Cisco.350-101.v2026-09-30.q51

Exam Code:	350-101
Exam Name:	Implementing and Operating Cisco Wireless Core Technologies
Certification Provider:	Cisco
Free Question Number:	51
Version:	v2026-09-30
# of views:	105
# of Questions views:	513
https://www.freecram.net/torrent/Cisco.350-101.v2026-09-30.q51.html	

NEW QUESTION: 1
A deployment requires that several APs be connected to edge switches, and each AP must support management and guest Wi-Fi traffic. The APs tag guest traffic separately from management, and the organization expects to add more VLANs for IoT and voice soon, so the configuration must support scalability. The security team requires that guest traffic never mix with internal resources. Which port configuration must be used for the switch interfaces that connect to the APs?
A. Configure the central Layer 3 switch port as an access VLAN port that allows the management VLAN only.
B. Implement switch port access with the native VLAN for guest traffic and trunk with the management VLAN.
C. Set a trunk port with the management VLAN as the native VLAN, and allow only management and user VLANs.
D. Make the port an access port on the management VLAN because all traffic is tunneled back to the WLC.
Answer: (SHOW ANSWER)
The switch interfaces connected to the APs must be configured as 802.1Q trunk ports. The requirement states that AP management and guest Wi-Fi traffic must remain separate, and additional VLANs for IoT and voice are expected. An access port supports only one VLAN, so it cannot scale for multiple locally tagged client VLANs. Cisco's Catalyst AP guidance states that when multiple VLANs are used for client traffic, the AP switch port should trunk the VLANs, and management traffic is untagged; when a management VLAN is used, it should be configured as the native VLAN on the switch port. Cisco's Catalyst 9800 FlexConnect documentation also shows the AP connected to a trunk port with a native VLAN for AP IP connectivity and a separate VLAN for locally switched client traffic. Option C is therefore correct: configure a trunk, set the AP management VLAN as native, and restrict the allowed VLAN list to only required management and client VLANs such as guest, IoT, and voice. This supports segmentation and prevents unnecessary internal VLAN exposure.

NEW QUESTION: 2
A network administrator at a construction company manages a Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE 17.x. The WLAN named XYZ-Conference is set up for a large event, but attendees report slow network performance due to misbehaving clients. To improve connectivity, the network administrator decides to change the client exclusion policy on the WLAN to temporarily block the misbehaving clients. The XYZ-Conference WLAN must enable a client exclusion policy with a timeout of 120 seconds for misbehaving clients. Which set of Cisco IOS XE commands must be used?
A. wireless profile policy XYZ-Conference
XYZ Conference exclude 120
B. wireless profile policy XYZ-Conference
exclusionlist timeout 120
C. wir eless profile policy XYZ-Conference
security exclusion timeout 120

D. wir eless profile policy XYZ-Conference
client-exclusion 120
Answer: (SHOW ANSWER)
Client exclusion is a feature in Cisco Catalyst 9800 WLCs that allows the administrator to temporarily block clients exhibiting misbehavior, such as excessive retries, excessive bandwidth usage, or roaming issues. The IOS XE CLI command for enabling client exclusion in a WLAN policy is client- exclusion <timeout>, where <timeout> defines the duration (in seconds) the client is prevented from associating with the WLAN. Option D correctly uses client-exclusion 120 to block the misbehaving clients for 120 seconds.

NEW QUESTION: 3
What happens when a radio wave bends around objects?
A. absorption
B. diffusion
C. reflection
D. diffraction
Answer: (SHOW ANSWER)
When a radio wave bends around an obstacle in its path, this phenomenon is called diffraction.
Diffraction allows the RF signal to reach areas that are not in the direct line of sight of the transmitter, such as behind walls, corners, or other obstructions. The amount of bending depends on the wavelength of the signal relative to the size of the obstacle--longer wavelengths (lower frequencies) diffract more effectively than shorter wavelengths.

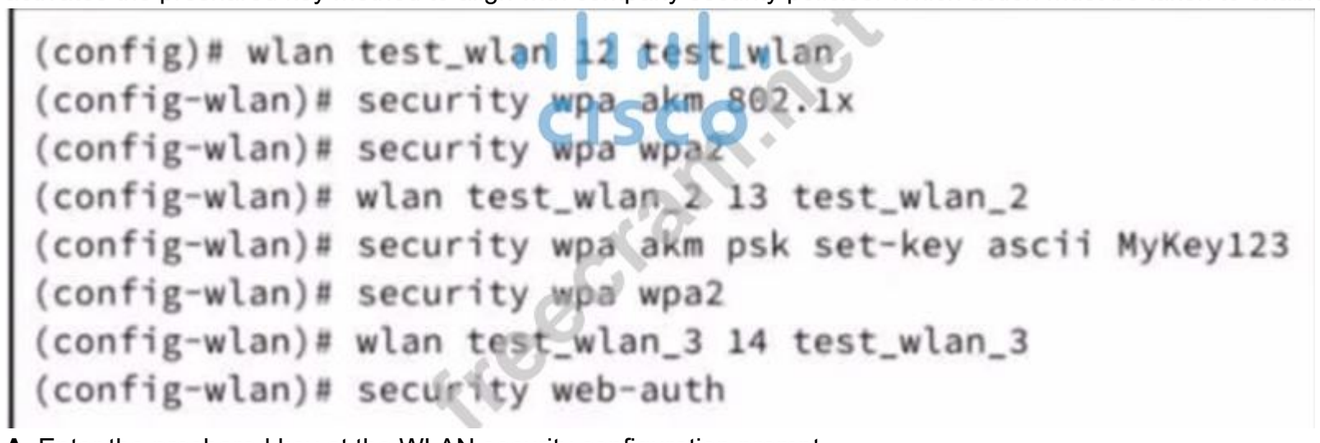
NEW QUESTION: 4
Which feature enables fast secure roaming in a wireless network?
A. DCA
B. 802.11r
C. 802.11ax
D. MIMO
Answer: (SHOW ANSWER)
Fast secure roaming in enterprise wireless networks is achieved using the 802.11r standard, also known as Fast BSS Transition (FT). 802.11r allows clients to authenticate with a new access point (AP) before disassociating from the current AP, significantly reducing the time required for the re- authentication process. This pre-authentication mechanism ensures that client sessions, such as voice or video calls, are maintained seamlessly when moving between APs in a mobility domain. DCA (Dynamic Channel Assignment) optimizes channel selection but does not affect roaming speed. 802.11ax enhances overall throughput and spectral efficiency but does not directly provide fast roaming. MIMO (Multiple Input Multiple Output) improves signal reliability and capacity but is unrelated to the authentication handoff process. Cisco Wireless Core Technologies highlight the deployment of 802.11r in conjunction with PMK caching and Opportunistic Key Caching (OKC) to further accelerate roaming in high-density environments.
Implementing 802.11r is critical for environments requiring minimal packet loss and low latency during client movement, such as voice over Wi-Fi or real-time video applications.

NEW QUESTION: 5
Refer to the exhibit. An organization wants to use Cisco Spaces for location analytics, and an engineer is setting up the Cisco Catalyst 9800 WLC to send location data. The Spaces connector has already been configured and is operational on the WLC. The engineer must now configure the controller to forward telemetry data to the correct Spaces cloud endpoint using TLS to complete the integration. Which CLI command must be added to the box in the code?



