PassQueen
a.k.a dumpsqueen.com

Certified Wireless Network Administrator

CWNP CWNA-109

Version Demo

Total Demo Questions: 14

Total Premium Questions: 142

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Radio Frequency (RF) Technologies	33
Topic 2, WLAN Regulations, Standards, and Protocols	37
Topic 3, WLAN Hardware and Software	16
Topic 4, WLAN Design, Installation, and Validation	16
Topic 5, WLAN Security	22
Topic 6, WLAN Troubleshooting and Support	18
Total	142

QUESTION NO: 1

A wireless client sends a data frame to a server on the wired network through its associated AP. The frame has the To DS bit set to 1 and the From DS bit set to 0. Which address field contains the MAC address of the wired server?

A. Address 1

B. Address 2

C. Address 4

D. Address 3

ANSWER: D

Explanation:

Address 3 contains the destination address when a station transmits a frame from the wireless medium to the distribution system. In this direction, the To DS bit is set and the From DS bit is clear. Address 1 identifies the receiving AP, which is also the BSSID; Address 2 identifies the transmitting client station; and Address 3 identifies the final destination on the distribution system.

Understanding the address-field interpretation is important when analyzing 802.11 captures because the meaning of the fields changes according to the To DS and From DS values.

QUESTION NO: 2

What is appended to the end of each 802.11 data frame after the payload?

A. Preamble

B. MAC header

C. PHY header

D. FCS

ANSWER: D

Explanation:

FCS is appended as the final field of an 802.11 MAC data frame, immediately following the frame body (payload). FCS stands for Frame Check Sequence and is a 4-octet field used to detect unintentional corruption during transmission. The transmitting station calculates a 32-bit cyclic redundancy check value over the MAC header and frame body, then places that value in the FCS field. On receipt, the wireless station performs the corresponding calculation and compares its result with the received FCS. A matching result provides a very high degree of confidence that the protected portion of the frame was received without bit errors; a failed check means the frame is treated as corrupted and is not delivered as a valid MAC frame. This error-detection mechanism is particularly important in RF environments, where interference, noise, attenuation, and collisions can affect a transmission. The IEEE 802.11 MAC frame format identifies the Frame Check Sequence as the trailing field of a MAC frame. See the IEEE 802.11 standard overview and the CWNP CWNA certification overview.

QUESTION NO: 3

What factor does not influence the distance at which an RF signal can be effectively received?

A. Receiving station’s radio sensitivity

B. Receiving station’s output power

C. Transmitting station’s output power

D. Free Space Path Loss

ANSWER: B

Explanation:

Receiving station's output power is correct because RF reception is determined by the signal arriving at a receiver's input and whether that received signal meets the receiver's required sensitivity threshold for the selected data rate and modulation. A station's transmit-power setting controls the strength of frames that *it sends*; it is not a receiver characteristic and does not increase the power of a signal arriving from another transmitter. Therefore, when evaluating the one-way distance at which a particular RF transmission can be decoded, the receiving station's own output power is not part of that receive-direction link budget.

This distinction is particularly important when assessing asymmetric WLAN links. A client may receive an access point's transmission successfully, yet its own transmission power can only affect the reverse client-to-access-point path. It cannot improve the client's ability to decode the access point's already-arriving frame. Practical RF design evaluates each direction independently and then verifies that both directions support reliable communication. CWNP's CWNA certification coverage includes RF fundamentals and WLAN operation: CWNP CWNA certification. Cisco also provides a useful explanation of wireless transmit-power values and their RF context: Cisco Wireless Power Levels.

QUESTION NO: 4

Which IEEE 802.11 physical layer (PHY) specification includes support for operation in the 2.4 GHz, 5 GHz, and 6 GHz bands?

A. VHT (802.11ac).

B. HT(802.11n)

C. HR/DSSS (802.11b)

D. HE (802.11ax)

ANSWER: D

Explanation:

HE (802.11ax) is correct because High Efficiency wireless was designed as a multiband PHY, supporting 2.4 GHz and 5 GHz operation and serving as the PHY basis for Wi-Fi 6E operation in the 6 GHz band. In practical WLAN terminology, 802.11ax devices operating in 2.4 GHz or 5 GHz are commonly called Wi-Fi 6, while 802.11ax devices operating in 6 GHz are called Wi-Fi 6E. The underlying HE mechanisms, including OFDMA, uplink and downlink MU-MIMO, target wake time, and improved operation in dense client environments, are associated with this PHY across those permitted bands. Actual 6 GHz use depends on the regulatory domain and local spectrum rules, as well as client and access point support, but that does not change the PHY identification tested by the question. The Wi-Fi Alliance describes Wi-Fi 6E as extending Wi-Fi 6 into 6 GHz, and IEEE identifies 802.11ax as the High Efficiency WLAN amendment. See the Wi-Fi Alliance Wi-Fi 6E overview and the IEEE 802.11ax standard page.

