DUMPSARENA

Certified Wireless Design Professional

CWNP CWDP-304

Version Demo

Total Demo Questions: 30

Total Premium Questions: 301

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, WLAN Design Fundamentals	123
Topic 2, Requirements Gathering	25
Topic 3, WLAN Design	70
Topic 4, Site Surveys	37
Topic 5, WLAN Validation	29
Topic 6, WLAN Documentation	17
Total	301

QUESTION NO: 1

What are some significant drawbacks that are present with WPA/WPA2-Enterprise that are not present with WPA/WPA2-Personal?(Choose all that apply.)

Response:

A. WPA/WPA2-Enterprise does not support the use of usernames/passwords for client authentication.

B. WPA/WPA2-Enterprise often requires additional backend infrastructure components that are not required with WPA/WPA2-Personal.

C. WPA/WPA2-Enterprise often requires more administrative overhead for configuration than WPA/WPA2-Personal.

D. WPA/WPA2-Enterprise always requires X.509 certificates for server authentication.

E. WPA/WPA2-Enterprise does not provide a way to perform per-user authorization and access control.

ANSWER: B C

Explanation:

WPA/WPA2-Enterprise often requires additional backend infrastructure components that are not required with WPA/WPA2-Personal. Enterprise authentication is based on IEEE 802.1X and Extensible Authentication Protocol methods, which normally require an authentication, authorization, and accounting service such as a RADIUS server. The wireless infrastructure must be configured to communicate with that service, and the RADIUS service commonly integrates with a directory, identity store, certificate authority, or other source of user and device credentials. By contrast, Personal mode uses a pre-shared key and does not need that centralized authentication infrastructure.

WPA/WPA2-Enterprise often requires more administrative overhead for configuration than WPA/WPA2-Personal. Administrators must select and deploy suitable EAP methods, configure supplicant profiles, maintain RADIUS policies, manage identity lifecycle processes, and, when certificate-based EAP is used, handle certificate issuance, renewal, trust, and revocation. These activities provide important enterprise benefits, including individual authentication and policy enforcement, but they increase deployment planning and ongoing operational effort. Microsoft's overview of Network Policy Server describes its role as a RADIUS server for centralized network-access policies, while the Wi-Fi Alliance describes Enterprise security as an 802.1X-based authentication framework: Microsoft Learn: Network Policy Server and Wi-Fi Alliance: Wi-Fi Security.

QUESTION NO: 2

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 the client producing RF transmissions that access points can receive and report to a location engine. Common techniques use received signal information from client frames, such as data, management, and probe-request frames, to estimate the device's position relative to multiple APs. A client whose Wi-Fi radio is disabled cannot transmit or receive 802.11 frames, so the WLAN has no RF observations from which to derive a location. Similarly, a device that is powered off produces no Wi-Fi activity and therefore cannot be located through the WLAN infrastructure. This limitation applies specifically to locating ordinary client devices without a dedicated 802.11 location tag: unlike purpose-built tags, a normal client is not guaranteed to send periodic beacons solely for location tracking. Location accuracy and update frequency consequently depend on the

client being powered, having its WLAN radio enabled, and generating detectable Wi-Fi traffic. Cisco's location-services overview describes use of Wi-Fi signal measurements for client location, while the IEEE 802.11 standard defines the wireless MAC and PHY behavior on which those observable transmissions rely. See Cisco Wi-Fi location services overview and IEEE 802.11 standard.

QUESTION NO: 3

One of your customers plans on providing wireless coverage to a warehouse facility. After performing an initial walkthrough, you collect the

following information:

The central part of the warehouse is between 400 and 600 feet (122 to 183 meters) from the warehouse switches mounted on the walls.

☞ The warehouse storage is composed of metallic racks with varying inventory levels and contents, from electronics and plastic toys to food

pallets and juice bottles.

☞ Workers need basic data coverage from their working location, and are not highly mobile. They usually work from one single aisle, and their

laptop is on a cart with wheels.

What would be your one recommendation to provide coverage to the central area of the warehouse?

A. Equip workers laptops with a directional antenna and install APs less than 328 feet (100m) away from the switch.

B. In this case, extend the cable length just beyond 328 feet (100 m) and position APs as close as possible to the central area of thewarehouse.

C. Position APs along the walls, and equip the APs with Yagi antennas to cover the central area.

D. Install APs for client access in the central area and use a mesh backhaul link to connect to the DS.

ANSWER: A

Explanation:

Equip workers laptops with a directional antenna and install APs less than 328 feet (100m) away from the switch is the appropriate recommendation. Copper Ethernet horizontal cabling, including its channel components, is designed around a maximum 100-meter channel distance. Keeping each AP within that limit preserves standards-compliant Ethernet and PoE operation without relying on an unsupported extended copper run. The APs can therefore be placed at practical wired locations near the warehouse perimeter or aisle ends.

