PassQueen
a.k.a dumpsqueen.com

Certified Wireless Technology Specialist - Sales

CWNP PW0-071

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Wireless Networking Fundamentals	16
Topic 2, RF Fundamentals	24
Topic 3, Wireless LAN Hardware and Software	24
Topic 4, Wireless LAN Security	15
Topic 5, Wireless LAN Applications	14
Total	93

QUESTION NO: 1

Which statement best defines SNR?

A. The difference between the noise floor and a signal's strength

B. The technology used to detect objects using RF waves

C. The absolute measurement of signal strength at the receiver

D. The frequency of the RF signal compared to that of an interferer

ANSWER: A

Explanation:

The difference between the noise floor and a signal's strength correctly defines signal-to-noise ratio (SNR) in a wireless context. SNR expresses how far above the received noise level a desired wireless signal is measured, normally in decibels. For example, if a client receives a signal at −60 dBm and the local noise floor is −90 dBm, the resulting SNR is 30 dB. This margin is important because a receiver must distinguish the intended 802.11 transmission from the background RF energy present in its channel.

A higher SNR generally provides the radio with a cleaner, more reliable signal to decode. This supports use of more efficient modulation and coding choices, increasing potential data rates and reducing retransmissions. A lower SNR means the desired signal is closer to the noise floor, leaving less margin for successful decoding and making wireless performance more vulnerable to changing environmental noise. SNR is therefore a relative quality measurement, not merely a received-power reading. Cisco's wireless troubleshooting guidance describes SNR as the relationship between received signal and noise and uses it as a key indicator of RF link quality: Cisco: Understanding Signal-to-Noise Ratio. Additional RF measurement context is available from CWNP: Understanding RSSI and SNR.

QUESTION NO: 2

Given: In order to reduce travel-related expenses, your CFO has enacted a company policy that eliminates cellular data connectivity for traveling users. Many of your users must connect to the office network during travel, but you have security concerns about wireless hot-spot usage.

To address these concerns, what advice should you give to your traveling users with regard to wireless hot-spot usage? (Choose 2)

A. Only use hot-spots that offer either WPA2-PSK or 802.1X/EAP user-based security.

B. Before connecting at hot-spots, conduct a scan to see if hacking tools are in use.

C. Verify that personal firewall and antivirus software are both enabled before connecting.

D. You should only use fee-based hot-spots which are more secure than free hot-spots.

E. Always use company-provided VPN client software after connecting to the Wi-Fi network.

ANSWER: C E

Explanation:

"Verify that personal firewall and antivirus software are both enabled before connecting." is sound guidance because public Wi-Fi places an endpoint on an untrusted network shared with unknown devices. A properly configured personal firewall helps limit unsolicited inbound connections and unnecessary exposure of local services, while current antivirus or endpoint-protection software helps detect and block malicious files or activity that may target the traveler's device. These protections should be active and updated before joining any hotspot.

"Always use company-provided VPN client software after connecting to the Wi-Fi network." is equally essential when users need access to office resources. A company-managed VPN establishes an authenticated, encrypted tunnel between the user and the organization, protecting business traffic from interception or modification over the untrusted hotspot. It also lets the organization apply its approved access controls and security configuration consistently. Users should connect to the

hotspot first, then immediately establish the corporate VPN before accessing internal applications, files, email, or other sensitive services. CISA specifically recommends using a virtual private network on public Wi-Fi and maintaining endpoint security protections; see CISA: Using Public Wi-Fi and CISA Secure Our World.

QUESTION NO: 3

As part of a pre-deployment manual RF site survey, your manager has assigned to you the task of documenting security and interference details about existing WLANs in the building. What is the best tool for locating and collecting information about existing APs in the building?

A. Spectrum analyzer

B. Wi-Fi client utilities

C. Wireless protocol analyzer

D. Predictive analysis software

E. WLAN controller

ANSWER: C

Explanation:

Wireless protocol analyzer is the best tool because it captures and decodes the 802.11 management and control traffic transmitted by nearby access points and wireless clients. During a manual pre-deployment survey, beacon and probe-response frames reveal essential details for each detectable WLAN, including the SSID, BSSID, operating channel, supported data rates, PHY capabilities, and advertised security configuration. The RSN information element in management frames can identify security information such as the authentication and encryption suites being advertised. This gives the surveyor evidence-based documentation of the existing wireless environment and helps identify neighboring WLANs that may contribute co-channel or adjacent-channel contention. A protocol analyzer can also show frame activity, retries, and other MAC-layer conditions that provide useful context when assessing WLAN interference and performance behavior. For example, Wireshark can capture and dissect IEEE 802.11 frames when used with an appropriate wireless adapter and capture configuration; see the Wireshark WLAN capture setup guide and the Wireshark User's Guide on capture setup. This frame-level visibility makes a wireless protocol analyzer particularly suitable for documenting existing AP information before a new WLAN deployment.

