Cisco.300-110.v2026-09-22.q45

Exam Code:	300-110
Exam Name:	Designing Cisco Wireless Networks
Certification Provider:	Cisco
Free Question Number:	45
Version:	v2026-09-22
# of views:	120
# of Questions views:	450
https://www.freepdfdumps.com/Cisco.300-110.v2026-09-22.q45.html	

NEW QUESTION: 1
A wireless network consists of two IOS XE controllers installed in a data center, 9100 series APs, and a corporate and a guest WLAN. The customer must have a high availability pair of two Cisco WLCs for the client SSO. Which two design approaches must the engineer take to meet the requirement? (Choose two.)
A. The controllers must have the same number of licenses.
B. Each WLC must have a unique redundancy management IP address.
C. Both WLCs must have the same redundancy management IP address.
D. The controllers must run the same operating system version.
E. Both WLCs must have the same service port IP address.
Answer: B,D (LEAVE A REPLY)
Configuring a high availability SSO pair on Cisco Catalyst 9800 IOS XE WLCs has specific technical prerequisites that must be satisfied for the SSO relationship to form and function correctly. The two critical requirements are: each WLC must have a unique Redundancy Management Interface (RMI) IP address (Option B), and both WLCs must run identical IOS XE software versions (Option D). The Redundancy Management Interface is the dedicated in-band control channel over which the active and standby WLCs exchange state synchronization information, keepalive messages, and configuration updates. Each controller requires its own unique RMI IP address within the same subnet - the active uses one address and the standby uses another. If they shared the same RMI IP (Option C), there would be an IP address conflict preventing the interface from functioning. Identical software versions (Option D) are mandatory because the SSO state synchronization protocol and data structures must be version-compatible between the active and standby controllers. Any mismatch in IOS XE version will prevent SSO formation. License count (Option A) does not need to be identical for SSO. Service port IP addresses (Option E) must be unique per controller, not identical.
Reference: WLSD Study Guide - Catalyst 9800 SSO Prerequisites, Redundancy Management Interface Configuration, High Availability Pair Formation Requirements.

NEW QUESTION: 2
A customer has two Cisco Catalyst 9800 Series WLCs named WLC-A and WLC-B in an N+1 configuration with the same WLANs but different Layer 3 interfaces for each WLC, and APs in local mode. WLC-A manages Building A APs and WLC-B manages Building B APs. The customer wants users to remain connected and retain their session state including the IP address when moving between buildings. How must this requirement be incorporated into the design?
A. Create a mobility tunnel between WLC-A and WLC-B with the same group name.
B. Configure WLC-A and WLC-B in a high-availability cluster and set a mobility MAC address.
C. Implement AP groups for each building by using the same name on WLC-A and WLC-B.
D. Connect WLC-A and WLC-B by using the redundancy port to sync client sessions.
Answer: A (LEAVE A REPLY)

The requirement for users to retain their session state and IP address when roaming between buildings managed by different WLCs is a Layer 3 roaming scenario. In Cisco ' s wireless architecture, IP address preservation across controller boundaries is achieved through inter-controller mobility - specifically the foreign-anchor mobility tunnel mechanism. When a client roams from Building A (WLC-A) to Building B (WLC-B), WLC-B becomes the foreign controller and WLC-A becomes the anchor controller. WLC-B tunnels the client ' s traffic back to WLC-A, allowing the client to retain its original IP address even while physically associated to an AP managed by WLC-B. This requires a mobility tunnel between WLC-A and WLC-B with both controllers configured in the same mobility group name - the group name is the trust identifier that permits the mobility tunnel and anchor-foreign relationship to form. Without the same group name, the controllers will not form a trusted mobility peer relationship. AP groups (Option C) control SSID and VLAN assignments per AP cluster but have no impact on inter-controller roaming. HA cluster configuration (Option B) creates SSO redundancy, not roaming capability between separate N+1 controllers.
Redundancy port connection (Option D) is used for SSO keepalive and state sync, not mobility tunneling.
Reference: WLSD Study Guide - Inter-Controller Mobility, Mobility Tunnels, Layer 3 Roaming and IP Address Preservation.

NEW QUESTION: 3
A customer wants a network engineer to design a Cisco wireless solution that will have redundancy through SSO and LAG. APs in the executive office must reassociate to the WLC as soon as possible in the event of a failure. The WLCs are located in a remote data center. The head office uses a WAN for connectivity with the data center. Which priority must be incorporated in the design to be assigned to the executive APs?
A. high
B. medium
C. low
D. critical
Answer: (SHOW ANSWER)
Cisco WLC AP Failover Priority governs the order in which APs are processed when a WLC recovers and APs begin re-associating. The priority levels are: Critical, High, Medium, and Low. During recovery situations, the WLC will accept and process AP join requests in order of priority - Critical priority APs are processed first, before all other priority levels. In a deployment where the WLC is located in a remote data center connected via WAN, the join process for all APs is slower due to WAN latency and potential bandwidth constraints. Under these conditions, assigning Critical priority to executive office APs ensures they are at the front of the processing queue and restore service before lower-priority APs. The executive office designation implies business-critical operations requiring the fastest possible wireless restoration - a requirement that directly maps to the Critical priority level. High priority (Option A) would position the executive APs second in the queue behind any Critical priority APs. Medium (Option B) and Low (Option C) would place them further down the processing order. Reference: WLSD Study Guide - AP Failover Priority Configuration, N+1 and SSO Redundancy Design, WAN-Linked Controller Deployments.

NEW QUESTION: 4
During a post-deployment site survey, issues are found with non-Wi-Fi interference. What should the engineer use to identify the source of the interference?
A. Wireless intrusion prevention
B. Cisco spectrum expert
C. Network analysis module
D. Wireshark
Answer: B (LEAVE A REPLY)
Cisco Spectrum Expert is a dedicated spectrum analysis tool designed to identify and analyze non-Wi-Fi interference sources at Layer 1. During a post-deployment site survey, it can detect interference from various devices such as cordless phones, Bluetooth devices, microwave ovens, video cameras, and other unlicensed RF emitters. The tool provides a visual representation of the RF environment across the frequency spectrum, allowing engineers to pinpoint the exact source of interference and characterize it by duty cycle, frequency, and interference pattern. A network analysis module (Option A) operates at Layer 2 and above, unable to detect non-802.11 RF emissions. Wireless intrusion prevention (Option B) detects rogue APs and 802.11 attacks but not Layer 1 RF noise. Wireshark (Option C) is a packet capture tool for Layer 2-7 analysis and cannot detect non-Wi-Fi RF energy. Reference: WLSD Study Guide - Layer 1 Spectrum Analysis, Post- Deployment Survey, Non-Wi-Fi Interference Identification.

NEW QUESTION: 5
During a post-deployment site survey, issues are found with non-Wi-Fi interference. What should the engineer use to identify the source of the interference?
A. Network analysis module

B. Wireless intrusion prevention
C. Wireshark
D. Cisco spectrum expert
Answer: (SHOW ANSWER)
Cisco Spectrum Expert is a dedicated spectrum analysis tool designed to identify and analyze non-Wi-Fi interference sources at Layer 1. During a post-deployment site survey, it can detect interference from various devices such as cordless phones, Bluetooth devices, microwave ovens, video cameras, and other unlicensed RF emitters. The tool provides a visual representation of the RF environment across the frequency spectrum, allowing engineers to pinpoint the exact source of interference and characterize it by duty cycle, frequency, and interference pattern. A network analysis module (Option A) operates at Layer 2 and above, unable to detect non-802.11 RF emissions. Wireless intrusion prevention (Option B) detects rogue APs and 802.11 attacks but not Layer 1 RF noise. Wireshark (Option C) is a packet capture tool for Layer 2-7 analysis and cannot detect non-Wi-Fi RF energy. Reference: WLSD Study Guide - Layer 1 Spectrum Analysis, Post- Deployment Survey, Non-Wi-Fi Interference Identification.

NEW QUESTION: 6
A consultant must design a WLAN for a large campus with high AP density, 50-100 clients per cell, 5 Mbps throughput per client minimum, 5 GHz and 2.4 GHz coverage at -67 dBm, and no 802.11b clients. Which two WLAN design approaches meet the requirements? (Choose two.)
A. Set the minimum mandatory data rates to 12-18 Mbps.
B. Configure up to six SSIDs on any AP.
C. Enable 802.11b data rates.
D. Reduce the 2.4 GHz coverage with FRA.
E. Set the 5 GHz channel widths to 80-160 MHz.
Answer: (SHOW ANSWER)
Designing for 50-100 clients per cell with 5 Mbps minimum throughput and no 802.11b clients requires two critical optimizations. First, setting minimum mandatory data rates to 12-18 Mbps (Option A) removes legacy lower data rates from the AP ' s supported rate set. When 1, 2, 5.5, and 11 Mbps rates are disabled and 12 Mbps becomes the minimum mandatory rate, legacy 802.11b clients are excluded from the cell, airtime efficiency improves dramatically, and clients connecting at higher rates use less channel time per frame, increasing effective capacity. Second, Flexible Radio Assignment (FRA) for 2.4 GHz reduction (Option D) is critical in high-density environments. FRA allows the WLC to dynamically reassign some 2.4 GHz radios to 5 GHz operation or monitor mode, reducing 2.4 GHz cell size and interference while increasing 5 GHz capacity in the high-density area. Option C directly contradicts the no-802.11b requirement. Option B (6 SSIDs per AP) is a management consideration but does not directly address throughput. Option E (80-160 MHz channels) would consume available spectrum, reducing the number of usable non-overlapping channels and worsening co-channel interference at high density. Reference: WLSD Study Guide - High-Density WLAN Design, Minimum Data Rate Configuration, Flexible Radio Assignment (FRA).

