Free Cisco 350-101 WLCOR Practice Questions

Shared by Good on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is a characteristic of 20 MHz channel width in a wireless network?

Options:

A- Narrowest channel width in the 2.4 GHz band
B- Increases authentication handoff frequency
C- Supports automatic client reassociation
D- Higher throughput than wider channels

Answer:

A

Explanation:

In wireless networks, the 20 MHz channel width is the standard and narrowest channel allocation in the 2.4 GHz frequency band. Using narrower channels reduces adjacent-channel interference and allows for better coexistence in high-density environments, which is particularly important in the crowded 2.4 GHz spectrum. A 20 MHz channel uses less RF bandwidth than 40 MHz or 80 MHz channels, providing more non-overlapping channels (channels 1, 6, and 11 in 2.4 GHz) to reduce co-channel interference. Option B is incorrect, as channel width does not inherently increase authentication handoff frequency; handoff behavior is determined by RSSI, client roaming thresholds, and 802.11r fast roaming settings. Option C describes client reassociation support, which is handled by the wireless controller and client firmware, not the channel width itself. Option D is incorrect because wider channels (40 MHz, 80 MHz) provide higher throughput than 20 MHz, at the expense of increased interference potential. Cisco Wireless Core Technologies emphasize that 20 MHz channels are preferred for dense deployments in the 2.4 GHz band to maximize non-overlapping channels and reduce interference, ensuring predictable coverage and reliable client connectivity. Reference topics: RF Fundamentals --- 20 MHz channels, 2.4 GHz spectrum planning, interference management, channel allocation.

Question 2

Question Type: MultipleChoice

Which process is managed by Ministry of Internal Affairs and Communications in Japan?

Options:

A- RF technical standards
B- manufacturing batch inspection
C- customer onboarding documentation
D- supplier chain evaluation

Answer:

A

Explanation:

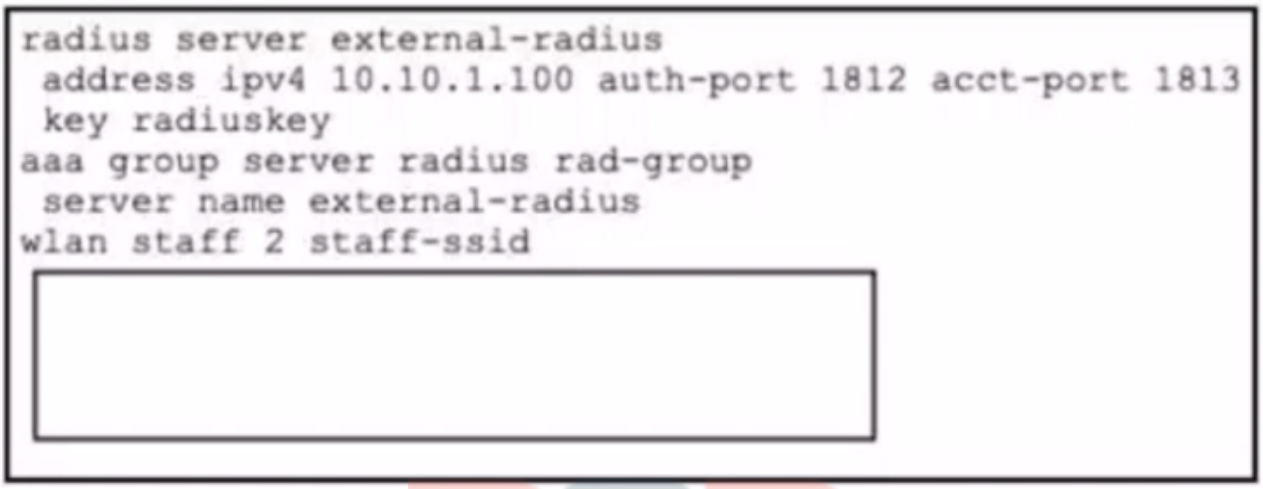
The correct answer is RF technical standards. In Japan, wireless LAN and other radio equipment must operate under national RF regulatory requirements controlled by the Ministry of Internal Affairs and Communications, commonly referenced as MIC. TELEC, a registered certification body in Japan, states that specified radio equipment such as wireless LAN equipment used in Japan must conform to technical regulations regulated by MIC, and that radio equipment conformity certification validates conformance to the technical standards under Japan's Radio Act.