A. profile spaces-profile ip address 198.51.100.10 receiver tls-native
B. receiver protocol tls-native profile spaces-profile ip address 198.51.100.10 57555
C. receiver ip address 198.51.100.10 57555 protocol tls-native profile spaces-profile
D. profile spaces-profile receiver 198.51.100.10 57555 protocol tls-native
Answer: (SHOW ANSWER)
The correct command is receiver ip address 198.51.100.10 57555 protocol tls-native profile spaces-profile because it matches the Cisco IOS XE model-driven telemetry subscription syntax used on Catalyst 9800 controllers. Cisco documents the receiver statement under telemetry ietf subscription as receiver ip address ip-address receiver-port protocol protocol profile name, and describes it as the command that configures the receiver IP address, port, protocol, and profile for telemetry notifications.
In the exhibit, the subscription already defines the telemetry feed: encode-tdl encoding, a native stream, the TDL URI for ewlc/wlan_config, the WLC source address, and an on-change update policy. What is missing is the collector destination. For Cisco Spaces or Catalyst Center-style integrations, the WLC must know where to export telemetry and which secure transport profile to use. Cisco troubleshooting examples for Catalyst 9800 telemetry use the same command structure: receiver ip address X.X.X.X 25103 protocol tls-native profile ... under the telemetry subscription.
Options A, B, and D are invalid because they reorder the CLI keywords. IOS XE telemetry configuration is parser-order sensitive: the command begins with receiver ip address, followed by the receiver port, then protocol, then profile.

NEW QUESTION: 6
Refer to the exhibit. A wireless controller is deployed at a branch location to facilitate secure client connectivity. A network engineer configures one WLAN using WPA2 Personal authentication and activates the preshared key method to align with company security policies. Which action must be taken to enable the client to connect to the WLAN?



A. Enter the preshared key at the WLAN security configuration prompt
B. Enable MAC filtering for security group assignment
C. Configure Active Directory integration for WLAN authentication
D. Import a client certificate for WPA2 authentication
Answer: (SHOW ANSWER)

WPA2 Personal (PSK) authentication relies on a shared secret (preshared key) configured on both the wireless LAN controller (WLC) and the client device. In the exhibit, the WLAN is configured with WPA2 and PSK (set-key ascii MyKey123), which means the network expects clients to use the same preshared key to authenticate. To enable client connectivity, the preshared key must be manually entered on each client device; this aligns the client and WLC authentication parameters.

NEW QUESTION: 7
Refer to the exhibit. A JSON response from a wireless management API contains access point inventory and interface state information. Which JSON expression retrieves the MAC address of the second interface on the first access point?



A. accessPoints[0].interfaces[1].macAddress
B. accessPoints[1].interfaces[0].macAddress
C. accessPoints[0].interfaces[0].macAddress
D. accessPoints[1].interfaces[1].macAddress

Answer: (SHOW ANSWER)
The correct expression is accessPoints[0].interfaces[1].macAddress. The JSON object contains a top-level key named accessPoints, whose value is an array. Array indexing begins at zero, so accessPoints[0] selects the first access point object, ap-west-1. Inside that object, the interfaces key also contains an array. Therefore, interfaces[1] selects the second interface object, which has slot: 1, status: "down", and macAddress: "CC:FA:00:11:22:34". The final selector, .macAddress, returns that MAC address value.
This structure is directly aligned with Cisco automation workflows, where RESTCONF and Catalyst Center APIs exchange structured data in JSON. Cisco documents that Catalyst Center REST API payloads are JSON-formatted, and its example describes JSON as key-value data separated by colons. Cisco also states that Catalyst 9800 RESTCONF uses structured XML or JSON with YANG models for programmatic device access. Option B selects ap-east-2. Option C selects the first interface on ap- west-1. Option D references a non-existent second interface on ap-east-2.

NEW QUESTION: 8
An engineer troubleshooting AP join failures notices DTLS negotiation errors between APs and the controller. Which issue is MOST likely responsible?
A. Incorrect RF profile
B. Time synchronization or certificate validation failure
C. Excessive multicast traffic
D. Invalid DHCP Option 43 subnet mask
Answer: (SHOW ANSWER)
DTLS relies on valid certificates and accurate time synchronization. Significant clock mismatches or certificate validation problems frequently prevent secure CAPWAP tunnels from forming between APs and controllers. RF profiles and multicast conditions generally do not affect DTLS establishment directly.

NEW QUESTION: 9
A customer requires wireless clients to maintain uninterrupted voice calls while roaming between access points. Which Cisco wireless feature minimizes roaming delay?
A. WPA3 SAE
B. 802.11r Fast Transition
C. RADIUS accounting
D. AVC profiling
Answer: (SHOW ANSWER)
802.11r Fast Transition accelerates roaming by reducing the authentication exchange required when clients move between APs. This minimizes handoff delay and supports latency-sensitive applications such as VoIP. WPA3 improves security, while AVC and accounting services do not directly optimize roaming performance.

NEW QUESTION: 10
An engineer configures AAA override on a Cisco wireless LAN controller. What is the primary purpose of this feature?
Freecram.net
A. Override AP join priority
B. Apply per-user authorization attributes dynamically
C. Replace RF profiles automatically
D. Override DHCP relay settings
Answer: (SHOW ANSWER)
AAA override allows a RADIUS server to dynamically assign authorization attributes such as VLANs, ACLs, QoS policies, or session timeouts to authenticated users. This enables flexible user-based access control. The feature does not affect AP join behavior, RF tuning, or DHCP operations.

NEW QUESTION: 11
What is a characteristic of 20 MHz channel width in a wireless network?

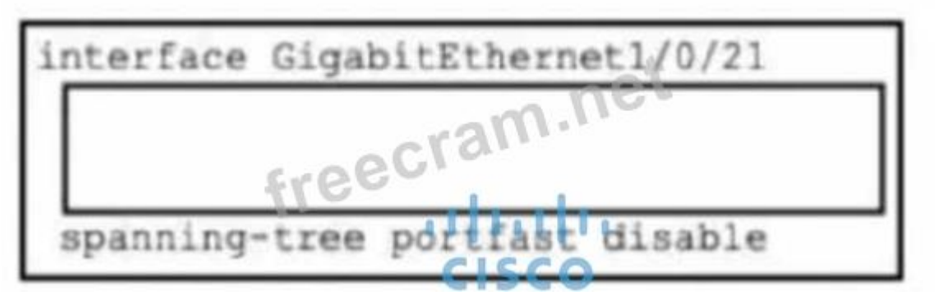
A. Narrowest channel width in the 2.4 GHz band
B. Increases authentication handoff frequency
C. Supports automatic client reassociation
D. Higher throughput than wider channels
Answer: (SHOW ANSWER)
In wireless networks, the 20 MHz channel width is the standard and narrowest channel allocation in the 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.

NEW QUESTION: 12
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?

```
wlan Dev_WiFi 2 Dev_WiFi
 security ft
 security wpa wpa3
 security wpa psk set-key ascii 0 1122334455
 no security wpa akm dot1x
 security wpa akm ft psk
 security wpa akm ft sae
 security wpa akm ft sae ext-key
 security wpa akm psk
 security wpa akm sae
 security wpa akm sae ext-key
 security pmf optional
```

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: (SHOW ANSWER)
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.

NEW QUESTION: 13
Refer to the exhibit. A network engineer is designing a Wi-Fi deployment for a high-density office environment. The engineer must select the appropriate channel plan to minimize co-channel interference (CCI) in the 2.4 GHz band. Which strategy is recommended to reduce CCI?



A. Use all 11 channels with overlapping frequencies in a contiguous pattern.
B. Select only non-overlapping channels (1, 6, 11) for adjacent access points.
C. Assign channels randomly to avoid predictable patterns.
D. Use a single channel for all access points to maintain consistency.
Answer: (SHOW ANSWER)
In the 2.4 GHz band, IEEE 802.11b/g/n Wi-Fi uses channels that are 20 MHz wide but only partially non-overlapping. Cisco Wireless design guides recommend using only non-overlapping channels to prevent co-channel interference (CCI), which occurs when adjacent APs transmit on overlapping frequencies and contend for airtime, resulting in reduced throughput and increased latency. The standard non-overlapping channels in North America are 1, 6, and 11. By carefully assigning these channels to adjacent access points, the RF designer ensures that no two neighboring APs share overlapping channels, thereby minimizing CCI and improving overall network performance.