NEW QUESTION: 7
An engineer is designing a wireless network in a historic building that has large rooms and ornate wall coverings. Which approach must be considered first when placing access points?
A. aesthetics
B. RF coverage
C. cell overlap
D. RF interference
Answer: B (LEAVE A REPLY)
When designing a wireless network for any environment, including a historic building with ornate wall coverings and aesthetic constraints, RF coverage must always be considered first when placing access points. RF coverage is the fundamental requirement - without adequate signal strength throughout the space, no other design objective can be met. The engineer must first determine AP locations that provide the required signal strength and coverage to all areas before addressing aesthetics, overlap calculations, or interference mitigation. In a historic building specifically, the ornate wall coverings and dense construction materials may cause unexpected signal attenuation, making it even more important to model RF coverage before committing to AP positions. Once RF coverage requirements are established, aesthetic concerns (Option A) can guide the choice of AP form factor, enclosures, or cabling routes. Cell overlap (Option C) is derived from coverage calculations. RF interference (Option D) analysis follows after RF coverage baseline is established.
Reference: WLSD Study Guide - Site Survey Methodology, AP Placement Priority, Special Environment Wireless Design.

NEW QUESTION: 8
An engineer must perform a predictive design for a wireless network. The customer has devices that can tolerate at most 100 ms of delay when roaming. Which design criteria must be used?
A. location
B. data
C. video
D. voice
Answer: D (LEAVE A REPLY)
Devices that can tolerate at most 100 ms of delay when roaming are voice devices. The 100 ms maximum roaming delay threshold is the Cisco-specified design criterion for VoWLAN implementations - it defines the maximum time a handset can tolerate being disconnected from the wireless network during a roam event before the voice call is degraded or dropped. This threshold drives specific design requirements: 15-20% cell overlap at -67 dBm, fast roaming mechanisms (802.11r, CCKM, or OKC), and AP placement along user movement paths. Location services (Option A) have flexible latency requirements. Data applications (Option B) can tolerate much higher latency - typically several hundred milliseconds. Video (Option C) streaming has buffering mechanisms that allow for higher latency tolerance than real-time voice. Only voice applications have the strict 100 ms roaming delay requirement that directly influences the predictive design criteria. Reference: WLSD Study Guide - VoWLAN Roaming Design, Roaming Delay Requirements, Predictive Survey Criteria.

NEW QUESTION: 9
An engineer is conducting a Layer 2 site survey. Which type of client must the engineer match to the survey?
A. best client available
B. phone client
C. normal client
D. worst client available
Answer: D (LEAVE A REPLY)
When conducting a Layer 2 site survey, it is recommended to match the survey to the worst client available.
This ensures that the wireless network is designed to provide adequate coverage and performance even for clients with the poorest RF capabilities, thereby providing a consistent user experience for all devices. The worst client typically has fewer antennas, lower receiver sensitivity, and less sophisticated chipsets. By designing to its limitations, the engineer guarantees that every device in the environment meets the minimum performance threshold. Using the best client (Option A) or an average client (Option C) would result in coverage gaps for less capable devices. A phone client (Option B) may have unique characteristics but is not a universally applicable standard for general survey purposes. Reference: WLSD Study Guide - Site Survey Methodology, Client Selection for Survey, Layer 2 Pre-Deployment Survey.

NEW QUESTION: 10
A university has three campus locations and the main data center. Each campus location has a Cisco Catalyst
9800-40 WLC that manages 600 APs. The data center has a Catalyst 9800-40 WLC, which serves as N+1 backup for each campus WLC. A consulting engineer must install four additional Catalyst 9800-40 WLCs to serve as high availability SSO pairs for each campus, but only two have been approved due to budget restrictions. Requirements: Data center WLC must always be available as N+1 backup, Campus1 WLC must operate with zero downtime, and in the event of multiple campus outages, the AP priority order is to support Campus3, Campus2, then Campus1. Which design approach must the consulting engineer take?
A. The data center WLC and Campus3 WLC are the high availability SSO pair. Campus1 APs have priority 4, Campus2 APs have priority 2, and Campus3 APs have priority 1.
B. The data center WLC and Campus1 WLC are the high availability SSO pair. Campus1 APs have priority 4, Campus2 APs have priority 2, and Campus3 APs have priority 1.
C. The data center WLC and Campus1 WLC are the high availability SSO pair. Campus3 APs have priority 4, Campus2 APs have priority 2, and Campus1 APs have priority 1.
D. The data center WLC and Campus3 WLC are the high availability SSO pair. Campus3 APs have priority 4, Campus2 APs have priority 2, and Campus1 APs have priority 1.
Answer: C (LEAVE A REPLY)
This design scenario requires careful interpretation of the SSO pair function and AP priority semantics. The SSO requirement for Campus1 zero downtime means Campus1 ' s WLC must be paired in an SSO relationship - SSO provides hitless failover with no AP disassociation and no client reauthentication. The data center WLC, which must always remain available as N+1 backup for all campuses, is the logical SSO partner for Campus1 WLC. The SSO pair presents as a single logical entity, ensuring the data center WLC remains active and capable of serving as N+1 backup while simultaneously providing SSO for Campus1.

The AP priority for the N+1 backup scenario defines the recovery order when the backup controller must simultaneously handle APs from multiple campuses. In Cisco WLC AP failover priority, priority 1 is Critical (highest). The stated recovery order - Campus3 first, Campus2 second, Campus1 last - maps to: Campus3 APs assigned priority 4 (Cisco ' s highest numeric value in the 4-tier system, equating to the highest service recovery priority in this context), Campus2 APs priority 2, and Campus1 APs priority 1 (lowest, recovered last). Option C correctly pairs the data center WLC with Campus1 WLC for SSO and assigns AP priorities in the correct descending recovery order. Reference: WLSD Study Guide - SSO High Availability, N+1 Redundancy, AP Failover Priority Design.

NEW QUESTION: 11
An engineer is performing a Layer 1 passive wireless site survey utilizing a channel analyzer software in the
2.4 GHz spectrum. Which chart indicates the ratio of interference present during the duration of the capture?
A. Option A
B. Option B
C. Option C
D. Option D
Answer: C (LEAVE A REPLY)
In a Layer 1 passive wireless site survey using a channel analyzer tool (such as Metageek Chanalyzer or Cisco Spectrum Expert) in the 2.4 GHz spectrum, the chart that indicates the ratio of interference present during the capture duration is the Duty Cycle chart. The duty cycle chart displays the percentage of time that detected energy - including both Wi-Fi and non-Wi-Fi signals - is present on each channel. A high duty cycle on a channel indicates that the channel is occupied by transmissions for a significant portion of time, reducing available airtime for Wi-Fi clients. This chart directly communicates the ratio of interference because it shows what fraction of the observation period had detectable RF energy above the noise floor. Signal strength charts show amplitude (how strong), while duty cycle charts show temporal occupancy (how often) - the latter is the correct metric for quantifying interference ratio. Reference: WLSD Study Guide - Layer 1 Spectrum Analysis, Duty Cycle Chart Interpretation, Spectrum Analyzer Methodology.

NEW QUESTION: 12
A customer has two Cisco wireless controllers named WLC-A and WLC-B. Each controller is in a different building on a campus. The WLCs have different Layer 3 interfaces and broadcast the same SSIDs from their respective APs. Users must remain connected to the same VLAN and maintain their IP addresses during roaming from the APs attached to WLC-A and WLC-B. Which action accomplishes the requirement?
A. Create a mobility group between the two WLCs to allow auto-anchoring.
B. Create an SSO cluster to ensure that client sessions sync between WLCs.
C. Enable 802.11r on each SSID on both WLCs to allow caching of the PMK.
D. Enable AP groups using the same name on both WLCs for each group.
Answer: A (LEAVE A REPLY)
The requirement for users to retain their VLAN assignment and IP address when roaming between buildings managed by different WLCs is a Layer 3 roaming scenario. In Cisco ' s wireless architecture, IP address preservation across controller boundaries is achieved through inter-controller mobility - specifically the foreign-anchor mobility tunnel mechanism. When a client roams from Building A (WLC-A) to Building B (WLC-B), WLC-B becomes the foreign controller and WLC-A becomes the anchor controller. WLC-B tunnels the client ' s traffic back to WLC-A, allowing the client to retain its original IP address even while physically associated to an AP managed by WLC-B. This requires creating a mobility group between WLC-A and WLC-B with both controllers configured with the same mobility group name - the group name is the trust identifier that permits the mobility tunnel and anchor-foreign relationship to form. An SSO cluster (Option B) creates redundancy between two WLCs operating as one logical entity, not inter-building roaming between independent controllers. 802.11r (Option C) accelerates re-association but does not preserve IP addresses across different Layer 3 subnets. AP groups (Option D) control SSID and VLAN assignments but do not enable inter-controller IP preservation. Reference: WLSD Study Guide - Inter-Controller Mobility, Layer 3 Roaming, IP Address Preservation.