QUESTION NO: 5

An organization uses WPA2-Enterprise with PEAP authentication. During a security review, you discover that managed client devices are configured to accept any server certificate during PEAP authentication. What is the most important corrective action?

A. Configure clients to validate the trusted CA and authentication server identity

B. Configure the SSID as a hidden network

C. Increase the AP transmit power for the enterprise WLAN

D. Replace PEAP with Open System Authentication

ANSWER: A

Explanation:

The clients should be configured to validate the authentication server certificate against a trusted CA and expected server identity. PEAP creates a TLS tunnel between the supplicant and authentication server before the inner authentication exchange occurs. If a client accepts any certificate, an attacker can impersonate the authentication server with an evil-twin AP and rogue RADIUS service.

Validating the trusted certificate authority and server name helps the client distinguish the legitimate authentication server from an untrusted server. Changing the SSID, hiding the SSID, or increasing AP transmit power does not address the certificate-validation weakness.

QUESTION NO: 6

You are evaluating access points for use in the 5 GHz frequency band. What PHY supports this band and supports 80 MHz channels?

A. HT

B. VHT

C. ERP

D. OFDM

ANSWER: B

Explanation:

VHT is correct because the Very High Throughput PHY is the PHY architecture introduced with IEEE 802.11ac, commonly called Wi-Fi 5. IEEE 802.11ac operates exclusively in the 5 GHz band and expands channel-width support beyond the 20 MHz and 40 MHz widths associated with HT operation. A central VHT capability is use of an 80 MHz channel, formed by bonding four adjacent 20 MHz channels. This wider channel provides substantially more PHY capacity, subject to available contiguous spectrum, regulatory requirements, and proper radio configuration. VHT also adds other efficiency and throughput features, including support for more spatial streams, higher-order modulation, and downlink multi-user MIMO in applicable implementations. Therefore, when the stated requirements are 5 GHz operation and 80 MHz channels, VHT identifies the applicable PHY. The Wi-Fi Alliance's overview of Wi-Fi 5 describes 802.11ac as a 5 GHz technology: Wi-Fi CERTIFIED ac. Cisco's 802.11ac technology overview also documents 80 MHz channel support and the VHT capabilities associated with 802.11ac: Cisco 802.11ac overview.

QUESTION NO: 7

You are implementing a multi-AP WLAN and fast secure roaming is essential. Which one of the following methods is an IEEE 802.11 standard method for fast roaming?

A. FT

B. OKC

C. Load balancing

D. Band steering

ANSWER: A

Explanation:

FT is correct because Fast BSS Transition is the IEEE 802.11r amendment, now incorporated into the IEEE 802.11 standard. It was specifically designed to reduce the time required for a client to roam securely between access points in the

same mobility domain. With conventional WPA2/WPA3-Enterprise roaming, a client may need to perform substantial authentication and key-establishment exchanges when it joins the new AP. FT establishes key material that can be used for a faster transition and supports either over-the-air or over-the-DS transition procedures. This is particularly valuable for latency-sensitive applications, such as voice calls, where lengthy roaming interruptions can cause audible gaps or dropped calls. FT can be used with personal or enterprise authentication methods, subject to compatible client and WLAN infrastructure configuration. The Wi-Fi Alliance describes Wi-Fi CERTIFIED Agile Multiband features, including 802.11r Fast Transition, as mechanisms intended to improve roaming behavior and reduce transition delay. IEEE's 802.11 working group also identifies 802.11r as the amendment defining fast basic service set transition. See the IEEE 802.11 Working Group and the Wi-Fi Alliance Wi-Fi CERTIFIED Agile Multiband overview.

QUESTION NO: 8

What best describes WPA2 in relation to 802.11 wireless networks?

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

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

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

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

ANSWER: B

Explanation:

WPA2 is a Wi-Fi Alliance interoperability certification program for WLAN devices, built on the robust security mechanisms introduced by IEEE 802.11i and subsequently incorporated into the IEEE 802.11 standard. A device bearing WPA2 certification has been tested for interoperable implementation of the required WPA2 security capabilities, including use of the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol with the Advanced Encryption Standard cipher, commonly written as CCMP/AES. This distinction matters: IEEE develops the technical standard, whereas the Wi-Fi Alliance defines certification programs and tests products against their interoperability requirements. In practical WLAN administration, WPA2 certification indicates that client and infrastructure products are expected to securely interoperate when configured with WPA2 and CCMP/AES. WPA2 may support either Personal authentication using a pre-shared key or Enterprise authentication using 802.1X and an authentication server; the shared encryption and integrity protection foundation is CCMP/AES. The Wi-Fi Alliance's security overview describes WPA2 as a certification based on IEEE 802.11i, while the IEEE standard catalog identifies 802.11 as the governing WLAN standard: Wi-Fi Alliance security overview and IEEE 802.11 standard information.