This aligns directly with Cisco wireless regulatory-domain behavior. Cisco's Catalyst 9800 country-code documentation explains that APs use legal frequencies approved for their regulatory domain, and for Japan regulatory-domain devices, Japan country codes must be configured so the controller and APs operate within permitted channel and power constraints. Cisco also states that country codes are assigned and verified on APs or wireless controllers to ensure regulatory compliance for wireless operation. Manufacturing batch inspection, customer onboarding, and supplier-chain evaluation are not RF spectrum regulatory functions. Reference topics: RF Fundamentals --- regulatory domains, country codes, channel legality, transmit-power limits, and wireless compliance.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



A network administrator is working on a Cisco Catalyst 9800 WLC running Cisco IOS XE Software to enable user access for staff smartphones using WPA2-Enterprise with RADIUS. The administrator verifies the external authentication configuration and plans to test network connectivity. Which configuration command must be added to the box in the code to configure the WLC to support authentication with an external server?

Options:

A- security wpa enable
B- security dot1x authentication-list rad-group
C- security dot1x method-list rad-group
D- security wpa wpa2 akm dot1x

Answer:

D

Explanation:

To enable WPA2-Enterprise with RADIUS authentication on a Cisco Catalyst 9800 WLC, the WLAN configuration must specify the use of 802.1X as the authentication mechanism. The command security wpa wpa2 akm dot1x explicitly instructs the WLAN to use WPA2 encryption with the 802.1X authentication key management (AKM), which leverages the configured RADIUS server group for client authentication. Option B (security dot1x authentication-list) and Option C (security dot1x method-list) are legacy or IOS-style commands that define AAA method lists but do not directly bind the WLAN to WPA2-Enterprise security. Option A (security wpa enable) only enables WPA but does not define the authentication mode or RADIUS integration, which is insufficient for WPA2-Enterprise deployments. Cisco Wireless design guides emphasize that for staff or enterprise-class WLANs using external RADIUS servers, the WLAN's security profile must use WPA2 with AKM set to 802.1X. This ensures clients perform EAP authentication with the external server, supporting secure credential exchange and proper authorization. Correctly applying security wpa wpa2 akm dot1x in the WLAN configuration guarantees the WLC enforces encryption and authentication policies in line with enterprise security requirements. Reference topics: Client Connectivity Configuration --- WPA2-Enterprise, 802.1X,

AKM, RADIUS integration on Cisco WLCs.

Question 4

Question Type: MultipleChoice

A network engineer has been tasked with migrating the management mode of a Cisco 9176 AP named "Cisco-AP053540555" in a large enterprise wireless deployment. The AP is currently managed by a Cisco Catalyst 9800 Series WLC, but the organization is transitioning to Meraki cloud management for centralized control and monitoring. To complete this migration, the engineer needs to change the AP's management mode to Meraki with force and noprompt to skip validations using the CLI on the wireless controller. What command must the engineer use?

