PassQueen
a.k.a dumpsqueen.com

Certified Wireless Design Professional

CWNP CWDP-305

Version Demo

Total Demo Questions: 33

Total Premium Questions: 335

Buy Premium PDF

Topic Break Down

Topic	No. of Questions
Topic 1, WLAN Design	102
Topic 2, RF Design	76
Topic 3, WLAN Assessment	78
Topic 4, WLAN Infrastructure Design	79
Total	335

QUESTION NO: 1

What best describes ensuring coverage requirements in a deployed WLAN?

A. Measuring the signal strength and number of APs at each location and comparing it to the requirement specifications

B. Verifying that the WLAN can be seen from all required locations

C. Verifying that you can connect to the WLAN from all required locations with the least capable device

D. Verifying that a 3x3:3 gaming laptop can connect to the WLAN from all required locations

ANSWER: A

Explanation:

Measuring the signal strength and number of APs at each location and comparing it to the requirement specifications is the appropriate way to ensure deployed WLAN coverage meets the design. Coverage is an objectively testable design requirement, normally expressed through criteria such as minimum received signal strength, required signal-to-noise ratio, data-rate or modulation support, and, where resilience or roaming requirements apply, a minimum number of usable APs heard at a client location. A post-deployment validation survey gathers measurements throughout the required service area and compares those results against the requirements established during design. This validates the actual RF environment, including effects from construction materials, installed AP placement, transmit power, antennas, and RF conditions that can differ from predictive modeling. CWNP design work emphasizes validating the WLAN against documented business and technical requirements rather than relying on a simple association test. Cisco similarly describes wireless site-survey validation as measuring RF coverage and verifying that the implementation satisfies the defined coverage objectives. Useful references include the CWNP CWDP certification overview and Cisco's Wireless LAN Design Guide.

QUESTION NO: 2

An engineering firm upgraded from nine 802.11n APs to nine 802.11ac APs, retaining the same channel and power configuration. Despite this, throughput remains unchanged. What is the most likely reason for the lack of improvement?

A. APs are transmitting at a low transmit power

B. The clients were not upgraded

C. APs are mounted on the wall

D. The APs are still using the 5 GHz lower band

ANSWER: B

Explanation:

The clients were not upgraded is correct because an AP upgrade alone does not make existing client radios communicate using 802.11ac capabilities. Wi-Fi performance is negotiated per client association and is constrained by the PHY features supported by both the AP and the client. An 802.11n client associating to an 802.11ac AP continues to use the 802.11n PHY rates, channel-width support, modulation and coding schemes, and spatial-stream capabilities available to that client. Consequently, the AP's 802.11ac support cannot by itself increase that client's maximum link rate or its resulting application throughput.

802.11ac introduced higher-capacity 5 GHz operation, including support for wider channels and higher modulation options, but a client must support those features and successfully negotiate their use to benefit. Retaining the existing RF channel and transmit-power plan also means the upgrade does not inherently change the RF conditions experienced by the clients. In a real design validation, the engineer should inventory client Wi-Fi chipsets, confirm their supported standards, channel widths, spatial streams, and MCS capabilities, then measure throughput using representative 802.11ac-capable clients. Cisco's overview of 802.11ac technology describes the client/AP feature relationship, and the Wi-Fi Alliance Wi-Fi CERTIFIED ac overview summarizes the capabilities that compatible devices can use.

QUESTION NO: 3

In a convention center, you have received complaints about the WLAN infrastructure. At this moment, there are only two APs in one auditorium. After analyzing the situation, you determined that there are more client devices than the infrastructure was designed for. There are only two APs to support more than 300 devices using Wi-Fi at the same time. What should you do to make the Wi-Fi work as expected?

A. Redesign the entire WLAN

B. Upgrade the Ethernet connections to MultiGig

C. Quickly add more APs

D. Turn up the output power on the APs so that they can handle more clients

ANSWER: A

Explanation:

Redesign the entire WLAN is correct because the auditorium has a capacity-design problem, not merely an isolated equipment or coverage problem. Supporting more than 300 concurrent Wi-Fi devices with only two APs creates excessive client contention for shared RF airtime and leaves too little total capacity for the expected application demand. A proper redesign begins by collecting requirements such as the expected number of concurrent clients, device types and capabilities, applications, throughput expectations, and the physical seating layout. The resulting high-density design should use an appropriate number of APs, deliberate placement and antenna choices, a channel-reuse plan, suitable transmit-power settings, and validation that the wired access layer can support the redesigned AP population. This approach creates smaller, controlled RF cells and distributes clients and airtime demand across multiple radios while limiting contention and co-channel interference. It also permits an informed decision about whether uplink upgrades are required as part of the overall solution, rather than assuming that an uplink change alone resolves the issue. CWDP design practice emphasizes translating business and capacity requirements into an RF design that is validated after deployment. See CWNP's CWDP certification overview and the CWDP exam objectives.

QUESTION NO: 4

Before beginning a predictive design for a multi-floor office building, which physical-site information should be collected or verified? (Select three.)

A. The construction and likely RF attenuation characteristics of walls, floors, and major obstructions

B. The available AP mounting locations, ceiling types, and mounting-height constraints

C. The cable pathways, switch locations, and PoE availability for planned AP locations

D. The email-domain naming convention used by employees

E. The desktop wallpaper standard used by corporate workstations

ANSWER: A B C

Explanation:

Construction materials, mounting constraints, and cable and power availability are critical site inputs. Wall, floor, glass, shelving, and other construction details affect attenuation and propagation, so generic floor-plan objects should be verified where possible. Ceiling construction, AP mounting height, and permitted mounting locations affect antenna patterns, cell shape, serviceability, and the practicality of the design.

Cable pathways and power availability determine whether the planned AP locations can actually be deployed and whether the required PoE infrastructure can support them. Employee email-domain naming and desktop wallpaper standards have no meaningful effect on the RF or physical infrastructure design.

