Free Questions for CWNA-109 by go4braindumps

Shared by Richard on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are using a tool that allows you to see signal strength for all Aps in the area with a visual representation. It shows you SSIDs available and the security settings for each SSID. It allows you to filter by frequency band to see only 2.4 GHz networks or only 5 GHz networks. No additional features are available.

What kind of application is described?

Options:

A- Protocol analyzer

B- Site survey utility

C- Spectrum analyzer

D- WLAN scanner tool

Answer:

D

Explanation:

The tool described is a WLAN (Wireless Local Area Network) scanner tool. WLAN scanner tools are designed to provide information about the wireless networks in a given area, including:

Signal Strength: They show the signal strength of all access points (APs) in the vicinity, which is crucial for understanding the coverage area and potential interference.

SSID Visualization: These tools display the SSIDs (Service Set Identifiers) of available networks, allowing users to identify different wireless networks easily.

Security Settings Information: WLAN scanner tools often show the type of security implemented on each network, such as WPA2, WEP, etc.

Frequency Band Filtering: They allow users to filter and view networks based on the frequency band (2.4 GHz or 5 GHz), which is useful for analyzing network distribution and planning.

While protocol analyzers, site survey utilities, and spectrum analyzers are also used in wireless networking, their functions are distinct from what is described:

Protocol Analyzers are more sophisticated and are used to capture and analyze network traffic.

Site Survey Utilities are used to map signal coverage and plan network layouts, often with more advanced features for detailed site surveys.

Spectrum Analyzers provide a detailed view of the frequency spectrum and non-Wi-Fi interference but don't typically focus on SSIDs or security settings.

Thus, the correct answer is D, a WLAN scanner tool, based on the functionalities described.

CWNA Certified Wireless Network Administrator Official Study Guide: Exam PW0-105, by David D. Coleman and David A. Westcott.

Tools and techniques for wireless network analysis and troubleshooting.

Question 2

Question Type: **MultipleChoice**

XYZ Company has decided to install an 802.11 WLAN system that will support 1083 wireless users, but they are concerned about network security. XYZ is interested in deploying standardized security features. In addition to WPA2-Enterprise with PEAP and role-based access control, XYZ would like to support management frame protection as well as a fast secure roaming protocol for future mobile handsets.

As XYZ Company selects a product to deploy, what two IEEE amendments, which are included in 802.11-2016, and 802.11-2020 should be supported to provide the management frame protection and fast secure roaming security features?

Options:

A- 802.11j and 802.11z

B- 802.11r and 802.11w

C- 802.11j and 802.11k

D- 802.11k and 802.11v

Answer:

B

Explanation:

The two IEEE amendments that should be supported to provide the management frame protection and fast secure roaming security features are 802.11r and 802.11w12.

802.11r (Fast BSS Transition): This amendment to the IEEE 802.11 standard permits continuous connectivity aboard wireless devices in motion, with fast and secure client transitions from one Basic Service Set to another1.

802.11w (Management Frame Protection): This amendment increases the security of its management frames2.

Question 3

Question Type: MultipleChoice

What terms accurately complete the following sentence?

The IEEE 802.11-2016 standard specifies mandatory support of the ________________ cipher suite for Robust Security Network Associations, and optional use of the _________________ cipher suite, which is designed for use with pre-RSNA hardware and is deprecated.

Options:

A- 802.1X/EAP, WEP

B- CCMP, TKIP

C- TLS, SSL

D- RC5, RC4

Answer:

B

Question 4

Question Type: **MultipleChoice**

What security solution is required to be used in place of Open System Authentication for all open network 802.11 implementations in the 6 GHz band?

Options:

A- OWE

B- Kerberos

C- WPA3-Enterprise

D- WPA3-SAE

Answer:

A

Question 5

Question Type: **MultipleChoice**

What authentication method is referenced in the 802.11-2016 and 802.11-2020 specifications and is recommended for robust WI-AN client security?

