PassQueen
a.k.a dumpsqueen.com

Certified Wireless Network Administrator

CWNP CWNA-107

Version Demo

Total Demo Questions: 17

Total Premium Questions: 176

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Radio Frequency (RF) Technologies	46
Topic 2, Wi-Fi Antennas and Hardware	21
Topic 3, Wireless LAN Topologies and Architecture	27
Topic 4, 802.11 MAC and Frame Exchanges	19
Topic 5, WLAN Security	28
Topic 6, WLAN Troubleshooting	34
Topic 7, Mix Questions	1
Total	176

QUESTION NO: 1

A client STA must choose the best AP for connectivity. As part of the evaluation, it must verify compatible data rates. What can the client STA use to verify that an AP supports the same data rates that it supports?

A. Beacon frames transmitted by the AP

B. Data frames sent between the AP and current clients STAs

C. Authentication frames transmitted by the other client STAs

D. Probe request frames transmitted by other client STAs

ANSWER: A

Explanation:

Beacon frames transmitted by the AP are the correct source for this evaluation. An AP periodically transmits beacon management frames to advertise the characteristics of its basic service set to nearby stations, allowing clients to discover and evaluate the WLAN before associating. Beacon frames include the Supported Rates information element and, when needed, the Extended Supported Rates information element. These elements identify the PHY data rates supported by the AP, with basic rates specifically marked as mandatory for stations that join the BSS.

A client STA can compare the advertised rate set in a received beacon with its own supported rates and determine whether it can communicate with the AP using compatible modulation and coding capabilities. This is part of passive scanning: the STA listens for AP beacons and uses their advertised information, including SSID, capabilities, channel-related parameters, and rates, to make an AP-selection decision. The same rate information can also be provided in probe responses during active scanning, but beacon frames are the applicable choice here. Cisco's management-frame analysis describes the Supported Rates element carried in beacon frames: Cisco Community: 802.11 management-frame analysis. See also the Wireshark WLAN management-field reference for the Supported Rates fields.

QUESTION NO: 2

When a STA has authenticated to an AP (AP-1), but still maintains a connection with another AP (AP-2), what is the state of the STA on AP-1?

A. Transitional

B. Unauthenticated and Unassociated

C. Authenticated and Unassociated

D. Authenticated and Associated

ANSWER: C

Explanation:

Authenticated and Unassociated is correct. IEEE 802.11 treats authentication and association as separate relationships between a station and each individual access point. After the STA successfully exchanges authentication frames with AP-1, AP-1 records the STA as authenticated. However, the STA has not yet completed association with AP-1 because it remains connected to AP-2. Therefore, with respect to AP-1, the STA is in the authenticated-but-unassociated state.

This state is useful during roaming. A client may authenticate with a candidate AP before it actually moves its association, reducing work that may be required at the time of the roam. Authentication alone does not create the data-service relationship needed to send normal user traffic through AP-1. That relationship begins only after association is completed with AP-1. The AP maintains authentication state independently from association state, and the STA can be authenticated to more than one AP while associated to only one AP at a time in the normal infrastructure BSS roaming model.

Cisco's enterprise mobility documentation describes the 802.11 client state progression and roaming behavior: Cisco Enterprise Mobility Design Guide. CWNP's CWNA certification overview also identifies 802.11 operation and client connectivity as core knowledge areas: CWNP CWNA certification.

QUESTION NO: 3

During a WLAN troubleshooting capture, which observations can indicate that an RF impairment is affecting client performance? (Choose all that apply.)

A. A high number of retransmitted unicast frames

B. Frequent use of lower PHY data rates

C. Frames received with invalid FCS values

D. A successful DHCP lease acquisition

E. An AP advertising the expected SSID

ANSWER: A B C

Explanation:

High retry rates, failed frame-check sequences, and frequent rate adaptation to lower PHY rates can all indicate an impaired RF link. Interference, low SNR, multipath, and weak received signal can corrupt frames or prevent acknowledgments, causing MAC-layer retransmissions. Stations may also select lower modulation and coding schemes to maintain decodability when RF conditions worsen. These observations should be correlated with RSSI, SNR, channel utilization, and spectrum-analysis data before identifying a root cause. A successful DHCP exchange does not demonstrate that the RF environment is healthy; it only confirms that the client obtained IP configuration. Wireshark provides 802.11 decoding references at Wireshark: IEEE 802.11.

QUESTION NO: 4

You are attempting to locate the cause of a performance problem in two WLAN cells in a mostly overlapping coverage area. You note that one AP is on channel 1 and the other is on channel 2. When you document your findings, what term do you use to describe the problem in this configuration?