QUESTION NO: 5

A WLAN is being designed for handheld clients that transmit at substantially lower power than the APs. Which design practices help ensure that coverage is usable in both directions? (Select three.)

A. Model the handheld client transmit capability in the link budget

B. Validate uplink performance with representative handheld clients

C. Use AP power settings that support a balanced bidirectional cell design

D. Set every AP to its maximum permitted transmit power

E. Base the coverage boundary only on AP beacon RSSI

ANSWER: A B C

Explanation:

The designer should model the client transmit capability, validate uplink performance with representative clients, and avoid assuming that AP transmit power alone defines the cell boundary. Wi-Fi communication is bidirectional: a client must be able to reach the AP reliably as well as receive AP transmissions. A high AP transmit power can create an apparently strong downlink while leaving the client unable to sustain the uplink at the required data rate. Raising AP power without evaluating the client link budget can therefore worsen an asymmetric design.

QUESTION NO: 6

When using a WLAN design tool with propagation modeling capabilities, what critical step must be performed before adding APs, antennas, and attenuation factors like walls?

A. Set the transmit power for all APs

B. Add pictures of the environment

C. Nothing; just begin by adding APs, antenna and attenuators

D. Calibrate the floor plan to increase accuracy

ANSWER: D

Explanation:

Calibrate the floor plan to increase accuracy is correct because a predictive WLAN design tool must first know the real-world scale of the imported drawing. Calibration associates a measured distance on the floor plan with its actual physical distance, allowing the tool to interpret dimensions correctly. Once the plan is scaled, the model can place APs at meaningful locations and calculate the distance-dependent effects that drive RF predictions, including free-space path loss, coverage boundaries, expected signal level, and the placement and extent of wall or other attenuation objects.

Accurate scale is foundational to propagation modeling: if a drawing is too large or too small in the software, AP-to-client and AP-to-AP distances will be incorrect, which in turn distorts predicted cell size, overlap, and capacity-related design decisions. CWNP design methodology treats the floor plan and its dimensions as input data that must be validated before modeling the RF environment and selecting infrastructure. The survey or design workflow can then apply appropriate wall-loss values, antenna patterns, mounting details, and AP settings to a correctly dimensioned representation of the facility. See CWNP's CWDP certification overview at https://www.cwnp.com/certifications/cwdp/ and the Ekahau guidance on importing and scaling floor plans at https://support.ekahau.com/hc/en-us/articles/115003747148-Importing-Floor-Plans.

QUESTION NO: 7

A business traveler from North America is in Europe. The hotel only provides coverage in 2.4 GHz. The traveler connects to the hotel's SSID and notices an AP in the hotel room. However, the laptop reports a very low RSSI when connected. The traveler does not have the same problem when connecting in the lobby. What would be the most likely cause of the low RSSI in the hotel room?

A. The AP in the room is using ZigBee instead of Wi-Fi.

B. The AP in the room is transmitting on channel 13 and the traveler associated to a non-channel 13 AP located elsewhere.

C. The switchport that the AP is connected to is only capable of transmitting at 10 Mbps.

D. The AP in the room is using Bluetooth instead of Wi-Fi.

ANSWER: B

Explanation:

The AP in the room is transmitting on channel 13 and the traveler associated to a non-channel 13 AP located elsewhere. This is the most likely explanation because 2.4 GHz channel availability is controlled by a client device's regulatory-domain configuration. European deployments can use channels through channel 13, while North American client configurations have historically limited operation to channels 1 through 11. If the in-room AP uses channel 13 and the traveler's laptop does not support or actively scan that channel under its current regulatory settings, the laptop cannot use the nearby AP despite its physical proximity. It may instead associate to another AP advertising the same SSID on a supported channel, such as an AP farther down the hall or in another part of the hotel. RSSI is a measurement of the received signal from the AP to which the client is actually associated, so that distant association produces the observed low RSSI. In the lobby, the client can associate to a nearby AP operating on a channel it supports, resulting in normal signal strength. Regulatory-domain and country-code behavior is therefore a key client-compatibility consideration in enterprise WLAN design, particularly for international travelers. See CWNP's CWDP certification overview and Cisco's regulatory domains guidance.

QUESTION NO: 8

A museum requires its wireless access points to be discreetly integrated into the environment without sacrificing performance. Which design choice best meets this requirement while maintaining optimal functionality?

A. Lock the AP inside of a metal box

B. Place the APs in between walls and I-beams

C. Use an 802.11b AP, so it looks old enough to be in a museum

D. Use a plastic cover that could blend in with the environment

ANSWER: D

Explanation:

Use a plastic cover that could blend in with the environment is the best choice because a properly selected nonmetallic enclosure or concealment cover can preserve the access point's RF performance while allowing the device to fit the museum's architectural and exhibit aesthetics. Plastic and other RF-transparent materials generally have far less effect on Wi-Fi propagation than conductive materials, provided the cover is designed for the AP, does not obstruct ventilation, and is not excessively thick or placed directly against the antenna system. A design professional should validate the selected cover and mounting arrangement through predictive design assumptions and, ideally, post-installation verification, since material composition, paint, nearby structures, and antenna placement can still affect coverage and capacity. The solution also supports practical deployment requirements: the AP remains serviceable, can use current Wi-Fi standards and security capabilities, and can be placed according to the RF design rather than hidden in a location that undermines the cell design. CWNP design guidance emphasizes accounting for building materials and installation environment during WLAN design, including the RF effects of obstacles and mounting choices. See CWNP's CWDP certification overview at https://www.cwnp.com/certifications/cwdp/ and Cisco's guidance on access-point placement and environmental considerations at https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-6/b_Cisco_Wireless_Deployment_Guide_8_6/b_Cisco_Wireless_Deployment_Guide_8_6_chapter_010.html.