A directional antenna at each cart-mounted laptop is well suited to this operational model. The workers are largely stationary in a single aisle rather than continuously roaming throughout the facility, so antenna orientation can be selected for the relevant serving AP and need not support frequent changes in direction. Directionality supplies additional link gain and reduces reception of reflected energy and interference from other directions. That is valuable in an environment containing metal racks and inventory whose RF attenuation and reflection characteristics change as stock changes. The improved client-side link budget supports the stated goal of reliable basic data coverage over the longer indoor RF path while retaining valid wired AP uplinks. See the IEEE 802.3 Ethernet standard overview and Cisco's Antenna Reference Guide.

QUESTION NO: 4

What is the DSCP Per Hop Behavior equivalent classification of the 802.11 AC_VO priority level?

A. AF31

B. CS3

C. VO

D. EF

ANSWER: D

Explanation:

EF is the appropriate DSCP Per-Hop Behavior classification for the 802.11e/WMM voice access category, AC_VO. In an end-to-end QoS design, interactive voice media requires very low delay, jitter, and loss. The Expedited Forwarding PHB is specifically defined to provide this type of preferential forwarding behavior, making it the conventional Layer 3 marking for voice bearer traffic. EF uses DSCP decimal 46 (binary 101110), and network devices can use that marking to place voice packets into priority treatment queues across routed portions of the network. At the WLAN edge, QoS policy commonly maps voice-classified traffic into WMM's voice access category so that it receives the enhanced contention parameters associated with AC_VO. This preserves the intended priority as traffic moves between the wired IP network and the 802.11 medium. RFC 3246 defines the Expedited Forwarding PHB and its low-loss, low-latency forwarding objective: RFC 3246. RFC 4594 also identifies EF as the recommended DSCP for telephony/voice-admit traffic in a QoS service-class model: RFC 4594.

QUESTION NO: 5

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

Response:

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 a broad category of systems that determine or report the location of people, devices, or assets. It is not limited to a single radio technology. **Sound** can be used in acoustic or ultrasonic location systems, where propagation time or signal characteristics support position estimation. **802.11-capable laptops** can be located through Wi-Fi-based location services using received signal strength, angle, timing, or association and telemetry data collected by the WLAN infrastructure. Both **Active RFID** and **Passive RFID** support asset-location workflows: active tags transmit using their own power, while passive-tag deployments can establish an asset's presence or location at readers, portals, or defined zones. **Infrared** is also used for room-level or zone-level tracking, often where line-of-sight detection is appropriate. **UWB** is a major RTLS technology because its wide bandwidth enables highly accurate ranging and position estimation, commonly using time-of-flight techniques. CWNP's CWDP body of knowledge treats location design as a consideration across WLAN and complementary location technologies. See the CWNP CWDP certification overview and the Bluetooth SIG overview of direction finding and location for related location-system concepts.

QUESTION NO: 6

Before performing a pre-deployment passive RF survey of a new deployment using survey mapping software, which of the following must be performed?

A. Determining AP transmit power

B. Scaling the map

C. Selecting antennas

D. Checking client DTPC settings

ANSWER: B

Explanation:

Scaling the map must be performed before conducting a survey using mapping software because the software needs a known real-world distance to relate collected RF measurements to physical locations. A floor-plan image, PDF, or CAD drawing initially has only graphical dimensions; it does not inherently tell the application how many feet or meters are represented by a line on the drawing. By setting the map scale against a reliable reference, such as a documented building dimension, the survey tool can accurately calculate distances, display the survey path in the correct physical context, and produce meaningful coverage and signal-level visualizations. Accurate scaling also supports dependable placement of measurement points and later comparison of RF behavior across areas of the facility. This foundational step ensures that the resulting design and survey deliverables correspond to the actual building rather than an arbitrary image coordinate system. CWNP's CWDP certification scope includes the use of site-survey and design information to create reliable WLAN designs; see the CWDP certification overview. For practical mapping workflow guidance, see Ekahau's instructions for setting floor-plan scale.

QUESTION NO: 7

You are tasked with designing the WLAN to accommodate certain high density areas on your university campus where users frequently come and

go. With a limited DHCP pool size (subnet mask = 255.255.252.0) for this WLAN subnet, you want to ensure that your DHCP addresses are used

efficiently and are not exhausted, which would prevent new client Layer 3 connections. The DHCP server is a Windows Server 2012 R2 machine.

Your design task is to determine the best configuration to allow as many users as possible while avoiding WLAN service interruptions and also to

use the available addresses as efficiently as possible.

What setting would be most effective at achieving this design task?

A. Set the RTS threshold to 2346 bytes

B. Set the inactive wireless client timeout (client age-out) to 5 minutes

C. Set the maximum client limit per radio to 64

D. Set the DHCP lease for this pool to 20 minutes

ANSWER: D

Explanation:

Set the DHCP lease for this pool to 20 minutes. A /22 DHCP scope has 1,022 usable IPv4 addresses after excluding the network and broadcast addresses, so address availability can become the limiting factor in a high-turnover university WLAN. DHCP leases remain allocated after a client leaves until the lease expires or the client explicitly releases it, and many mobile devices simply disappear from the WLAN without sending a release. A relatively short lease therefore returns addresses from departed users to the available pool promptly, allowing new clients to obtain Layer 3 connectivity.