Options:

A- management meraki force noprompt mode
B- ap management mode meraki force noprompt
C- ap management meraki force noprompt mode
D- management-mode meraki force noprompt

Answer:

B

Explanation:

Migrating a Cisco Catalyst AP to Meraki cloud management requires issuing a specific CLI command on the WLC to switch the AP's management mode. The correct syntax is ap management mode meraki force noprompt, which instructs the controller to transition the AP to Meraki mode, bypassing validation prompts that normally require manual confirmation. The force keyword ensures the command is executed even if the AP is actively associated or configured, and noprompt suppresses confirmation dialogues for unattended migration. Options A, C, and D are invalid syntax or improperly order the parameters, which would result in a CLI error. Cisco Wireless Core Technologies recommend this approach during enterprise migration scenarios where multiple APs are moved from Catalyst WLC management to cloud-based Meraki management, enabling centralized configuration and monitoring in a large-scale deployment. Using this command ensures a seamless transition without service disruption, while maintaining inventory consistency and supporting automation for mass AP migrations. Reference topics: Wireless Network Implementation --- AP management mode migration, Meraki cloud integration, CLI AP management, Catalyst 9176 WLC migration.

Question 5

Question Type: MultipleChoice

high-availability configurations and relies heavily on consistent visibility into device health. Event logging and alerting must be ensured throughout maintenance windows, and the maintenance process must be centrally managed. Which process meets the requirements?

Options:

A- Monitor the Device 360 dashboard
B- Monitor the device in Cisco Spaces
C- Use the WLC dashboard
D- Use scheduled maintenance for the device

Answer:

D

Question 6

Question Type: MultipleChoice

An organization must manage ongoing firmware updates for redundant controllers in the network. They will use Cisco Catalyst Center for deployment and visibility. The current environment uses centralized and distributed management approaches. Automation and reporting are critical to minimize operational workload. Which method must be used to manage structured update processes and monitor progress throughout the update cycle?

Options:

A- inventory snapshots from hardware report
B- software templates
C- software image management workflows
D- lifecycle workflow

Answer:

C

Explanation:

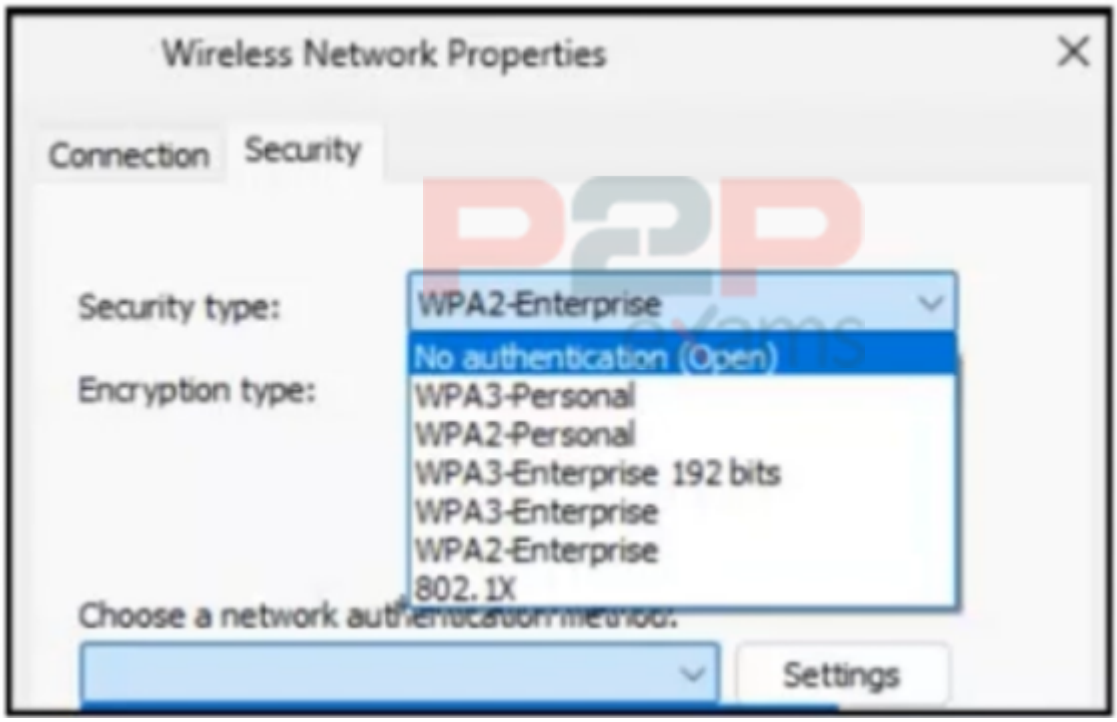
The correct method is software image management workflows, specifically Cisco Catalyst Center Software Image Management, commonly referenced as SWIM. Cisco documents SWIM as the mechanism used to manage software upgrades and maintain consistency of image versions across the network. It provides an image repository, golden-image assignment, image distribution, activation, readiness checks, and scheduled execution. Cisco's wireless automation guidance specifically states that SWIM is used to update Catalyst 9800 Series Wireless Controller software by distributing the image from the Catalyst Center repository to wireless controllers and upgrading the images running on those controllers; both stages can run immediately or be scheduled for a defined maintenance window.