Options:

A- SSL

B- 802.1X/EAP

C- IPSec

D- WEP

Answer:

B

Explanation:

The authentication method that is referenced in the 802.11-2016 and 802.11-2020 specifications and is recommended for robust WLAN client security is802.1X/EAP. 802.1X/EAP stands for IEEE 802.1X Port-Based Network Access Control with Extensible Authentication Protocol and is a framework that provides strong authentication and dynamic encryption key generation for WLAN clients. 802.1X/EAP involves three parties: the supplicant (the client), the authenticator (the AP or the controller), and the authentication server (usually a RADIUS server). The supplicant sends its credentials (such as username and password, certificate, or token) to the authenticator, which forwards them to the authentication server. The authentication server verifies the credentials and sends a response to the authenticator, which grants or denies access to the supplicant. The authentication server also generates a master key that is used to derive encryption keys for the data frames between the supplicant and the authenticator. 802.1X/EAP supports various EAP methods that offer different levels of security and flexibility, such as EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST, and EAP-SIM. SSL, IPSec, and WEP are not authentication methods, but rather encryption or security protocols that are not specific to WLANs or referenced in the 802.11 specifications.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 299; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 289.

Question 6

Question Type: **MultipleChoice**

What is an advantage of using WPA3-Personal instead of WPA2-Personal as a security solution for 802.11 networks?

Options:

A- WPA3-Personal, also called WPA3-SAE, uses an authentication exchange and WPA2-Personal does not

B- WPA3-Personal, also called WPA3-SAE, uses a stronger authentication exchange to better secure the network

C- WPA3-Personal, also called WPA3-SAE, uses AES for encryption and WPA2-Personal does not

D- WPA3-Personal, also called WPA3-SAE, uses a better encryption algorithm than WPA2-Personal

Answer:

B

Explanation:

An advantage of using WPA3-Personal instead of WPA2-Personal as a security solution for 802.11 networks is thatWPA3-Personal, also called WPA3-SAE, uses a stronger authentication exchange to better secure the network. WPA3-Personal uses Simultaneous Authentication of Equals (SAE) as the key exchange protocol, which provides stronger protection against offline dictionary attacks and password guessing than WPA2-Personal. SAE uses a Diffie-Hellman key exchange with elliptic curve cryptography (ECC) to establish a pairwise master key (PMK) between the AP and the client without revealing it to any eavesdropper. SAE also provides forward secrecy, which means that if one PMK is compromised, it does not affect the security of other PMKs. WPA2-Personal uses Pre-Shared Key (PSK) as the key exchange protocol, which is vulnerable to offline brute-force attacks if the passphrase is weak or leaked. Both WPA3-Personal and WPA2-Personal use AES for encryption, so there is no difference in that aspect. WPA3-Personal does not use a different encryption algorithm than WPA2-Personal, but rather a different key exchange protocol.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 307; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 297.

Question 7

Question Type: **MultipleChoice**

You are troubleshooting a controller-based AP that is unable to locate the controller. DHCP is not use and the controller is located at 10.10.10.81/24 while the AP is on the 10.10.16.0/24 network. What should be inspected to verify proper configuration?

Options:

A- NTP

B- BOOTH

C- DNS

D- AP hosts file

Answer:

C

Explanation:

What should be inspected to verify proper configuration isDNS. DNS stands for Domain Name System and is a service that resolves hostnames to IP addresses. In a controller-based AP deployment, DNS can be used to help the AP locate the controller by using a predefined hostname such as CISCO-CAPWAP-CONTROLLER or aruba-master. The AP sends a DNS query for this hostname and receives an IP address of the controller as a response. Therefore, if DNS is not configured properly or if there is no DNS entry for the controller hostname, the AP may not be able to locate the controller. NTP, BOOTP, and AP hosts file are not relevant for this scenario.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 374; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 364.

Question 8

Question Type: MultipleChoice

You support a WLAN using dual-band 802.11ac three stream access points. All access points have both the 2.4 GHz and 5 GHz radios enabled and use 40 MHz channels in 5 GHz and 20 MHz channels in 2.4 GHz. A manager is concerned about the fact that each access point is connected using a 1 Gbps Ethernet link. He is concerned that the Ethernet link will not be able to handle the load from the wireless radios. What do you tell him?