QUESTION NO: 9

Main Topic:Designing for Specific Applications

Question:

Location technology (RTLS) can use which of the following methods? (Choose all that apply.)

A. Sound

B. 802.11-capable laptops

C. Active RFID

D. Infrared

E. UHV

F. UWB

G. Passive RFID

ANSWER: A B C D F G

Explanation:

RTLS is an application category rather than a single radio technology, so deployments can use several sensing and signaling methods according to the required accuracy, coverage, tag cost, battery life, and environment. Sound, most commonly ultrasonic signaling, can determine distance from measured propagation time. 802.11-capable laptops can act as Wi-Fi client devices whose received-signal measurements or other Wi-Fi location techniques are used to estimate their position through the WLAN infrastructure. Active RFID uses battery-powered tags that periodically transmit, enabling location across a reader or receiver network. Passive RFID can establish the presence or location of a tagged item when it is energized and read near an RFID reader. Infrared is also used for room-level or zone-level location where optical coverage is appropriate. UWB supports highly accurate ranging and positioning because its wide-band signals enable precise time-based measurements. These technologies may be deployed independently or combined, with the chosen method driven by the precision and operational requirements of the RTLS use case. The Wi-Fi Alliance describes Wi-Fi location capabilities at Wi-Fi Location, and the FCC provides technical information on UWB operations at Ultra-Wideband.

QUESTION NO: 10

Main Topic:Infrastructure Design

Question:

An enterprise customer is subject to the highest standards for network uptime. When designing their wireless network, you should consider which of the following? (Choose all that apply)

A. The failover of the wireless network only

B. The failover of the wired network only

C. The failover of the wireless and wired network

D. The physical aspects such as power and cabling

ANSWER: C D

Explanation:

“The failover of the wireless and wired network” is essential because wireless availability depends on an end-to-end service path, not merely on access points. A highly available design considers resilient access-layer connectivity, redundant switching and uplinks, alternate paths to network services, and high availability for the systems that provide WLAN control and services. The wireless infrastructure must be able to continue serving clients, or recover rapidly, when a component or path fails; likewise, the wired infrastructure carrying access-point traffic must not create a single point of failure.

“The physical aspects such as power and cabling” are equally fundamental to uptime. Access points, switches, controllers, and associated services require reliable power delivery, appropriate backup power where required by the availability target, and resilient, properly designed cabling pathways. Physical infrastructure should be assessed for failure domains so that a localized power, cable, or equipment failure does not unnecessarily affect a broad portion of the WLAN. CWNP’s CWDP curriculum includes designing WLAN infrastructure to meet organizational requirements, while Cisco’s enterprise campus guidance describes resilient physical and network infrastructure as a key availability consideration. See [CWNP CWDP certification information] and [Cisco Enterprise Campus Network Design].

QUESTION NO: 11

Which one of the following might be detected as a source of CCI during a post-validation survey in the 5 GHz band?

A. Other OFDM networks

B. Other ERP networks

C. Microwave ovens

D. Other HR/DSSS networks

ANSWER: A

Explanation:

Other OFDM networks is correct because co-channel interference (CCI) occurs when multiple Wi-Fi transmitters use the same RF channel and their signals overlap at a receiving location. During a post-validation survey in the 5 GHz band, an analyzer or survey tool can identify neighboring or otherwise unmanaged 5 GHz WLANs operating on the same channel as the designed WLAN. These networks may use OFDM-based PHYs, including 802.11a, 802.11n, 802.11ac, or 802.11ax operation in 5 GHz. Their frames contend for the same shared medium, increasing channel utilization and potentially creating contention, retries, and reduced capacity. The survey should assess the signal strength, channel assignment, airtime use, and location of these co-channel transmitters to determine whether they materially affect the design’s capacity and performance objectives. CCI is not necessarily a physical-layer collision every time two APs share a channel; when devices can detect one another, CSMA/CA coordination and deferral are expected. Nevertheless, excessive same-channel cell overlap or significant traffic from external OFDM WLANs consumes airtime and is a key post-validation finding. CWNP’s Wi-Fi design material identifies CCI as a same-channel Wi-Fi condition requiring proper channel reuse and cell-size design. See [CWNP CWDP certification] and the IEEE [802.11 wireless LAN standard].

QUESTION NO: 12

Which definition correctly describes the "local MAC" variation of the centralized WLAN architecture?

A. All MAC functions are performed by the AP. A minimal subset of network control is offloaded to the WLAN controller along with management and monitoring functions.

B. PHY functions are performed directly by the AP. MAC functions are divided almost equally between the WLAN controller and the AP, according to the time sensitivity of the feature or service.

C. The AP provides the RF termination point for the WLAN, but performs very few of the WLAN functions or services. The WLAN controller performs all MAC functions and the AP is very simple and lightweight.

D. All RF-, data-, and control-related WLAN functions are performed by the AP. APs coordinate network services with one another and are managed by a WNMS.

ANSWER: A

Explanation:

“All MAC functions are performed by the AP. A minimal subset of network control is offloaded to the WLAN controller along with management and monitoring functions.” correctly describes the local MAC variation of a centralized WLAN architecture. In this design, the access point retains responsibility for time-sensitive IEEE 802.11 MAC-layer work at the wireless edge, where immediate handling is needed for efficient client communication and radio operation. The controller remains central to the overall WLAN system by providing management, monitoring, configuration coordination, policy-related control, and visibility across the access-point deployment. This division preserves the operational benefits of centralization without requiring every wireless MAC decision to traverse the network to a controller. Keeping MAC processing local to the AP can reduce dependency on controller-path latency for wireless operations while still allowing administrators to use centralized tools and policies. It is therefore a controller-managed architecture whose APs have substantial local intelligence, rather than a fully distributed deployment with no controller role. CWNP's CWDP certification scope includes WLAN architecture and design decisions such as where WLAN functions are performed; see the CWNP CWDP certification page and the CWNP CWNA certification page for the associated WLAN fundamentals and design domains.