NEW QUESTION: 14
An IT team is deploying Meraki APs at a remote branch and must ensure that they are automatically assigned to the correct network in the Meraki dashboard. The branch is scheduled to receive 20 new APs, and site connectivity to headquarters was set up. Before shipping the APs, the team must make sure that each one is claimed by the intended network for management and monitoring.
Which deployment action must they take before physically connecting the APs?
A. Activate mesh networking mode for all the new APs before installation.
B. Add the AP serial numbers to the required network within the Meraki dashboard.
C. Preconfigure SSID names and VLAN tags on the local page of each AP in the Meraki dashboard.
D. Create a separate DHCP scope for all the new APs on the local server.
Answer: (SHOW ANSWER)
When deploying Meraki APs, it is essential to claim each AP in the Meraki dashboard to ensure that they are automatically assigned to the correct network and can be managed remotely. This process involves registering the APs with the Meraki cloud, which is done by adding the AP serial numbers to the network within the Meraki dashboard before physically installing them at the branch.
Option B: "Add the AP serial numbers to the required network within the Meraki dashboard." This is the correct answer. Before the APs are physically connected, the administrator needs to log into the Meraki dashboard and add the serial numbers of the new APs to the intended network.
This ensures that once the APs are powered on and connected, they automatically join the correct network and are ready for monitoring and management without requiring further configuration.

NEW QUESTION: 15
A Catalyst 9800 controller deployment requires seamless mobility across multiple controllers in the same mobility domain. Which feature enables this capability?
A. Mobility groups
B. AVC policies

C. Hyperlocation
D. MAC filtering
Answer: (SHOW ANSWER)
Mobility groups allow wireless clients to roam seamlessly between controllers without losing connectivity or session information. Controllers exchange mobility data to preserve client state during roaming events. AVC and Hyperlocation provide analytics and location services rather than inter-controller mobility support.

NEW QUESTION: 16
Refer to the exhibit. A network engineer must create a PSK WLAN that will be anchored to the DMZ. After this WLAN is created, users cannot connect to it. Based on the output from the RA trace, which action must the engineer take to resolve the issue?

```
[client-keymgmt] [17419]: (ERR): MAC: 1111.2222.3333  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [17419]: (ERR): MAC: 1111.2222.3333  Keymgmt: Failed to validate eapol key m2. 11r MIC validation faile
[client-keymgmt] [17419]: (ERR): MAC: 1111.2222.3333  Keymgmt: Failed to eapol key m1 retransmit failure. Max retries fo
[client-orch-sm] [17419]: (note): MAC: 1111.2222.3333  Send delete mobile. Sending DELETE MOBILE succesfully for BSSID:
```

freecram.net

A. Disable fast transition 802.11r on the WLAN.
B. Configure matching passwords on the client and the WLAN.
C. Remove the anchor WLC from the mobility group.
D. Configure matching WLANs on the foreign and the anchor.
Answer: (SHOW ANSWER)
The failure is occurring during WPA/WPA2 key management, not during mobility anchoring. The radioactive trace shows Failed to validate eapol mic. MIC mismatch followed by Failed to validate eapol key m2, which means the authenticator and supplicant derived different key material during the PSK handshake. Cisco's Catalyst 9800 client-connectivity troubleshooting maps this log pattern directly to a wrong password condition and lists the corrective actions as fixing the password on the endpoint or on the SSID/WLAN. The 11r MIC validation failed phrase does not automatically make 802.11r the root cause; it only shows that the failed MIC validation occurred while Fast Transition key logic was in use. Disabling 802.11r would be a workaround only for client capability or FT interoperability issues, but the trace points to PSK mismatch. Removing the anchor WLC would break the intended DMZ anchoring design, and matching WLANs on foreign and anchor is required for anchor deployments, but it would not produce this EAPOL M2 MIC failure. The correct remediation is to ensure the client-entered PSK matches the WLAN PSK.

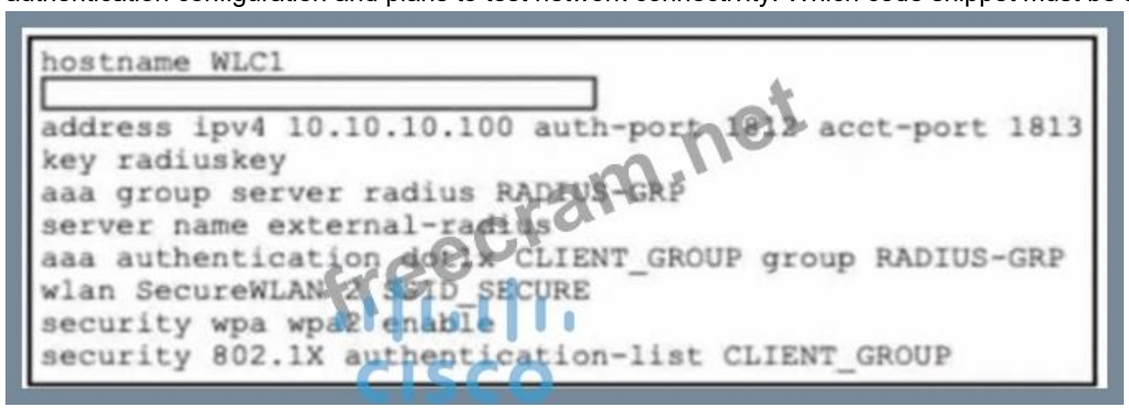
Valid 350-101 Dumps shared by EduDump.com for Helping Passing 350-101 Exam! EduDump.com now offer the **newest 350-101 exam dumps**, the EduDump.com 350-101 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 350-101 dumps with Test Engine here: https://www.edudump.com/exams/Cisco/350-101/premium/ (**127** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 17
Which feature does bridge mode provide in a Cisco wireless mesh architecture?
A. It enables point-to-point communication between network segments.
B. It switches all traffic passing through the AP to 2.4 GHz by default.
C. It adjusts RF transmit power on any neighbor nodes.
D. It communicates with WAN edge by default.
Answer: (SHOW ANSWER)

Bridge mode in a Cisco wireless mesh deployment allows access points to operate as mesh infrastructure nodes, typically as a Root AP (RAP) or Mesh AP (MAP), so Ethernet segments can be connected across a wireless backhaul. Cisco's mesh design documentation states that in a point-to-point bridging scenario, a mesh AP can extend a remote network by using the backhaul radio "to bridge two segments of a switched network." This directly maps to option A: point-to- point communication between network segments.
In Catalyst 9800 mesh deployments, Cisco documents converting an AP to bridge mode with capwap ap mode bridge, after which the AP rejoins the controller in bridge mode and can be assigned a mesh role. Cisco also defines the RAP as the AP with the wired connection toward the WLC, while the MAP joins through its radio path toward the RAP. Option B is incorrect because bridge mode does not force all traffic to 2.4 GHz; Cisco mesh backhaul can use configured backhaul radios. Option C describes RRM/TPC behavior, not bridge mode. Option D incorrectly associates mesh bridge mode with WAN edge functions.

NEW QUESTION: 18
What is the main benefit of using AI Enhanced RRM on the Cisco Catalyst 9800 wireless controller?
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: (SHOW ANSWER)
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.

NEW QUESTION: 19
Refer to the exhibit. A network administrator is working on a WLC to enable user access for employee tablets using PEAP-MSCHAPv2 with a RADIUS backend. The administrator verifies the external authentication configuration and plans to test network connectivity. Which code snippet must be added to the configuration for the WLC to support authentication with an external server?



A. radius server external-radius
B. external-radius RADIUS-GRP
C. radius server RADIUS-GRP

D. external-radius aaa server

Answer: (SHOW ANSWER)

The missing command is radius server external-radius. On a Catalyst 9800 WLC, the external RADIUS server object must be declared first with radius server <server-name>. The following lines, address ipv4 10.10.10.100 auth-port 1812 acct-port 1813 and key radiuskey, are subcommands entered under that RADIUS server configuration mode. Cisco's Catalyst 9800 802.1X configuration workflow starts by declaring the RADIUS server, then adding it to a RADIUS server group, then creating the authentication method list, and finally mapping that list to the WLAN. Cisco's configuration guide example uses the same IOS XE structure: radius server <name>, followed by address ipv4 ... auth- port 1812 acct-port 1813 and key ....