Option C is also validated by Catalyst Center's update-status and workflow views. Cisco documents Image Update Status as the view that shows all update tasks, filters by in-progress, success, or failure, and displays a progress bar for active updates. The workflow view then exposes distribution and activation task status, timing, prechecks, postchecks, checksum verification, and AP pre-image download details. Inventory snapshots and templates do not execute controller firmware upgrades, and ''lifecycle workflow'' is too generic. Reference topics: Wireless Monitoring and Management --- Catalyst Center SWIM, image compliance, golden images, controller upgrade automation, and update progress reporting.

Question 7

Question Type: MultipleChoice

Exhibit:



Refer to the exhibit. An onsite engineer is working to connect devices to the wireless network in a corporate environment. The network requirements dictate that WPA2-Enterprise security

must be used with certificate-based mutual authentication to align with enterprise policy, which requires client and server certificates for secure access. After the initial wireless settings are applied on a Windows-based workstation, the engineer must Choose the appropriate authentication method in the client network properties to complete a successful enterprise Wi-Fi connection. Which option in the "Choose a network authentication method" dropdown meets this requirement?

Options:

A- MSCHAPv2
B- TEAP
C- EAP-TLS
D- PEAP

Answer:

C

Explanation:

The correct authentication method is EAP-TLS. WPA2-Enterprise uses 802.1X/EAP authentication rather than a pre-shared key, and the supplicant, authenticator, and RADIUS authentication server participate in the enterprise authentication exchange. Cisco documentation states that in enterprise WPA/WPA2 operation, 802.1X/EAP is used for authentication and provides strong authentication between the client and authentication server.

The decisive requirement in the question is certificate-based mutual authentication requiring both client and server certificates. Cisco explicitly describes EAP-TLS as requiring both server-side and client-side certificates, while PEAP requires only a server-side certificate and normally authenticates the client with password-based credentials inside the protected tunnel. Cisco Secure ACS documentation also states that EAP-TLS uses the certificates of the authentication server and the end-user client, enforcing mutual authentication.

MSCHAPv2 is a password-based inner authentication method, not certificate-based mutual authentication. PEAP protects credential exchange with a server certificate but does not inherently require a client certificate. TEAP can support flexible tunneled authentication, but the strict client-and-server certificate requirement maps directly to EAP-TLS. Reference topic: Client Connectivity Configuration --- WPA2-Enterprise, 802.1X supplicant configuration, EAP methods, certificates, and RADIUS authentication.

Question 8

Question Type: MultipleChoice

What is an attribute of the workgroup bridge mode for an AP in a wireless network?

Options:

A- allows clients on the 2.4 GHz radio to speak to clients on the 5 GHz radio
B- broadcast domains are extended across all network interfaces
C- traffic movement between two of its Ethernet ports
D- device integration of a wired segment into a wireless network

Answer:

D

Explanation:

The workgroup bridge mode on a Cisco access point is designed to integrate a wired network segment into an existing wireless infrastructure. In this mode, the AP acts as a client to a root AP or wireless controller-managed network, bridging Ethernet-connected devices on its wired ports to the wireless LAN. This is commonly deployed in environments where wired devices, such as printers, legacy systems, or isolated office equipment, require network connectivity but cannot directly connect to the wired backbone.