A. Bluetooth interference

B. Non-Wi-Fi interference

C. ACI (adjacent-channel interference)

D. ACI

ANSWER: C D

Explanation:

Adjacent-channel interference (ACI) describes the impairment produced when overlapping WLAN cells use channels that are close enough in frequency for their RF energy to overlap. In the 2.4 GHz band, Wi-Fi channel centers are spaced only 5 MHz apart, while a normal 20 MHz Wi-Fi channel occupies substantially more spectrum. Consequently, channels 1 and 2 overlap significantly. Stations and access points in the overlapping coverage area can receive energy from the neighboring channel while attempting to demodulate their own transmissions, reducing signal quality and increasing retransmissions. This creates reduced throughput, increased latency, and inconsistent client performance even though the APs are not configured for the same channel. Documenting this condition as ACI accurately identifies that the issue is caused by partially overlapping Wi-Fi channels. WLAN channel plans should instead use non-overlapping 2.4 GHz channels appropriate to the regulatory domain—commonly 1, 6, and 11 where those channels are available—and should also account for channel width and cell overlap. CWNP's CWNA certification scope includes RF behavior, channel planning, and interference analysis: CWNP CWNA certification. Additional practical discussion of channel overlap and planning is available from Ekahau's 2.4 GHz Wi-Fi guide.

QUESTION NO: 5

Lynne runs a small hotel, and as a value added for his customers he has implemented a Wi-Fi hot-spot. Lynne has read news articles about how hackers wait at hot-spots trying to take advantage of unsuspecting users. He wants to avoid this problem at his hotel.

What is an efficient and practical step that Lynne can take to decrease the likelihood of active attacks on his customers' wireless computers?

A. Implement Network Access Control (NAC) and require antivirus and firewall software along with OS patches.

B. Implement an SSL VPN in the WLAN controller that initiates after HTTPS login.

C. Enable station-to-station traffic blocking by the access points in the hotel.

D. Require EAP_FAST authentication and provide customers with a username/password on their receipt.

ANSWER: C

Explanation:

Enable station-to-station traffic blocking by the access points in the hotel. This feature, commonly called client isolation, peer-to-peer blocking, or intra-BSS traffic blocking, prevents one associated guest wireless client from directly communicating with another guest wireless client through the access point. That is especially valuable for a public hotel hotspot, where guests are generally unknown to one another and should not need local device-to-device connectivity.

By stopping direct peer traffic, the hotel reduces opportunities for an attacker on the guest WLAN to actively probe nearby clients, initiate unsolicited connections, or conduct local attacks that depend on access to other guests' devices. The control is efficient because it is enforced by the wireless infrastructure rather than requiring the hotel to install, manage, and validate endpoint security software on each visitor's personally owned computer. It also preserves the intended guest service: clients can still reach permitted upstream resources such as the Internet, while being separated from other guest stations.

Client isolation should be applied consistently to the guest SSID and guest network policy, with any necessary exceptions designed deliberately for services such as wireless printing. Cisco documents this capability as peer-to-peer blocking for WLAN clients; see Cisco Wireless Controller Configuration Guide. CWNP also identifies client isolation as a WLAN security design consideration in its CWNA certification overview.

QUESTION NO: 6

You are troubleshooting a WLAN problem and you suspect hidden node as the cause. What should you look for in a protocol analyzer?

A. Frames with the HN bit set to 1

B. Frames with the retry bit set to 0

C. Frames transmitted from the AP without acknowledgement

D. Retransmitted frames from multiple STAs at higher rates than other STAs

ANSWER: D

Explanation:

Retransmitted frames from multiple STAs at higher rates than other STAs are a strong packet-capture indicator of a hidden-node condition. A hidden node occurs when two or more client stations can communicate with the access point but cannot reliably hear one another. Because each station senses the medium as idle before transmitting, they may transmit at the same time. Their transmissions then collide at the AP, which is within range of both clients. Since the sender does not receive the expected acknowledgment, it retransmits the same MAC protocol data unit; in a capture, this is identified through the 802.11 Frame Control Retry subfield and repeated sequence-control information.