The server group later references server name external-radius, so the RADIUS server object must be named external-radius exactly. Option C would incorrectly create a server named RADIUS-GRP, which is already the AAA server group name, not the RADIUS server object.

Options B and D are invalid IOS XE syntax. PEAP-MSCHAPv2 itself is handled through the 802.1X/EAP exchange with the RADIUS server; the WLC acts as the authenticator and forwards authentication requests through the configured AAA method list.

NEW QUESTION: 20

An engineer has been tasked with configuring a Cisco Catalyst 9100 AP to join a WLC using a static configuration as DHCP and DNS discovery methods are not available. The engineer has set the AP hostname to `AP053540555', and has configured the AP with a static IP address, subnet mask, and default gateway. The engineer must now configure the AP to discover the primary WLC with hostname `WLC-PRIMARY' and IP address `192.168.100.10'. Which CLI command must the engineer use on the AP?

Freecram.net

A. capwap ap WLC-PRIMARY 192.168.100.10

B. ap primary-base WLC-PRIMARY capwap 192.168.100.10

C. capwap ap primary-base 192.168.100.10

D. capwap ap primary-base WLC-PRIMARY 192.168.100.10

Answer: (SHOW ANSWER)

The correct AP-side command is capwap ap primary-base WLC-PRIMARY 192.168.100.10.

Cisco's Catalyst AP command reference shows the syntax for configuring the primary controller as capwap ap primary-base <controller-name> <controller-ip-address>, and provides the same structure in its example: capwap ap primary-base wlc-5520 209.165.200.224. Cisco's Catalyst 9800 AP join documentation also identifies the primary controller discovery entry as capwap ap primary-base <wlc-hostname> <wlc-IP-address>.

This command statically primes the lightweight AP with the preferred WLC when DHCP option 43, DNS discovery, broadcast discovery, or prior learned controller information is unavailable.

The hostname AP053540555 is only the AP's local identity and is not part of the WLC discovery command. Option A omits the primary-base keyword, so it is not valid syntax. Option B places keywords in the wrong order and does not match Cisco CAPWAP AP CLI. Option C omits the required controller name before the IP address.

NEW QUESTION: 21

What is used for measuring gain on a Wi-Fi antenna?

A. length of the antenna

B. decibels relative to dBi

C. voltage against dBm

D. blend of analog and digital signals

Answer: (SHOW ANSWER)

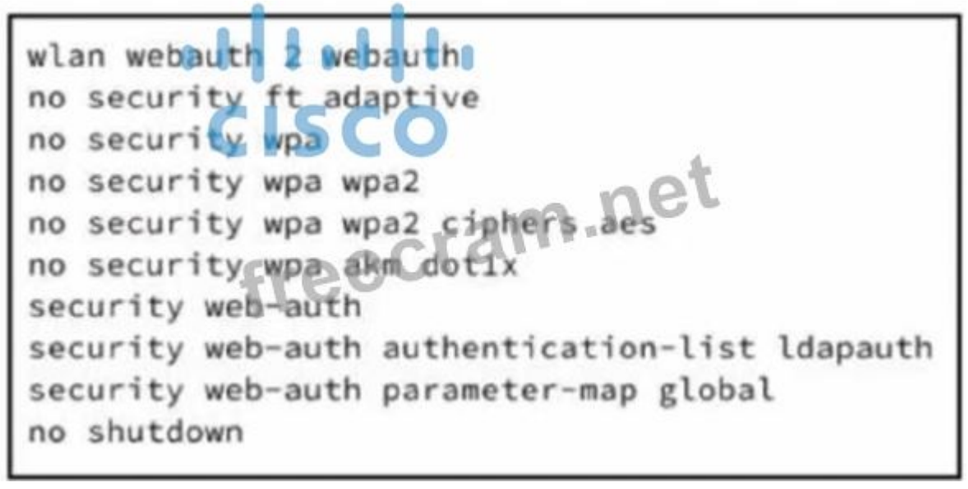
Wi-Fi antenna gain is measured in dBi, meaning decibels referenced to an isotropic radiator.

Cisco's Wireless RF Reference Guide states that antennas have gain measured in decibels relative to isotropic gain, or dBi, and further explains that antenna gain is a ratio comparing the gain of a specific antenna to a theoretical isotropic antenna. Cisco's RF design documentation also defines dBi as the power gain rating of antennas, where real antennas are compared to an isotropic antenna that radiates the same power density equally in all directions.
Option B is therefore the correct selection, although the technically precise phrase is decibels relative to isotropic, abbreviated dBi. Antenna length can influence resonance and design, but it is not the measurement unit for gain. Voltage against dBm is incorrect because dBm references absolute power relative to 1 milliwatt, not antenna gain. Analog/digital signal blending is unrelated to RF antenna performance.

NEW QUESTION: 22
A wireless engineer notices high retransmission rates on a WLAN supporting IoT devices operating at low data rates. Which configuration change is MOST appropriate?
A. Increase DTIM interval dramatically
B. Disable lower data rates carefully
C. Enable MAC filtering
D. Reduce RADIUS retransmissions
Answer: (SHOW ANSWER)
Disabling extremely low data rates improves airtime efficiency and reduces retransmissions caused by slow clients occupying the channel excessively. However, engineers must verify device compatibility before removing legacy rates. DTIM and RADIUS settings are unrelated to RF retransmission optimization.

NEW QUESTION: 23
To double the range of a transmitter, which value must the transmitter be changed to if it is currently at 17 dBm?
A. 20 dBm
B. 27 dBm
C. 100 dBm
D. 17 dBm
Answer: (SHOW ANSWER)
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: 10log 10(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.

NEW QUESTION: 24
Refer to the exhibit. A wireless controller is deployed at a branch location to facilitate guest client connectivity. A network engineer configures one WLAN using Web authentication and activates web-based method to align with company security policies. Which configuration enables client authentication for this WLAN?



A. security web-auth
B. wlan webauth 2 webauth
C. no security wpa wpa2
D. no security wpa akm dot1x
Answer: A (LEAVE A REPLY)
The command that enables web-based client authentication on the WLAN is security web-auth. Cisco's Catalyst 9800 Web-Based Authentication guide shows the WLAN configuration workflow: enter WLAN configuration mode, disable WPA security for the open Layer 2 guest WLAN, then "Enable web authentication for WLAN" using security web-auth. Cisco then applies the authentication list and parameter map with security web-auth authentication-list ... and security web-auth parameter-map ..., which refine the WebAuth method and portal behavior after WebAuth itself is enabled.
Cisco's LDAP authentication example mirrors the exhibit exactly: wlan webauth 2 webauth, removal of WPA/802.1X Layer 2 security, security web-auth, security web-auth authentication-list ldapauth, and security web-auth parameter-map global. Option B only creates or enters the WLAN profile with WLAN ID 2 and SSID name. Options C and D disable WPA2 and 802.1X AKM; they do not authenticate clients.

NEW QUESTION: 25
Which function does FRA use to optimize client experience and network coverage?
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: (SHOW ANSWER)
Flexible Radio Assignment dynamically changes the role of dual-band radios based on RF conditions, allowing the AP to improve coverage, capacity, and client experience by adapting radio operation to the wireless environment.

