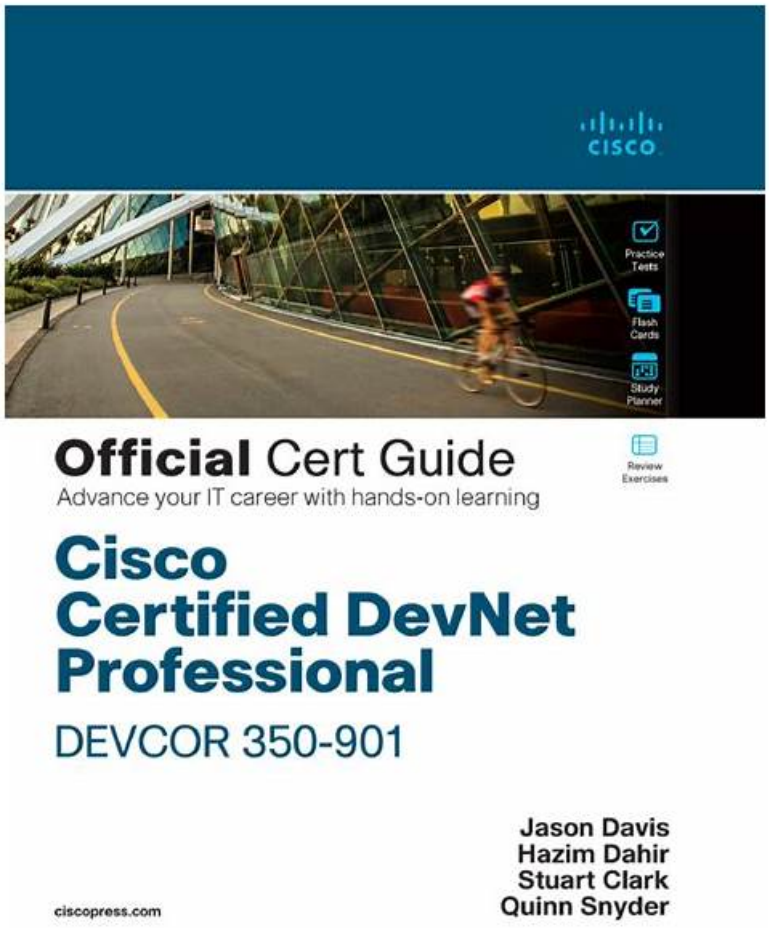
Fast Download 350-101 Test Discount–The Best Latest Learning Materials for 350-101 - Reliable 350-101 Instant Access



We will provide you with three different versions of our 350-101 exam questions on our test platform. You have the opportunity to download the three different versions from our test platform. The three different versions of our 350-101 Test Torrent include the PDF version, the software version and the online version. The three different versions will offer you same questions and answers, but they have different functions.

To help customers pass the Cisco 350-101 exam successfully. PassTorrent with 365 days updates. Valid 350-101 350-101 exam dumps, exam cram and exam dumps demo. You can download these at a preferential price. We continually improve the versions of our 350-101 Exam Guide so as to make them suit all learners with different learning levels and conditions.

>> 350-101 Test Discount <<

Free Cisco 350-101 Exam Questions Updates and Demos

If you are interested in purchasing valid and professional test prep materials, our 350-101 exam questions will be our wise choice. To know our questions details and format we provide free PDF demo of our 350-101 exam questions for your reference before purchasing. You will have a better understanding for your products. You will find our 350-101 Exam Guide torrent is accurate and helpful and then you will purchase our 350-101 training braindump happily. We provide free demo of 350-101 study guide download before purchasing.

Cisco 350-101 Exam Syllabus Topics:

Topic	Details
Topic 1	• Automation and AI: Covers Python scripting basics, NETCONF • YANG, wireless API interpretation, and AI-driven analytics, operations, and radio resource management within Catalyst Center.
Topic 2	• RF Fundamentals: Covers the behavior of radio waves, how RF signals are measured and interpreted, the mathematics behind RF calculations, and the characteristics of Wi-Fi antennas.
Topic 3	• Client Connectivity Configuration: Covers configuring authentication both on and off the controller, setting up client connectivity across different operating systems, roaming behavior, and wireless guest network configuration.
Topic 4	• Wireless Network Operation: Covers initial configuration of Cisco wireless infrastructure, AP discovery and join processes, AP modes, WLAN setup, and client management policies across platforms like Catalyst Center, ISE, and Spaces.
Topic 5	• 802.11 Technology Fundamentals: Covers Wi-Fi governance bodies, regional channel and power regulations, and the core technical principles of 802.11 including modulation, channel width, MIMO, topologies, and frame types.
Topic 6	• Wireless Monitoring and Management: Covers network maintenance tasks, client monitoring configuration, troubleshooting client connectivity issues, and integrating with external devices and platforms.

Cisco Implementing and Operating Cisco Wireless Core Technologies Sample Questions (Q32-Q37):

NEW QUESTION # 32
A retail store is setting up guest Wi-Fi on a Cisco 9800 WLC. The IT team has these requirements:
When a guests associates, they 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. Central web authentication on the guest WLAN and apply an ACL that denies traffic between devices that use the internal subnets.
- C. MAC filtering on the guest WLAN and enable client exclusion for segregation.
- D. Local web authentication on the guest SSID and apply ACLs to allow all traffic except FTP and SSH from the guest WLAN.

Answer: B

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.

