PassQueen
a.k.a dumpsqueen.com

Certified Wireless Technician

CWNP CWT-100

Version Demo

Total Demo Questions: 8

Total Premium Questions: 82

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Radio Frequency (RF) Technologies	25
Topic 2, 802.11 Standards and Protocols	13
Topic 3, Wireless LAN Hardware and Software	17
Topic 4, Wireless LAN Security	18
Topic 5, Wireless LAN Troubleshooting	9
Total	82

QUESTION NO: 1

When configuring a standalone AP with a web-based interface, what should be changed to protect the HTTP interface used to manage the AP?

A. Admin account password

B. WPA2 passphrase

C. SSID

D. WPA passphrase

ANSWER: A

Explanation:

Admin account password is correct because the AP's web-management interface is protected primarily by administrator authentication. Standalone access points commonly ship with a known, default administrative username and password. If that credential remains unchanged, an unauthorized person who can reach the management interface may be able to sign in and alter wireless settings, disable security controls, change network connectivity, or take control of the device. During initial AP configuration, the installer should replace the default administrator password with a unique, sufficiently long, strong password and store it according to the organization's credential-management practices. This is especially important for an HTTP management interface because HTTP does not encrypt credentials in transit; where the AP supports it, management should also be switched to HTTPS and restricted to an appropriate management network. Changing the administrator password directly removes the risk associated with factory-default management credentials and is a fundamental device-hardening action. NIST wireless-security guidance specifically recommends changing default passwords and using secure management practices for wireless infrastructure. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks and CISA guidance on default passwords and device security.

QUESTION NO: 2

An AP radio transmits at 17 dBm. The cable and connector loss is 2 dB, and the antenna gain is 8 dBi. What is the approximate EIRP? Select one:

A. 7 dBm

B. 19 dBm

C. 23 dBm

D. 27 dBm

ANSWER: C

Explanation:

23 dBm is correct. EIRP is calculated by adding antenna gain to conducted transmitter power and subtracting cable and connector losses. In this case, 17 dBm minus 2 dB plus 8 dBi equals 23 dBm EIRP. EIRP represents the effective radiated power referenced to an isotropic antenna and is used when evaluating WLAN coverage and regulatory compliance. See the CWNP RF math overview and FCC Part 15 regulations.

QUESTION NO: 3

In addition to modulation, coding and spatial streams, what has the most impact on available data rates in a WLAN link?

A. Output power of the AP above 100 mW

B. Output power of the client above 100 mW

C. Antenna gain above 11 dBi

D. Channel width

ANSWER: D

Explanation:

Channel width has the greatest additional impact on the available PHY data rate because it determines how much RF spectrum is available to carry OFDM subcarriers in a single transmission. Wider channels provide more usable subcarriers and therefore support substantially higher data rates when the same modulation and coding scheme and number of spatial streams are used. For example, 802.11ac and 802.11ax define operation with 20, 40, 80, and 160 MHz channels; moving to a wider channel can increase the theoretical PHY rate proportionally, subject to the capabilities negotiated by the access point and client. The actual usable throughput remains lower than the advertised PHY rate because of MAC overhead, contention, retransmissions, and environmental conditions. Channel-width selection must also account for the amount of clean spectrum available: a wide channel is beneficial only when its constituent spectrum is usable and supported by both endpoints. CWNP training materials describe channel width as a fundamental rate-affecting PHY characteristic alongside MCS and spatial streams. See the CWNP Certified Wireless Technician certification overview and the IEEE 802.11 wireless LAN standard information.

QUESTION NO: 4

What AP configuration option is often thought to provide security but actually provides no security because of the simple spoofing attack weakens it?

A. MAC filtering

B. WEP

C. Shared Key Authentication

D. SSID hiding

ANSWER: A

Explanation:

MAC filtering is correct because it controls association by comparing a client's presented MAC address with an allowlist or denylist configured on the access point. Although this can appear to restrict network access, a wireless MAC address is not a trustworthy identity or authentication credential. It is transmitted in readily observable 802.11 management traffic, so an attacker within radio range can identify the address of an authorized client. The attacker can then configure their own wireless adapter to use that same address—a straightforward MAC-spoofing technique—and attempt to associate as the approved device. MAC filtering therefore does not establish that a device is genuinely the authorized device or that the person using it is authorized. At most, it can provide minor administrative control or help inventory known devices; it must not be treated as a meaningful security boundary. Effective WLAN access control requires strong authentication and encryption, such as WPA2-Enterprise or WPA3-Enterprise with 802.1X, rather than reliance on a client-controlled address. NIST similarly notes the weakness of MAC-address filtering and recommends stronger WLAN security controls. See NIST SP 800-153: Guidelines for Securing WLANs and CWNP Certified Wireless Technician.