NEW QUESTION: 26
Refer to the exhibit. An engineer configured a static IP address on a LWAPP, but it is not reachable for management. The engineer configured the wrong gateway and must now change the default gateway to 172.16.100.1. Which CLI command must the engineer use?

```
AP-1# show interfaces wired 0

wired0    Link encap:Ethernet  HWaddr C8:8B:5E:BA:D0 eMac Status: UP
          inet addr:172.16.100.104  Bcast:172.16.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:2400  Metric:1
          full Duplex, 1000 Mb/s

Wired0 Port Statistics:
ID          :              2          TYPE        :              0
RX PKTS     :          35109/431      TX PKTS     :          1307/11
RX OCTETS   :        2899435/34925    TX OCTETS   :        377424/1575
RX ERR      :            287/0        TX ERR      :            0/0
```

freecram.net

A. capwap ap ip default-gateway 172.16.100.1

B. capwap ap controller ip address 172.16.100.1

C. capwap ap ip 172.16.100.104 255.255.255.192 172.16.100.1

D. capwap ap ip 172.16.100.104 255.255.255.0 172.16.100.1

Answer: (SHOW ANSWER)

When deploying a Lightweight Access Point (LWAPP) in a Cisco wireless network, proper Layer 3 configuration is essential for management and connectivity to the Wireless LAN Controller (WLC). Each LWAPP requires a valid IP address, subnet mask, and default gateway to communicate beyond its local subnet. In the exhibit, the AP is assigned 172.16.100.104/24, but the previously configured gateway was incorrect, preventing communication with the WLC. Cisco IOS XE requires that the AP's IP interface be configured with the correct default gateway to route traffic properly. The correct syntax is capwap ap ip <AP-IP> <Subnet-Mask> <Default-Gateway>.

Option D matches the IP, subnet mask, and gateway for the given network, ensuring the AP can reach the WLC for LWAPP registration.

NEW QUESTION: 27

Refer to the exhibit.

```
import requests
import json
API_ENDPOINT = "https://your-api-server.com/api/v1/devices/wireless"
AUTH_TOKEN = "YOUR_SECRET_API_TOKEN"
headers = {
"Accept": "application/json",
"Authorization": f"Bearer {AUTH_TOKEN}"
}
print("Fetching wireless inventory from the API...")
try:
response = requests.get(API_ENDPOINT, headers=headers, timeout=10)
response.raise_for_status()
```

```
wireless_inventory_list = response.json()
print("Successfully retrieved and parsed device data.\n")
print("--- Wireless Device Summary ---")
if isinstance(wireless_inventory_list, list) and
wireless_inventory_list:
for device in wireless_inventory_list:
mac = device.get("macAddress", "N/A")
ip = device.get("ipAddress", "N/A")
print(f"Device Found -> MAC: {mac}, IP: {ip}")
else:
print("No wireless devices were found in the inventory.")
except requests.exceptions.RequestException as e:
print(f"Error during API request: {e}")
except json.JSONDecodeError:
print("Error: Failed to parse the response from the API. It is not
valid JSON.")
```

A Cisco engineer is analyzing how a dictionary interacts with key-value pairs in a Python script that processes device records collected from a wireless controller. The engineer reviews the construction of the script to interpret the sequence used for data extraction. Which element performs the interaction within the script?

A. pop operation
B. import function
C. get() method
D. format expression

Answer: (SHOW ANSWER)

The correct element is the get() method. In the script, each device object is treated as a Python dictionary created from parsed JSON API output. The lines device.get("macAddress", "N/A") and device.get("ipAddress", "N/A") perform direct key-based lookup against the dictionary and return the associated value when the key exists. Python documentation defines dictionaries as key- value mappings and states that get() is used to avoid a KeyError by returning None or a specified default value when the key is absent.

This behavior is exactly what automation scripts need when consuming controller or wireless inventory APIs, because returned device records may not always contain every field. Cisco API inventory models commonly return structured device objects containing properties such as MAC address, model, network ID, product type, and wireless-related inventory attributes, which are then parsed by automation code. The pop operation would remove a dictionary key, not safely read it. The import function only loads modules such as requests and json. The format expression only builds the printed output string.

NEW QUESTION: 28

What is a benefit of applying TACACS authentication for device access?

A. static user grouping without role differentiation
B. fragmented statistics across controllers and devices
C. streamlined administrator access across platforms
D. single user for device and network access

Answer: (SHOW ANSWER)

TACACS+ is used for device administration, especially for GUI and CLI access to infrastructure platforms such as Cisco Catalyst 9800 WLCs, switches, and routers. Cisco defines TACACS+ as a security application that provides centralized validation for users attempting to access a device or network access server, and it separates authentication, authorization, and accounting functions for

administrative control. Cisco ISE device administration documentation further states that TACACS+ is used to control and audit network device configuration, allowing devices to query ISE for administrator authentication and authorization while sending accounting records for logging administrator actions.
Therefore, the primary benefit is streamlined administrator access across platforms. Instead of maintaining local administrator accounts independently on every WLC or network device, TACACS+ enables centralized identity validation, role-based authorization, and consistent audit trails. Option A is incorrect because TACACS+ supports differentiated authorization rather than static grouping. Option B is the opposite of centralized accounting. Option D is inaccurate because TACACS+ is mainly for device administration, whereas client or endpoint network access is typically handled with RADIUS.

NEW QUESTION: 29
Which hierarchy in a YANG data modeling approach describes a relationship in the context of NETCONF device configuration?
A. object and attribute model
B. child and parent structure
C. hub and spoke model
D. tree and leaf-based structure
Answer: (SHOW ANSWER)
YANG represents network configuration and operational state as a hierarchical data model. In Cisco model-driven programmability, YANG is used with NETCONF to model configuration and state data so that client applications can programmatically retrieve, edit, and manage device configuration. Cisco states that YANG is used with NETCONF for automated and programmable network operations, and that YANG primarily models the configuration and state data used by NETCONF operations.
The correct hierarchy is the tree and leaf-based structure. Cisco's YANG model structure description defines it as a hierarchical framework that organizes data into a tree with top-level nodes and nested child nodes, and groups related data through containers, lists, and leaves. In this model, containers and lists create structure, while leaf nodes hold actual values such as interface names, VLAN IDs, descriptions, IP addresses, or policy parameters. Option B describes a relationship inside the hierarchy, but it is not the full YANG modeling hierarchy. Options A and C are not valid YANG/NETCONF structural models.

NEW QUESTION: 30
A business is deploying Cisco Catalyst 9100 APs managed by Catalyst 9800 WLCs. The IT team needs policies that adapt based on user identity and device posture and also provide visibility into device activity and location. Which configuration meets these requirements?
Freecram.net
A. Integrate Cisco Catalyst Center with Cisco ISE for policy control, add mobile device management for posture checks, and use Cisco Spaces for location visibility.
B. Use Cisco Catalyst 9800 ACLs combined with mobile device management integration without Catalyst Center or Catalyst Spaces.
C. Configure Cisco Catalyst Center assurance for visibility and apply static per-service set identifier virtual LAN assignments without Cisco ISE integration.
D. Integrate Cisco ISE for identity-based policies and omit mobile device management and location services.
Answer: (SHOW ANSWER)
To enforce adaptive policies based on user identity, device posture, and provide comprehensive visibility into device activity and location, Cisco recommends integrating Cisco Catalyst Center, Cisco ISE, and Cisco Spaces. Cisco ISE provides identity-based access control and posture assessment, allowing dynamic policy enforcement for users and devices. Mobile device management integration further extends posture checks for endpoint compliance. Cisco Catalyst Center enables real-time assurance and monitoring of network performance, device activity, and service health, while Cisco Spaces provides location analytics and visibility of client devices across the wireless environment.

NEW QUESTION: 31
A retail store is setting up guest Wi-Fi on a Cisco 9800 WLC. The IT team has these requirements:
- Guests are prompted for web authentication.
- After login, traffic is restricted to internet-only access.
- Guest WLAN must be available throughout all sales floors.

- Guest WLAN must not impact the existing corporate WLAN.
- Guest SSID must not require a password.
Which set of configurations must the IT team deploy to meet the requirements?
A. WPA2-Enterprise authentication on the guest WLAN and use dynamic VLAN assignment.
B. Local web authentication on the guest SSID and apply ACLs to allow all traffic except FTP and SSH from the guest WLAN.
C. Central web authentication on the guest WLAN and apply an ACL that denies traffic between devices that use the internal subnets.
D. MAC filtering on the guest WLAN and enable client exclusion for segregation.
Answer: (SHOW ANSWER)
For a retail guest WLAN deployment, Cisco best practices dictate using central web authentication (web-auth) combined with access control lists (ACLs) to enforce network segmentation and restrict guest traffic to internet-only access. Central web authentication allows all guest devices to be redirected to a captive portal for login without requiring a pre-shared key or WPA2-Enterprise credentials, satisfying the "no password" requirement. Applying an ACL that blocks access to internal subnets ensures that guest traffic cannot interfere with corporate networks while still permitting internet connectivity.