QUESTION NO: 9

A technician captures traffic in monitor mode on a WPA2-Enterprise WLAN. Beacon, probe, and association frames decode normally, but protected data-frame payloads cannot be decoded. The capture is on the correct channel and includes frames from the target client. What additional information is required to decrypt the client data?

A. The client's pairwise temporal key or derivation material

B. The WLAN SSID

C. The AP radio BSSID

D. Additional beacon frames from the AP

ANSWER: A

Explanation:

The applicable pairwise temporal key, or the key material needed to derive it, is required to decrypt the protected unicast data. Management frames such as beacons and probe responses are normally visible because they are not encrypted in the

same manner as protected data traffic. WPA2-Enterprise data encryption uses session-specific keying material established for the authenticated client connection.

The SSID and BSSID identify the WLAN but do not provide decryption capability. A client MAC address is also insufficient. Capturing only additional beacon frames does not reveal the temporal keys used to protect a client's unicast data frames.

QUESTION NO: 10

What is required when operating 802.11ax APS in the 6 GHz band using passphrase-based authentication?

VHT PHY

A. HT PHY

B. SAE

C. CCMP

ANSWER: B

Explanation:

SAE is required for passphrase-based authentication on a Wi-Fi network operating in the 6 GHz band. SAE (Simultaneous Authentication of Equals) is the authentication method used by WPA3-Personal. Rather than using the WPA2-Personal pre-shared-key authentication exchange, SAE performs a password-authenticated key exchange that establishes session keys without exposing information that enables practical offline password-guessing attacks. It also provides forward secrecy, so compromise of a password at a later time does not reveal keys used for previously captured sessions.

Wi-Fi 6E operation in the 6 GHz band has security requirements intended to ensure modern protection. WPA3 is required for personal, passphrase-protected 6 GHz WLANs, and WPA3-Personal specifically uses SAE. Therefore, an 802.11ax access point configured for 6 GHz service with a shared passphrase must support and use SAE for client authentication. This requirement applies to the security mode, not merely to the RF PHY used by the access point. The Wi-Fi Alliance describes WPA3-Personal as using SAE and identifies WPA3 security as part of Wi-Fi CERTIFIED 6 requirements. See the Wi-Fi Alliance security overview and its Wi-Fi CERTIFIED 6 overview.

QUESTION NO: 11

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

A. Increased range of the RF signal

B. Fewer MCS values in the MCS table

C. Increased amplitude of the RF signal

D. Excessive VSWR

ANSWER: D

Explanation:

Excessive VSWR is caused by an impedance mismatch between RF-system components, such as cables, connectors, antennas, and radio equipment. WLAN RF systems are generally designed around a 50-ohm impedance. When the characteristic impedance is not consistently maintained through the RF path, not all transmitted energy is delivered to the antenna. Part of the forward RF signal is reflected back toward the transmitter, producing standing-wave behavior on the transmission line. Voltage Standing Wave Ratio expresses the magnitude of this mismatch: a 1:1 VSWR represents an ideal match, while higher ratios indicate increasingly significant reflected power. In a practical WLAN installation, damaged coaxial cable, poorly installed connectors, water intrusion, incorrect components, or an antenna fault can create the mismatch that raises VSWR. High VSWR reduces the power effectively radiated by the antenna and, depending on the radio design and severity of the reflection, can stress or trigger protective behavior in transmitter circuitry. This makes VSWR an important diagnostic measurement when evaluating antenna feed lines and external RF connections. CWNP's CWNA curriculum

identifies RF cables, connectors, impedance matching, reflected power, and VSWR as core RF fundamentals. See the CWNP CWNA certification overview and the Analog Devices overview of VSWR.

QUESTION NO: 12

You are the network administrator for ABC Company. Your manager has recently attended a wireless security seminar. The seminar speaker taught that a wireless network could be hidden from potential intruders if you disabled the broadcasting of the SSID in Beacons and configured the access points not to respond to Probe Request frames that have a null SSID field.

Your manager suggests implementing these security practices. What response should you give to this suggestion?