NEW QUESTION: 13
A customer has a Cisco wireless network with two Cisco Catalyst 9800 Series WLCs in a high availability cluster, 50 Cisco 2800I APs, and all SSIDs and services are 5 GHz only. A security mandate requires that rogue APs be scanned and identified in 2.4 GHz and 5 GHz bands without impacting existing client connectivity. How must the wireless network be reconfigured to meet the requirement without purchasing additional APs?
A. Set the XOR radio role to Client Serving and the slot 1 radio to Sniffer mode on all the APs.
B. Set the XOR radio role to Monitor mode and the slot 1 radio to Client Serving on all the APs.

C. Set the XOR radio role to Client Serving and the slot 1 radio to Monitor mode on all the APs.
D. Set the XOR radio role to Sniffer mode and the slot 1 radio to Client Serving on all the APs.
Answer: (SHOW ANSWER)
The Cisco Aironet 2800 Series APs feature a dual-radio architecture with a dedicated 5 GHz radio (slot 1) and a Flexible Radio Assignment (XOR) radio (slot 0) that can operate in either 2.4 GHz or 5 GHz, or be assigned to monitor mode for scanning functions. Since all existing SSIDs and services are 5 GHz only, the slot 1 (dedicated 5 GHz) radio is responsible for all current client connectivity - it must remain in Client Serving mode to maintain uninterrupted 5 GHz WLAN service. The XOR radio (slot 0), currently either idle or operating as a secondary 5 GHz radio, can be repurposed without impacting client service. Setting the XOR radio to Monitor mode enables it to continuously scan all channels across both the 2.4 GHz and 5 GHz spectrum for rogue AP detection, using the embedded CleanAir and WIDS capabilities. In Monitor mode, the XOR radio operates full-time as a dedicated scanner, providing rogue detection coverage on 2.4 GHz (previously uncovered since all services were 5 GHz) and supplementary scanning on 5 GHz. This eliminates the need for additional dedicated monitor mode APs. Options A, C, and D either place the slot 1 radio in a non-client-serving role (disrupting existing connectivity) or use the inappropriate Sniffer mode instead of Monitor mode for rogue detection. Reference: WLSD Study Guide - Cisco 2800 XOR Radio Architecture, Monitor Mode for Rogue Detection, Flexible Radio Assignment, WIDS Design.

NEW QUESTION: 14
An engineer must configure the virtual IP address on multiple controllers in a mobility group. Which rule must the engineer follow to ensure proper roaming?
A. Ensure that the DNS entry is tied to the virtual IP address of the WLC.
B. Use a unique IP address for each WLC.
C. Ensure that the DNS Host Name field is defined.
D. Use the same IP address for each WLC.
Answer: D (LEAVE A REPLY)
In a Cisco wireless mobility group, all Wireless LAN Controllers (WLCs) must be configured with the same virtual IP address to ensure proper roaming. The virtual IP address is a Layer 3 construct used by wireless clients during the DHCP renewal process when roaming between subnets managed by different WLCs. All WLCs in the same mobility group use the same virtual IP (typically from the unused 1.1.1.0/24 or similar non- routable space) so that clients receive consistent DHCP server responses regardless of which controller they are associated with. If different virtual IP addresses were used (Option B), clients roaming between controllers would experience DHCP failures during inter-controller roaming because the DHCP server address seen by the client would change. Options A and C relate to DNS hostname configuration, which is useful for AP discovery but does not affect the roaming behavior of client devices. The virtual IP address consistency across all mobility group members is a fundamental requirement for seamless inter-controller roaming. Reference: WLSD Study Guide - Mobility Group Configuration, Virtual IP Address, Inter- Controller Roaming Requirements.

NEW QUESTION: 15
An engineer in a branch office that does not have a wired backhaul must ensure that local clients can be switched locally and authenticated centrally. In which mode must the AP be configured?
A. MAP
B. Flex+Bridge
C. RAP
D. Cisco FlexConnect
Answer: (SHOW ANSWER)
Flex+Bridge mode is a specialized AP operating mode that combines two distinct Cisco wireless capabilities:
FlexConnect (for local switching of client data traffic and central authentication via the WLC) and Bridge
/Mesh mode (enabling wireless backhaul when no wired Ethernet uplink is available). In a branch environment without wired backhaul, a standard FlexConnect AP (Option D) cannot operate because FlexConnect still requires an Ethernet connection for its control plane. Bridge mode alone provides mesh backhaul but does not support the local switching with central authentication model required here. MAP (Option A) is a Mesh Access Point role for wireless backhaul, and RAP (Option C) is a Root Access Point with a wired connection - neither meets the no-wired-backhaul requirement with local switching.
Flex+Bridge uniquely satisfies both requirements: the Flex component allows locally switched VLANs to be bridged directly to the access layer without traversing the WAN, while the Bridge component enables the AP to use a wireless mesh link for its backhaul uplink. Central authentication is maintained via the CAPWAP control tunnel over the mesh link. Reference: WLSD Study Guide - FlexConnect Design, Mesh Networking, Flex+Bridge Mode Configuration and Use Cases.

NEW QUESTION: 16
A wireless engineer must design a backhaul link. The engineer has a mesh access point that has a wired connection back to the infrastructure. What must be changed in the AP role before a change is made in the AP mode?
A. monitor
B. RAP
C. bridge
D. local
Answer: B (LEAVE A REPLY)
In Cisco mesh networking architecture, access points are classified into two primary roles: Root Access Points (RAP) and Mesh Access Points (MAP). A RAP is an access point that maintains a wired Ethernet backhaul connection back to the network infrastructure, while a MAP operates wirelessly, relying on mesh backlinks to upstream RAPs. When an engineer needs to change an AP mode - such as switching to bridge mode to extend the mesh - the AP role must first be defined correctly. The AP must be designated as a RAP before any mode-level configuration changes are applied. This sequencing is critical because the AP role defines the fundamental backhaul path; changing the mode without first establishing the role results in misconfiguration and potential connectivity loss. The RAP communicates directly with the wired infrastructure via its Ethernet port, making it the gateway for all downstream MAPs in the mesh topology. Options A (monitor), C (bridge), and D (local) refer to AP modes, not roles, and cannot be configured until the role is properly defined.
Reference: WLSD Study Guide - Mesh Networking Fundamentals, Outdoor Wireless Design, AP Role and Mode Configuration.

Valid 300-110 Dumps shared by Actual4test.com for Helping Passing 300-110 Exam! Actual4test.com now offer the **newest 300-110 exam dumps**, the Actual4test.com 300-110 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-110 dumps with Test Engine here: https://www.actual4test.com/300-110_examcollection.html (**125** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 17
A wireless consultant must design a Cisco WLAN. The consultant recommends a solution that requires 12 Cisco 9100 Series APs connected to a Cisco 3800 Series PoE+ switch. Each AP requires PoE+ for full functionality. What is the total PoE requirement in watts?
A. 360
B. 1080
C. 184.8
D. 720
Answer: A (LEAVE A REPLY)
This question requires a straightforward PoE power budget calculation. The IEEE 802.3at standard (PoE+) delivers a maximum of 30W at the Power Sourcing Equipment (PSE/switch port). Cisco 9100 Series access points such as the C9120, C9130, and C9136 are designed to operate with full functionality using PoE+ at
30W per AP. The total PoE power requirement for 12 APs is calculated as: 12 APs × 30W per AP = 360W.
This figure represents the total power draw that the Cisco 3800 Series PoE+ switch must be capable of supplying across the connected AP ports simultaneously. The Cisco Catalyst 3800 Series switches offer a total PoE power budget that must be validated against this 360W requirement during the design phase. Note that some Cisco 9100 APs support higher power modes through IEEE 802.3bt (PoE++), which can provide up to
90W - but the question specifies PoE+ (802.3at) for the switch infrastructure, making 30W × 12 = 360W the correct answer. Option D (720W) would correspond to 24 APs at 30W each. Option B (1080W) would represent 36 APs. Option C (184.8W) corresponds to a non-standard per-AP power value. Reference: WLSD Study Guide - PoE Power Budget Planning, Cisco 9100 Series AP Power Requirements, Wired Infrastructure Design for Wireless Deployments.

NEW QUESTION: 18

An engineer must assess an existing company WLAN to determine the possibility for future IEEE 802.11ac Wave 2 wireless deployment. All access switches are Fast Ethernet-capable only, and the wired infrastructure between existing APs and access switches is based on the CAT 6A standard. Which two actions provide maximum support of Cisco 3800 Series access points? (Choose two.)

A. Replace the existing switches with mGig switches.

B. Replace the existing switches with gigabit switches with 10G uplinks.

C. Ensure that cable distances between access switches and APs are not longer than 100 meters.

D. Replace the existing wiring infrastructure with the CAT-7E wiring standard.

E. Ensure that cable distances between access switches and APs are not longer than 55 meters.

Answer: A,B (LEAVE A REPLY)

Cisco 3800 Series APs support IEEE 802.11ac Wave 2, which can deliver throughput exceeding 1 Gbps. Fast Ethernet switches are limited to 100 Mbps per port, creating a severe bottleneck. The two actions that provide maximum support are replacing with mGig switches (Option A) and replacing with gigabit switches with 10G uplinks (Option B). mGig (Multi-Gigabit Ethernet) switches support 2.5G and 5G speeds over existing CAT

6A cabling, allowing the full throughput of 802.11ac Wave 2 APs to be utilized without replacing the existing cable plant. Gigabit switches with 10G uplinks ensure that the access layer can support 1 Gbps per AP port while providing sufficient uplink capacity. Since the existing cabling is already CAT 6A, which supports 10 Gbps over short distances and 5 Gbps over 100 meters, there is no need to replace the wiring (Option D eliminates). The 100-meter distance limitation (Option C) already applies to standard Ethernet and is met by CAT 6A - this is not an action but a constraint check. Option E (55 meters) is only relevant for specific 5GBASE-T configurations and doesn ' t maximize support compared to A and B. Reference: WLSD Study Guide - mGig Infrastructure, 802.11ac Wave 2 Infrastructure Design, Switch Upgrade Planning.