The important diagnostic pattern is that elevated retransmissions affect particular client stations more than the WLAN population generally, especially stations located where they are mutually out of carrier-sense range. Comparing retry percentages by transmitter, timing, RSSI, and the AP's view of the affected clients helps distinguish this localized contention pattern. The 802.11 MAC uses positive acknowledgments and retransmission to provide reliable delivery, so absent

acknowledgments naturally produce retries when concurrent hidden-station transmissions corrupt reception at the AP. CWNP's CWNA curriculum covers 802.11 medium access and troubleshooting concepts: CWNP CWNA Certification. Wireshark documents the 802.11 Retry flag used when examining these retransmissions: Wireshark WLAN field reference.

QUESTION NO: 7

Which statements are true about 802.11 retransmissions? (Choose all that apply.)

A. A retransmitted unicast frame has the Retry bit set.

B. A missing ACK can result from loss of either the original frame or the ACK frame.

C. Broadcast frames use the normal ACK-based retransmission process.

D. A station may retry a unicast frame until its configured retry limit is reached.

E. An ACK confirms that an application successfully processed the payload.

ANSWER: A B D

Explanation:

802.11 retransmissions are normally used for unicast frames when the sender does not receive the expected acknowledgment. The transmitting station sets the Retry bit on a retransmitted frame so that the receiving station can identify a potential duplicate. A missing ACK does not prove that the original frame was never received; the original data frame or the ACK itself may have been corrupted. For this reason, receivers use sequence-control information and the Retry bit to avoid delivering duplicate frames unnecessarily.

Broadcast and multicast frames are not acknowledged at the 802.11 MAC layer, so they are not retransmitted through the normal ACK-based retry process. The IEEE 802.11 MAC defines acknowledgment and retransmission behavior for reliable unicast delivery. See the IEEE 802.11 Working Group for standards information.

QUESTION NO: 8

You are attempting to locate the cause of a performance problem in two WLAN cells in a mostly overlapping coverage area. You note that one AP is on channel 1 and the other is on channel 2. When you document your findings, what term do you use to describe the problem in this configuration?

A. Bluetooth interference

B. Non-Wi-Fi interference

C. CCI

D. ACI

ANSWER: C D

Explanation:

CCI and ACI are relevant interference terms to document when closely located WLAN cells have substantial overlapping RF coverage. In the 2.4 GHz band, channels 1 and 2 are only 5 MHz apart while a typical 20 MHz Wi-Fi channel occupies much more spectrum than that spacing. Their transmitted energy therefore overlaps significantly, preventing the cells from operating as independent RF domains and reducing usable airtime. This adjacent-channel condition is ACI: frames and energy from one channel can interfere with reception on the neighboring channel. In practical WLAN troubleshooting documentation, CCI is also an important capacity and contention classification to track anywhere overlapping cells create competing WLAN activity in the same coverage area, because co-channel reuse and client/AP airtime behavior must be assessed alongside the adjacent-channel overlap. Recording both terms helps identify that the design needs a nonoverlapping channel plan and appropriate cell-size control. CWNA-level RF design emphasizes channel planning, airtime efficiency, and minimizing interference in overlapping coverage areas; see the CWNP CWNA certification overview and Cisco's discussion of co-channel and adjacent-channel interference.

QUESTION NO: 9

What best describes WPA2 in relation to 802.11 wireless networks?

A. WPA2 is specified in the 802.11 standard as implementing CCMP/AES.

B. WPA2 is the standard that defines security for WLANs.

C. WPA2 is a certification created by the Wi-Fi Alliance that validates devices correctly implement CCMP/AES.

D. WPA2 is the second version of WPA and it enhances security through the use of TKIP instead of WEP.

ANSWER: C

Explanation:

WPA2 is a certification created by the Wi-Fi Alliance that validates devices correctly implement CCMP/AES. It is the Wi-Fi Alliance interoperability certification based on the robust security architecture developed in IEEE 802.11i and subsequently incorporated into the broader IEEE 802.11 standard. In practical terms, WPA2 certification gave WLAN vendors and customers confidence that certified access points and client devices could interoperate while using the required AES-based CCMP data-confidentiality and integrity protection.

This distinction between an IEEE technical standard and a Wi-Fi Alliance certification program is important. IEEE creates and maintains the underlying 802.11 specifications, including the security mechanisms associated with RSN/802.11i. The Wi-Fi Alliance tests products against applicable requirements and grants the WPA2 certification mark when those requirements are met. WPA2 also supports both personal and enterprise authentication deployments, but its defining cryptographic data-protection requirement is CCMP using AES rather than the legacy WEP mechanism. The Wi-Fi Alliance describes WPA2 as a security certification program, while IEEE identifies 802.11i as the amendment that established robust security enhancements for wireless LANs. See the Wi-Fi Alliance WPA2 overview and the IEEE 802.11i standard record.

