Free Questions for CWNA-109

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 have implemented an 802.11ax WLAN for a customer. All APs are four stream HE APs. The customer states that it is essential that most of the clients can use the OFDMA modulation scheme. What do you tell the customer?

Options:

A- The clients that must support OFDMA must also be upgraded to 802.11ax
B- OFDMA is an optional feature of 802.11ax and most APs don't even support it
C- All 5 GHz PHYs use OFDM modulation, so you will achieve OFDMA everywhere in 5 GHz
D- If the devices support 802.11ac, they can be updated to support OFDMA through driver upgrades

Answer:

A

Explanation:

OFDMA is a new modulation scheme introduced in 802.11ax that allows multiple users to share the same channel by dividing it into smaller subchannels called resource units (RUs). This improves the efficiency and capacity of the WLAN by reducing contention and overhead. However, to use OFDMA, both the AP and the client must support 802.11ax and negotiate the parameters of the subchannel allocation.Therefore, the customer needs to upgrade the clients that require OFDMA to 802.11ax devices12.

The other options are not correct because they do not reflect the reality of OFDMA.Option B is incorrect because OFDMA is a mandatory feature of 802.11ax for both downlink and uplink transmissions, and all 802.11ax APs must support it1. Option C is incorrect because OFDM and OFDMA are different modulation schemes, and OFDM does not allow multiple users to share the same channel.Option D is incorrect because 802.11ac devices cannot support OFDMA through driver upgrades, as they lack the hardware and firmware capabilities to do so2.

Question 2

Question Type: MultipleChoice

You administer a small WLAN with nine access point. As a small business, you do not rum a

RADIUS server and use WPA2-Personal for security. Recently, you changed the passphrase for WPA2-personal in all Aps and clients. Several users are now reporting the inability to connect to the network at time and it is constrained to one area of the building. When using scanner, you see that the AP covering that area is online

Options:

A- The AP that covers the problem area requires a firmware update
B- The clients are improperly configured
C- The AP that covers the problem area has failed
D- The AP that covers the problem area is improperly configured

Answer:

B

Explanation:

This is because the passphrase for WPA2-Personal is case-sensitive and must match exactly on both the AP and the client. If the passphrase is entered incorrectly on the client, the client will not be able to authenticate with the AP and connect to the network. The AP that covers the problem area is not likely to require a firmware update, fail, or be improperly configured, as it is online and works with other clients that have the correct passphrase. To troubleshoot this issue, you can check the passphrase settings on the clients and make sure they match with the AP. You can also try to reconnect the clients to the network or reboot them if necessary. For more information on how to configure WPA2-Personal on your router

Question 3

Question Type: MultipleChoice

An RF signal sometimes bends as it passes through a material rather than around an obstacle. What is the RF behavior that this statement best describes?

Options:

A- Diffraction
B- Refraction
C- Scattering

D- Reflection

Answer:

B

Explanation:

Refraction is the bending of an RF signal as it passes through a material of different density. Refraction can cause the signal to change its direction and angle of arrival. For example, when a light beam passes from air to water, it bends because of the difference in the refractive index of the two mediums.Similarly, when an RF signal passes from one medium to another, such as from air to glass, it can bend due to the change in the dielectric constant of the materials12.Reference:1: CWNA-109 Official Study Guide, page 672:Refraction

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

You are attempting to explain RF shadow and how it can cause lack of coverage. What common building item frequently causes RF shadow and must be accounted for in coverage plans?