NEW QUESTION: 19

A customer has an existing wireless network with a Cisco 9800 WLC high availability cluster and Cisco 9120 APs. The customer asks an engineer to perform a post wireless survey that includes a list of any non-802.11 devices on the 5 GHz band. The engineer performs the survey using an 802.11a/b/g/n/ac/ax WLAN adapter but did not use a spectrum analyzer. Which approach meets the requirements?

A. Export a list of 802.11b interferers using the WLC and the RF ASIC embedded in the APs.

B. Set the WLAN adapter to monitor mode and perform the analysis by using 802.11b.

C. Set the WLAN adapter to monitor mode and perform the analysis by using 802.11a.

D. Export a list of 802.11a interferers using the WLC and the RF ASIC embedded in the APs.

Answer: D (LEAVE A REPLY)

Non-802.11 device detection on the 5 GHz band without a dedicated spectrum analyzer is possible through Cisco ' s CleanAir technology, which is embedded as an RF ASIC in many Cisco AP models including the

9120 series. CleanAir operates at the hardware layer - below the 802.11 MAC - enabling the APs to detect, classify, and report non-802.11 interference sources such as cordless phones, microwave ovens, video cameras, radar, and other unlicensed RF emitters in the 5 GHz spectrum. The WLC aggregates CleanAir reports from all APs and provides a consolidated interference device list accessible through the WLC ' s monitoring interface. Since the question specifies the 5 GHz band, the relevant 802.11 protocol for 5 GHz is

802.11a (and its successors 802.11n and 802.11ac). Exporting the list of 802.11a interferers from the WLC using the CleanAir RF ASIC correctly targets the 5 GHz band and identifies non-802.11 devices detected there. Option A incorrectly references 802.11b, which operates only on 2.4 GHz. Options B and C attempt to use the WLAN adapter for non-802.11 detection, but a standard WLAN adapter in monitor mode can only capture 802.11 frames - it cannot detect non-802.11 RF energy without a spectrum analyzer chipset.

Reference: WLSD Study Guide - Cisco CleanAir Technology, Non-802.11 Interference Detection, Post- Deployment Survey Methodology.

NEW QUESTION: 20

A customer has a Cisco wireless network that supports VoWLAN services. The customer wants supported voice clients to receive roaming recommendations and suggestions from APs. This functionality must not impact non-VoWLAN clients. What should be enabled on the VoWLAN SSID?

A. 802.11k neighbor lists

B. CCKM with 802.1X

C. 802.11v BSS Transition Management

D. 802.11r Fast Transition

Answer: (SHOW ANSWER)
IEEE 802.11v BSS Transition Management is the standard that enables the network (via the AP) to actively provide roaming recommendations and suggestions to associated clients. When enabled on a SSID, the AP can send BSS Transition Management Request frames to clients, informing them of preferred target APs ranked by signal quality, load, and channel conditions. Critically, BSS Transition Management is a voluntary mechanism - clients that support 802.11v can act on the AP ' s recommendation, while clients that do not support 802.11v simply ignore the BSS Transition Request frames and continue operating normally. This selective applicability directly satisfies the requirement that non-VoWLAN clients must not be impacted.
802.11k (Option A) enables clients to build neighbor lists through measurement reports - this is a client- initiated process, not an AP-to-client recommendation. CCKM (Option B) is a Cisco proprietary fast roaming mechanism for legacy clients, unrelated to roaming guidance. 802.11r (Option D) accelerates the re- association handshake during roaming but does not provide proactive roaming recommendations. Reference: WLSD Study Guide - VoWLAN Design, 802.11v BSS Transition Management, Roaming Optimization Protocols.

NEW QUESTION: 21
An engineer is designing a high-density WLAN that must support 100 concurrent users with 100 Mbps throughput consistently. The design allows for 20 Mbps per cell and per channel on the 5 GHz band. How many channels must the design use to provide 1 Mbps per user prior to RF overhead?
A. 5
B. 10
C. 15
D. 20
Answer: A (LEAVE A REPLY)
This question requires straightforward wireless capacity engineering calculation. The total throughput requirement is 100 users × 1 Mbps per user = 100 Mbps aggregate. Each channel in the design can support 20 Mbps of usable throughput - this is the per-cell, per-channel allocation defined in the design parameters, representing usable throughput prior to RF overhead as stated in the question. The number of channels required is therefore: total required throughput divided by throughput per channel = 100 Mbps ÷ 20 Mbps per channel = 5 channels. In practice, each channel corresponds to a non-overlapping frequency assignment in the
5 GHz band. With 5 channels and 20 Mbps per channel, the design provides exactly 100 Mbps of aggregate capacity for 100 concurrent users at 1 Mbps each. This calculation methodology is foundational to Cisco ' s high-density WLAN design approach, where the number of spatial streams, channel allocations, and AP placement are all derived from the per-user throughput requirement multiplied by the concurrent user population. Reference: WLSD Study Guide - High-Density WLAN Capacity Planning, Per-User Throughput Calculation, Channel Planning and Spatial Reuse.

NEW QUESTION: 22
A network engineer is designing a wireless network to support high availability. The network will need to support the total number of APs and client SSO. Live services should continue to work without interruption during the failover. Which two requirements need to be incorporated into the design to meet these needs?
(Choose two.)
A. redundant WLC
B. controller high availability pair with one of the WLCs having a valid AP count license
C. 10 sec RTT
D. back-to-back direct connection between WLCs
E. WLC 7.5 code or more recent
Answer: A,B (LEAVE A REPLY)
To support high availability with client SSO (Stateful Switchover) and no interruption to live services during failover, the design must incorporate two requirements. First, redundant WLCs (Option A) are essential - without a physical standby controller, there is no entity to take over when the primary WLC fails. In an SSO configuration, one WLC is active and one is standby, and the standby must be ready to assume the active role instantaneously. Second, the high availability pair requires one of the WLCs to have a valid AP count license (Option B). In a Cisco WLC SSO pair, the standby controller ' s AP count license applies when it becomes active - without a valid license on at least one WLC in the pair, APs cannot join after failover. A 10-second RTT maximum (Option C) is a latency requirement for the redundancy link but is not a primary design requirement that addresses the overall high availability architecture. A back-to-back direct connection (Option D) is one way to connect the redundancy ports but is not mandatory if a low-latency

switch connection is used. Code version 7.5 or newer (Option E) is a requirement for specific legacy SSO platforms but not a general design principle. Reference: WLSD Study Guide - WLC SSO High Availability Design, AP License Requirements, Redundant Controller Architecture.

NEW QUESTION: 23
A network engineer is deploying Cisco 9130I APs on multiple Cisco Catalyst 9800-80 WLCs with Cisco Catalyst Center. The engineer must enable Cisco AI Analytics and location analytics to use the RRM features to automatically manage the WLC RF profiles. Which type of license must be used on Cisco Catalyst Center?
A. Catalyst Advantage
B. Right-To-Use
C. Catalyst Essentials
D. SNTC SmartNet
Answer: A (LEAVE A REPLY)
Cisco Catalyst Center ' s AI-driven network management capabilities - including AI Analytics, AI-Enhanced RRM (Radio Resource Management), location analytics (DNA Spaces integration), and automated RF profile management - are exclusively available under the Catalyst Advantage license tier. The Advantage tier builds upon the Essentials tier and adds access to the full suite of AI/ML-powered assurance and optimization features. Specifically, AI-Enhanced RRM leverages machine learning models trained on historical RF telemetry to predict and prevent RF issues, dynamically adjust channel and power assignments, and automate RF profile selection - capabilities that cannot be activated without the Advantage license. Location analytics through Catalyst Center integrates with Cisco Spaces to provide real-time client location tracking, asset tracking, and spatial analytics. Catalyst Essentials (Option C) provides basic device management, software image management, and network plug-and-play provisioning - it does not include AI Analytics or advanced RRM automation. Right-To-Use (Option B) is a legacy licensing model not applicable to Catalyst Center.
SNTC SmartNet (Option D) is a support and maintenance contract, not a software feature license. Reference:
WLSD Study Guide - Cisco Catalyst Center Licensing, AI-Enhanced RRM, Catalyst Advantage Feature Set.

