Cisco

350-101

Implementing and Operating Cisco Wireless Core Technologies

Questions & Answers (Demo)

Version: 4.0

Question: 1

A school district is deploying Cisco Catalyst 9176 APs to remote sites with occasional WAN outages. The IT team wants the APs to attempt joining a secondary or tertiary Catalyst 9800 WLC if the primary controller is unreachable. The team must preconfigure all controller IP addresses using the AP CLI before deploying. Which set of CLI commands sets the primary, secondary, and tertiary controller IP addresses on a Catalyst 9176 AP?

A.
set controller primary-base main-wlc 10.10.10.10
set controller secondary-base backup 10.10.10.20
set controller tertiary-base tertiary-wlc 10.10.10.30

B.
capwap ap primary-base main-wlc 10.10.10.10
capwap ap secondary-base backup-wlc 10.10.10.20
capwap ap tertiary-base tertiary-wlc 10.10.10.30

C.
ap join primary 10.10.10.10
ap join secondary 10.10.10.20
ap join tertiary 10.10.10.30

D.
capwap ap wlc primary 10.10.10.10
capwap ap wlc secondary 10.10.10.20
capwap ap wlc tertiary 10.10.10.30

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

Cisco lightweight and Catalyst access points use CAPWAP for AP-to-controller discovery and join operations. For AP-side preconfiguration, Cisco documents the syntax as capwap ap {primary-base | secondary-base | tertiary-base} controller-name controller-ip-address, specifically for configuring primary, secondary, and tertiary controllers on the AP. This matches option B exactly because it includes the CAPWAP AP command, the controller priority keyword, the controller name, and the controller management IP address. (Cisco)

The Catalyst 9800 AP join process also recognizes these configured controller entries in priority order: primary controller using capwap ap primary-base, secondary controller using capwap ap secondary-base, and tertiary controller using capwap ap tertiary-base. (Cisco) This allows the AP to attempt a backup controller when the preferred controller is unavailable, which is appropriate for remote sites with intermittent WAN reachability. Option A uses obsolete or invalid set controller syntax. Option C invents an ap join command format. Option D incorrectly inserts wlc into the AP CAPWAP command. Reference topics: Wireless Network Implementation — CAPWAP discovery, AP join process, Catalyst 9800 controller redundancy, and AP CLI provisioning.

Question: 2

Refer to the exhibit.

```
WLC#show run | include wireless management
wireless management interface Vlan10

WLC#show run interface vlan 10
Building configuration...

Current configuration : 132 bytes
!
interface Vlan10
ip address 10.10.1.2 255.255.255.0
no ip proxy-arp
ip igmp version 3
end
```

An engineer is setting up a new WLC in a branch office. The IT security policy states that all management access must use encrypted protocols, administrators will connect remotely, and network scans will be run to check for any noncompliant management protocol exposure. Which

action must the engineer take to achieve the required management access policy?

A. Permit only HTTP, Telnet, and SSH across all VLANs for 10.10.1.0/24.
B. Enable Telnet, SSH, and HTTPS across the management and guest interfaces.
C. Permit console access for 10.10.1.0/24 only with HTTP disabled.
D. Enable HTTPS and SSH, and disable HTTP and Telnet on the WLC.

Answer: D

Explanation:

The correct action is to expose only encrypted management services: HTTPS for WebUI administration and SSH for remote CLI administration. The exhibit confirms the WLC wireless management interface is VLAN 10 with IP address 10.10.1.2, but interface placement alone does not enforce secure management protocol policy. Cisco Catalyst 9800 documentation identifies web admin settings as controller management configuration that determines administrator access, protocols, and interfaces for remote management. Cisco further states that administrators can connect securely over HTTPS, while HTTP “is not a secure connection,” and that HTTPS encrypts data to and from the server.

For CLI access, Cisco’s Catalyst 9800 Secure Shell guidance states that SSH enables secure remote access, and using transport input ssh prevents non-SSH Telnet connections, limiting the device to SSH-only access. Therefore, options A and B violate policy because they permit Telnet and/or HTTP. Option C fails because console access is local, not remote, and disabling only HTTP still leaves Telnet exposure unresolved. Reference topics: Wireless Monitoring and Management — WLC management access, secure administration, HTTPS, SSH, and management-plane hardening.

Question: 3

How does the optimized roaming function operate in a WLC implementation?

A. It disassociates clients when the RSSI is lower than the set threshold.
B. It is integrated with external services for client wireless experience.
C. Device locations are determined through peer-to-peer beacons.
D. Load balancing is statically defined for all locations.