Options:

A- Wooden doors
B- Carpeted floors
C- Elevators
D- Cubicle partitions

Answer:

C

Explanation:

Elevators are a common building item that frequently causes RF shadow and must be accounted for in coverage plans. RF shadow is a term that describes an area where wireless signals are blocked or significantly weakened by an obstacle or an object that absorbs or reflects RF energy. RF shadow can cause lack of coverage or poor performance in a WLAN because wireless devices in those areas may not be able to communicate with access points or other devices. RF shadow can be mitigated by adjusting access point placement, antenna orientation, transmit power level, or channel selection to avoid or overcome the obstacle or object that causes it. Elevators are a common building item that frequently causes RF shadow because they are made of metal and they move up and down within a shaft. Metal is a material that has high attenuation and reflection values, which means it can block or bounce off wireless signals very effectively. A moving elevator can create dynamic RF shadow that changes depending on its position and direction. Therefore, elevators must be accounted for in coverage plans to ensure adequate WLAN coverage and performance throughout the facility. The other options are not common building items that frequently cause RF shadow or must be accounted for in coverage plans. Wooden doors are not likely to cause RF shadow because they are made of wood, which is a material that has low attenuation and reflection values, which means it can pass through or slightly weaken wireless signals. Carpeted floors are not likely to cause RF shadow because they are made of fabric, which is a material that has low attenuation and reflection values, which means it can pass through or slightly weaken wireless signals. Cubicle partitions are not likely to cause RF shadow because they are made of thin plastic or cardboard, which are materials that have low attenuation and reflection values, which means they can pass through or slightly weaken wireless signals.Reference:CWNA-109 Study Guide, Chapter 13: Wireless LAN Site Surveys - Types & Processes , page 433

Question 6

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 7

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 8

Question Type: MultipleChoice

You are deploying a WLAN monitoring solution that utilizes distributed sensor devices. Where should sensors be deployed for best results? Choose the single best answer.

Options:

A- In switching closets
B- Every 5 meters and alongside each AP
C- In critical areas where WLAN performance must be high
D- Above the plenum on each floor

Answer:

C

Explanation:

Sensors should be deployed in critical areas where WLAN performance must be high for best results when using a WLAN monitoring solution that utilizes distributed sensor devices. A WLAN monitoring solution is a system that collects, analyzes, and reports on the status and performance of a WLAN. A WLAN monitoring solution can use different methods to gather data from the WLAN, such as embedded software agents, external hardware probes, or distributed sensor devices. Distributed sensor devices are dedicated devices that are deployed throughout the WLAN coverage area to monitor the wireless traffic and environment. Distributed sensor devices can perform various functions, such as scanning the spectrum, capturing wireless frames, measuring signal quality, detecting rogue access points, testing connectivity, and generating alerts. Distributed sensor devices can provide more accurate and comprehensive data than other methods, but they also require more planning and deployment costs. Therefore, it is important to deploy sensors strategically in critical areas where WLAN performance must be high, such as high-density zones, high-priority applications, or high-security locations. By deploying sensors in critical areas, the WLAN monitoring solution can ensure optimal WLAN performance and reliability in those areas and identify and resolve any issues or problems that may arise. The other options are not the best places to deploy sensors for best results. Deploying sensors in switching closets is not effective because sensors need to be close to the wireless medium to monitor it properly. Deploying sensors every 5 meters and alongside each AP is not efficient because sensors may overlap or interfere with each other and cause unnecessary redundancy or complexity.Deploying sensors above the plenum on each floor is not practical because sensors may not capture the wireless traffic and environment accurately due to attenuation or reflection from the ceiling materials or objects.Reference:CWNA-109 Study Guide, Chapter 14: Troubleshooting Wireless LANs, page 4831

Question 9

Question Type: MultipleChoice

You are troubleshooting a problem with a new 802.11ax AP. While the AP supports four spatial streams, most clients are only achieving maximum data rates of 150 Mbps. What is the likely cause?