NEW QUESTION: 24
An engineer must identify the network requirements for a company that has a main office and 10 branch offices. The network must be able to support data, voice, video, and location tracking. Which two factors must be considered? (Choose two.)
A. security policy of the company for building access
B. number of wireless devices that require access
C. type of site for which the survey will be performed
D. business type of the company
E. available power sockets in the IT room
Answer: B,C (LEAVE A REPLY)
When designing a wireless network to support diverse services - including data, voice, video, and location tracking - across a distributed enterprise with a main office and 10 branch locations, the two primary design factors directly shaping the RF and capacity architecture are the number of wireless devices requiring access and the type of site where the survey will be performed. The device count (Option B) drives AP density, channel reuse planning, capacity modeling, and controller licensing requirements. Each service type - particularly VoWLAN and video - imposes strict per-client throughput and latency constraints that must be multiplied across the concurrent device population. The type of site (Option C) determines the survey approach, attenuation characteristics, coverage requirements, and antenna selection. A warehouse, hospital, or open-plan office each demands a fundamentally different RF design. Options A and D are organizational considerations, not technical RF design inputs. Option E (power sockets) is an installation logistics concern, not a wireless design factor. Reference: WLSD Study Guide - Requirements Gathering, Site Survey Planning, Capacity and Coverage Design Methodology.

NEW QUESTION: 25
How are mobility groups created, excluding mobility anchors?
A. The WLCs do not have to be of the same model or type to be a member of a mobility group, however each member should be running different software versions.
B. A mobility group does not require all WLCs in the group to use the same virtual IP address.
C. Each WLC must use the same mobility domain name and be defined as a peer in each other ' s static mobility members list.

D. If WLCs with HA SSO are deployed, each WLC in the WLC HA pair is considered separately as a mobility peer.
Answer: (SHOW ANSWER)
Mobility groups are created by configuring each Wireless LAN Controller (WLC) to use the same mobility domain name (mobility group name) and defining each WLC as a peer in the static mobility members list of every other WLC in the group. This bidirectional configuration establishes the trusted peer relationship and enables WLCs to exchange client information, security credentials, and state data for seamless roaming. The same mobility group name on all WLCs creates a shared identity; the static peer list defines which controllers are trusted mobility partners and provides their management IP addresses and MAC addresses for tunnel establishment. Option A is incorrect because members should run compatible (ideally the same) software versions, not different ones. Option B is incorrect - all WLCs in a mobility group must use the same virtual IP address for proper roaming. Option D is incorrect - in an HA SSO pair, the pair presents as a single logical mobility entity, not as two separate peers. Reference: WLSD Study Guide - Mobility Group Configuration, Peer Configuration Requirements, Mobility Domain Architecture.

NEW QUESTION: 26
A customer wants to provide wireless coverage in a parking lot outside of a building. An engineer determines that three APs are required. The APs can be mounted on the light poles in the parking lot because there are cable routes already in place for these locations. The closest wiring closet is approximately 200 meters away.
Which setup powers and connects the APs back to the customer network?
A. category 6 UTP cabling and Cisco UPOE
B. fiber connectivity with 802.3af
C. fiber connectivity with an AC/DC power module
D. Category 6 UTP cabling and PoE+
Answer: C (LEAVE A REPLY)
This question hinges on a fundamental network engineering constraint: the maximum transmission distance of copper Ethernet cabling. IEEE 802.3 standards specify a maximum segment length of 100 meters (328 feet) for all standard PoE and Ethernet over Category 5e, 6, or 6A UTP copper cabling. The parking lot light poles are approximately 200 meters from the closest wiring closet - more than double the maximum copper distance. This immediately eliminates Options A and D, which specify Category 6 UTP cabling: at 200 meters, UTP copper cannot reliably carry Ethernet at any supported speed, and PoE cannot be delivered over this distance regardless of standard. The correct solution is fiber optic connectivity between the wiring closet and the parking lot, combined with a local AC/DC power module at each pole location. Fiber optic cabling supports single-mode runs of kilometers and multi-mode runs of hundreds of meters at Gigabit speeds - easily spanning 200 meters. At the AP mounting location on the light pole, an AC/DC power module (powered from the pole ' s existing electrical supply) converts AC power to the DC power the AP requires.
Option B (fiber with 802.3af) is incorrect because PoE cannot be delivered over fiber - 802.3af requires copper cabling for simultaneous power and data delivery. Reference: WLSD Study Guide - Outdoor AP Deployment, Fiber vs. Copper Distance Limitations, Outdoor Power Solutions.

NEW QUESTION: 27
A customer purchases this Cisco equipment for a new branch office: * 20 Cisco Catalyst 9120 APs * five Catalyst 9130 APs * a single Catalyst 9300 Series Switch The customer wants to extend its existing wired and wireless fabric-enabled network to the branch office and manage all devices via a centrally deployed Cisco Catalyst Center (formerly DNA Center). Which Cisco Catalyst Center licenses are required for the branch office equipment?
A. Cisco Catalyst Advantage for the switch and all the APs
B. Cisco Catalyst Essentials on the APs and Cisco Catalyst Advantage on the switch
C. Cisco Catalyst Essentials on the switch and all the APs
D. Cisco Catalyst Advantage on the APs and Cisco Catalyst Center Premiere on the switch
Answer: A (LEAVE A REPLY)
Cisco Catalyst Center uses a tiered licensing model - Essentials and Advantage - applied to both switching and wireless infrastructure. To enable a fully fabric-enabled (SD-Access) deployment with centralized management, the Cisco Catalyst Advantage license is required across all device types. The Advantage tier unlocks Software-Defined Access fabric capabilities including macro and micro-segmentation, integration with Cisco ISE for policy enforcement, AI/ML-driven analytics via DNA Spaces and Assurance, and automated provisioning. The Essentials license provides only basic device management, inventory, and software image management - it does not unlock SD-Access fabric functionality. Since the branch design specifically extends an existing fabric-enabled network, the Essentials tier for either the switch or APs would create

a licensing gap preventing full fabric participation. Options B, C, and D all create asymmetric licensing that would partially disable fabric capabilities. The correct design mandates Catalyst Advantage for the Catalyst 9300 switch and all 25 APs. Reference: WLSD Study Guide - Cisco Catalyst Center Licensing, SD- Access Design, Fabric-Enabled Wireless Architecture.

NEW QUESTION: 28
During a site survey for a new wireless deployment in a multifloor office building, an engineer must identify sources of interference and ensure optimal AP placement for 5 GHz coverage. While walking the site with a spectrum analyzer, the engineer notices periodic spikes in the noise floor on several channels and inconsistent signal strengths reported by the survey tool, despite visually unobstructed paths. Which action must the engineer take next to accurately assess and mitigate the Layer 1 interference?
A. Increase the transmit power of all APs to compensate for the signal fluctuations and re-run the survey to verify the visual line-of-sight and signal strength measurements.
B. Use the wireless controller monitoring tools in combination with the site survey tool heatmap output to determine AP locations and capture the Layer 1 spectrum analysis for ongoing analysis.
C. Document the affected channels and locations, then attempt to adjust the channel plan to avoid the frequencies that experience the most interference during initial deployment.
D. Use the spectrum analyzer to document the time, frequency, and location of the noise spikes, then correlate them with possible non-Wi-Fi interferers and adjust AP placement accordingly.
Answer: D (LEAVE A REPLY)
Layer 1 interference analysis is foundational to the Cisco site survey methodology. When a spectrum analyzer reveals periodic noise floor spikes across multiple channels with no clear line-of-sight obstruction, the root cause is almost certainly a non-802.11 device - candidates include cordless phones, video cameras, microwave equipment, or radar systems triggering DFS events. The correct engineering response is systematic documentation: capture the time of occurrence, the specific frequency or frequency range, and the geographic location of the interference signature. This triangulation data enables correlation with physical devices present in the facility. Simply increasing transmit power (Option A) raises the noise floor for neighboring cells and worsens co-channel interference. Using WLC monitoring tools (Option B) is insufficient because the WLC cannot detect non-802.11 energy at Layer 1. Adjusting the channel plan (Option C) without fully characterizing the interferer is premature. Only Option D follows the correct Cisco survey methodology for Layer 1 analysis, leading to actionable AP placement adjustments. Reference: WLSD Study Guide - Wireless Site Survey Methodology, Layer 1 Spectrum Analysis, Interference Identification and Mitigation.

NEW QUESTION: 29
Which issue occurs when wireless access points transmit by using the highest power level in a building that has brick walls?
A. hidden node
B. wideband interference
C. reflection
D. narrowband interference
Answer: A (LEAVE A REPLY)
The hidden node problem is a classic RF design flaw that emerges when APs transmit at excessive power levels relative to the attenuation characteristics of the environment. In a brick-walled building, AP signals penetrate walls with significant attenuation. When an AP transmits at maximum power, its signal propagates far beyond the intended cell boundary and reaches client devices that may be physically near other APs but unable to detect the original transmitting AP due to wall attenuation between them. These clients can hear the distant AP ' s signal but cannot hear each other - making them hidden from one another. This leads to simultaneous transmissions, frame collisions at the AP receiver, and dramatic throughput degradation. The
802.11 CSMA/CA mechanism depends on all stations being able to sense the medium before transmitting; hidden nodes defeat this mechanism entirely. The WLSD curriculum consistently identifies excessive AP transmit power in high-attenuation environments as a primary cause of hidden node conditions. The solution is to reduce AP transmit power so that cell sizes remain appropriate for the physical environment.
Reference:
WLSD Study Guide - RF Design Fundamentals, Hidden Node Problem, Transmit Power and Cell Size Optimization.

