VirtuLearn
Trusted, Accurate & Reliable

TRUSTED, ACCURATE AND RELIABLE

The most comprehensive IT certification preparation materials in the industry!

Expert-Verified | Exam-Ready | Regularly Updated

https://www.virtulearner.com
support@virtulearner.com

Cisco

350-101

Implementing and Operating Cisco Wireless Core Technologies (WLCOR)

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

Answer(s): 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(s): 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.