A 20-minute duration is also practical for an area where clients come and go frequently. Clients that remain associated and connected renew their leases before expiry, typically beginning at half of the lease duration, so they can continue service without interruption when the DHCP service is reachable. Windows DHCP supports configuring a scope-specific lease duration, allowing this busy WLAN scope to use a shorter value without imposing the same policy on less transient networks.

Microsoft describes DHCP lease administration and scope configuration in its DHCP overview; the associated DHCP deployment guidance covers scope-based DHCP service configuration.

QUESTION NO: 8

Prior to meeting with the customer for the first time, you should do which of the following?

Response:

A. Decide which vendor they will benefit most from.

B. Research the customer as much as possible. Try to understand what their business is, who their customers are, and any other information you can find regarding product lines and recent press announcements.

C. Find out what vendor their competitors use.

D. Plan an initial design to present to them.

ANSWER: B

Explanation:

Research the customer as much as possible. Try to understand what their business is, who their customers are, and any other information you can find regarding product lines and recent press announcements. This is the appropriate preparation before an initial customer meeting because a wireless design engagement must begin with understanding the organization's business context and the drivers behind its technical requirements. Publicly available information about the customer's operations, products, locations, growth plans, users, and recent announcements helps the designer ask relevant discovery questions rather than making assumptions. It also makes it easier to identify likely WLAN considerations, such as customer-facing connectivity, mobility workflows, device types, security obligations, capacity needs, or planned facility changes.

Early research does not replace a formal requirements-gathering meeting or site survey. Instead, it equips the designer to structure that conversation around the customer's actual environment and objectives, establish credibility, and determine which requirements need validation. This approach aligns with the CWDP role's emphasis on gathering and documenting business and technical requirements before producing a WLAN design. CWNP describes CWDP as validating the ability to design enterprise Wi-Fi networks, including the foundational design-process skills needed to translate customer needs into an effective solution. See CWNP's CWDP certification overview and CWDP-304 exam objectives.

QUESTION NO: 9

What two 802.11 amendments deal with regulatory and transmission requirements?

Response:

A. 802.11k

B. 802.11i

C. 802.11d

D. 802.11f

E. 802.11h

ANSWER: C E

Explanation:

802.11d and **802.11h** address the operational requirements that allow WLAN devices to function legally and appropriately in differing regulatory domains. 802.11d adds country-information capabilities to management frames. An access point can advertise its country or regulatory domain along with valid channel and transmit-power constraints, enabling client devices to

select parameters authorized for that location. This is especially important for products deployed internationally, where permitted frequency bands, channels, and power levels vary by country.

802.11h extends 802.11 operation in the 5 GHz band with mechanisms designed for regulatory compliance and coexistence. Its Transmission Power Control capability supports adapting transmit power to the level required for reliable communication, while Dynamic Frequency Selection helps devices detect radar systems and move operation away from affected channels when necessary. Together, these functions support spectrum-sharing requirements and reduce interference risk while maintaining compliant WLAN operation. The IEEE 802.11 Working Group provides the standards framework at IEEE 802.11, and the regulatory context for 5 GHz DFS requirements is described by the FCC.

QUESTION NO: 10

A lecture hall will support predominantly modern dual-band clients, and the 2.4 GHz band shows excessive co-channel contention during busy periods. Which design recommendations are appropriate? (Select two.)

A. Encourage capable clients to use 5 GHz or 6 GHz operation.

B. Disable selected 2.4 GHz radios after validating legacy-device coverage.

C. Add more 2.4 GHz radios throughout the lecture hall at the same power level.

D. Increase 2.4 GHz transmit power to make each cell larger.

E. Use partially overlapping 2.4 GHz channels to create more channel choices.

ANSWER: A B

Explanation:

Encouraging capable clients to use 5 GHz or 6 GHz reduces demand on the limited 2.4 GHz spectrum and provides access to more non-overlapping channels. Disabling selected 2.4 GHz radios can also reduce co-channel contention in a dense deployment, provided that a survey confirms adequate service for any devices that still require 2.4 GHz operation.

Adding more active 2.4 GHz radios in the same area normally increases contention because the band has limited non-overlapping channels. Increasing transmit power enlarges 2.4 GHz cells and can increase co-channel interference. Configuring partially overlapping channels does not create additional independent capacity and introduces adjacent-channel interference.