QUESTION NO: 4

Given: A customer has Ethernet switches that do not provide Power over Ethernet (PoE). The customer needs to power several access points through their existing Ethernet cabling without replacing the switches.

What device should be installed between each switch and access point?

A. PoE midspan injector

B. Wireless LAN controller

C. Lightning arrestor

D. Wireless workgroup bridge

E. Ethernet media converter

ANSWER: A

Explanation:

A **PoE midspan injector** is the appropriate device because it adds DC power to an Ethernet cable between a non-PoE switch port and a powered device such as an access point. The injector receives Ethernet data from the switch, inserts

power onto the cable, and forwards both data and power to the AP. This allows the customer to use the existing switching infrastructure while placing APs where AC outlets may not be available.

By contrast, a PoE-capable switch is endpoint power-sourcing equipment because it supplies power directly from its switch ports. Cisco provides an overview of PoE power-sourcing equipment at Cisco: What Is Power over Ethernet?.

QUESTION NO: 5

You are hired by ABC Company to recommend an appropriate solution for their wireless network. They would like to operate in the 2.4 GHz ISM frequency band and will require data throughput in excess of 10 Mbps. To meet that need, you recommend equipment compliant with the _____ or _____ amendments to the 802.11 standard. (Choose 2)

A. 802.11a

B. 802.11b

C. 802.11i

D. 802.11g

E. 802.11n

ANSWER: D E

Explanation:

802.11g and **802.11n** meet both stated requirements: operation in the 2.4 GHz ISM band and throughput capability exceeding 10 Mbps. IEEE 802.11g was designed for the 2.4 GHz band and specifies PHY data rates up to 54 Mbps using OFDM. Its practical application throughput is lower than its PHY rate because of protocol overhead and radio conditions, but it is designed to support performance well above the requested threshold under suitable conditions.

IEEE 802.11n also supports operation in the 2.4 GHz band, in addition to 5 GHz. It introduced high-throughput enhancements such as MIMO, channel bonding, frame aggregation, and more efficient modulation and coding choices. These capabilities allow 802.11n equipment to provide substantially higher throughput than the stated requirement when deployed appropriately. Therefore, either 802.11g or 802.11n equipment is an appropriate recommendation for a 2.4 GHz WLAN requiring more than 10 Mbps. The IEEE 802.11 working group summarizes these amendment families and their scope at IEEE 802.11 Working Group; Wi-Fi Alliance background on Wi-Fi technology is available at Wi-Fi Alliance.

QUESTION NO: 6

Virtual Private Network (VPN) solutions are often used in conjunction with Wi-Fi networks for what purpose?

A. Endpoint security for travelling users connected to unsecure Wi-Fi hot-spots

B. Validating user identity when using 802.1X/EAP security

C. Capturing and analyzing wireless network frames

D. Managing access points that are connected to WLAN controllers

ANSWER: A

Explanation:

Endpoint security for travelling users connected to unsecure Wi-Fi hot-spots is correct because a VPN creates an encrypted, authenticated tunnel between the user's device and a trusted VPN gateway. Public Wi-Fi hotspots are commonly treated as untrusted access networks: although the radio connection may provide some local protection, the user may still be exposed to insecure network infrastructure, malicious hotspot impersonation, local attacks, or interception risks when applications do not independently protect their traffic. A VPN helps protect the confidentiality and integrity of traffic carried from the endpoint across that untrusted network, allowing the traveller to reach organizational resources or the Internet through a trusted security boundary. In practical deployments, the VPN client authenticates to the organization's gateway and encapsulates

traffic so that sensitive business communications are not sent in clear text across the hotspot. This is an endpoint-focused use of VPN technology and complements, rather than replaces, appropriate Wi-Fi security and application-layer protections. NIST describes remote-access VPNs as providing protected communications for remote users over public networks in its Guide to SSL VPNs. The U.S. Cybersecurity and Infrastructure Security Agency also recommends using a VPN to protect connections when working remotely; see its telework guidance.