QUESTION NO: 13

Which DHCP option, when required, should be configured and enabled to help APs locate their wireless LAN controller?

A. 150

B. 62

C. 43

D. 22

ANSWER: C

Explanation:

43 is correct because DHCP Option 43 carries vendor-specific information that an access point can use during its controller-discovery process. In controller-based WLAN architectures, an AP must learn the address of a compatible wireless LAN controller before it can establish its control-plane connection and complete registration. When DNS-based discovery, broadcast discovery, preconfigured controller addresses, or other supported discovery methods are not appropriate for the deployment, an administrator can configure Option 43 in the DHCP scope serving the AP management VLAN. The option payload is vendor-specific: for example, it may encode one or more controller management IP addresses in the format expected by the AP vendor. Thus, merely enabling the option is not sufficient; its value must be correctly formatted for the relevant AP/controller platform. DHCP Option 43 is especially useful when APs and controllers reside in different IP subnets and no local broadcast discovery path exists. The DHCP standard defines Option 43 as the Vendor-Specific Information option, allowing vendors to deliver this type of bootstrap information to their devices. See RFC 2132, section 9.13 and Cisco's DHCP Option 43 configuration guidance.

QUESTION NO: 14

A centralized WLAN uses WPA2-Enterprise, DHCP addressing, and DNS-based controller discovery for APs. Which components should be included in the availability plan because their failure can prevent AP operation, client connectivity, or new client authentication? (Select four.)

A. Wireless controller

B. RADIUS service

C. DHCP service

D. DNS service

E. Spectrum analyzer

ANSWER: A B C D

Explanation:

The wireless controller, RADIUS service, DHCP service, and DNS service should be included in the availability plan. The controller provides the centralized WLAN control function. RADIUS is required for new WPA2-Enterprise authentication attempts. DHCP is required for clients that need dynamically assigned IP configuration. Because the APs use DNS-based controller discovery, DNS availability is needed for APs to discover or rediscover the controller. A spectrum analyzer is valuable for RF troubleshooting, but it is not a production dependency for AP operation or client connectivity.

QUESTION NO: 15

What functions may be performed by a WIPS? (Choose all that apply.)

A. Distributed protocol analysis

B. Client access to the distribution system

C. Performance monitoring and response

D. Data forensics and analysis

E. Automated threat mitigation

ANSWER: A C D E

Explanation:

A Wireless Intrusion Prevention System operates through distributed sensors or access points that observe the RF environment and capture management, control, and data traffic for centralized or distributed protocol analysis. This visibility lets the system identify wireless threats, rogue devices, impersonation attempts, policy violations, and anomalous frame behavior. WIPS platforms can also perform performance monitoring and response by correlating RF conditions, device behavior, and WLAN events so that administrators can investigate conditions affecting reliable operation and respond according to policy.

Data forensics and analysis is a core operational capability because WIPS alerts are most useful when supported by event histories, captured frame information, device classifications, timestamps, and reporting. These records help security staff reconstruct an incident and establish its scope. Automated threat mitigation is also a WIPS function when authorized by organizational policy. Depending on the platform and deployment design, the system may initiate containment actions such as alerting integrated systems, blocking network access, or transmitting wireless countermeasures. CWNP's security curriculum describes wireless monitoring, threat detection, classification, and response as essential WLAN security capabilities. See CWNP's CWSP certification overview and Cisco's guidance on wireless intrusion prevention.

QUESTION NO: 16

Your customer's 802.11n laptops are not able to see the SSID in the 5 GHz band in the conference room. When doing a walkthrough using one of these laptops, you confirm that it is unable to see the SSID in the 5 GHz band in the conference room. When using your own 802.11ac laptop, you're able to see the SSID. What is the most likely cause of this problem?

A. The AP is configured to use channel 36

B. The customer laptop does not support Transmit Beamforming

C. The AP is on channel 144

D. Their laptops are SISO clients

ANSWER: C

Explanation:

The AP is on channel 144 is the most likely cause because 5 GHz client support is not determined solely by whether a client supports 802.11n. A client must also support the specific channel used by the access point under its hardware, firmware, and configured regulatory domain. Channel 144 is in the 5 GHz U-NII-2e range and was not implemented by many older client radios, including a substantial number of 802.11n-era adapters. Consequently, an 802.11n laptop that does not include channel 144 in its supported-channel list cannot detect beacons transmitted on that channel, so the SSID will not appear during scanning. A newer 802.11ac laptop may have a more current radio and regulatory-channel implementation that includes channel 144, which accounts for its ability to see the same SSID in the same location. This behavior is especially important during design validation: AP channel plans must account for the actual channel support of the deployed client population, rather than assuming that all 5 GHz-capable devices support every permitted 5 GHz channel. The FCC rules identify the applicable 5 GHz frequency ranges and operating requirements in 47 CFR § 15.407. Cisco also documents 5 GHz channel availability and client support considerations in its 802.11ac deployment guide.

QUESTION NO: 17

What statements are true regarding jitter and latency?(Choose all that apply.)

Response:

A. Jitter is a measurement of latency variability from one frame to another.

B. Jitter is a measurement of the variance of the number of frames received from an application for a specific time interval.

C. Jitter is a measurement of average latency based on a sample of >100 frames.

D. Latency is a measurement of the time delay experienced in the delivery of a frame.

E. Latency is a measurement of the time required to transmit two subsequent frames.

ANSWER: A D

Explanation:

Jitter is a measurement of latency variability from one frame to another. In packet-based communications, jitter describes changes in packet delay over time rather than delay itself. For real-time wireless services such as voice and interactive video, consistent packet arrival is important: even when the overall delay is acceptable, variation in arrival timing can require buffering and can affect perceived media quality. This aligns with the Internet Engineering Task Force definition of IP packet delay variation, which is based on the difference in delay experienced by selected packets. See IETF RFC 3393: IP Packet Delay Variation Metric.