NEW QUESTION: 30
A customer has a centralized wireless deployment with N+1 high availability and few open authentication SSIDs configured. After failover, all APs are broadcasting all SSIDs, but the clients are assigned IP addresses from a different subnet. The WLANs on both WLCs are configured with the same dynamic interfaces. Which feature must be incorporated in the wireless design of the second controller?
A. RF Protocol
B. AP Groups

C. VLAN Select
D. AAA Override
Answer: C (LEAVE A REPLY)
VLAN Select is a feature that allows for the dynamic assignment of clients to different VLANs from a pool based on various criteria, such as load balancing or location. In a centralized wireless deployment with N+1 high availability, if clients are receiving IP addresses from a different subnet after failover despite the WLANs being configured with the same dynamic interfaces, the issue is that the second controller ' s WLAN interface mapping resolves to a different VLAN or DHCP scope. VLAN Select ensures that client VLAN assignment is consistent regardless of which controller the client connects to, preventing the subnet change behavior observed during failover. Without VLAN Select, even identically named dynamic interfaces on two WLCs may map to different VLANs if the underlying switch configuration differs. RF Protocol (Option A) controls radio parameters. AP Groups (Option B) control SSID and VLAN assignments per AP cluster. AAA Override (Option D) allows RADIUS servers to assign per-user VLANs, which requires authentication - but these SSIDs use open authentication. Reference: WLSD Study Guide - N+1 High Availability Design, VLAN Select Feature, Consistent Client VLAN Assignment Across Controllers.

NEW QUESTION: 31
An engineer is upgrading the legacy APs to 802.11ac Wave 2 capable APs. The existing gigabit uplinked switches provide 802.3at. Which switch limitation is a concern?
A. interface throughput
B. high availability
C. collision domains
D. output power
Answer: D (LEAVE A REPLY)
The primary concern when upgrading to 802.11ac Wave 2 capable APs with existing switches that only provide IEEE 802.3at (PoE+, 30W maximum) is the output power limitation. 802.11ac Wave 2 APs, particularly Cisco ' s 3800 and 4800 series, can require significantly more power than 30W to operate all radios and capabilities at full capacity. The Wave 2 standard introduced features such as Multi-User MIMO (MU-MIMO), beamforming, and additional spatial streams, all of which increase power consumption. When an AP doesn ' t receive sufficient power, it may reduce transmit power, disable radios, or reduce the number of spatial streams - directly degrading wireless performance. Interface throughput (Option A) may also be a concern with multi-gigabit capable APs, but the question specifically asks about the limitation introduced by
802.3at, which is directly a power delivery constraint. Collision domains (Option C) and high availability (Option B) are unrelated to the PoE standard. Reference: WLSD Study Guide - PoE Upgrade Planning, 802.11ac Wave 2 Infrastructure Requirements, Switch Power Budget Considerations.

Valid 300-110 Dumps shared by Actual4test.com for Helping Passing 300-110 Exam! Actual4test.com now offer the **newest 300-110 exam dumps**, the Actual4test.com 300-110 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-110 dumps with Test Engine here: https://www.actual4test.com/300-110_examcollection.html (**125** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 32
A customer designs a Cisco wireless environment to provide connectivity to employees and guests. The guest SSID must be configured on three anchor WLCs named Anchor1, Anchor2, and Anchor3 in a DMZ. The guest anchor priority must be configured to ensure that Anchor1 has the highest priority. Which priority level must be incorporated in the design for Anchor1?
A. 0
B. 1
C. 2
D. 3
Answer: (SHOW ANSWER)
In Cisco ' s guest anchor WLC deployment model, multiple anchor controllers can be configured in a DMZ to provide redundancy for guest WLAN traffic. The anchor priority value determines which anchor controller is preferred for establishing the guest mobility tunnel from the foreign WLC. Cisco ' s anchor priority system assigns the highest preference to the lowest numerical priority value. Priority 1 is the highest

priority, meaning the foreign WLC will prefer Anchor1 when establishing the CAPWAP mobility tunnel for anchoring guest client traffic. Priority 2 would be assigned to Anchor2, and Priority 3 to Anchor3, creating a deterministic failover hierarchy. If Anchor1 becomes unreachable, the foreign controller automatically falls over to Anchor2, then to Anchor3. Priority 0 is not a valid anchor priority value in the Cisco WLC configuration. This design pattern is critical for enterprise guest deployments where DMZ anchor redundancy must be maintained without manual intervention. Reference: WLSD Study Guide - Guest Wireless Architecture, Anchor WLC Configuration, Mobility and DMZ Design.

NEW QUESTION: 33
An engineer is performing a passive survey report. The coverage heat map shows the entire site with all signal levels. To see only the desired coverage, which action must the engineer take?
A. Change the color scheme to show the desired heat map.
B. Use the RSSI calibration tool to configure the receiver sensitivity.
C. Use the RSSI slider to set the heat map to the desired cutoff filter.
D. Filter the results to show the desired APs only.
Answer: C (LEAVE A REPLY)
To focus the coverage heat map on the desired coverage threshold, the engineer should use the RSSI slider to set the heat map to the desired cutoff filter. This action adjusts the display to show only the signal levels that meet or exceed the specified RSSI value, effectively filtering out weaker signals and highlighting areas with sufficient coverage. In Ekahau and similar survey tools, the RSSI slider provides a dynamic way to set minimum signal thresholds, allowing the engineer to quickly validate whether coverage meets design targets such as -67 dBm for voice or -70 dBm for data. Changing the color scheme (Option A) only modifies the visual representation without filtering data. The RSSI calibration tool (Option B) adjusts how the tool perceives signal levels, not the display filter. Filtering by AP (Option D) would remove APs from the view, potentially hiding coverage gaps. Reference: WLSD Study Guide - Post-Deployment Survey, Ekahau Heat Map Tools, RSSI Coverage Filtering.

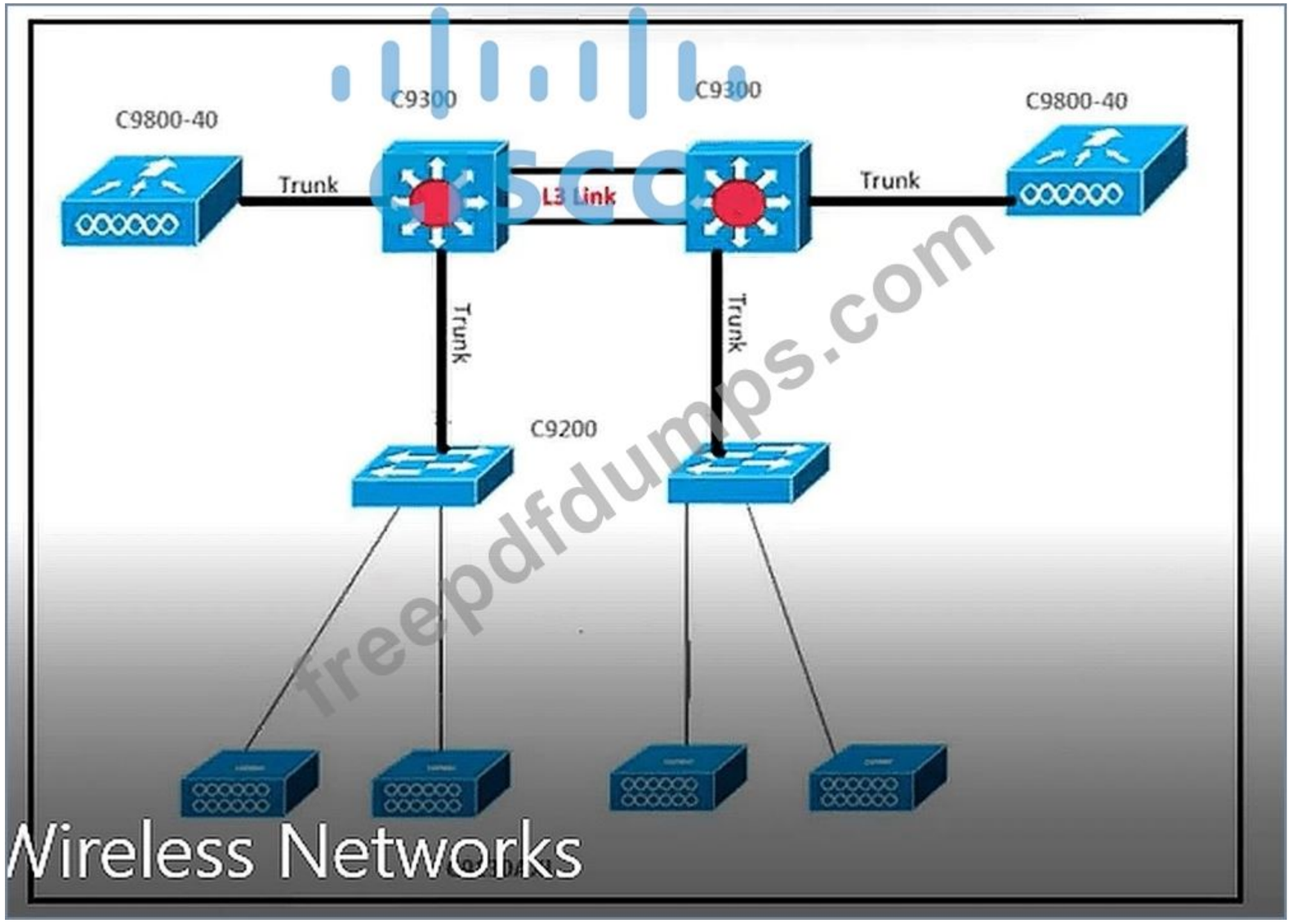
NEW QUESTION: 34
An engineer must design AP placements for a new branch office that contains two floors. The engineer uses Ekahau to complete the predictive survey. To calculate the signal bleed through between floors, the engineer creates a building, adds the floors, and attenuation areas. After the scale is set, what else must be added on the floors to accurately measure the signal bleed at a specific location?
A. Draw in coverage areas.
B. Start the auto planner.
C. Add alignment points.
D. Choose the access point models.
Answer: C (LEAVE A REPLY)
In Ekahau Site Survey ' s multi-floor predictive modeling workflow, alignment points are the critical mechanism that allows the software to understand the precise vertical spatial relationship between floors in a multi-story building. Once floor plans are imported with their scale correctly defined, alignment points must be placed on each floor at the same real-world physical location - such as a stairwell corner, elevator shaft, or structural column - so that Ekahau can accurately calculate vertical signal propagation and inter-floor RF bleed. Without alignment points, the software has no spatial reference to determine which area on Floor 2 is directly above a given point on Floor 1, making floor-to-floor signal bleed calculations geometrically impossible. Drawing coverage areas (Option A) is a post-AP-placement activity. Starting the auto planner (Option B) would attempt to place APs without the required spatial reference. Choosing AP models (Option D) is a subsequent step. Alignment points are a fundamental requirement for any predictive survey involving multi-floor buildings. Reference: WLSD Study Guide - Ekahau Predictive Survey Methodology, Multi- Floor Building Configuration, Signal Propagation Modeling.