QUESTION NO: 11

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

Response:

A. Leaves

B. Tree height growth

C. Water density

D. Reflection factor

ANSWER: A B

Explanation:

Leaves are an important design consideration because foliage in, or close to, the radio path can attenuate and scatter RF energy. This effect is particularly relevant for the higher frequencies commonly used by outdoor point-to-point systems, and it can vary substantially with season, moisture, and whether deciduous trees are bare or in full leaf. A path that appears clear during a winter survey may therefore have inadequate performance after spring leaf growth.

Tree height growth must also be considered because a PTP design requires more than a visually unobstructed line between antennas: it needs adequate Fresnel-zone clearance. Trees that are currently below the path may grow into the Fresnel zone over the expected service life of the link, reducing fade margin and throughput or causing intermittent outages. The site survey and link budget should account for existing canopy height, probable future growth, seasonal foliage conditions, and a clearance margin appropriate to the frequency and path length. These considerations support a durable link rather than one that works only under the conditions present on installation day. See Cambium Networks' PTP bridging guidance and the FCC's Office of Engineering and Technology resources.

QUESTION NO: 12

What strategy can be used to ensure efficient cell overlap for VoIP site surveys?

Response:

A. Measure the percentage of cell overlap using the cell overlap feature in the site survey software.

B. Increase the output power of the radio in all APs.

C. Install higher gain antennas in the APs.

D. Ensure at least two APs can be seen with appropriate signal strengths from each location.

ANSWER: D

Explanation:

Ensure at least two APs can be seen with appropriate signal strengths from each location. This is the practical design strategy for VoIP coverage because a wireless voice client must be able to discover and roam to a viable neighboring AP before its connection to the current AP becomes unusable. During a predictive design or validation survey, the designer should therefore evaluate the overlap of coverage areas at the voice-service signal threshold, rather than merely seeking broad RF coverage. The required threshold is defined by the voice client, codec, data rates, and design requirements; a commonly used planning target is approximately −67 dBm or better for both the serving and neighboring APs, together with acceptable SNR and low contention. Maintaining this redundant, usable coverage supports timely roaming and helps prevent audible gaps, dropped calls, or degraded call quality as users move. The overlap must also be engineered with an appropriate channel plan and transmit-power plan so that the neighboring AP is a real roaming candidate rather than simply a detectable signal. CWNP identifies voice applications as sensitive to latency, jitter, packet loss, and roaming behavior, all of which make verified overlapping voice-grade cells essential. See CWNP CWDP certification information and Cisco Voice over Wireless LAN design guidance.

QUESTION NO: 13 - (SIMULATION)

While configuring your site survey software for an upcoming manual survey project, you notice the configuration option for " Network Card

Simulation " . What is the purpose of such a feature and when would you use it?

ANSWER: See the explanation for the answer

Explanation:

Network Card Simulation lets the survey application model the behavior of a different Wi-Fi adapter than the physical adapter currently connected to the survey laptop. It applies that adapter's known receive sensitivity, transmit power, supported bands/channels, antenna characteristics, and sometimes data-rate/capability profile to collected survey measurements.

Use it when the survey adapter is not representative of the client devices that will use the WLAN—for example, when collecting manual survey data with a high-quality external USB adapter but designing/validating coverage for lower-power handheld scanners, tablets, VoWiFi handsets, or older client NICs. Select/simulate the target client's NIC profile so the resulting coverage, signal, and data-rate predictions reflect the intended client device rather than the survey adapter.

It is also useful when the target client hardware is unavailable during the survey. The simulation is an estimate based on the selected NIC profile; it does not replace validation with real representative clients where possible.

QUESTION NO: 14

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

A. management and monitoring functions.

B. MAC functions are divided between the controller and AP according to the time sensitivity of the feature or service.

C. performs all MAC functions and the AP is very simple and lightweight.

D. managed by a WNMS,

ANSWER: B

Explanation:

MAC functions are divided between the controller and AP according to the time sensitivity of the feature or service. This describes the local MAC (also commonly called split-MAC) model used in centralized WLAN designs. Functions requiring immediate response to radio events remain local to the access point, because the timing requirements of 802.11 frame exchanges and wireless-medium operation make a controller round trip impractical. The centralized controller retains functions that do not require that immediate per-frame response, allowing policy, configuration, and WLAN-wide operational control to be administered centrally while the AP handles latency-sensitive radio duties locally.

This division is fundamental to scalable enterprise WLAN architecture: the controller supplies centralized control and consistency, while AP-local processing protects time-critical wireless behavior from controller-path latency. CWNP's CWDP certification scope includes centralized WLAN architectures and the placement of MAC-layer functions as a core design consideration. See the CWNP Certified Wireless Design Professional certification overview and the CWDP exam objectives for the architecture and design domains covered by the certification.