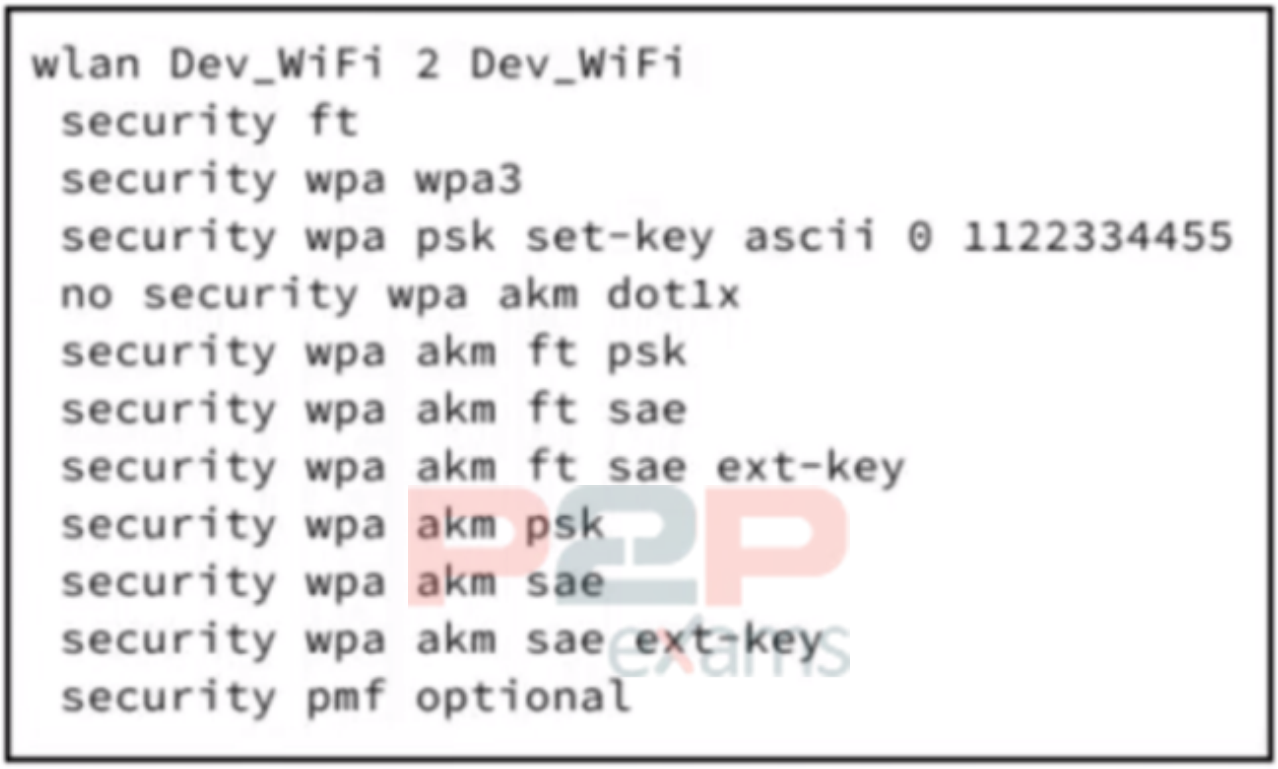
Traffic from devices on the wired segment is encapsulated and transmitted over the wireless link to the root AP, effectively extending network access without running physical cabling. Unlike bridging between multiple AP radios (2.4 GHz vs. 5 GHz), or providing inter-Ethernet port forwarding, the primary attribute of a workgroup bridge is wireless-to-wired integration, not radio-to-radio communication or internal LAN segmentation. Broadcast domains are limited to the bridged wired segment and the wireless uplink; they are not automatically extended across all interfaces without VLAN configuration.