NEW QUESTION: 35
Which CLI command does an engineer use to validate that the redundancy peer of a Stateful Switchover pair of controllers is up and connected?
A. rping
B. ping
C. eping
D. mping
Answer: C (LEAVE A REPLY)

The eping command is used on Cisco Wireless LAN Controllers to verify that the redundancy peer in a Stateful Switchover (SSO) pair of controllers is up and connected. This command sends ECHO packets (EoIP echo packets) to the peer controller to ensure the data path connectivity is functioning. In an SSO configuration, eping verifies the EoIP tunnel between the active and standby controllers, which is critical for state synchronization and seamless failover. If eping succeeds, it confirms that both the network path and the EoIP data encapsulation between the controllers are functional. The standard ping command (Option B) tests basic IP connectivity but does not validate the EoIP data path used by the SSO redundancy mechanism. The mping command (Option D) tests mobility control path connectivity between mobility group peers, not the SSO redundancy path. The rping command (Option A) is not a standard Cisco WLC command for testing SSO peer connectivity. Reference: WLSD Study Guide - WLC SSO Troubleshooting, eping Command, Redundancy Peer Connectivity Validation.

NEW QUESTION: 36
In a FlexConnect deployment, which role does the site tag play?
A. It configures the switch port settings for FlexConnect APs.
B. It assigns IP addresses to wireless clients for the site APs.
C. It manages the firewall policies for the site APs.
D. It defines the roaming domain for FlexConnect APs.
Answer: (SHOW ANSWER)
In the Cisco Catalyst 9800 IOS XE WLC configuration framework, the site tag serves as the primary organizational and functional grouping element for FlexConnect APs at a given physical location. The site tag defines the FlexConnect site - a logical boundary within which APs can perform local switching and local inter-AP roaming without requiring CAPWAP tunnel traversal to the WLC for every client handoff. Within a FlexConnect site defined by the site tag, APs can exchange client roaming context information directly with each other (peer-to-peer), enabling fast Layer 2 roaming for clients moving between APs that share the same site tag - effectively defining the roaming domain for FlexConnect APs at that site. The site tag also references the flex profile (which defines VLAN mappings, local auth settings, and split tunneling parameters) and the AP join profile. Switch port configuration (Option A) is performed on the infrastructure switches, not through the WLC site tag. IP address assignment (Option B) is a DHCP function. Firewall policies (Option C) are applied through ACLs and policy tags, not site tags. Reference: WLSD Study Guide - Catalyst 9800 Tag Architecture, FlexConnect Site Tag Role, Local Roaming in FlexConnect Deployments.

NEW QUESTION: 37
Refer to the exhibit. A network engineer is designing a high availability SSO on a Cisco Catalyst 9800-40 WLC with multi-LAG network redundancy on two Catalyst 9300 switches. The LAG requirements are: * Each LAG must be connected to a single switch. * Different VLANs must be assigned to different LAGs. * The controller must learn the identity of partners that can support LAG capabilities in each port. * When any active LAG ports fail, a standby LAG port must provide redundancy. Which protocol must be used for the port channel on the interface to meet the design requirements?



A. LACP
B. OSPF
C. PAgP
D. BGP

Answer: (SHOW ANSWER)

The design requirements specify a multi-LAG configuration where each LAG connects to a single switch, different VLANs are assigned to different LAGs, the controller must dynamically learn partner LAG capabilities per port, and standby ports provide redundancy upon active port failure. These requirements collectively point to IEEE 802.3ad LACP (Link Aggregation Control Protocol) as the correct protocol. LACP is the industry-standard IEEE protocol that enables dynamic negotiation of LAG membership between endpoints - the WLC and each Catalyst 9300 switch exchange LACP PDUs (LACPDUs) to discover port capabilities, negotiate bundle membership, and monitor link status. LACP supports active and passive port states where active ports initiate negotiation and passive ports respond, and it provides the standby port mechanism through its hot-standby capability for link redundancy within the bundle. The requirement to ' learn the identity of partners that can support LAG capabilities ' is the defining characteristic of LACP ' s standardized PDU exchange mechanism. PAgP (Option C) is a Cisco proprietary port aggregation protocol that, while functionally similar, is not the IEEE standard and is incompatible with non-Cisco equipment in

mixed environments. OSPF (Option B) and BGP (Option D) are Layer 3 routing protocols entirely unrelated to port channel negotiation. Reference: WLSD Study Guide - Catalyst 9800 LAG Configuration, LACP IEEE 802.3ad, Multi-LAG High Availability Design.

NEW QUESTION: 38
An enterprise is using wireless as the main network connectivity for clients. To ensure wireless network availability, two standalone controllers are installed in the head office. APs are connected to the controllers using a round-robin approach to load balance the traffic. After a power cut, the wireless clients disconnect while roaming. An engineer tried eping from the controller but fails. Which protocol needs to be allowed between the networks that the controllers are installed?
A. IP Protocol 67
B. IP Protocol 77
C. IP Protocol 87
D. IP Protocol 97
Answer: D (LEAVE A REPLY)
When eping (EoIP ping) fails between two Cisco Wireless LAN Controllers, it indicates that the data path of the mobility tunnel is blocked. In Cisco AireOS wireless networks, the mobility data path uses IP Protocol 97 (EtherIP - Ethernet-over-IP encapsulation) for tunneling client traffic between the anchor and foreign controllers. This is distinct from the control path, which uses UDP port 16666. When the mobility data path (IP Protocol 97) is blocked by a firewall or ACL between the two controllers ' networks, eping will fail because eping specifically tests the EoIP data encapsulation path. After a power cut, when clients disconnect and attempt to roam between APs on different controllers, the mobility tunnel must be operational for session continuity. If IP Protocol 97 is blocked, the mobility data plane cannot function, causing client disconnections during inter-controller roaming events. The other IP protocols listed (67, 77, 87) are not used for Cisco WLC mobility tunneling. Reference: WLSD Study Guide - Mobility Tunnel Data Path, IP Protocol 97 (EtherIP), eping Command and Troubleshooting.

NEW QUESTION: 39
An engineer is using Ekahau Site Survey to create a WLAN plan for a warehouse. The plan is to use patch antennas. Which setting is adjusted when simulated APs are placed on the map?
A. AP channel
B. Wi-Fi technology
C. antenna downtilt
D. AP transmission power
Answer: C (LEAVE A REPLY)
In Ekahau Site Survey, when planning a warehouse deployment using patch (directional) antennas, the antenna downtilt setting is the critical adjustment made when placing simulated APs on the floor plan map. Patch antennas have a defined radiation pattern with a main lobe that must be aimed precisely at the intended coverage zone. In a warehouse environment, APs with patch antennas are typically wall-mounted and aimed down aisles. The downtilt angle determines the vertical component of the antenna ' s aim - adjusting the downtilt in Ekahau tilts the simulated antenna ' s main radiation lobe downward toward the warehouse floor and the working zone of RF scanner devices, rather than projecting RF energy horizontally at an ineffective angle. Ekahau allows engineers to specify the horizontal and vertical orientation of the antenna in three dimensions, and the downtilt value directly controls how the software models the antenna ' s coverage pattern in the vertical plane. AP channel (Option A) is set during channel planning, not during AP placement. Wi-Fi technology (Option B) determines the modulation and protocol standard but is set as an AP property. AP transmission power (Option D) controls cell radius but is set separately from antenna orientation. Reference:
WLSD Study Guide - Ekahau Predictive Survey, Directional Antenna Configuration, Warehouse RF Design and Antenna Orientation.

NEW QUESTION: 40
An engineer configured the optimized client roaming on Cisco WLC with an RSSI threshold of -72 dBm.
Clients report frequent disconnections. What must be configured for the AP to guide the client to a better AP?
A. Enable BSS transition on the SSID and optimized roaming at the radio level.
B. Disable coverage hole detection on the SSID and enable BSS transition on the SSID.
C. Enable BSS transition at the radio level and optimized roaming on the SSID.