QUESTION NO: 15

A table of VLANs in a _____ document should include what device performs _____ services.(Fill in the blanks)

A. network design; DHCP

ANSWER: A

Explanation:

The correct completion is **network design; DHCP**. A network design document records the logical network services that support the WLAN, not merely RF or access-point placement details. Since VLANs define separate Layer 2 broadcast domains and normally correspond to distinct IP subnets, the VLAN table should identify the device responsible for DHCP services for each applicable VLAN. This gives implementation teams the information needed to ensure that wireless clients associated with a particular SSID and mapped to its VLAN can receive the intended IP addressing, subnet mask, default gateway, DNS settings, and other DHCP-provided parameters. Identifying the DHCP-serving device is especially important where services are centralized, relayed across VLAN boundaries, or provided by a firewall, router, Windows server, or dedicated IP-address-management platform. It also makes the design actionable during deployment and troubleshooting by documenting service ownership and the expected path to address assignment. DHCP is the protocol used to dynamically provide host configuration parameters, as specified by the IETF in RFC 2131. CWNP's CWDP certification scope includes creating and documenting enterprise wireless designs; see the CWDP certification overview.

QUESTION NO: 16

Which of the following items could be considered constraints when performing a network design?(Choose all that apply.)

A. Timeline

B. Personnel

C. Politics

D. Budget

ANSWER: A B C D

Explanation:

Timeline, Personnel, Politics, and Budget can all constrain a wireless network design because each limits the practical solution that can be designed, approved, deployed, or supported. A timeline establishes deadlines for surveying, design, procurement, installation, migration, and validation; the design may need to be phased to meet an operational date. Personnel constrains the available technical skills, installation resources, and ongoing operational capacity, affecting choices such as architecture complexity and management tooling. Politics includes organizational priorities, stakeholder influence, approval processes, departmental ownership, and policy requirements that can determine acceptable designs and rollout sequencing. Budget constrains equipment selection, licensing, cabling, power improvements, professional services, and spare capacity. CWDP design work requires identifying and documenting such business and technical constraints as part of requirements gathering so that the recommended WLAN is both technically appropriate and feasible for the customer. This aligns with the CWNP CWDP certification's focus on translating customer requirements into a viable wireless design and with general project-management practice of balancing schedule, resources, stakeholder conditions, and cost. See the CWNP CWDP certification overview and the Project Management Institute discussion of project constraints.

QUESTION NO: 17

During post-deployment validation, measured RF results differ significantly from the predictive model in several areas. Which conditions should be documented and, where appropriate, retested before concluding that the installed WLAN design has failed? (Select three.)

A. The operating state of movable equipment, doors, and partitions

B. Changes to furniture, storage racks, or construction materials

C. Time-varying RF interference sources and their operating schedules

D. Whether the SSID broadcast has been disabled

E. Whether an additional survey-software licence has been purchased

F. Whether users have recently changed their passwords

ANSWER: A B C

Explanation:

The operational state of movable equipment, doors, and partitions can alter attenuation and multipath relative to the conditions assumed in the predictive model. Furniture, storage racks, and other material changes can likewise change RF propagation and should be compared with the original plans. Time-varying interference sources must be documented because a survey performed when machinery, wireless devices, or other emitters are inactive may not represent normal operating conditions.

Hiding the SSID does not affect RF propagation or the validity of survey measurements. Purchasing an additional software license may be operationally necessary for some tools, but it does not explain an RF difference between predictive and validation results. Changing user passwords is unrelated to RF validation.

QUESTION NO: 18

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?

Response:

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

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

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

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

ANSWER: A

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 regulatory-domain settings can limit the 2.4 GHz channels that a client device is permitted to use. North American client devices are commonly configured for channels 1 through 11, while European WLAN deployments may use channels 12 and 13. If the in-room AP is operating only on channel 13, a laptop restricted to the North American channel set cannot join that nearby radio. It may instead associate with the same hotel SSID on a more distant AP using a permitted channel, producing the reported low RSSI. In the lobby, the client likely has access to a nearby AP operating on a channel it supports, so its received signal is stronger. This behavior illustrates why WLAN designers must account for client regulatory domains and supported channel sets when planning international or hospitality deployments. The United States rules for unlicensed 2.4 GHz operation are published by the FCC, while European wideband data-transmission requirements are specified in ETSI EN 300 328.

QUESTION NO: 19

As a device starts to shift to lower PHY rates, what factors usually influence a device decision to shift to lower PHY rates?(Choose all that apply.)

Response:

A. Signal degradation

B. Packet loss

C. Interference

D. Retransmissions

ANSWER: A B C D

Explanation:

Signal degradation, packet loss, interference, and retransmissions can all contribute to a wireless client or access point selecting a lower PHY rate through its rate-adaptation algorithm. As received signal quality declines, the signal-to-noise ratio and usable modulation margin diminish. A lower PHY rate generally uses a more robust modulation and coding combination, increasing the probability that frames can be decoded successfully under degraded RF conditions. Packet loss is an important observable outcome used by many rate-control implementations, especially when the losses occur without successful MAC-layer acknowledgments. Interference can reduce frame-decoding reliability even where received signal strength appears adequate, because it raises the effective noise floor or corrupts airtime during transmission. Retransmissions provide direct feedback that prior frame transmissions were unsuccessful; repeated retries commonly cause the rate-control process to reduce the transmission rate in an effort to improve delivery reliability. The precise algorithm and thresholds are vendor- and driver-specific, but these RF conditions and transmission results are the practical inputs that drive downward rate adaptation. See the IEEE 802.11 overview at IEEE 802.11 Working Group and Cisco's discussion of wireless data rates at Cisco Wireless LAN data-rate guidance.