Valid 350-101 Dumps shared by EduDump.com for Helping Passing 350-101 Exam! EduDump.com now offer the **newest 350-101 exam dumps**, the EduDump.com 350-101 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 350-101 dumps with Test Engine here: https://www.edudump.com/exams/Cisco/350-101/premium/ (**127** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
Which condition is required for a line-of-sight RF connection?
A. Wireless multipath signal propagation to the client
B. MIMO connection support on both wireless radios
C. Delay on wireless signal delivery introduced by reflection
D. No physical objects between the transmitter and receiver
Answer: (SHOW ANSWER)
A line-of-sight (LOS) RF connection requires a clear, unobstructed path between the transmitter and receiver. This ensures that the transmitted signal reaches the receiving device without attenuation, reflection, or diffraction caused by physical obstacles such as walls, furniture, or other structures. LOS conditions are critical for high-frequency RF links, particularly in the 5 GHz band, where signals cannot easily penetrate objects.

NEW QUESTION: 33
What is used for measuring gain on a Wi-Fi antenna?
A. length of the antenna
B. decibels relative to dBi
C. voltage against dBm
D. blend of analog and digital signals
Answer: (SHOW ANSWER)
Wi-Fi antenna gain is measured in dBi, meaning decibels referenced to an isotropic radiator.
Cisco's Wireless RF Reference Guide states that antennas have gain measured in decibels relative to isotropic gain, or dBi, and further explains that antenna gain is a ratio comparing the gain of a specific antenna to a theoretical isotropic antenna. Cisco's RF design documentation also defines dBi as the power gain rating of antennas, where real antennas are compared to an isotropic antenna that radiates the same power density equally in all directions.

Option B is therefore the correct selection, although the technically precise phrase is decibels relative to isotropic, abbreviated dBi. Antenna length can influence resonance and design, but it is not the measurement unit for gain. Voltage against dBm is incorrect because dBm references absolute power relative to 1 milliwatt, not antenna gain. Analog/digital signal blending is unrelated to RF antenna performance.

NEW QUESTION: 34
An engineer must prevent unauthorized rogue APs from connecting to the enterprise wired network. Which Cisco feature best addresses this requirement?
A. CleanAir
B. Rogue containment
C. ClientLink
D. Optimized Roaming
Answer: (SHOW ANSWER)
Rogue containment identifies unauthorized access points connected to the network and can actively disrupt associated wireless clients to mitigate threats. CleanAir detects RF interference, while ClientLink and Optimized Roaming improve client performance rather than network security enforcement against rogue devices.

NEW QUESTION: 35
Refer to the exhibit. An engineer must configure a wireless guest WLAN, which requires clients to use VLAN 10 for a deployment at site A. Based on the configuration commands shown, which additional configuration meets the requirements?

```
config t
wlan guest-ssid 4 guest-ssid
mac-filtering <authorization-list>
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
no shutdown
```

A. wlan guest-ssid 4 guest-ssid
access vlan 10
no shutdown
B. wlan guest-ssid 4 guest-ssid
vlan 10
no shutdown
C. wlan policy profile guest-policy
access vlan 10
no shutdown
D. wireless profile policy guest-policy
vlan 10
no shutdown
Answer: (SHOW ANSWER)

On a Catalyst 9800 WLC, client VLAN assignment is configured in the wireless policy profile, not directly under the WLAN. Mapping the guest WLAN to a policy profile that specifies VLAN 10 ensures guest clients are placed into the required VLAN.

NEW QUESTION: 36
Refer to the exhibit. 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?

```
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
```

cisco
passcram.net

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: (SHOW ANSWER)
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.

NEW QUESTION: 37
Which wireless connection occurs when there are no physical obstacles between the receiver and transmitter?
A. attenuation
B. line-of-sight
C. reflection
D. beamforming

Answer: (SHOW ANSWER)
The correct answer is line-of-sight. In RF terminology, line-of-sight describes a wireless path where the transmitting antenna and receiving antenna have an unobstructed visual or RF path between them. Cisco's RF power documentation defines this directly: antennas that can see each other without obstacles between them are considered to be in line of sight. This is especially important in outdoor, bridge, mesh, and point-to-point wireless designs, where buildings, terrain, foliage, or other obstructions can degrade or block the RF path.
The other options describe different RF behaviors. Attenuation is signal loss as RF energy travels through free space, cables, walls, or other materials. Reflection occurs when RF energy bounces off a surface such as metal, glass, or concrete, often contributing to multipath. Beamforming is an antenna/transmission technique that focuses RF energy toward a client or receiver to improve signal quality; it is not the condition of having no obstacles. Cisco mesh planning guidance also emphasizes verifying whether a wireless link has clear line of sight before deployment, reinforcing that LOS is a path condition, not a modulation or security feature.

NEW QUESTION: 38
What defines device sensitivity in a wireless environment?
A. capability to process the signal
B. detection of redundant gateways
C. synchronization of beacon intervals
D. implementation of key refresh schedules
Answer: (SHOW ANSWER)
Device sensitivity in a wireless environment refers to receiver sensitivity: the minimum RF signal level a client or AP radio must receive to successfully detect, demodulate, and decode a transmission. Cisco defines receiver sensitivity as the minimum signal power level, expressed in dBm or mW, required for a receiver to accurately decode a given signal. Cisco RF design guidance further states that sensitivity indicates the lowest received power before the receiver considers the signal unintelligible.
Therefore, option A is correct because sensitivity is fundamentally about the radio's capability to process a received signal at low power levels. A more sensitive receiver can decode weaker frames, improving effective coverage and receive performance, provided the signal-to-noise ratio and interference conditions remain acceptable. Cisco also notes that individual device sensitivity determines how well a device can hear and demodulate RF energy, which directly affects contention behavior and WLAN performance in dense environments. Redundant gateways, beacon interval synchronization, and key refresh schedules are Layer 3 availability, 802.11 timing, and security-key management topics; they do not define RF receiver sensitivity.

NEW QUESTION: 39
What does a low SNR value result in?
A. Scheduling of firmware maintenance windows
B. Activation of automatic failover features
C. Improved channel reliability
D. Decreased data integrity with possible errors
Answer: (SHOW ANSWER)
The Signal-to-Noise Ratio (SNR) is an important metric used to determine the quality of a wireless signal. It compares the strength of the signal to the level of background noise. A low SNR indicates that the signal is weak relative to the noise, leading to poor signal quality.
Option D: Decreased data integrity with possible errors is the correct answer. When SNR is low, the quality of the data transmission is compromised. The noise interferes with the signal, leading to potential data errors and a decrease in data integrity. This can cause packets to be lost or corrupted, requiring retransmissions, and reducing the overall performance and reliability of the network.

NEW QUESTION: 40
Which Cisco Ultra-Reliable Wireless Backhaul process enables devices to establish a reliable connection with the next AP along their path before losing connectivity to the current one in a wireless network during roaming?
Freecram.net
A. Open roaming

B. Fast client handoff
C. 802.11v high speed roaming
D. Make-before-break handover logic
Answer: (SHOW ANSWER)
The correct answer is Make-before-break handover logic. This is a key feature in Cisco's Ultra- Reliable Wireless Backhaul (URWB) process that allows devices to establish a connection to the next AP (Access Point) before disconnecting from the current AP. This seamless transition ensures that there is no disruption in the wireless connection as the client roams between APs, which is especially important in environments where consistent, low-latency connectivity is essential, such as in real-time applications (e.g., voice or video).