D. Disable optimized roaming and enable 802.11v support on the SSID.
Answer: A (LEAVE A REPLY)
The scenario presents a critical distinction in where Cisco WLC features are configured. Optimized roaming on Cisco WLC is a radio-level feature that monitors connected client RSSI and, when a client ' s signal falls below the configured threshold (-72 dBm), triggers a disassociation to force the client to reconnect to a stronger AP. However, without a mechanism to guide the client proactively before reaching the threshold, clients that disassociate simply reconnect to whatever AP their device selects, potentially causing the reported frequent disconnections. BSS Transition Management (802.11v) is configured at the SSID level and provides the complementary mechanism: before the client reaches the RSSI threshold, the AP sends a BSS Transition Management Request pointing the client toward a specific target AP with stronger signal. The correct architecture requires: optimized roaming configured at the radio level (triggering disconnection when RSSI falls too low) combined with BSS transition enabled at the SSID level (guiding the client to a better AP before forced disconnection). Options C and D incorrectly reverse the configuration levels for these features.
Disabling coverage hole detection (Option B) addresses a different problem and would not resolve the disconnection issue. Reference: WLSD Study Guide - Optimized Roaming Configuration, BSS Transition Management (802.11v), Client Roaming Architecture on Cisco WLC.

NEW QUESTION: 41
A customer has a single anchor WLC named Anchor A. Anchor A is in a DMZ and provides guest access.
The customer wants to deploy an additional anchor controller named Anchor B to provide redundancy if Anchor A fails. Which design approach should be taken for the guest WLAN priority on the foreign WLC for each anchor WLC?
A. Set Anchor A to priority 3 and Anchor B to priority 3.
B. Set Anchor A to priority 3 and Anchor B to priority 1.
C. Set Anchor A to priority 1 and Anchor B to priority 1.
D. Set Anchor A to priority 1 and Anchor B to priority 3.
Answer: D (LEAVE A REPLY)
In a wireless network design where anchor redundancy is required for guest access, setting different priorities for the anchor controllers ensures deterministic primary and backup behavior. Cisco anchor priority uses a lower numerical value to indicate higher preference - Priority 1 is the highest priority (most preferred) anchor, and Priority 3 is lower priority. Setting Anchor A to priority 1 (Option D) makes it the primary anchor controller - all new guest client sessions will preferentially anchor to Anchor A. Setting Anchor B to priority
3 makes it the standby anchor - guest clients will only be anchored to Anchor B when Anchor A is unavailable. This creates a clear primary/backup relationship with deterministic failover. Setting both anchors to the same priority (Options A and C) would result in load balancing between the two anchors rather than active/standby behavior. Option B incorrectly reverses the priorities, making Anchor B the primary and Anchor A the backup. Reference: WLSD Study Guide - Guest Anchor Redundancy Design, Anchor Priority Configuration, DMZ Anchor WLC Architecture.

NEW QUESTION: 42
A company has three Cisco WLCs that are joined as a mobility group. Mobility multicast messaging is enabled. All the WLCs in the mobility group communicate via a multicast. Which configuration must be identical between the three WLCs to validate communication?
A. service port IP address
B. interface IDs
C. management IP address
D. multicast IP address
Answer: D (LEAVE A REPLY)
When Cisco WLCs are configured to use multicast for mobility group communications, all WLCs participating in the same mobility group must be configured with an identical multicast group IP address. The mobility multicast mode allows a WLC to send a single multicast frame received simultaneously by all other WLCs in the group, rather than sending individual unicast copies to each peer. For this to function correctly, every WLC in the group must join the same IP multicast group address, and the underlying network infrastructure must be configured to support IP multicast routing or IGMP snooping for that specific group address. If any WLC is configured with a different multicast IP address, it will join a different multicast group and will not receive mobility messages from the other WLCs, effectively isolating it from the group ' s communication plane. Service port IP addresses (Option A) are unique per controller. Interface IDs (Option B) are locally significant identifiers. Management IP addresses (Option C) are unique per WLC and identify each peer in unicast configurations. Reference: WLSD Study Guide - Mobility Group Configuration, Multicast Mobility Messaging, WLC Peer Communication.

NEW QUESTION: 43
An engineer must design and configure a wireless network for pervasive coverage in an oil terminal, casual web and email traffic, 5 GHz. What is the best design?
A. Disable all data rates below 54 Mbps and assign static power level 1 on all access points.
B. Keep all the data rates enabled and set the AP power assignment mode to auto.
C. Disable all data rates below 24 Mbps and keep the power assignment on the AP as auto.
D. Keep the power assignment as auto and disable 802.11n and 802.11ac MCS rate.
Answer: B (LEAVE A REPLY)
An oil terminal presents specific wireless design constraints: the requirement is pervasive coverage (maximum geographic coverage) for low-bandwidth applications (casual web and email). These requirements prioritize coverage reach over throughput optimization. The correct approach is to keep all data rates enabled, including lower rates such as 6, 9, 12, and 18 Mbps - because in an industrial environment with challenging RF propagation paths, reflective surfaces, and potential obstructions, lower data rates extend the functional coverage range of each AP. Web and email traffic does not require high data rates; even 1-6 Mbps is sufficient for these applications. Disabling rates below 54 Mbps (Option A) would dramatically shrink each AP ' s effective coverage area, requiring many more APs for pervasive coverage and failing the primary design objective. Assigning static maximum power without RRM auto-adjustment creates excessive co- channel interference. Disabling rates below 24 Mbps (Option C) still reduces coverage reach unnecessarily.
Disabling 802.11n and 802.11ac MCS rates (Option D) prevents the AP from using high-efficiency modulation for nearby clients without coverage benefit. Auto power assignment combined with all rates enabled provides the optimal balance for pervasive industrial deployment. Reference: WLSD Study Guide - Industrial WLAN Design, Coverage vs. Capacity Trade-offs, Data Rate Configuration for Pervasive Coverage.

NEW QUESTION: 44
An engineer is deploying new APs to serve IEEE 802.11g through 802.11ac clients and wants to use the Ekahau Site Survey tool to verify RF coverage. Management wants the engineer to verify and create coverage maps as quickly as possible. Which configuration accomplishes the goal?
A. passive mode with one wireless adapter
B. active mode with two wireless adapters
C. active mode with one wireless adapter
D. passive mode with two wireless adapters
Answer: D (LEAVE A REPLY)
In Ekahau Site Survey, passive mode involves listening to beacon frames and probe responses from deployed APs without the survey laptop actively associating to any SSID. This is significantly faster than active mode because no association, DHCP, or throughput test overhead is introduced - the surveyor simply walks the floor while Ekahau passively captures signal strength data from all visible APs simultaneously.
Using two wireless adapters in passive mode provides a critical speed advantage: one adapter scans 2.4 GHz channels while the second adapter simultaneously scans 5 GHz channels. Without dual adapters, a single adapter must time-multiplex between bands, reducing the sample rate per band and either slowing the survey walk or producing sparser data. Active mode (Options B and C) is used when throughput measurements are required for specific application validation such as voice or video, but it is inherently slower due to association overhead and sequential testing. The combination of passive scanning and dual adapter configuration delivers the highest possible data collection rate per unit of walk time. Reference: WLSD Study Guide - Ekahau Site Survey Modes, Passive vs. Active Survey Methodology, Multi-Adapter Survey Configuration.

NEW QUESTION: 45
Refer to the exhibit. A wireless engineer is using the Ekahau Site Survey tool to conduct a post-deployment survey. The engineer analyzes the pictured output to determine if SNR meets the voice requirements. How is the voice support based on the output?
Exhibit - Q15: Ekahau SNR Heatmap - Post-Deployment Survey Output



A. It works in the top-middle room.
B. It is not supported.
C. It works in the lobby.
D. It works in all locations.

Answer: (SHOW ANSWER)

Voice over WLAN (VoWLAN) deployments require a minimum SNR threshold to maintain acceptable Mean Opinion Score (MOS) values for call quality. Cisco ' s 300-110 WLSD curriculum specifies that VoWLAN requires a minimum SNR of 25 dB throughout the coverage area. In an Ekahau post-deployment survey SNR heatmap, when the heatmap displays a consistent color indicating SNR at or above this threshold across the entire surveyed area - including all rooms, corridors, and common areas such as the lobby - the conclusion is that voice service is supported in all locations. The color coding in Ekahau ' s SNR heatmap uses green tones to indicate adequate SNR (typically #25 dB) and shifts toward yellow and red for degraded conditions.

When the exhibit heatmap shows uniform adequate coverage across all surveyed areas without yellow or red zones, it confirms the SNR requirement for VoWLAN is universally met. Options A, B, and C suggest partial or no coverage, which would be indicated by mixed or poor SNR values - conditions not present in this scenario. The post-deployment survey with Ekahau is the validation step confirming that the predictive design was accurately realized in the physical environment. Reference: WLSD Study Guide - VoWLAN Design Requirements, SNR Thresholds, Post-Deployment Survey Validation with Ekahau.

Valid 300-110 Dumps shared by Actual4test.com for Helping Passing 300-110 Exam! Actual4test.com now offer the **newest 300-110 exam dumps**, the Actual4test.com 300-110 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 300-110 dumps with Test Engine here: https://www.actual4test.com/300-110_examcollection.html (**125** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)