Latency is a measurement of the time delay experienced in the delivery of a frame. In a WLAN design context, this represents the time associated with carrying traffic from its source toward its destination; the observed value can include transmission, processing, queuing, contention, and propagation components. Latency is therefore a delay metric, while jitter characterizes how that delay changes between packet or frame deliveries. Designing for latency-sensitive applications requires both a suitably low delivery delay and stable delivery timing. The IETF's one-way delay metric provides the underlying definition of delay for a packet traversing a network path: IETF RFC 2679: A One-way Delay Metric for IPPM.

QUESTION NO: 18

When performing a spectrum analysis walkthrough of a facility for which you will be creating a WLAN design, you detect an interferer. What should you do?

A. Make a mental note of it so that you can include it in your design

B. Make note of it using the reporting features of your spectrum analyzer or by documenting it elsewhere

C. Locate and remove the interferer immediately so that your WLAN works well

D. Walk away from the project because it is best to only deploy in clean environments with no other RF signals

ANSWER: B

Explanation:

Make note of it using the reporting features of your spectrum analyzer or by documenting it elsewhere is correct because spectrum analysis during the WLAN design process is intended to identify, characterize, and record sources of RF energy that may affect the planned network. A designer should capture useful details such as the location where the signal was observed, affected frequency range or channel, signal strength, duty cycle, and, when possible, the likely device type. This evidence allows the designer and customer to evaluate the operational impact and decide on an appropriate design response, such as avoiding affected channels, modifying AP placement, using a different band, or coordinating mitigation with the party responsible for the interfering device. Recording the observation also creates an auditable baseline for later validation and troubleshooting. The CWNP CWDP curriculum identifies spectrum analysis as a means to discover RF interference and incorporate those findings into the WLAN design rather than relying on assumptions about the RF environment. Spectrum-analysis tools commonly provide capture, classification, and reporting capabilities that support this documentation workflow. See CWNP's CWDP certification overview and Cisco's spectrum analysis overview for background on detecting and documenting RF interference.

QUESTION NO: 19

Main Topic:Designing for Specific Applications

Question:

For what purposes are VPNs typically used in modern WLANs? (Choose all that apply.)

A. Remote AP tunneling to a corporate WLAN controller or VPN concentrator

B. Client device connectivity to corporate resources from unsecured public networks

C. Initial 802.11 authentication with the AP and subsequent data encryption

D. Tunneling APs and WLAN controllers to cloud-based management platforms

E. Tunneling APs and WLAN controllers to RADIUS and token servers

F. Bridging client connectivity in ad hoc networks

ANSWER: A B

Explanation:

VPNs are typically used to create an encrypted tunnel across an untrusted IP network, preserving the confidentiality and integrity of organizational traffic when it must traverse the Internet or another network outside the organization's control. **Remote AP tunneling to a corporate WLAN controller or VPN concentrator** is a common deployment model for branch, teleworker, and temporary locations. The remote infrastructure can establish a protected connection back to the organization, allowing centrally provided network services and policy enforcement to be extended to that site without exposing internal traffic in transit.

Client device connectivity to corporate resources from unsecured public networks is also a core VPN use case. A user on hotel, airport, café, or other public Wi-Fi can establish a VPN session before accessing internal applications and resources. The encrypted tunnel protects corporate communications over the local WLAN and intermediate networks, while the VPN gateway can apply the organization's remote-access controls. NIST describes VPNs as a common means of protecting remote-access communications over public networks; its guidance is available in NIST SP 800-77 Rev. 1. NIST's remote-access security guidance also addresses protecting telework and remote connections in NIST SP 800-46 Rev. 2.

QUESTION NO: 20

During your first pre-deployment meeting with the deployment team, you hand out the full design documentation to everyone. What is your primary goal during this meeting?

A. To explain design decisions and ensure understanding of design documents

B. To discuss AP functionality

C. To explain how Wi-Fi works

D. To justify the budget

ANSWER: A

Explanation:

To explain design decisions and ensure understanding of design documents is correct because the initial pre-deployment meeting is the formal design handoff between the wireless design team and the personnel who will implement the WLAN. Providing complete documentation is useful only when the deployment team understands how to apply it: the access point placement plan, mounting requirements, antenna selections and orientations, channel and power assumptions, switch-port and cabling needs, logical network settings, and validation requirements. Reviewing the reasoning behind these choices enables installers to recognize design-critical details rather than treating the documentation as a generic installation checklist.

This meeting also establishes a shared implementation baseline. The deployment team can identify site changes, construction constraints, missing prerequisites, or ambiguities before hardware is installed. Clarifying such items early helps preserve the RF assumptions and capacity objectives established during the design process, reduces avoidable rework, and supports an effective post-installation validation survey. CWNP's CWDP curriculum identifies implementation documentation and communication with installation personnel as important elements of moving a WLAN design into deployment. See the CWNP CWDP certification overview and CWNP's CWDP-305 exam information.

QUESTION NO: 21

During requirements gathering for a WLAN that will support mobile warehouse scanners, which information should be documented before completing the RF design? (Select three.)

A. The maximum number of concurrently active scanners in each work area

B. The application response-time and roaming requirements for scanner transactions

C. The supported bands, PHY capabilities, and security methods of the scanners

D. The brand of Internet service provider used at the facility

E. The exterior color selected for the scanner enclosures

ANSWER: A B C

Explanation:

The number of concurrent devices, application performance requirements, and client radio capabilities are essential inputs to the WLAN design. The concurrent device count helps determine capacity requirements and expected airtime demand. Application requirements, such as acceptable transaction delay, packet loss tolerance, and roaming behavior, define the performance target that the WLAN must support.

Client radio capabilities are equally important because scanner capabilities may limit supported bands, channels, channel widths, security methods, data rates, roaming features, and transmit power. A design cannot assume that specialized devices behave like current laptops or smartphones. The brand of ISP circuit and the physical color of a scanner enclosure do not determine the RF cell design or WLAN capacity requirements.

