for the remaining three client-serving APs. The HQ WLC set as N+1 backup ensures that if the branch EWC fails, the remaining APs fall back to the centralized controller. For the guest WLAN, local web authentication on the guest VLAN provides the locally routed guest access requirement without requiring WAN connectivity to HQ. For the employee WLAN, adding the HQ ISE AAA server to the EWC's RADIUS configuration enables 802.1x PEAP authentication to traverse the WAN to ISE at the time of client association. Once authenticated, traffic is locally switched --- satisfying both the central authentication and local traffic routing requirements simultaneously. Option D's use of guest anchor for the employee WLAN is architecturally incorrect and would route traffic through HQ rather than locally.
Reference: WLSD Study Guide --- EWC Design, N+1 Redundancy, AAA Integration for Branch WLANs, Local Web Authentication.

To Get Premium Files for 300-110 Visit

https://www.p2pexams.com/products/300-110

For More Free Questions Visit

https://www.p2pexams.com/cisco/pdf/300-110