QUESTION NO: 10

Which statements are true about IEEE 802.11k and IEEE 802.11v WLAN features? (Choose all that apply.)

A. 802.11k can provide neighbor reports to a client station.

B. 802.11v can provide BSS Transition Management requests.

C. Both features force a client to roam immediately when instructed by an AP.

D. These features can reduce the time a client spends discovering roam candidates.

E. 802.11k replaces 802.1X authentication.

ANSWER: A B D

Explanation:

IEEE 802.11k provides radio-resource-management information, including neighbor reports that can help a client identify candidate APs and channels for roaming. IEEE 802.11v provides wireless network management capabilities, including BSS Transition Management, through which an AP can suggest a preferred roaming candidate to a client. These mechanisms can improve roaming efficiency, but roaming decisions remain client-controlled. Neither 802.11k nor 802.11v replaces the authentication and key-management procedures used to secure a roam. IEEE identifies the 802.11 working-group standards and amendments at the IEEE 802.11 Working Group.

QUESTION NO: 11

When using an RF splitter to connect one transceiver to sector antennas loss is incurred. What is this loss called?

A. Conversion loss

B. Intentional loss

C. Through loss

D. Active loss

ANSWER: C

Explanation:

Through loss is the correct term for the attenuation introduced when an RF signal passes through a splitter on its way from a transceiver to connected sector antennas. A splitter is a passive RF component that divides the input signal power among multiple output ports. Because the available power is divided, each output necessarily receives less power than the input. In addition to this theoretical division of power, practical splitter circuitry and connectors introduce a small amount of component attenuation. This reduction is specified in decibels and must be included in the RF link budget so that the effective transmit power, received signal level, and coverage expectations remain accurate.

For example, an equal two-way division ideally delivers half the input power to each output, which corresponds to about 3 dB of power reduction at each output; actual specifications can be slightly greater because of device losses. In CWNA RF terminology, the loss associated with signal passage through the splitter is called through loss. Reviewing the splitter's datasheet at the operating frequency range is essential because its stated loss value is the figure used for installation and link-budget planning. See CWNP's CWNA certification overview and Cisco's antenna and RF accessory documentation for relevant RF design context.

QUESTION NO: 12

The center frequency of channel 1 in the 2.4 GHz band is 2.412 GHz (2412 MHz). What is the center frequency of channel 4?

A. 2.413

B. 2.427

C. 2.422

D. 2.417

ANSWER: B

Explanation:

The center frequency of channel 4 is 2.427 GHz (2427 MHz). In the 2.4 GHz IEEE 802.11 band, adjacent channel center frequencies are normally spaced 5 MHz apart. Starting with channel 1 at 2.412 GHz, channel 2 is 2.417 GHz, channel 3 is 2.422 GHz, and channel 4 is 2.427 GHz. This can also be calculated directly: channel 4 is three channel numbers above channel 1, so its center frequency is 2.412 GHz + (3 × 0.005 GHz) = 2.427 GHz. Knowing this 5 MHz center-frequency increment is important when planning WLAN channel assignments, particularly because 20 MHz-wide 2.4 GHz channels overlap substantially despite their center frequencies being only 5 MHz apart. Regulatory domains can affect which channel numbers may be used, but they do not alter the standard center-frequency relationship for channels that are permitted. IEEE maintains the 802.11 working group information at IEEE 802.11 Working Group, and the Wi-Fi Alliance provides background on Wi-Fi technology at Wi-Fi Alliance: Discover Wi-Fi.

QUESTION NO: 13

What can an impedance mismatch in the RF cables and connectors cause?

A. Fewer MCS values in the MCS table

B. Excessive VSWR

C. Increased amplitude of the RF signal

D. Increased range of the RF signal

ANSWER: B

Explanation:

An impedance mismatch in RF cables, connectors, antennas, or other transmission-line components can cause excessive VSWR (Voltage Standing Wave Ratio). Wi-Fi RF systems are ordinarily designed around a 50-ohm impedance. When connected components do not present the same characteristic impedance, not all of the transmitter's forward RF energy is accepted by the load. Part of that energy is reflected back toward the transmitter, where it combines with the forward wave and creates standing waves along the cable. VSWR expresses the severity of this mismatch as the ratio between maximum and minimum voltage along the line; a larger ratio indicates more reflected power and poorer power transfer. Excessive VSWR can therefore reduce the RF energy delivered to the antenna and, at sufficiently high levels, may stress transmitter circuitry. Correct selection of 50-ohm cable and connectors, proper connector installation, and verification with suitable RF test equipment help minimize reflections and maintain an efficient antenna system. The Federal Communications Commission's antenna-system guidance discusses reflected power and VSWR measurements at FCC Antenna Systems. Additional technical background on transmission lines, reflections, and standing waves is available from Antenna-Theory.com.