QUESTION NO: 22

What might limit the ability to locate 802.11 clients using a WLAN infrastructure without an 802.11 tag? (Choose all that apply.)

A. Lack of 802.11k support

B. When its radio is disabled

C. When it is off

D. RF channel selection

ANSWER: B C

Explanation:

“When its radio is disabled” and “When it is off” are correct because infrastructure-based Wi-Fi location depends on receiving RF transmissions from the client device. Unlike a dedicated location tag, an ordinary 802.11 client is not necessarily designed to transmit location beacons at a predictable interval or at a power level optimized for tracking. The WLAN location system therefore needs the client’s Wi-Fi radio to be powered, enabled, and emitting frames that can be heard by multiple access points or sensors.

When a client’s radio is disabled, it cannot send management, control, or data frames, so the WLAN infrastructure has no RF observations from which to estimate its position. Similarly, a device that is off has no powered radio and cannot participate in Wi-Fi communications at all. In both circumstances, the system may retain a historical last-known location, but it cannot establish or update the device’s current location. This is a fundamental availability limitation for locating untagged Wi-Fi clients and should be accounted for when defining location-service requirements during WLAN design. CWNP’s CWDP certification scope includes planning and validating WLAN services such as location-related capabilities: CWDP certification overview. Cisco also describes client location as relying on wireless observations collected by the infrastructure: Cisco wireless location configuration guide.

QUESTION NO: 23

What functions do the control plane of centralized and distributed WLAN architectures help solve? (Choose all that apply.)

A. Channel reuse plans

B. Mobility management

C. Transmit power

D. Load balancing

ANSWER: A B C D

Explanation:

Channel reuse plans, mobility management, transmit power, and load balancing are all control-plane functions in WLAN architectures. The control plane makes network-wide decisions and distributes the policies or parameters needed for access points to operate cohesively. Channel reuse planning uses RF information to select and coordinate channels, reducing co-channel and adjacent-channel interference while supporting efficient spectrum reuse. Transmit-power control similarly uses RF conditions and coverage requirements to set or recommend appropriate AP power levels, helping maintain usable coverage without unnecessarily increasing contention and interference.

Mobility management is a control-plane responsibility because the WLAN must maintain client context and support roaming decisions as a station moves between APs. This includes coordinating client state and applying mobility-domain policies so that roaming can occur predictably. Load balancing also relies on a broader view than a single AP possesses: the WLAN can evaluate client counts, airtime utilization, and available capacity across neighboring APs and steer association decisions toward suitable resources. These functions may be implemented by a centralized controller or coordinated among distributed APs, but each represents control and policy logic rather than ordinary user-data forwarding. See the CWNP overview of WLAN architecture concepts at CWNP and Cisco’s discussion of wireless RF management at Cisco Wireless Controller RF Profiles documentation.

QUESTION NO: 24

Main Topic:Infrastructure Design

Question:

What are methods of providing RF high availability?

A. Power APs to maximum power.

B. Use the HSRP/VRRP protocol.

C. Deploy using 100 percent overlap.

D. Deploy 802.3af.

E. Use dual spectrums.

ANSWER: C E

Explanation:

Deploying using 100 percent overlap provides RF high availability by designing the WLAN so that a client location is within usable coverage from at least two access points. If an access point, its radio, or its power/network connection fails, clients can reassociate to another access point that already provides an adequate signal at that location. This redundancy must be engineered with an appropriate channel plan and transmit-power design so that the added coverage does not create unnecessary co-channel contention.

Using dual spectrums—more precisely, designing service across both the 2.4 GHz and 5 GHz bands—also improves RF resilience. A dual-band client can retain connectivity through the alternate band when a band becomes impaired by interference, excessive utilization, or a radio-specific problem, provided the alternate band has been designed with sufficient coverage and capacity. The bands have distinct channel resources and propagation characteristics, so each requires its own predictive and validation survey considerations. Cisco's wireless design guidance discusses redundant RF coverage and roaming design at Cisco WLAN design guidance. CWNP's wireless design curriculum overview is available at CWNP CWDP certification.

QUESTION NO: 25

While configuring your site survey software for an upcoming manual survey project, you notice the configuration option for "Network Card Simul-ation". What is the purpose of such a feature and when would you use it?

A. This setting allows the site survey software to convert the APs measured downlink RF data into a simulated data set as if the same data were transmitted by a specific client station. It is useful for determining uplink client performance when clients are located far from APs as well as projecting cell size for ad hoc networks.

B. Since WLAN adapters are not typically calibrated by manufacturers, this setting is a form of software calibration in which you can calibrate an (uncalibrated) adapter to match one of the calibrated adapters shown in the list. This process improves the reliability of RF data collection and reporting when uncalibrated adapters are used.

C. This is the configuration area in which you specify the adapter type that will be used for the site survey so that the survey software can interpret that adapter's reported metrics (based on proprietary formulas) into an RF measurement that is standardized by the survey software and known to its users. This is done for every survey.

D. The site survey software manufacturer allows you to view the collected RF data as if it were collected by a different type of adapter. This functionality allows you to review survey data to determine how the RF environment will likely look based on the receive sensitivity and other RF capabilities of a specific client.

ANSWER: D

Explanation:

The correct answer is: "The site survey software manufacturer allows you to view the collected RF data as if it were collected by a different type of adapter. This functionality allows you to review survey data to determine how the RF environment will likely look based on the receive sensitivity and other RF capabilities of a specific client." Network-card simulation applies the selected client device's radio characteristics—particularly receive sensitivity and supported capabilities—to the survey data already collected. This gives the designer a client-centric prediction of coverage, signal quality, and expected connectivity rather than treating the survey adapter as representative of every client device.