Cisco deployment guides emphasize that workgroup bridge mode is ideal for connecting remote wired clusters to a centralized WLAN, providing seamless connectivity while maintaining security and management under the controller or root AP. Reference topic: Wireless Network Implementation --- AP operational modes, workgroup bridge, and wired segment integration.

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



Refer to the exhibit. A startup company has recently moved to new offices and performed a full network refresh. The application development team requested a high-speed reliable wireless network to use for testing real-time applications. Although, the wireless network is Wi-Fi 7 enabled, the wireless clients are connecting using lower speeds. Which configuration must be applied on the WLC to increase throughput?

Options:

A- security wpa3 akm sae ext-key
B- security wpa wpa2 wpa3 aes512
C- security wpa wpa2 wpa3 tkip512
D- security wpa wpa2 ciphers gcmp256

Answer:

D

Explanation:

The correct configuration is security wpa wpa2 ciphers gcmp256. The WLAN already contains WPA3, SAE, FT-SAE, SAE-EXT-KEY, and FT-SAE-EXT-KEY AKMs, so adding another SAE-EXT-KEY command is not the missing element. For Wi-Fi 7 operation, Cisco states that WPA3-Personal requires GCMP256 with SAE-EXT-KEY and/or FT + SAE-EXT-KEY, and that AES/CCMP128 clients do not operate as Wi-Fi 7 clients when the required stronger cipher combination is absent. Cisco's Catalyst 9800 WPA3 security enhancement guide gives the CLI syntax directly: security wpa wpa2 ciphers gcmp256, which configures GCMP-256 cipher

support.

Option D is therefore the only valid WLC command that enables the required cipher for Wi-Fi 7-capable client operation and higher throughput behavior. Option A uses incorrect syntax and is already functionally represented in the exhibit as security wpa akm sae ext-key. Options B and C use invalid cipher constructs; TKIP is legacy and incompatible with modern high-throughput WLAN operation. Reference topics: 802.11be/Wi-Fi 7 security requirements, WPA3-Personal, SAE-EXT-KEY, GCMP-256 cipher support, and Catalyst 9800 WLAN security configuration.

Question 10

Question Type: MultipleChoice

To double the range of a transmitter, which value must the transmitter be changed to if it is currently at 17 dBm?

Options:

A- 20 dBm
B- 27 dBm
C- 100 dBm
D- 17 dBm

Answer:

B

Explanation:

Doubling the range of a wireless transmitter does not require a linear increase in power due to the inverse-square law of RF propagation. Free-space path loss (FSPL) increases with the square of the distance, meaning to double the distance, the required power must increase by a factor of four in linear terms. In decibel units, power increases are logarithmic: 10log10(4)610 \log_{10}(4) \approx 610log10(4)6 dB.

Given a transmitter at 17 dBm, increasing its output by 6 dB to 23 dBm would theoretically double the coverage in free-space conditions. However, due to environmental factors like multipath, absorption, and antenna efficiency, Cisco RF design guides often round to practical increments, suggesting an increase from 17 dBm to 27 dBm to achieve a robust doubling of coverage under real-world conditions.

Options A (20 dBm) and D (17 dBm) are insufficient because they do not provide the necessary power increase to overcome the logarithmic path loss for doubling range. Option C (100 dBm) is

unrealistic and exceeds regulatory limits for enterprise wireless deployments. Proper power planning must balance coverage, interference, and regulatory compliance. Reference topic: RF Fundamentals --- Free-space path loss, power control, and transmitter range planning in enterprise WLAN design.

Question 11

Question Type: MultipleChoice

Which function does FRA use to optimize client experience and network coverage?