Options:

A- His concern is valid and the company should upgrade all Ethernet links to 10 Gbps immediately.

B- His concern is valid and the company should immediately plan to run a second 1 Gbps Ethernet link to each AP.

C- His concern is invalid because the AP will compress all data before transmitting it onto the Ethernet link.

D- Due to 802.11 network operations and the dynamic rates used by devices on the network, the two radios will likely not exceed the 1 Gpbs Ethernet link.

Answer:

D

Explanation:

What you should tell him is thatdue to 802.11 network operations and the dynamic rates used by devices on the network, the two radios will likely not exceed the 1 Gbps Ethernet link. This is because the actual throughput of an 802.11 network is much lower than the theoretical data rates due to factors such as overhead, contention, interference, retransmissions, and environmental conditions. Moreover, the data rates used by devices on the network vary depending on their distance, signal quality, capabilities, and configuration. Therefore, it is unlikely that both radios of the AP will simultaneously use the maximum data rates and saturate the 1 Gbps Ethernet link. Upgrading to a 10 Gbps Ethernet link or running a second 1 Gbps Ethernet link may be unnecessary and costly. Compressing all data before transmitting it onto the Ethernet link may introduce additional overhead and latency.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 227; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 217.

Question 9

Question Type: MultipleChoice

What common feature of MDM solutions can be used to protect enterprise data on mobile devices?

Options:

A- Over-the-air registration

B- Onboarding

C- Containerization

D- Self-registration

Answer:

C

Explanation:

A common feature of MDM solutions that can be used to protect enterprise data on mobile devices iscontainerization. Containerization is a technique that creates a separate and secure environment on the mobile device where enterprise data and applications are stored and accessed. Containerization isolates the enterprise data from the personal data and prevents unauthorized access, leakage, or loss of sensitive information. Containerization can also enforce security policies, encryption, authentication, and remote wipe on the enterprise data and applications. Over-the-air registration, onboarding, and self-registration are features of MDM solutions that facilitate the enrollment and management of mobile devices, but they do not directly protect enterprise data on mobile devices.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 336; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 326.

Question 10

Question Type: MultipleChoice

What feature of 802.1 lax (HE) is managed with beacon and trigger frames and is primarily a power management method, but also provides more efficient access to the channel used within a BSS?

Options:

A- TWT

B- BSS Color

C- UL-MU-MIMO

D- OFDMA

Answer:

A

Explanation:

TWT is the feature of 802.11ax (HE) that is managed with beacon and trigger frames and is primarily a power management method, but also provides more efficient access to the channel used within a BSS. TWT stands for target wake time, which is a mechanism that allows an access point and a client device to negotiate and schedule specific times for data transmission and reception. This enables the client device to enter a low-power sleep mode when it is not expected to communicate with the access point, which saves battery life and reduces power consumption. TWT also reduces contention and interference on the channel used within a BSS, as it coordinates the transmissions of multiple client devices and avoids collisions. TWT is managed with beacon and trigger frames, which are two types of management frames that are used to announce and initiate data exchanges. A beacon frame is a frame that is periodically sent by an access point to advertise its presence, capabilities, and parameters to client devices. A trigger frame is a frame that is sent by an access point or a client device to request or initiate a data transmission with another device. BSS color, UL-MU-MIMO, and OFDMA are other features of 802.11ax (HE) that are not primarily power management methods, but rather performance enhancement methods. BSS color is a feature that assigns a color code to each BSS to differentiate it from other BSSs that use the same channel. This reduces interference and improves spatial reuse of the channel. UL-MU-MIMO is a feature that allows an access point to receive multiple simultaneous transmissions from different client devices using multiple spatial streams. This increases capacity and throughput of the uplink direction. OFDMA is a feature that divides a channel into smaller subchannels called resource units (RUs) that can be allocated to different devices for concurrent transmissions. This increases efficiency and flexibility of the channel utilization.Reference:CWNA-109 Study Guide, Chapter 10: Wireless LAN Operation, page 323

Question 11

Question Type: **MultipleChoice**

Three access points are used within a facility. One access point is on channel 11 and the other two are on channel 1. The two access points using channel 1 are on either side of the access point using channel 11 and sufficiently apart so that they do not interfere with each other when they transmit frames. Assuming no other APs are in the vicinity, is CCI still a possibility in this network and why?