Answer: A

Explanation:

Optimized roaming is a Cisco WLC feature designed to reduce sticky-client behavior. A sticky client remains associated to an AP even after moving far enough away that another AP would provide better RF service. Cisco describes optimized roaming as actively monitoring client data RSSI and disconnecting clients when received signal strength falls below the configured threshold. The official

Catalyst 9800 documentation states that optimized roaming “disassociates client when the RSSI is lower than the set threshold,” which directly matches option A.

This function does not calculate device location through peer-to-peer beaconing, does not depend on external experience services, and is not static load balancing. It is an RF/client-roaming enforcement mechanism controlled by the wireless infrastructure. In practical operation, the AP/WLC evaluates client signal quality and, when the configured optimized roaming criteria are met, forces the client to disconnect so it can reassess the RF environment and roam to a better AP. Cisco also notes that optimized roaming helps maintain client connectivity by managing disassociationn based on RSSI and data-rate thresholds. Reference topics: Client Connectivity Configuration — client roaming behavior, sticky-client mitigation, RSSI thresholds, and WLC roaming optimization

Question: 4

A network engineer must isolate all guest users connected to the WLAN on a Cisco 9800 WLC so they cannot communicate with each other but can access the internet. The WLAN must meet these requirements:
•SSID named VisitorAccess assigned to VLAN 30
•guests prohibited from sharing files with other guests
•must be scalable to multiple access points in the building

Which action must the network engineer take to meet the requirements?

A. Enable P2P blocking in the policy profile and map the WLAN to a dedicated guest VLAN.
B. Set up local authentication and map the WLAN to a dedicated guest VLAN.
C. Set up a FlexConnect group and use local switching for the guest WLAN internet access.
D. Enable multicast mode and associate a RADIUS server with the guest WLAN.

Answer: A

Explanation:

The requirement is guest client isolation, not merely guest authentication or internet breakout. On a Catalyst 9800 WLC, peer-to-peer blocking is the correct control because it prevents wireless clients associated to the same WLAN from communicating directly with one another. Cisco defines peer-to-peer blocking as a WLAN security feature applied to individual WLANs, where each client inherits the WLAN’s P2P blocking behavior, and traffic can be bridged locally, dropped, or forwarded upstream. For this scenario, the appropriate action is the drop behavior, because guest-to-guest file sharing must be prohibited while upstream internet access remains available.

The dedicated guest VLAN, VLAN 30, provides traffic segmentation from production networks and creates a clean policy boundary for VisitorAccess. Cisco’s Catalyst 9800 configuration model maps WLANs to policy profiles, and the policy profile defines client network and switching policy, including VLAN association. Options B, C, and D do not solve client isolation: local authentication validates

users, FlexConnect/local switching changes traffic forwarding behavior, and multicast/RADIUS does not block unicast guest-to-guest traffic. Reference topics: Client Connectivity Configuration — guest WLAN design, P2P blocking, VLAN segmentation, and Catalyst 9800 WLAN-to-policy mapping.

Question: 5

How does MIMO operate during wireless transmission?

A. It uses multiple radio paths to increase throughput and reliability.
B. It applies frequency hopping to prevent crosstalk.
C. It shares a single connection among endpoints for coverage expansion.
D. It limits data paths to a single antenna for error reduction.

Answer: A

Explanation:

MIMO, or Multiple-Input Multiple-Output, is a core 802.11n and later wireless technology that uses multiple transmit and receive radio chains and antennas to improve wireless performance. Cisco's Wireless RF Reference Guide explains that IEEE 802.11n introduced MIMO, replacing the older single-radio SISO model with multiple radios, each using its own antenna, to increase data rates and improve reception in multipath environments. Cisco also notes that weak or distorted multipath signals can be received by more than one radio and reconstructed, improving decode quality and reliability.

This directly supports option A: MIMO exploits multiple RF paths rather than treating multipath as purely destructive. Depending on implementation, MIMO can use spatial diversity, maximal ratio combining, and spatial streams to increase throughput, improve signal-to-noise ratio, reduce retries, and make more efficient use of airtime. Cisco describes spatial stream notation such as 4x4:4 as four transmitters, four receivers, and four spatial streams. Option B describes frequency hopping, not MIMO. Option C is not a MIMO function. Option D is the opposite of MIMO because MIMO deliberately uses multiple antennas and radio paths. Reference topics: 802.11 Technology Fundamentals — MIMO, spatial streams, multipath, SISO versus MIMO, and 802.11n/ac/ax PHY enhancements.