Options:

A- Monitoring on the physical interface level in the AP
B- Enhances roaming by redirecting the client to move to the appropriate AP
C- Implementation by local data path control
D- Dynamically adapts the roles of dual-band radios in an AP

Answer:

B

Explanation:

FRA (Flexible Radio Assignment) is a feature in Cisco wireless networks designed to optimize the client experience and enhance network coverage. FRA functions by managing roaming behavior and ensuring that clients are connected to the most appropriate access point (AP) based on signal quality and other factors. This helps in ensuring a seamless experience when clients move across coverage areas, by actively guiding them to the best AP.

The key functionality of FRA involves redirecting clients to the appropriate AP when they are experiencing suboptimal performance on the current AP, which is typically influenced by factors such as interference or distance. This optimization helps improve both coverage and user experience by making sure clients stay on the most optimal radio connection.

Option A, which refers to monitoring on the physical interface level, is not directly related to FRA but more to basic radio management. Option C, which mentions local data path control, refers to how data paths are managed locally within an AP but does not address the dynamic nature of client roaming. Option D, about dual-band radios, involves how radios are configured but does not directly describe FRA's function.

FRA is vital for dynamically enhancing wireless network performance, particularly in large, dense environments where clients are constantly moving.

YANG (Yet Another Next Generation) is a data modeling language primarily used in conjunction with the NETCONF (Network Configuration Protocol) to model configuration and operational data for network devices, including Cisco wireless controllers. YANG is a human-readable, hierarchical language designed to define the structure of data, allowing for consistent representation of configuration parameters, operational state, and notifications. It is extensively used in network automation and management systems to ensure standardized configuration management across various devices, making it easier for network administrators to automate and configure network devices using NETCONF.

NETCONF is the protocol that facilitates the transport of these data models (defined in YANG) between network devices and management systems. YANG's role is to define the structure and constraints of the data that NETCONF will configure or retrieve from devices. This allows administrators to configure network devices programmatically while adhering to a standardized data structure, which is essential for scalability, automation, and integration across various systems.

Options B, C, and D do not describe the actual purpose of YANG in the context of NETCONF and Cisco wireless controllers. Option B describes a security protocol (which could be TLS or SSH), Option C refers to protocols like RESTCONF, and Option D is incorrect because YANG is not a scripting language but a data modeling language.

Question 12

Question Type: MultipleChoice

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?

Options:

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 13

Question Type: MultipleChoice

What is the main benefit of using AI Enhanced RRM on the Cisco Catalyst 9800 wireless controller?

Options:

A- It is an automatic tuning tool that is used to adjust RF parameters based on static thresholds.
B- It focuses on increasing the transmit power of access points to maximize coverage regardless of interference.
C- It disables dynamic channel assignment and power control to maintain a fixed wireless environment for stability.
D- It uses machine learning and cloud analytics to proactively optimize RF parameters.

Answer:

D

Explanation:

AI Enhanced RRM is not a static-threshold tuning feature and it is not designed to simply raise AP transmit power. Cisco defines AI Enhanced RRM as a radio resource management technology that applies artificial intelligence and machine learning to optimize RF environments, uses distributed data collection from Cisco wireless controllers with cloud-based analytics, and automates adaptive RF parameter tuning for Cisco wireless networks.

The operational model is telemetry-driven. RF telemetry is collected from APs by the Catalyst 9800 WLC, sent through Cisco Catalyst Center to the Cisco AI Analytics Cloud, analyzed by RRM algorithms, and then configuration-change information is returned through Catalyst Center toward the managed wireless infrastructure. Cisco's AI-Enhanced RRM deployment guide further identifies DCA, TPC, FRA, and DBS as examples of optimizations performed, meaning the feature enhances dynamic RF control rather than disabling it.

Therefore, option D is the only correct answer. Options A, B, and C describe either legacy/static behavior, harmful power-only logic, or a fixed RF design model that contradicts Cisco AI Enhanced RRM. Reference topics: Automation and AI --- AI/ML-driven RF optimization, Catalyst Center assurance, RRM telemetry, DCA, TPC, FRA, and DBS.