A. Any 802.11 protocol analyzer can see the SSID in clear text in frames other than Beacons frames. This negates any security benefit of trying to hide the SSID in Beacons and Probe Response frames.

B. To improve security by hiding the SSID, the AP and client stations must both be configured to remove the SSID from association request and response frames. Most WLAN products support this.

C. Any tenants in the same building using advanced penetration testing tools will be able to obtain the SSID by exploiting WPA EAPOL-Key exchanges. This poses an additional risk of exposing the WPA key.

D. This security practice prevents manufacturers' client utilities from detecting the SSID. As a result, the SSID cannot be obtained by attackers, except through social engineering, guessing, or use of a WIPS.

ANSWER: A

Explanation:

Any 802.11 protocol analyzer can see the SSID in clear text in frames other than Beacons frames. This negates any security benefit of trying to hide the SSID in Beacons and Probe Response frames. Suppressing the SSID in Beacon frames and declining broadcast (null-SSID) probe requests is often called using a "hidden SSID," but it is not an access-control or encryption mechanism. A client that is already configured for the WLAN must identify the desired SSID when it attempts to join, and the SSID can consequently be observed in management traffic such as directed probe requests and association or reassociation requests. An observer using a monitor-mode adapter and an 802.11 protocol analyzer can capture that traffic, particularly when a legitimate client connects or roams. The SSID is only a network identifier; it is not a secret and should never be treated as one. Effective WLAN protection instead requires strong authentication and encryption, such as WPA3-Enterprise or WPA2-Enterprise with 802.1X where appropriate, along with sound credential and access-point management. The Wi-Fi Alliance describes WPA3 security capabilities at Wi-Fi Alliance Security, and CWNP provides WLAN security education at CWNP.

QUESTION NO: 13

You are evaluating a connection that states the data rate is 150 Mbps. What is the expected throughput of this connection?

A. Less than 150 Mbps because of 802.11 overhead and contention

B. 54 Mbps because that is the actual maximum throughput of an 802.11 connection

C. More than 150 Mbps because of compression

D. 150 Mbps because the data rate is equal to the throughput

ANSWER: A

Explanation:

Less than 150 Mbps because of 802.11 overhead and contention is correct. The 150 Mbps value is a PHY data rate: the rate at which bits are signaled over the radio medium under the currently selected modulation, coding, channel width, and spatial-stream conditions. It is not a guarantee that 150 Mbps of application data can be delivered. Every WLAN transmission consumes airtime for MAC-layer framing and coordination, including preambles, PHY headers, MAC headers, acknowledgments, interframe spaces, and contention backoff. Management and control traffic also uses airtime, and the

shared, half-duplex nature of the RF medium means stations must contend for transmission opportunities. Environmental conditions and retransmissions caused by interference or frame errors can further reduce delivered throughput. Consequently, useful payload throughput must be lower than the reported PHY rate, although no single fixed percentage can be calculated from the PHY rate alone. The actual result depends on packet sizes, client capabilities, signal quality, channel utilization, protection mechanisms, security overhead, and the number and behavior of other devices using the channel. CWNP's WLAN fundamentals distinguish the advertised physical-layer data rate from the practical throughput achievable by user traffic; see CWNP CWNA certification information and the IEEE's overview of the IEEE 802.11 wireless LAN standard.

QUESTION NO: 14

You administer a WLAN that offers a guest SSID of GUESTNWORK. Users connect to the GUESTNWORK SSID, but report that they cannot browse the Internet. The devices simply report no Internet connection. What common problem causes this scenario?

A. NTP issues

B. Hardware issues

C. IP routing issues

D. Captive portal issues

ANSWER: D

Explanation:

Captive portal issues are a common cause of this guest-WLAN symptom. A client can successfully associate to the GUESTNWORK SSID, complete Wi-Fi security negotiation, and obtain an IP configuration, yet still be intentionally blocked from general Internet access until it completes a portal workflow. That workflow may require accepting terms of use, entering credentials, providing a voucher, or completing another authorization step. If the portal redirection page does not appear, users commonly interpret the condition as having "no Internet connection."

The portal process depends on several services working together, including client DNS resolution, DHCP-provided addressing and gateway information, web redirection or walled-garden policy, certificate handling, and reachability of the portal service itself. Modern devices may also test connectivity with HTTPS-based probes, which can make portal detection less reliable when interception or certificate behavior is not compatible with the device's expectations. Consequently, validating that unauthenticated clients are redirected to and can reach the portal is a key guest-access troubleshooting step. Captive portal architecture and signaling are described in RFC 8910; CWNA certification coverage is outlined by CWNP.