NEW QUESTION: 41
A company deploys wireless networks in multiple countries. Why is configuring the correct AP regulatory domain critical?
A. It determines DHCP relay behavior
B. It controls permitted channels and transmit power levels
C. It enables QoS trust boundaries
D. It changes CAPWAP encapsulation
Answer: (SHOW ANSWER)
Regulatory domains ensure APs comply with regional wireless laws governing allowed channels, transmit power limits, and DFS requirements. Incorrect regulatory configuration can violate legal requirements and cause interoperability problems. DHCP and CAPWAP operations are unrelated to regulatory compliance settings.

NEW QUESTION: 42
Refer to the exhibit. A client authenticates via 802.1X against an ISE server that is configured to return a specific VLAN ID (VLAN 100) via an attribute value pair. However, the administrator notices that the client is placed in the wrong VLAN (VLAN 50). What must the administrator implement to resolve the issue?

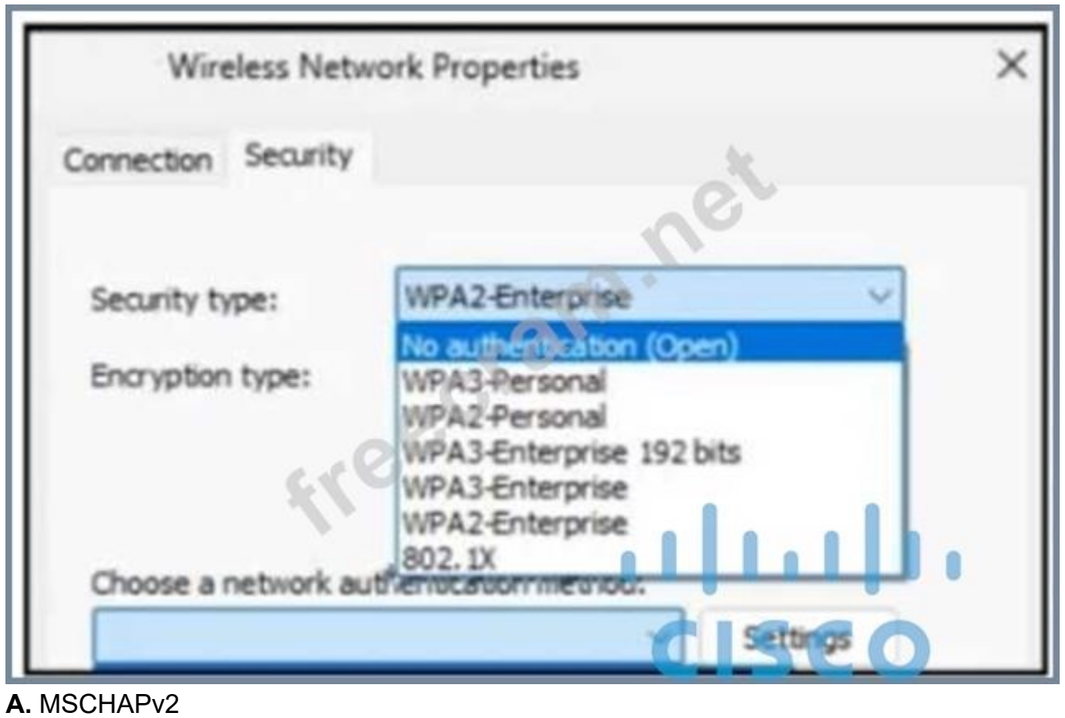
```
[client-orch-sm] [17419]: (note): MAC: 1111.2222.3333  Association received. BSSID 1234.5678.abcd, WLAN Corp-WLAN,
[client-orch-sm] [17419]: (debug): MAC: 1111.2222.3333  Received Dot11 association request.
[client-auth] [17419]: (note): MAC: 1111.2222.3333  L2 Authentication initiated. method DOT1X, Policy VLAN 50, AAA overri
[auth-mgr] [17419]: (info): [1111.2222.3333:capwap_90000005] auth mgr attr add/change notification is received for attr a
[radius] [17419]: (info): RADIUS: Received from id 1812/115 192.168.1.11:0, Access-Accept, len 309
[radius] [17419]: (info): RADIUS:  Tunnel-Type          [64]    6  VLAN                [13]
[radius] [17419]: (info): RADIUS:  Tunnel-Medium-Type   [65]    6  ALL_802             [6]
[radius] [17419]: (info): RADIUS:  Tunnel-Private-Group-Id[81]    6  "100"
[radius] [17419]: (info): Valid Response Packet, Free the identifier
[client-auth] [17419]: (note): MAC: 1111.2222.3333  L2 Authentication Key Exchange Start. Resolved VLAN: 50
```

A. Configure the policy profile to allow ISE to override the VLAN.
B. Configure VLAN 100 as an SVI on the WLC.
C. Configure VLAN 100 on the trunk ports of the WLC.
D. Configure AAA VLAN enable on the WLAN.
Answer: (SHOW ANSWER)
In this scenario, the client is placed in the wrong VLAN (VLAN 50) even though the ISE server is configured to assign VLAN 100. The key part of the issue is that the VLAN assignment returned by ISE is not being applied correctly.
Option A: "Configure the policy profile to allow ISE to override the VLAN." This is the correct answer. The policy profile on the Wireless LAN Controller (WLC) should be configured to allow the ISE server's VLAN assignment to override the locally configured VLAN settings on the WLC.
Without this, the WLC might default to its pre-configured VLAN (VLAN 50) instead of the VLAN assigned by ISE (VLAN 100).

NEW QUESTION: 43
A managed service is rolling out advanced wireless infrastructure to support an expanding organization with diverse device types. The implementation requires integration of dynamic endpoint profiling for secure access and device classification. According to the baseline deployment with ISE policy sets, the engineering group must enforce access parameters based on device category rules. Which configuration action must be taken to fulfill the initiative?
A. Create device-type groups.
B. Configure profiling groups.
C. Implement user ID groups.
D. Define endpoint group mapping.
Answer: (SHOW ANSWER)
Dynamic endpoint profiling in Cisco wireless networks is used to classify devices based on type, behavior, and attributes, enabling policy enforcement that adapts to device posture. In a deployment integrated with Cisco ISE, profiling groups are created to define rules and categories for device types such as smartphones, laptops, printers, and IoT devices. These profiling groups allow the wireless controller to map devices to the correct ISE policy sets dynamically, ensuring that security policies, VLAN assignments, and access controls are applied according to the device profile.

NEW QUESTION: 44
What is the maximum transmit power level allowed for 2.4 GHz in the United States?
A. 20 dBm
B. 23 dBm
C. 30 dBm
D. 36 dBm
Answer: (SHOW ANSWER)
The correct answer is 30 dBm, which equals 1 watt of conducted transmit power. In the United States, the 2.4-GHz ISM band used by 802.11b/g/n/ax Wi-Fi falls under FCC Part 15.247. The FCC rule permits digital modulation systems in the 2400?483.5 MHz band and specifies that the maximum conducted output power is 1 Watt. Converting watts to dBm uses the formula dBm = 10 log10(mW): 1 watt equals 1000 mW, and 10 log10(1000) = 30 dBm.
This is also consistent with Cisco wireless configuration behavior, where Cisco controller Radio Resource Management transmit-power limits use dBm values and support a configurable transmit-power range up to 30 dBm. The key distinction is that 30 dBm is conducted transmit power, while 36 dBm commonly represents an EIRP value when antenna gain is included, such as 30 dBm transmitter output plus 6 dBi antenna gain. Cisco RF fundamentals emphasize that antenna gain affects coverage and radiated energy, so transmit power and EIRP must not be confused.

NEW QUESTION: 45
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 select 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?



A. MSCHAPv2
B. TEAP
C. EAP-TLS
D. PEAP
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 46
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?
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: (SHOW ANSWER)
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.