Options:

A- The clients are 802.11n devices

B- The clients are only two stream 802.11ax clients
C- Contention caused by an overlapping BSS
D- Non-Wi-Fi interference in the channel

Answer:

A

Explanation:

The scenario described suggests that while the Access Point (AP) is capable of 802.11ax (Wi-Fi 6) with four spatial streams, the clients are only achieving data rates typical of 802.11n (Wi-Fi 4) devices, which indicates that the clients are likely 802.11n devices. Here's why this is the most plausible explanation:

802.11n Limitations: Devices that adhere to the 802.11n standard have lower maximum data rates compared to 802.11ax devices due to differences in technology such as modulation, spatial streams, and channel bandwidth. An 802.11n device with a single spatial stream operating on a 20 MHz channel can achieve a maximum data rate of 72.2 Mbps. Even with two spatial streams under ideal conditions, this would only double to approximately 144.4 Mbps, which is close to the 150 Mbps mentioned.

Spatial Stream Capability: The fact that the AP supports four spatial streams suggests it can achieve much higher data rates with 802.11ax clients that also support multiple spatial streams. However, if the clients are 802.11n devices, they may not be capable of using more than two spatial streams, and many earlier 802.11n devices were limited to just one.

The other options are less likely to be the primary cause based on the information provided:

B . Two Stream 802.11ax Clients: If the clients were 802.11ax with only two spatial streams, they would likely achieve higher data rates than 150 Mbps due to the efficiency improvements in 802.11ax.

C . Contention and D. Non-Wi-Fi Interference: While these could affect performance, they would not inherently limit clients to 150 Mbps, especially in the context of an 802.11ax environment where mechanisms to handle interference and contention are more advanced.

IEEE 802.11n-2009: Enhancements for Higher Throughput.

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

Question 10

Question Type: MultipleChoice

What frame type is used to reserve the wireless medium for the transmission of high data rate frames that may not be understood by all clients connected to the BSS?

Options:

A- RTS
B- ACK
C- Beacon
D- PS-Poll

Answer:

A

Explanation:

The frame type that is used to reserve the wireless medium for the transmission of high data rate frames that may not be understood by all clients connected to the BSS isRTS. RTS stands for Request to Send and is a control frame that is sent by a station to request access to the medium for a specified duration. The RTS frame contains the source and destination MAC addresses, as well as a Network Allocation Vector (NAV) value that indicates how long the medium will be occupied. The destination station responds with a Clear to Send (CTS) frame that echoes the NAV value and grants permission to the source station. All other stations in the BSS hear either the RTS or CTS frame and update their NAV timers accordingly, deferring their transmissions until the medium is free. The RTS/CTS mechanism can be used to prevent hidden node problems, reduce collisions, and protect high data rate frames that use features such as 802.11n or 802.11ac that may not be compatible with legacy stations. ACK, Beacon, and PS-Poll are not used to reserve the medium for high data rate frames.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 112; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 102.

Question 11

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 12

Question Type: MultipleChoice

A natural disaster has occurred in a remote area that is approximately 57 miles from the response team headquarters. The response team must implement a local wireless network using 802.11 WLAN access points. What is the best method, of those listed, for implementation of a network back-haul for communications across the Internet in this scenario?

Options:

A- 802.11 bridging to the response team headquarters
B- Cellular/LTE/5G
C- Turn up the output power of the WLAN at the response team headquarters
D- Temporary wired DSL

Answer:

B

Explanation:

Cellular/LTE/5G is the best method for implementing a network backhaul for communications across the Internet in a remote area that is affected by a natural disaster. This is because cellular/LTE/5G networks are wireless and do not depend on physical infrastructure that may be damaged or unavailable in such scenarios. Cellular/LTE/5G networks also offer high-speed data transmission and wide coverage area, which are essential for emergency response operations. 802.11 bridging to the response team headquarters is not feasible because it requires line-of-sight and has limited range. Turning up the output power of the WLAN at the response team headquarters is not effective because it may cause interference and does not guarantee reliable connectivity.Temporary wired DSL is not practical because it requires installing cables and equipment that may not be available or accessible in a remote are a.

Temporary wired DSL is not practical because it requires installing cables and equipment that may not be available or accessible in a remote are a.Reference:CWNA-109 Study Guide, Chapter 7: Wireless LAN Topologies, page 2031