NEW QUESTION # 33
Which wireless connection occurs when there are no physical obstacles between the receiver and transmitter?

- A. attenuation
- B. beamforming
- C. line-of-sight
- D. reflection

Answer: C

Explanation:
The correct answer isline-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.Attenuationis signal loss as RF energy travels through free space, cables, walls, or other materials.Reflectionoccurs when RF energy bounces off a surface such as metal, glass, or concrete, often contributing to multipath.Beamformingis 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.
Reference topic:RF Fundamentals - RF propagation, path loss, line-of-sight, obstruction effects, and wireless link planning.

NEW QUESTION # 34
What is a benefit of network adaptability in terms of improved operational outcomes when using AI-RRM in Cisco Catalyst Center?

- A. provisioning of static device addresses
- B. categorization of users by authentication type
- C. reduction of co-channel interference
- D. transmission of regular software update schedules

Answer: C

Explanation:
The correct answer isreduction of co-channel interference. AI-RRM in Cisco Catalyst Center is designed for RF optimization, not IP addressing, software scheduling, or user identity classification. Cisco describes AI- enhanced RRM as applying artificial intelligence and machine learning to optimize RF environments and automate/adapt RF parameter tuning for Cisco wireless networks. This is directly tied to operational RF outcomes such as improved channel planning, transmit power behavior, channel width decisions, and better spectrum utilization.
Co-channel interference occurs when multiple AP radios operate on the same channel within hearing range, forcing devices to share airtime and increasing contention. AI-RRM uses telemetry, analytics, and learned RF behavior to recommend or apply more optimal RF configurations. Cisco specifically states that AI-enhanced RRM optimization can produce improvements such as up to a40 percent reduction in co-channel interferenceand SNR gains for wireless clients. Cisco's AI-RRM deployment guidance also identifies AP radio distribution and utilization analysis as critical for minimizing co-channel interference and optimizing wireless performance. Therefore, option B is the only operational outcome aligned with AI-RRM's purpose. Reference topic:
Automation and AI - Cisco Catalyst Center AI-RRM, RF analytics, RRM automation, channel optimization, and wireless AIOps.

NEW QUESTION # 35

Refer to the exhibit. A wireless controller is deployed at a branch location to facilitate secure client connectivity. A network engineer configures a WLAN using 802.1X to align with company security policies.
Which configuration enables client authentication for this WLAN?

- A. wlan branch1 policy branch1_policy
- B. security dot1x authentication-list ISE_GROUP
- C. aaa override enable
- D. no ip mac-binding

Answer: B

Explanation:
The command that enables 802.1X client authentication for this WLAN issecurity dot1x authentication-list ISE_GROUP. On a Cisco Catalyst 9800 WLC, the WLAN configuration defines Layer 2 security behavior, including whether the SSID uses 802.1X and which AAA method list is used for EAP/RADIUS authentication. Cisco documents the CLI workflow for 802.1X WLAN authentication as entering WLAN configuration mode and applyingsecurity dot1x authentication-list < authenticate-list-name > , explicitly describing this as the step to enable the authentication list for 802.1X security. Cisco's Catalyst 9800 configuration example also shows the exact formsecurity dot1x authentication-list ISE_GROUPand states that the WLAN is then configured with 802.1X authentication.
no ip mac-bindingdisables IP-to-MAC binding checks and does not select a RADIUS method list.aaa override enableallows authorization attributes from AAA/ISE to be applied after authentication, but it does not initiate 802.1X authentication.wlan branch1 policy branch1_policymaps the WLAN to a policy profile through a policy tag, but it is not the authentication command. Reference topics:802.1X WLAN security, RADIUS AAA method lists, Catalyst 9800 WLAN configuration, and secure client onboarding.

NEW QUESTION # 36
A wireless engineer is rolling out a group of new Meraki APs across multiple office floors. The APs must be centrally managed through the Meraki dashboard and be set up for automatic cloud registration. Network connectivity has been established, and the company firewall follows standard security policies. To minimize manual configuration for each AP the engineer must configure them to automatically discover the dashboard.

Which action must the engineer take?

- A. Set up a site-to-site VPN between the switch on each floor and the data center.
- B. Connect APs to a network with internet and allow outbound access to Meraki cloud.
- C. Assign a static management IP to each AP using the local status page.
- D. Register the AP serial numbers in the lease table of the DHCP server.

Answer: B

Explanation:
Meraki AP onboarding is designed around cloud-initiated registration, not manual controller discovery. A Meraki AP must obtain network reachability, resolve Meraki cloud services, and establish outbound connectivity to the Meraki dashboard. Cisco Meraki documentation states that the dashboard provides centralized management and that, for dashboard management, a Meraki device must communicate with the Cisco Meraki cloud over a secure tunnel. The MR quick-start process further describes that, after power-on, the AP requests an IP address by DHCP, reaches the Meraki cloud through the Internet, and checks in to the dashboard.
Therefore, the required action is to connect the APs to a network with Internet access and permit the necessary outbound firewall flows to Meraki cloud services. A site-to-site VPN is unnecessary for dashboard discovery. Static management addressing may be used in constrained environments, but it increases manual work and is not required for automatic registration. DHCP lease-table serial registration is not a Meraki onboarding mechanism. Reference topics:Wireless Network Implementation - Meraki AP cloud onboarding, DHCP/DNS reachability, outbound firewall policy, and dashboard-based AP lifecycle management.

NEW QUESTION # 37
.....

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes