Get Free Cisco 350-101 Dumps PDF Questions

Why risk failure? Download updated Cisco Implementing and Operating Cisco Wireless Core Technologies exam PDF questions today. Practice with real 350-101 dumps and verified answers designed to help you ace your certification quickly using PrepBolt 350-101 exam pdf questions and answers.

Thank you for Downloading 350-101 exam PDF Demo

https://prepbolt.com/350-101.html

Question 1

Question Type: MultipleChoice

A wireless engineer must manage scheduled maintenance for a guest WLAN that uses Cisco Catalyst Center as the primary monitoring solution. The engineer must coordinate downtime and verify that all services resume as intended after planned tasks are complete. The network

How does viewing trend deviation in Cisco Catalyst Center AI Analytics benefit wireless operation?

Options:

A- It maintains server time synchronization
B- It exports event thresholds to external dashboards
C- It allows earlier notice of abnormal wireless behavior
D- It backs up existing log files to remote hosts

Answer:

C

Explanation:

Cisco Catalyst Center AI Analytics provides predictive and proactive insights into wireless network behavior. Viewing trend deviation allows network administrators to identify abnormal patterns or shifts in network performance compared to historical baselines. This capability enables earlier detection of potential issues such as unusual client disconnections, spikes in interference, or unexpected throughput degradation. By monitoring deviations, administrators can proactively troubleshoot and resolve problems before they impact user experience. Option A, server time synchronization, is unrelated to trend analysis. Option B, exporting event thresholds, is a reporting function, not a predictive monitoring feature. Option D, backing up logs, pertains to data retention but does not provide operational insight. Trend deviation analytics leverage historical and current performance metrics to generate alerts when behaviors fall outside normal parameters, enhancing operational awareness and enabling faster remediation. Cisco Wireless Core Technologies emphasize using AI-driven analytics for continuous monitoring, anomaly detection, and trend-based alerts, which improves network reliability and reduces downtime in large-scale enterprise deployments. Reference topics: Wireless Monitoring and Management --- Catalyst Center AI Analytics, trend deviation, anomaly detection, proactive wireless monitoring.

Question 2

Question Type: MultipleChoice

What defines RSSI in radio signal measurements?

Options:

A- Detected amplitude level at radio receiver
B- Noise generated by interference
C- QoS network packet marking method
D- Wireless radio signal service ID

Answer:

A

Explanation:

RSSI, or Received Signal Strength Indicator, is a measure of the detected power level of a radio signal at the receiver, expressed in dBm. It reflects the strength of the wireless signal received by the client or access point and is a critical metric for assessing coverage, link quality, and roaming decisions. Higher RSSI values (closer to 0 dBm) indicate stronger signals, while lower values (more negative) represent weaker signals. RSSI is used by Cisco wireless controllers and clients to make roaming decisions, select access points, and optimize transmit power levels. Option B, noise generated by interference, affects signal-to-noise ratio but does not define RSSI. Option C, QoS packet marking, pertains to network traffic prioritization, not RF measurements. Option D, wireless radio service ID, refers to identifying services on a network and is unrelated to signal strength measurement. Understanding RSSI is fundamental in RF planning, AP placement, and troubleshooting wireless coverage issues. Cisco Wireless Core Technologies emphasize monitoring RSSI to maintain adequate signal levels across the deployment, ensuring seamless connectivity and performance in high-density or challenging RF environments. Reference topics: RF Fundamentals --- RSSI, signal strength, link quality, roaming, RF planning.

Question 3

Question Type: MultipleChoice

Which CleanAir feature is used to avoid channels with interference from devices such as outdoor bridges and microwave ovens?

Options:

A- Persistent Device Avoidance
B- Spectrum Analysis
C- Air Quality Index
D- Channel Utilization

Answer:

A

Explanation:

Cisco CleanAir technology is designed to detect, classify, and mitigate RF interference in enterprise wireless networks. Persistent Device Avoidance is a CleanAir feature that identifies non-Wi-Fi sources of interference, such as microwave ovens, outdoor bridges, or other RF devices, and then instructs the wireless LAN controller (WLC) to avoid channels affected by these interferers. By doing so, APs can select cleaner channels, reducing packet loss, improving throughput, and maintaining optimal coverage. Spectrum Analysis (Option B) provides visibility into the RF environment and interference sources but does not automatically avoid channels. Air Quality Index (Option C) gives a real-time assessment of RF quality per channel but is a monitoring metric, not an avoidance mechanism. Channel Utilization (Option D) reports on the percentage of channel occupancy by Wi-Fi traffic, assisting in load balancing, but does not prevent interference from external sources. Persistent Device Avoidance ensures proactive channel selection in environments with consistent interference, enhancing overall network reliability and performance. This capability is critical in high-density or mixed-use environments, where interference from non-Wi-Fi devices can degrade client experience. Reference topics: Wireless Network Operation --- Cisco CleanAir, Persistent Device Avoidance, RF interference mitigation, channel optimization.

Question 4

Question Type: MultipleChoice

Which feature enables fast secure roaming in a wireless network?

Options:

A- DCA
B- 802.11r
C- 802.11ax
D- MIMO

Answer:

B

Explanation:

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. Reference topics: Client Connectivity Configuration --- 802.11r, Fast BSS Transition, secure fast roaming, mobility domains, PMK caching.

Question 5

Question Type: MultipleChoice

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

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

A

Explanation:

For configuring guest access on a Cisco Catalyst 9800 WLC using an external WebAuth server, the WLAN must be explicitly associated with the external server through a parameter map. The correct command syntax in Cisco IOS XE is wireless wlan <wlan-name> followed by security web-auth external . This configuration links the WLAN to the external WebAuth server defined in the parameter map, allowing guests to be redirected to the portal for authentication. The parameter map (webauth-ext) contains details such as server IP, port, and other authentication parameters required for the external WebAuth interaction. Option B is incorrect because it improperly uses multiple WLAN names in one command, which is not valid syntax. Option C uses parameter external security-map, which is invalid and does not associate the WLAN correctly with the WebAuth server. Option D incorrectly combines the security and parameter-map syntax and is not supported in IOS XE for external WebAuth. Cisco Wireless Core Technologies recommends this approach for centralized guest management, allowing consistent enforcement of guest policies, seamless authentication, and integration with external WebAuth servers across multiple WLANs and APs. Reference topics: Client Connectivity Configuration --- WebAuth, external guest portal, WLAN parameter map configuration, Cisco IOS XE 17.x.

Question 6

Question Type: MultipleChoice

What is a characteristic of gain in wireless antenna design?

Options:

A- Scale used for calculating system loss

B- Checksum figure appended to signal blocks
C- Amount of increased energy sent toward a specific direction
D- Standard temperature tolerance during wireless operation

Answer:

C

Explanation:

In wireless antenna design, gain refers to the measure of an antenna's ability to focus energy in a particular direction compared to a reference antenna, usually an isotropic radiator. Gain does not generate additional power; instead, it redistributes radiated energy to increase signal strength in the intended direction, enhancing the effective range and performance of the wireless link. This directional amplification is crucial in both point-to-point and point-to-multipoint deployments, as higher gain antennas can concentrate RF energy to overcome path loss and improve received signal strength at the target. Option A describes system loss calculation, which relates to link budgets, not antenna gain. Option B is unrelated, as checksum figures are part of digital error detection in wireless frames. Option D pertains to environmental tolerance, not RF signal characteristics. In Cisco Wireless Core Technologies, antenna gain is considered during RF planning, coverage modeling, and site surveys to ensure optimal signal distribution, proper overlap, and minimal interference, particularly for high-density deployments. Using high-gain directional antennas in corridors or long hallways, for instance, improves coverage and throughput while minimizing interference outside the target area. Reference topics: RF Fundamentals --- Antenna gain, directional radiation patterns, link budget, site survey planning.

Question 7

Question Type: MultipleChoice

Which condition is required for a line-of-sight RF connection?

Options:

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:

D

Explanation:

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. While multipath propagation (Option A) and MIMO (Option B) techniques enhance throughput and reliability in non-line-of-sight environments, they do not satisfy the definition of LOS. Reflections (Option C) actually introduce delays, fading, and interference, which can degrade signal quality. In Cisco Wireless Core Technologies, understanding LOS is foundational for designing point-to-point wireless backhaul links, outdoor Wi-Fi deployments, and high-performance campus networks. Ensuring LOS minimizes path loss, maximizes received signal strength, and supports predictable coverage patterns. Proper site surveys, RF planning, and AP placement are used to maintain LOS where required, particularly for directional antennas or high-gain links. Reference topics: RF Fundamentals --- Line-of-Sight (LOS), RF propagation, path loss, multipath effects, MIMO considerations.

Question 8

Question Type: MultipleChoice

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?

Options:

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:

C

Explanation:

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. Option A is unsuitable because WPA2-Enterprise and dynamic VLAN assignment are designed for employee or secure networks, not open guest access. Option B provides local web-auth, which is limited to a single WLC and does not scale across multiple floors effectively. Option D (MAC filtering) only enforces device-level access but does not provide web-based login or segmentation, failing the requirement for captive portal and internet-only access. Cisco Wireless Core Technologies recommend central web authentication with ACL enforcement for guest networks to provide consistent coverage, network isolation, and compliance with security policies across multiple APs and WLCs. Reference topics: Client Connectivity Configuration --- Guest WLAN deployment, central web-auth, ACL enforcement, segmentation from corporate WLAN.

Thank You for trying 350-101 PDF Demo

To try our 350-101 practice exam software visit link below

https://prepbolt.com/350-101.html

Start Your 350-101 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your 350-101 preparation with actual exam questions.