QUESTION NO: 20

An outdoor point-to-point WLAN bridge uses a radio with a maximum conducted transmit power of 15 dBm and an antenna with 9 dBi gain. Ignore cable loss. The regulatory limit for the selected channel is 20 dBm EIRP.

What is the highest conducted transmit-power setting that complies with the limit?

A. 9 dBm

B. 11 dBm

C. 15 dBm

D. 20 dBm

ANSWER: B

Explanation:

11 dBm is correct. EIRP is calculated by adding conducted transmit power and antenna gain when cable loss is ignored. To remain at or below 20 dBm EIRP with a 9 dBi antenna, the radio can be configured for no more than 11 dBm conducted power: 11 dBm + 9 dBi = 20 dBm EIRP.

Configuring 15 dBm would produce 24 dBm EIRP and exceed the stated limit. The other values are compliant but do not represent the highest allowable conducted transmit-power setting.

QUESTION NO: 21

Left to its simplest form, what method does a location algorithm use to determine location within a WLAN coverage area?

Response:

A. Inverse cube law

B. FSPL

C. RF fingerprinting

D. 802.11 clause 16

ANSWER: B

Explanation:

FSPL is correct because, at its most basic level, WLAN location estimation relates a client's received signal level to its estimated distance from known access-point locations. The free-space path-loss model expresses the expected reduction in RF signal power as distance and frequency increase. A location system can use received signal strength measurements and a path-loss estimate to derive approximate ranges to multiple access points, then combine those ranges to estimate a position within the coverage area. In practical enterprise WLANs, walls, floors, people, antenna patterns, multipath, and attenuation make actual propagation substantially more complex than ideal free space. Consequently, production location systems commonly apply calibration data, environmental models, confidence calculations, and other refinements. Nevertheless, FSPL is the fundamental simplified propagation relationship underlying the conversion of RF signal measurements into distance estimates for this type of location calculation. The ITU's propagation recommendation defines free-space basic transmission loss and its relationship to frequency and distance: ITU-R Recommendation P.525. CWDP design knowledge includes applying RF behavior and propagation principles to WLAN design decisions: CWNP CWDP certification.

QUESTION NO: 22

When analyzing published competitive tests by equipment vendors, what items are the tests usually lacking?(Choose all that apply.)

Response:

A. Client devices and configurations

B. Audit by a third party

C. Detailed test methodology

D. Detailed configurations of each vendor's equipment

ANSWER: A B C D

Explanation:

Published competitive testing should be treated as vendor-supplied evidence rather than as a fully reproducible, independent evaluation. The information needed to determine whether results apply to a specific WLAN design is commonly incomplete. **Client devices and configurations** are essential because client radios, drivers, antenna capabilities, roaming behavior, power-save settings, and traffic-generation tools materially affect observed WLAN performance. **Detailed test methodology** is needed to establish repeatability: it should identify the test environment, RF conditions, traffic profiles, measurement intervals, load levels, pass/fail criteria, and how results were calculated. Likewise, **Detailed configurations of each vendor's equipment** are necessary to verify that compared systems used equivalent channel widths, transmit-power settings, software versions, feature settings, and capacity-related parameters. An **Audit by a third party** provides independent validation that the published procedure, configuration, and reporting were applied consistently and that conclusions are not solely controlled by an interested vendor. These details enable a wireless designer to assess relevance, fairness, and reproducibility before using competitive claims in a technology recommendation. CWNP's design curriculum emphasizes validating requirements and conducting defensible design and validation work; see CWNP CWDP certification. For an example of the level of documented procedure expected in formal interoperability testing, see the Wi-Fi Alliance certification program.

QUESTION NO: 23

A customer requires WPA2/WPA3-Enterprise authentication for corporate users, with access policy based on directory-group membership. Which existing infrastructure components should be reviewed during requirements gathering? (Select three.)

A. RADIUS service

B. Directory service

C. Certificate infrastructure

D. Web proxy service

E. Network Time Protocol service

F. Wireless intrusion prevention system

ANSWER: A B C

Explanation:

The RADIUS service, directory service, and certificate infrastructure should be reviewed. The RADIUS service processes 802.1X/EAP authentication requests and can return authorization attributes. A directory service commonly supplies the identities and group memberships used by authentication policies. Certificate infrastructure is relevant when the selected EAP method uses server certificates, client certificates, or both.

A web proxy may be relevant to Internet-access policy but is not a required component of Enterprise WLAN authentication. NTP supports reliable timekeeping and can be operationally important, but it does not provide identity or authorization decisions. A wireless intrusion prevention system performs monitoring and threat-response functions rather than authenticating corporate users.

QUESTION NO: 24

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 use the IEEE 802.11i/WPA2 security architecture with AES-CCMP data confidentiality and integrity protection. AES-CCMP provides the robust link-layer protection expected for voice traffic while avoiding the legacy security weaknesses associated with earlier WLAN security schemes. WPA2-Personal is often suitable where a managed pre-shared key deployment is practical; after association, a client can complete the WPA2 key-establishment exchange without an external authentication transaction. WPA2-Enterprise is appropriate where per-user or per-device authentication, centralized authorization, and credential lifecycle management are required. In an Enterprise deployment, PMK caching can reduce reassociation delay by allowing a client to reuse previously derived keying material when returning to an access point in the same mobility domain, rather than performing a complete EAP exchange again. This is valuable for maintaining voice-call continuity when a dedicated fast-roaming mechanism is not deployed. EAP is used within WPA2-Enterprise to establish authentication and keying material, while WPA2 supplies the complete protected WLAN access framework. See NIST's Guide to IEEE 802.11i and the IETF's Extensible Authentication Protocol specification.

QUESTION NO: 25

What VoWiFi implementations frequently require multicast packet delivery support by the WLAN infrastructure?

A. All VoWiFi implementations

B. Push-to-Talk VoWiFi phones

C. All VoWiFi soft phones

D. All VoWiFi hard phones

ANSWER: B

Explanation:

Push-to-Talk VoWiFi phones frequently require multicast delivery because push-to-talk service is commonly based on group communications rather than only one-to-one calling. When a user transmits to a talk group, the same audio stream may need to reach many subscribed handsets simultaneously. Multicast enables the WLAN infrastructure to distribute one stream toward the group, instead of requiring a separate unicast stream from the source for every listener. This makes multicast behavior an important design consideration for group voice deployments, including how multicast is enabled, forwarded across VLANs where applicable, converted to wireless delivery, and protected from excessive airtime consumption. The wireless design must also account for the fact that multicast traffic is often transmitted differently from unicast traffic and may not receive the same acknowledgement and retransmission behavior. Consequently, voice quality and group-call reliability depend on appropriately designed multicast support, radio coverage, and capacity. Cisco's multicast deployment guidance discusses multicast forwarding considerations in wireless LANs, including the relationship between multicast applications and WLAN delivery behavior: Cisco Multicast Deployment Guide. RTP also supports delivery to multicast group addresses, a foundation used by real-time group-media applications: RFC 3550: RTP.

QUESTION NO: 26

In the enterprise, when is WPA/WPA2-Personal generally a recommended solution?(Choose all that apply.)

Response:

A. When client devices do not support 802.1X/EAP

B. When mobile device applications require high-latency roaming times between APs

C. When client devices are provisioned in bulk and would otherwise share 802.1X credentials

D. When the network security policy demands that each user have unique access credentials

ANSWER: A C

Explanation:

WPA/WPA2-Personal is generally appropriate when client devices do not support 802.1X/EAP. Personal mode authenticates stations with a pre-shared key, so it does not require the client-side EAP supplicant capability, certificate handling, or RADIUS-based authentication workflow required by Enterprise mode. This makes it a practical compatibility choice for legacy, constrained, or specialized devices that cannot participate in an 802.1X authentication exchange.

It is also appropriate when client devices are provisioned in bulk and would otherwise share 802.1X credentials. Sharing an individual 802.1X identity across many devices defeats the accountability and identity-management benefits normally associated with Enterprise authentication. For a managed group of similar devices, a deliberately assigned shared PSK can be operationally simpler than deploying one shared EAP account. The PSK should still be protected, changed when device-group membership changes, and limited to an appropriate network segment. Wi-Fi security guidance distinguishes Personal security, based on a shared password, from Enterprise security, which uses centralized per-user or per-device authentication. See the Wi-Fi Alliance security overview and Microsoft's WPA2-Enterprise configuration guidance.

QUESTION NO: 27

Given: In a site survey deliverable report, you are expected to explain the spectrum measurements taken at the customers site. What portion of a

spectrum analyzer view can be used to determine if a given channel is too active for use as the active channel for a new AP?

A. Device list

B. Frame decode

C. Real time FFT

D. Duty cycle

ANSWER: D

Explanation:

Duty cycle is the appropriate spectrum-analyzer measurement for deciding whether a channel is too active to be a suitable operating channel for a new access point. Duty cycle represents the percentage of observed time that RF energy is present in a frequency range or channel. Because Wi-Fi uses a shared, contention-based medium, substantial existing RF activity reduces the available airtime for the new AP and its clients. A high duty-cycle reading therefore indicates that the channel is already occupied for a significant portion of time, whether by Wi-Fi transmissions or non-Wi-Fi interferers, and should be avoided where a lower-utilization channel is available. In a survey deliverable, documenting duty cycle helps communicate measured channel occupancy in practical terms: it quantifies how much opportunity remains for reliable client transmissions rather than merely showing that energy was observed at some point. Measurements should be collected for an adequate observation period and at relevant survey locations so that intermittent as well as persistent activity is represented. This aligns with the CWNP emphasis on evaluating RF conditions and interference as part of a professional WLAN design and validation process. See the CWDP certification overview and MetaGeek's explanation of duty cycle.