Valid 350-101 Dumps shared by EduDump.com for Helping Passing 350-101 Exam! EduDump.com now offer the **newest 350-101 exam dumps**, the EduDump.com 350-101 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 350-101 dumps with Test Engine here: https://www.edudump.com/exams/Cisco/350-101/premium/ (**127** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 47
A persistent network issue is impacting connectivity for workstations in a training lab when connecting to a lab SSID. Wireless logs show clients never receive a DHCP offer when trying to obtain an IP address. The APs are operating in Local mode. Network monitoring systems indicate optimal signal quality and radio performance, VLAN assignments for the affected SSID have been configured, and all clients are affected. Which action resolves the issue?
A. Release or renew the client IP configuration.
B. Enable DHCP option 43.
C. Configure DHCP relay.
D. Disable multicast on the WLC.
Answer: (SHOW ANSWER)
The fault domain is DHCP forwarding, not RF, client-side addressing, or AP discovery. Cisco explains that when a wireless client associates, it sends a DHCP Discover broadcast, and depending on AP mode, that traffic is either forwarded through the WLC or passed to the next hop. Cisco further states that if no DHCP server exists in the client's local Layer 2 domain, the router or SVI for the client VLAN must forward DHCP discovery traffic using an IP helper address.
Because the APs are in Local mode, client traffic is centrally switched through CAPWAP to the WLC, where the client VLAN/SVI path must correctly relay DHCP toward the DHCP server.
Cisco's Catalyst 9800 DHCP configuration guide shows DHCP relay configuration under the client VLAN SVI by entering the IPv4 helper address, and the CLI example uses ip helper- address <ip-address> to forward UDP broadcasts such as DHCP requests.
Option C resolves the issue because all clients are affected and none receive a DHCP offer, indicating the DHCP Discover is not reaching the DHCP server or the offer is not returning through the relay path. DHCP option 43 is for AP controller discovery, not client DHCP addressing.

NEW QUESTION: 48
A wireless administrator must configure detailed and comprehensive monitoring for client devices across branch locations. The team wants to streamline operations for faster response during performance degradation. To support the organization's growth, the administrator needs a centralized reporting platform that displays aggregated data. Which solution must the administrator use to monitor the clients in the network?
A. Implement central syslog server.
B. Use Cisco Catalyst Center Assurance.
C. Run show logging on WLC CLI.
D. Use the WLC dashboard.
Answer: (SHOW ANSWER)
Cisco Catalyst Center Assurance is the correct solution because the requirement is centralized, scalable, multi-site client monitoring with aggregated health and troubleshooting data. Cisco states that Catalyst Center Assurance provides a Client health dashboard and supports both wired and wireless clients. It is specifically used to obtain a global view of all client device health and determine whether issues require action.
This directly matches the need for monitoring clients across branch locations and responding faster during performance degradation. Catalyst Center Assurance also provides location-based visibility, health scoring, client trend analysis, onboarding failure reasons such as AAA or DHCP, and Client 360 views for detailed troubleshooting. Cisco documents that Client 360 provides detailed client connectivity troubleshooting, including what problem occurred, when it occurred, why it occurred, and whether the impact is isolated or widespread. Cisco's Catalyst Center data sheet further describes

Network and Client Health dashboards as giving administrators a high- level overview of every network device and client, with expansion by geographical site, device list, client list, or topology. Syslog, WLC CLI logging, and a local WLC dashboard are useful operational tools, but they do not provide enterprise-scale assurance analytics.

NEW QUESTION: 49
Users report slowness on the network, and it is suspected that certain applications are consuming all the bandwidth. A network engineer must enable the NBAR protocol to improve wireless client traffic visibility and provide advanced, granular, application classification, and analytics. How should the network engineer configure NBAR on a 9800 WLC?
A. Enable NBARv2 on the WLAN.
B. Enable deep packet inspection on the WLAN.
C. Configure packet inspection on the policy profile.
D. Configure AVC on the policy profile.
Answer: (SHOW ANSWER)
The correct configuration approach is to enable Application Visibility and Control on the policy profile. On the Catalyst 9800, WLANs are not configured as isolated monolithic objects; the WLAN profile is mapped to a policy profile through a policy tag, and many client traffic services are applied from that policy profile. Cisco defines AVC as the wireless feature set that identifies and monitors applications using DPI, creates rules to manage application bandwidth and usage, and integrates with Flexible NetFlow for per-application or per-protocol statistics. Cisco further states that AVC benefits from NBAR running on the AP or controller, and that the NBAR2 engine analyzes and recognizes traffic flows.
Operationally, Cisco's 9800 AVC guide shows that AVC is enabled by navigating to Configuration > Services > Application Visibility and selecting the relevant Policy Profile. It also shows the CLI form under the policy profile: wireless profile policy AVC_testing followed by ip nbar protocol-discovery, with verification showing NBAR Protocol Discovery: Enabled. Options A and B are incorrect because the feature is not enabled directly on the WLAN. Option C is generic and incomplete; the Cisco feature construct is AVC.

NEW QUESTION: 50
A medium-sized enterprise must provide wireless internet to visitors in their lobby using a Cisco 9800 WLC. The solution must meet these requirements:
- Ensure that guests cannot access the corporate LAN.
- Guests are redirected to a login page before browsing.
- The guest network must use a separate VLAN from internal users.
- Access must be limited to web browsing only.
- Guest access does not require any preshared keys or certificates.
Which two actions must be taken to achieve this solution? (Choose two.)
Freecram.net
A. Create a WLAN that uses a web policy and points to a consent parameter map.
B. Apply a webauth WLAN with mDNS mode set to drop.
C. Configure a policy profile that uses an external only ACL and guest VLAN.
D. Implement a policy profile with p2p blocking enabled and a guest VLAN.
E. Deploy a WLAN policy that points wireless users to a webauth parameter map.
Answer: (SHOW ANSWER)
To implement a guest Wi-Fi network on a Cisco 9800 WLC with the requirements mentioned, the solution must ensure that guests are isolated from the corporate LAN and are redirected to a login page before being able to access the internet. Additionally, access needs to be restricted to web browsing only, with no need for preshared keys or certificates.
Option A: "Create a WLAN that uses a web policy and points to a consent parameter map." This is necessary to enforce the login page and redirect users to a webauth page. By creating a WLAN with web policy, you ensure that users are redirected to a captive portal where they can accept the terms and conditions or login to the network. This solution also helps in segregating the guest network from the corporate network, as users are contained within their VLAN.
Option E: "Deploy a WLAN policy that points wireless users to a webauth parameter map." Web authentication (webauth) is an essential part of guest access. Deploying a WLAN policy with webauth ensures that users are directed to the login page (a webauth parameter map), allowing them to authenticate before browsing the internet.

NEW QUESTION: 51
A network administrator at a marketing company manages a Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE 17.x. The WLAN named XYZ-Guest is set up for visitors, and the administrator wants to implement a web authentication (WebAuth) portal using an external server to manage guest access. To ensure seamless and secure guest authentication, the controller must be configured to use an external WebAuth server for the WLAN. The administrator must configure the XYZ-Guest WLAN to use an external WebAuth server with a parameter map named webauth-ext.
Which set of Cisco IOS XE commands must be used?
A. wireless wlan XYZ-Guest
security web-auth external webauth-ext
B. wireless wlan XYZ-Guest 2 XYZ-Guest
parameter-map webauth-ext
C. wlan XYZ-Guest 2
parameter external security-map webauth-ext
D. wlan XYZ-Guest 2 XYZ-Guest
security web-auth parameter-map webauth-ext
Answer: (SHOW ANSWER)
On a Cisco Catalyst 9800 WLC, the WLAN is entered with the wlan command, and the WebAuth parameter map is applied under the WLAN using the security web-auth parameter-map command so the guest WLAN uses the configured external WebAuth portal settings.

Valid 350-101 Dumps shared by EduDump.com for Helping Passing 350-101 Exam! EduDump.com now offer the **newest 350-101 exam dumps**, the EduDump.com 350-101 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com 350-101 dumps with Test Engine here: https://www.edudump.com/exams/Cisco/350-101/premium/ (**127** Q&As Dumps, **35%OFF Special Discount Code: freecram**)