Options:

A- Yes, because the client devices connected to one of the channel 1 APs will transmit frames that reach the other channel 1 AP as well as clients connected to the other channel 1 AP.

B- No, because the APs are far enough apart that no CCI will occur.

C- No, because CCI only occurs in the 5 GHz frequency band.

D- Yes, because channel 11 loops around and causes CCI with channel 1.

Answer:

A

Explanation:

CCI is still a possibility in this network because the client devices connected to one of the channel 1 APs will transmit frames that reach the other channel 1 AP as well as clients connected to the other channel 1 AP. CCI stands for co-channel interference, which is a type of interference that occurs when two or more devices transmit on the same channel within range of each other. CCI reduces performance and capacity because it causes contention and collisions on the wireless medium, which leads to retransmissions and delays. CCI can be mitigated by increasing physical separation between devices using the same channel or by reducing transmit power levels to limit coverage area. In this scenario, three access points are used within a facility. One access point is on channel 11 and the other two are on channel 1. The two access points using channel 1 are on either side of the access point using channel 11 and sufficiently apart so that they do not interfere with each other when they transmit frames. However, this does not prevent CCI from occurring between their client devices that are connected on channel 1. For example, if a client device connected to one of the channel 1 APs sends a frame to another device on the wired network or on another wireless network (such as an Internet server or a VoIP phone), that frame will be heard by both channel 1 APs as well as any other client devices connected to either of them on channel 1. This will cause CCI because these devices will have to wait for the channel to be clear before they can transmit their own frames. The answer that CCI only occurs in the 5 GHz frequency band is incorrect; CCI can occur in any frequency band where devices use the same channel. The answer that channel 11 loops around and causes CCI with channel 1 is also incorrect; channel 11 does not loop around and it operates in a different frequency band than channel 1.Reference:CWNA-109 Study Guide, Chapter 5: Radio Frequency Signal and Antenna Concepts, page 147

Question 12

Question Type: MultipleChoice

You are installing an AP to be used by 27 laptops. All laptops will connect on the 5 GHz frequency band. A neighbor network uses channels 1 and 6. What channel should be used for this AP and why?

Options:

A- Channel 6, because it is always best to use this channel

B- A 5 GHz channel, because channels 1 and 6 are 2.4 GHz channels they have no impact on the decision

C- Channel 1, because it is best to use the channel with the lowest frequency

D- Channel 11, because channels 1 and 6 are in use nearby

Answer:

B

Explanation:

A 5 GHz channel should be used for this AP because channels 1 and 6 are 2.4 GHz channels and they have no impact on the decision. The 5 GHz frequency band offers more non-overlapping channels than the 2.4 GHz frequency band, which reduces interference and improves performance. The 5 GHz frequency band also supports higher data rates and wider channel bandwidths than the 2.4 GHz frequency band, which increases capacity and throughput. The 5 GHz frequency band also has less interference from other devices and sources than the 2.4 GHz frequency band, which enhances reliability and quality of service. Therefore, it is recommended to use the 5 GHz frequency band for WLANs whenever possible. Channels 1 and 6 are two of the three non-overlapping channels in the 2.4 GHz frequency band (the other one is channel 11). They are used by a neighbor network in this scenario, but they do not affect the channel selection for this AP because they operate in a different frequency band than the 5 GHz frequency band. Channel 6 is not always best to use; it depends on the interference and congestion level in the environment. Channel 1 is not best to use because it has a lower frequency than channel 6; frequency does not determine channel quality or performance. Channel 11 is not best to use because it is also a 2.4 GHz channel and it may interfere with channels 1 and 6.Reference:CWNA-109 Study Guide, Chapter 4: Antenna Systems and Radio Frequency (RF) Components, page 113

20%
DISCOUNT