QUESTION NO: 28

Which of the following items could be considered constraints when performing a network design?(Choose all that apply.)

Response:

A. Timeline

B. Personnel

C. Politics

D. Budget

ANSWER: A B C D

Explanation:

Timeline, Personnel, Politics, and Budget can all constrain a wireless network design because each limits the practical set of solutions that can be implemented, even when RF requirements and coverage goals are clearly defined. A timeline may limit time available for requirements gathering, predictive design, on-site validation, phased deployment, or remediation. Personnel is a constraint because the customer and implementation team must have sufficient technical skills, availability, and operational capacity to install, support, and troubleshoot the selected solution. Politics includes organizational priorities, stakeholder disagreements, approval processes, ownership boundaries, and policies that influence technology selection or deployment scope. Budget constrains equipment choices, licensing, cabling, installation labor, survey work, redundancy, and ongoing support. In a professional WLAN design, these business and organizational constraints must be identified during discovery and incorporated into documented design requirements, assumptions, and risks. Doing so helps the designer recommend an achievable architecture and set expectations for scope, performance, schedule, and cost. CWNP describes CWDP as covering the translation of business requirements into wireless design decisions, while its certification materials emphasize a requirements-driven design process. See CWNP Certified Wireless Design Professional and CWNP Certification Program.

QUESTION NO: 29

When deploying a new WLAN infrastructure using PoE to power the APs, you realize that a known good AP is not powering up. You use the same

cable to connect your laptop and connect without any trouble. What is the most likely reason the AP did not power up?

A. Missing AP licenses in the controller

B. Spanning-tree convergence

C. Layer 3 routing

D. Lack of PoE budget on the switch

ANSWER: D

Explanation:

Lack of PoE budget on the switch is the most likely reason. Successful laptop connectivity on the same cable confirms that the horizontal cabling and Ethernet data path are functioning well enough to establish a network connection. However, a laptop normally supplies its own power and does not test whether the switch can allocate Power over Ethernet to an attached powered device. PoE-capable switches have a finite total power budget, determined by their power supplies and platform limits. As APs are connected, the switch reserves or delivers power to each device according to its negotiated power class and requirements. If the aggregate demand has consumed the available PoE budget, the switch may maintain data connectivity on a port while declining to energize a newly connected AP. This is particularly common during deployments when many APs are added at once, or when newer AP models require more power for full radio and feature operation. The appropriate next step is to check the switch's available PoE power and per-port power status, then increase available switch power, redistribute powered devices, or use an appropriate injector where supported. Cisco's overview of

PoE budgeting and power negotiation is available in Cisco Catalyst 9300 Series data sheet, and IEEE PoE standards are summarized by the IEEE 802.3af standard page.

QUESTION NO: 30

After designing and deploying a WLAN infrastructure, you realized the CCI is causing poor performance in the 2.4 GHz band. Primarily, you ' ve

designed the

WLAN for 5 GHz and 2.4 GHz as a best effort. You found out that the implementers didn ' t follow your guidelines when configuring the WLAN

infrastructure. What can you do to minimize as much as possible the CCI impact in the 2.4 GHz band?

A. Add more APs to the infrastructure

B. Increase the transmit power on all APs

C. Turn-off 2.4 GHz radios on some APs

D. Use all channels available in the 2.4 GHz band

ANSWER: C

Explanation:

Turn-off 2.4 GHz radios on some APs is the appropriate remediation for excessive co-channel interference in a densely deployed 2.4 GHz WLAN. The 2.4 GHz spectrum has very limited capacity for independent 20 MHz WLAN channels: in common regulatory domains, only channels 1, 6, and 11 are non-overlapping. When too many nearby AP radios are enabled on those same channels, stations and APs must contend for the same RF airtime using CSMA/CA. This reduces usable airtime and can substantially degrade throughput and latency even when signal strength is good.

Because the WLAN was designed primarily for 5 GHz, 2.4 GHz should be treated as an overlay for legacy-client support and limited coverage needs, rather than duplicated at every AP location. Disabling selected 2.4 GHz radios reduces the number of co-channel contenders while preserving sufficient coverage. The remaining radios should use a deliberate channel and transmit-power plan, with 20 MHz channel widths in 2.4 GHz, to maintain appropriate cell overlap and roaming support. This approach directly reduces the contention domain and improves available airtime for clients that must remain on 2.4 GHz. See Cisco’s discussion of co-channel interference and contention and the CWNP CWDP certification overview.