QUESTION NO: 5

What identifier uniquely identifies a specific basic service set (BSS) in an infrastructure WLAN? Select one:

A. SSID

B. BSSID

C. ESSID

D. AID

ANSWER: B

Explanation:

BSSID is correct because the Basic Service Set Identifier identifies a particular BSS and is normally the MAC address of the access point radio serving that BSS. Multiple APs can advertise the same SSID so that users see one WLAN name throughout a facility, but each AP radio uses a distinct BSSID. A client uses BSSID information to distinguish among the individual AP radios advertising the same WLAN. IEEE 802.11 defines BSSID use in management frames and BSS operation. See the IEEE 802.11 Working Group and the CWNP overview of 802.11 management frames.

QUESTION NO: 6

What kind of antenna chart shows the radiation pattern of an antenna from the side view of that antenna?

A. Top-down

B. Azimuth

C. Horizontal

D. Elevation

ANSWER: D

Explanation:

Elevation is correct because an elevation antenna chart plots the antenna's radiation characteristics in a vertical plane, producing the side-view representation of its coverage pattern. This plot shows how RF energy is distributed above and below the antenna's horizon, including vertical beamwidth, downtilt or uptilt, nulls, and side lobes. These details are essential when planning access-point placement and antenna orientation, particularly where coverage must extend across multiple floors, down a long aisle, or toward clients at a different vertical angle from the antenna. Antenna manufacturers commonly publish elevation and azimuth plots together so installers can understand radiation in both orthogonal planes. In practical WLAN work, the elevation plot helps determine whether the antenna's vertical coverage shape and mounting angle will place usable signal where clients are located. For example, a directional antenna with a narrow vertical beam may require careful mechanical downtilt to direct energy toward the intended service area. CWNP training materials describe antenna patterns in terms of azimuth and elevation planes, while Cisco's antenna documentation illustrates elevation patterns as vertical-plane plots. See CWNP and Cisco antenna fundamentals.

QUESTION NO: 7

What device type is configured to respond when a probe request is received in a BSS?

A. Desktop

B. Switch

C. Laptop

D. AP

ANSWER: D

Explanation:

An **AP** is configured to respond to a received probe request in an infrastructure basic service set (BSS). During active scanning, a wireless client station transmits a probe request management frame to discover available WLANs. Access points that support the requested network parameters respond with a probe response frame. That response provides information the client needs to evaluate and identify the BSS, such as the SSID, supported data rates, channel-related details, security capabilities, and other information elements. The client can then use this discovery information when selecting an access point and proceeding toward authentication and association. In IEEE 802.11 infrastructure networking, the AP performs the

coordination role for the BSS and advertises its WLAN service through beacon and probe-response management frames. This behavior is fundamental to active WLAN discovery and is distinct from a client merely sending the initial probe request. See the CWNP overview of 802.11 management frames at CWNP: 802.11 Management Frames and the IEEE 802.11 standard family information at IEEE 802.11 Working Group.

QUESTION NO: 8

A user reports sporadic performance problems with the WLAN. She works near the company lunch room, which has typical kitchen equipment. The problems seem to be worse during the lunch hour. What is the likely case?

A. Improper security settings

B. RF interference

C. Improper roaming settings

D. Improper band preference settings

ANSWER: B

Explanation:

RF interference is the likely cause because the issue is location-specific and becomes noticeably worse when the lunch room is actively used. Common kitchen appliances, particularly microwave ovens, can emit energy in the 2.4 GHz ISM band used by many Wi-Fi networks. When a microwave is operating, its emissions can raise the radio noise floor and reduce the signal-to-noise ratio for nearby Wi-Fi clients and access points. This can lead to sporadic retransmissions, lower data rates, increased latency, and temporarily poor application performance.

The time correlation is especially important: a recurring degradation during lunch hour strongly suggests that an environmental RF source is becoming active rather than a persistent WLAN configuration problem. A technician should validate the condition by checking client and access-point RF statistics during the affected period and, where available, using a spectrum analyzer to identify non-Wi-Fi energy in the affected channel range. Moving clients to 5 GHz or 6 GHz, selecting a cleaner 2.4 GHz channel where appropriate, and increasing separation from the appliance are typical mitigation approaches. Cisco discusses microwave ovens as a source of wireless interference in its wireless interference guidance; the FCC also describes the unlicensed equipment authorization framework applicable to devices operating in shared spectrum.