This is especially valuable when the survey was performed using a professional adapter but the WLAN must support devices with materially different radio performance, such as handheld scanners, voice devices, tablets, or legacy clients. A design can therefore be assessed against the actual client population and its requirements without repeating the entire walk survey for each adapter model. The simulation is a planning and validation aid: it helps determine whether the measured RF environment is likely to satisfy the practical receive capabilities of a target client. Ekahau describes using device profiles to account for client-device capabilities in survey and design analysis; see Ekahau: Managing Device Profiles and CWNP: Certified Wireless Design Professional.

QUESTION NO: 26

You have determined the best mounting locations for APs in a given installation. The facilities manager has asked you to change the locations for several APs due to aesthetic concerns. You suggest mounting the APs in the ideal locations and painting them so they go unnoticed in the environment. What is a valid recommendation or consideration when painting APs?

A. Always use paints with metallic dye in them to prevent potential RF propagation impact.

B. Painting APs will significantly reduce the output power.

C. Painting APs may void the product manufacturer's warranty.

D. Most AP models for indoor environments come in a variety of form factors and colors. Painting is never recommended.

ANSWER: C

Explanation:

Painting APs may void the product manufacturer's warranty. An access point enclosure, its antenna system, thermal design, LEDs, and ventilation are engineered and validated as a complete product. Applying paint can alter the RF characteristics around integrated antennas, particularly if the paint contains metallic pigments or is applied heavily. Paint may also obstruct vents, seams, connectors, reset controls, or status indicators, and it can affect the device's ability to dissipate heat. For these reasons, a wireless designer should not treat painting as a purely cosmetic facilities change. Before approving it, confirm the exact AP vendor's installation guidance and warranty terms, use only any explicitly approved paint or cover solution, and ensure the proposed treatment does not cover required openings or labels. This preserves the preferred RF mounting location while managing the operational and support risks introduced by an aesthetic modification. CWNP design guidance emphasizes considering physical installation constraints and coordinating with facilities stakeholders, while the specific permissibility of modifications remains manufacturer-dependent. See CWNP's CWDP certification overview at https://www.cwnp.com/certifications/cwdp/ and Cisco's access-point installation guidance at https://www.cisco.com/c/en/us/td/docs/wireless/access_point/1815/quick/guide/ap1815qg.html.

QUESTION NO: 27

Main Topic:Wireless Design Process

Question:

When designing for a PTP outdoor link, what important consideration should be made about local vegetation? (Choose all that apply.)

A. Leaves

B. Tree height growth

C. Water content

D. Reflection factor

ANSWER: A B C

Explanation:

Leaves, tree height growth, and water content are all important vegetation-related considerations for an outdoor point-to-point link. Foliage can introduce substantial and variable attenuation because leaves, branches, and other plant material lie in or near the RF propagation path. This effect is especially important at common outdoor WLAN and bridge frequencies, where dense foliage can reduce received signal strength and diminish fade margin. Leaf density also changes seasonally, so a path that appears acceptable during a dormant period may have materially different loss when trees are in full leaf.

Tree height growth must be considered over the expected service life of the link. A path survey should account for present and anticipated growth so that vegetation does not later intrude into the line of sight or the Fresnel zone. Water content is likewise relevant because plant tissue contains water, which absorbs RF energy and contributes to foliage loss; wetter, denser vegetation can therefore increase attenuation. A resilient design includes adequate clearance and fade margin for these foreseeable environmental changes. CWNP's CWDP objectives emphasize outdoor design considerations and RF propagation planning; see [CWNP CWDP certification information]. Vegetation attenuation principles are also addressed in [ITU-R Recommendation P.833].

QUESTION NO: 28

To ensure that your design meets the requirements of the WLAN, what should be defined in your WLAN design software that will result in different requirements at varying locations on the floor plan?

A. Requirement areas

B. Cable runs

C. Heatmap colors

D. Project name

ANSWER: A

Explanation:

Requirement areas are correct because they let the WLAN designer apply location-specific design criteria within the same floor plan. A facility rarely has uniform wireless needs throughout: an area supporting real-time voice, high-density client access, or business-critical applications may need a stronger minimum received signal strength, higher SNR, more stringent data-rate support, and greater capacity than a warehouse aisle, hallway, or low-use storage space. By drawing and configuring requirement areas in predictive design software, the designer can model these distinct targets and validate whether AP placement, transmit power, antenna selection, and channel design satisfy each area's intended service level. This supports a requirements-driven WLAN design rather than treating an entire floor as if it had one identical coverage and performance objective. CWNP's design curriculum emphasizes gathering requirements and translating them into measurable RF and capacity design targets before validation. Predictive-design platforms also document the use of requirement areas to establish separate coverage and capacity thresholds for selected portions of a plan. See the [CWNP Certified Wireless Design Professional certification overview] and the [Ekahau documentation on requirements].

QUESTION NO: 29

When designing an outdoor point-to-point WLAN bridge, which physical-installation factors should be evaluated in addition to the RF link budget? (Select three.)

A. Fresnel-zone clearance along the complete path

B. Lightning protection and grounding requirements

C. Mounting-structure suitability for wind and weather loading

D. The number of SSIDs broadcast by indoor APs

E. Maximum transmit power on unrelated indoor APs

ANSWER: A B C

Explanation:

Fresnel-zone clearance, lightning and grounding requirements, and structural suitability for wind loading are important physical-installation factors. A visually unobstructed path may still be unreliable if terrain, vegetation, or structures intrude into the Fresnel zone. Outdoor equipment and mounting structures must be designed in accordance with applicable grounding, surge-protection, and installation requirements. The mounting point must also withstand expected wind and weather loading without movement that misaligns the antennas. A larger SSID count or maximum AP transmit power does not address these physical deployment risks.

QUESTION NO: 30

In an RSN requiring low-latency reassociations and no fast secure roaming protocols, what security solutions are ideal for protecting VoWiFi communication?(Choose all that apply.)