QUESTION NO: 14

What ID is typically mapped to an APâ€™s MAC address if a single BSS is implemented?

A. VLAN ID

B. BSSID

C. Device ID

D. SSID

ANSWER: B

Explanation:

BSSID is correct because the Basic Service Set Identifier is the 48-bit identifier used to identify a specific IEEE 802.11 Basic Service Set on the air. For an infrastructure BSS implemented by one AP radio, the BSSID is typically derived directly from, and commonly identical to, that radio interface's MAC address. Stations use the BSSID in 802.11 management and data frames to identify the AP and the particular wireless cell to which they are associated. This mapping gives each BSS a unique radio-level identity that clients can discover in beacon and probe-response frames and then use during authentication and association. A single-radio AP serving one BSS therefore normally advertises its radio MAC address as that BSS's BSSID. In deployments with multiple BSSs on the same physical radio, such as multiple virtual APs, each BSS needs a distinct BSSID and the values may be assigned from a MAC-address block rather than simply using one unchanged interface MAC address. Cisco's wireless documentation describes the BSSID as the MAC address that identifies a wireless access point or BSS, while the IEEE 802.11 overview explains the role of a BSS in WLAN operation. See Cisco: 802.11 Wireless LAN Fundamentals and IEEE 802.11 Working Group.

QUESTION NO: 15

Which statements are true about Enhanced Distributed Channel Access (EDCA)? (Choose all that apply.)

A. EDCA defines voice, video, best effort, and background access categories.

B. Higher-priority categories can be configured with shorter contention values.

C. EDCA permanently prevents best-effort traffic from transmitting when voice traffic exists.

D. A station that wins EDCA contention may receive a TXOP.

E. EDCA replaces CSMA/CA with token passing.

ANSWER: A B D

Explanation:

EDCA is the contention-based quality-of-service method used by Wi-Fi Multimedia implementations. It defines four access categories: voice, video, best effort, and background. Each category uses its own contention parameters, including arbitration interframe space and contention-window values. Higher-priority categories are typically given shorter contention values, providing a statistical advantage when competing for airtime.

EDCA does not reserve the medium permanently for voice or video traffic. All traffic remains subject to the shared-medium contention process, although a successful contender can receive a Transmission Opportunity (TXOP) during which it may send one or more frames. The Wi-Fi Alliance WMM overview provides additional information about Wi-Fi multimedia quality of service.

QUESTION NO: 16

Which statements are true about WPA3-Personal? (Choose all that apply.)

A. It uses SAE for authentication.

B. It improves resistance to offline password-guessing attacks.

C. It uses TKIP as its required data-protection cipher.

D. It provides forward secrecy for established sessions.

E. It makes passphrase strength irrelevant.

ANSWER: A B D

Explanation:

WPA3-Personal uses Simultaneous Authentication of Equals (SAE) rather than the WPA2-Personal pre-shared-key authentication exchange. SAE provides resistance to offline password-guessing attacks using captured authentication exchanges and provides forward secrecy properties: compromise of a password does not expose previously captured session traffic. WPA3-Personal still depends on a suitably strong passphrase, because a weak password remains vulnerable to active guessing attempts. WPA3-Personal does not use TKIP; modern WPA3 deployments use AES-based protection. The Wi-Fi Alliance describes WPA3 security enhancements at Wi-Fi Security.

QUESTION NO: 17

Which statements are true about a predictive WLAN site survey? (Choose all that apply.)

A. It uses a computer model to estimate RF coverage before installation.

B. It relies on estimated attenuation values for walls and other materials.

C. It eliminates the need for a post-installation validation survey.

D. It can help determine preliminary AP locations and antenna choices.

E. It requires all production APs to be installed before measurements can begin.

ANSWER: A B D

Explanation:

A predictive survey uses a computer model, a floor plan, AP specifications, and estimated attenuation values for building materials to estimate WLAN coverage and capacity before equipment is installed. It is useful during initial design because it helps determine preliminary AP locations, antenna selections, and channel plans. However, its predictions depend on the accuracy of the building information and RF assumptions. An onsite validation survey is still needed after deployment to

verify actual coverage, interference, noise, and performance. See the CWNP CWNA certification overview for WLAN design and validation scope.