QUESTION NO: 7

When gathering requirements for a warehouse WLAN, which information is most important for determining the wireless design? (Choose 2)

A. The types and locations of Wi-Fi client devices

B. The number of concurrent devices and the applications they will use

C. The color of the access point enclosures

D. The number of available desktop web browsers

E. The brand of office furniture in the reception area

ANSWER: A B

Explanation:

The types and locations of Wi-Fi client devices are important because handheld scanners, vehicle-mounted terminals, tablets, voice devices, and laptops can have different radio capabilities, antenna characteristics, roaming behavior, and application requirements. Knowing where these devices will be used helps determine the required coverage areas and performance targets.

The number of concurrent devices and the applications they will use is equally important because capacity planning must account for the actual client density and traffic demand. Voice, real-time inventory applications, video, and bulk data transfers have different sensitivity to latency, packet loss, and throughput. This information helps determine AP density, channel reuse, QoS requirements, and backhaul capacity. Cisco discusses capacity and client requirements as key wireless design considerations in its WLAN Design Guide.

QUESTION NO: 8

Which explanations of antenna usage are the most accurate? (Choose 2)

A. A parabolic dish antenna is ideal for directing a beam down a long hallway.

B. An omni-directional antenna is well-suited to provide wireless coverage in most homes.

C. Patch antennas are mounted in the center of a lecture hall to provide circular coverage.

D. A dipole antenna is mounted to a perimeter wall in school buildings to provide coverage inside the building.

E. A grid antenna is designed to perform favorably as part of an outdoor point-to-point link under windy conditions.

ANSWER: B E

Explanation:

An omni-directional antenna is well-suited to provide wireless coverage in most homes because its radiation pattern distributes RF energy broadly around the access point in the horizontal plane. Homes commonly have users and client devices spread through rooms in several directions rather than concentrated along one narrow path. When the antenna is placed appropriately, such as near the center of the intended coverage area and at a practical elevation, this broad pattern supports general-purpose indoor WLAN coverage. Cisco describes omnidirectional antennas as providing a 360-degree horizontal coverage pattern: Cisco Aironet Antennas and Accessories.

A grid antenna is designed to perform favorably as part of an outdoor point-to-point link under windy conditions. Its highly directional, high-gain pattern concentrates transmitted and received energy toward the remote endpoint, which is the fundamental antenna requirement for a point-to-point wireless bridge. The open grid reflector also permits substantially more air to pass through than a solid reflector of similar size, reducing wind loading and helping make the antenna practical for exposed outdoor mounting locations. This combination of focused gain and wind-conscious physical construction is a standard use case for grid antennas. Ubiquiti's airGrid documentation illustrates this outdoor directional point-to-point application: airGrid User Guide.

QUESTION NO: 9

When implementing a wireless LAN, what is the area covered by an AP and usable by a client station called?

A. Basic Service Area

B. Independent Basic Service Set

C. Infrastructure Basic Service Set

D. Service Set Identifier

E. Basic Service Set Identifier

ANSWER: A

Explanation:

Basic Service Area is correct because it describes the physical RF coverage area provided by an access point in which client stations can establish and maintain wireless communication. In an infrastructure wireless LAN, the access point creates a Basic Service Set for associated stations, while the Basic Service Area is the geographic area over which that service is practically available. Its boundaries are not fixed circles: they depend on transmit power, antenna characteristics, attenuation from building materials, interference, receiver sensitivity, data-rate requirements, and the client device's own transmit capability. WLAN designers assess usable Basic Service Area coverage through predictive design and site surveys, validating that the signal level, signal-to-noise ratio, and performance satisfy the organization's application and roaming requirements. Adjacent access points are normally planned with deliberately overlapping Basic Service Areas so a client can roam while retaining appropriate connectivity. This distinction is useful in sales and design discussions because an access point's advertised range alone does not define reliable usable coverage; the real Basic Service Area must be designed for the intended environment and service level. See the IEEE 802.11 working group overview at IEEE 802.11 and Cisco's WLAN design guidance at Wireless LAN site-survey guidelines.