Response:

A. WPA2-Personal

B. WPA-Personal

C. WPA2-Enterprise

D. WEP

E. 802.1X/EAP

ANSWER: A C

Explanation:

WPA2-Personal and **WPA2-Enterprise** are appropriate RSN security solutions for VoWiFi because both provide robust link-layer protection using AES-CCMP and the RSN key-management framework. WPA2-Personal is often well suited to smaller or device-managed voice deployments: after the pre-shared-key-based PMK is available, reassociation can use the normal RSN four-way handshake to establish fresh temporal keys without performing a full enterprise authentication exchange. WPA2-Enterprise is appropriate where per-user or per-device credentials, centralized policy, and access control are required. Although an initial 802.1X/EAP authentication may take longer, a previously established PMK can be retained and reused through PMK caching where supported, reducing reassociation disruption even when a dedicated fast-roaming mechanism is not deployed. This helps preserve voice quality while maintaining strong authentication, key derivation, and encryption. The Wi-Fi Alliance identifies WPA2 as a security certification based on robust 802.11i/RSN protections, and CWNP's CWDP curriculum treats RSN authentication, encryption, and roaming behavior as key WLAN design considerations. See the Wi-Fi Alliance security overview and CWNP CWDP certification overview.

QUESTION NO: 31

During lunch time in the break room of a company, Wi-Fi connectivity on the 2.4 GHz band is intermittent. Every other time of the day, it works fine. What's the likely cause of this issue?

A. Employees are using their cell data instead of using the Wi-Fi

B. The AP in the cafeteria keeps rebooting due to lack of PoE budget on the switch

C. Microwaves in the cafeteria are interfering with the Wi-Fi on the 2.4 GHz band

D. Toasters and ovens are heating up the air, raising the noise floor with the Wi-Fi on the 2.4 GHz band

ANSWER: C

Explanation:

Microwaves in the cafeteria are interfering with the Wi-Fi on the 2.4 GHz band is the likely cause because microwave ovens operate using energy centered around 2.45 GHz, directly within the 2.4 GHz ISM band used by 802.11b/g/n and some 802.11ax WLAN operation. The strong time correlation is the important diagnostic clue: connectivity is intermittent specifically at lunch, when microwave use is expected to increase, and is normal during the rest of the day. Leakage from an operating microwave oven can create non-Wi-Fi radio-frequency interference that raises the effective noise level at nearby access points or clients. This can reduce signal-to-noise ratio, corrupt frames, cause retries, lower data rates, and make client connectivity appear unstable. The impact is usually localized and may vary based on distance, microwave shielding condition, client location, and which 2.4 GHz channel is in use. A wireless design and troubleshooting process should validate the suspected interference with spectrum analysis during the affected period, then mitigate it through channel and band-use planning, client migration to 5 GHz or 6 GHz where available, and physical separation or repair/replacement of the interfering appliance. CWNP identifies microwave ovens as a common non-Wi-Fi interferer in the 2.4 GHz band. See CWNP CWDP certification information and Wi-Fi Alliance information on Wi-Fi bands.

QUESTION NO: 32

Main Topic:Designing for Specific Applications

Question:

For what purpose is SSID hiding generally useful? (Choose all that apply.)

A. Preventing guests from attempting to join the secured corporate network

B. Obscuring the network name from potential attackers

C. Minimizing help desk calls from users and guests attempting to join the wrong network

D. Preventing legitimate corporate users from finding the guest network

ANSWER: A C D

Explanation:

SSID hiding is generally useful as an administrative and usability measure, rather than as a security control. **Preventing guests from attempting to join the secured corporate network** is a valid use because a nonbroadcast corporate SSID is less likely to appear in a casual scan of available networks. This can help guide visitors toward the intended guest WLAN instead of encouraging attempts to connect to an internal SSID.

Minimizing help desk calls from users and guests attempting to join the wrong network is also a practical benefit. Limiting the SSIDs displayed to a particular audience can simplify the visible network list and reduce confusion in environments that offer separate employee, guest, device, or application-specific WLANs. Similarly, **Preventing legitimate corporate users from finding the guest network** can be useful when the design goal is to steer managed corporate clients toward the corporate WLAN and avoid inadvertent use of a guest service.

Hidden SSIDs must not be treated as protection against attack. Clients disclose the SSID in management traffic when attempting to locate or join the WLAN, and wireless analysis tools can observe that traffic. CWNP design guidance therefore treats SSID suppression as a way to reduce casual visibility and improve user behavior, while relying on authentication, encryption, segmentation, and policy enforcement for actual security. See CWNP CWDP certification information and the Wi-Fi Alliance security overview.

QUESTION NO: 33

What might limit the ability to locate 802.11 clients using a WLAN infrastructure without an 802.11 tag?

A. Lack of 802.11k support

B. When its radio is disabled

C. When its radio is disabled

D. When it is off

E. Lack of 802.11k support

F. When its radio is disabled

G. When it is not authenticated

ANSWER: D

Explanation:

When it is off is correct because WLAN-based client location requires the infrastructure to receive RF transmissions from the client. In a tagless design, access points derive location estimates from ordinary 802.11 activity, such as probe requests, authentication and association exchanges, management traffic, or data frames. Multiple APs can use measurements such as received signal strength to estimate the client's position. A device that is powered off cannot transmit any 802.11 frames, so there is no signal for APs or a location engine to measure, correlate, or use in a location calculation. Consequently, the WLAN infrastructure has no RF evidence from which to determine that device's current location. This is a fundamental operational limitation of using the Wi-Fi client itself as the location source rather than a dedicated tag, whose radio is designed to transmit location-related frames or telemetry. Cisco's location-services documentation describes location processing based on wireless-device observations collected by access points, while CWNP's enterprise WLAN design material identifies location services as a WLAN design application that depends on client RF activity. See Cisco Wireless Controller Location Configuration Guide and CWNP CWDP certification overview.