CWNA-109 Q&As

Certified Wireless Network Administrator

Pass CWNP CWNA-109 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cwna-109.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP Official Exam Center

QUESTION 1

When a STA has authenticated to an AP (AP-1), but still maintains a connection with another AP (AP-2), what is the state of the STA on AP-1?

A. Transitional

B. Unauthenticated and Unassociated

C. Authenticated and Unassociated

D. Authenticated and Associated

Correct Answer: C

Authenticated and Unassociated. According to one of the web search results1, a STA can be authenticated to multiple APs, but it can only be associated to one AP at a time. Association is the process of establishing a logical link between the STA and the AP, which allows the STA to send and receive data frames through the AP2. Therefore, when a STA has authenticated to an AP-1, but still maintains a connection with another AP-2, it means that the STA is authenticated to both APs, but only associated to AP-2. The state of the STA on AP-1 is authenticated and unassociated, which means that the STA can switch to AP-1 without repeating the authentication process, but it cannot send or receive data frames through AP-1 until it becomes associated.

QUESTION 2

You recently purchased four laptops containing dual-band 802.11ac adapters. The laptops can connect to your 2.4 GHz network, but they cannot connect to the 5 GHz network. The laptops do not show the 5 GHz SSIds, which are different than the 2.4 GHz SSIDs. Existing devices can connect to the 5 GHz SSIDs with no difficulty. What is the likely problem?

A. Interference from non-Wi-Fi sources

B. Faulty drivers

C. DoS attack

D. Interference from other WLANs

Correct Answer: B

The likely problem that causes this scenario is faulty drivers. Drivers are software components that enable the communication between the operating system and the hardware devices, such as the wireless adapters. Faulty drivers can cause various issues with the wireless connectivity, such as not detecting or connecting to certain networks, dropping connections, or reducing performance. Faulty drivers can be caused by corrupted files, outdated versions, incompatible settings, or hardware defects. To fix faulty drivers, you can try to update, reinstall, or roll back the drivers, or contact the manufacturer for support. Interference from non-Wi-Fi sources, DoS attack, or interference from other WLANs are not likely to cause this scenario, as they would affect all devices in the same area, not just the new laptops. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 562; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 532.

QUESTION 3

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

Correct Answer: D

VSWR stands for Voltage Standing Wave Ratio, which is a measure of how well the impedance of the RF cable and connectors matches the impedance of the transmitter and the antenna. Impedance is the opposition to the flow of alternating current in an RF circuit, and it depends on the frequency, resistance, capacitance, and inductance of the components. A perfect impedance match would have a VSWR of 1:1, meaning that all the power is transferred from the transmitter to the antenna, and none is reflected back. However, in reality, there is always some degree of mismatch, which causes some power to be reflected back to the transmitter, creating standing waves along the cable. This reduces the efficiency and performance of the wireless system, and can also damage the transmitter. Excessive VSWR can be caused by using poor quality or damaged cables and connectors, or by using components that have different impedance ratings123. References: CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 90; CWNA-109Study Guide, Chapter 2: Radio Frequency Fundamentals, page 86; CWNP website, CWNA Certification.

QUESTION 4

What factors will have the most significant impact on the amount of wireless bandwidth available to each station within a BSS? (Choose 2)

A. The number of clientstations associated to the BSS

B. The power management settings in the access point\\'s beacons

C. The presence of co-located (10m away) access points on non-overlapping channels

D. The layer 3 protocol used by each station to transmit data over the wireless link

Correct Answer: A

The factors that will have the most significant impact on the amount of wireless bandwidth available to each station within a BSS are: The number of client stations associated to the BSS The presence of co-located (10m away) access points on non-overlapping channels The number of client stations associated to the BSS affects the wireless bandwidth because each station shares the same channel and medium with other stations in the same BSS. The more stations there are, the more contention and collision there will be for the channel access, which reduces thethroughput and efficiency of the wireless communication. The wireless bandwidth available to each station depends on how the access point allocates the channel resources and how the stations use the channel time. For example, if the access point uses a round-robin scheduling algorithm, each station will get an equal share of the channel time regardless of its data rate or traffic demand. However, if the access point uses a proportional fair scheduling algorithm, each station will get a share of the channel time that is proportional to its data rate and traffic demand, which may result in higher or lower bandwidth for different stations. The presence of co-located (10m away) access points on non-overlapping channels affects the wireless bandwidth because even though they use different channels, they may still cause interference and noise to each other due to channel leakage or imperfect filtering. The interference and noise can degrade the signal quality and SNR of the wireless communication, which reduces the data rate and throughput of the wireless communication. The wireless bandwidth available to each station depends on how well the access point and the station can cope with the interference and noise from other channels. For example, if the access point and the station support dynamic frequency selection (DFS) or adaptive radio management (ARM), they can switch to a less congested channel or adjust their

output power or antenna gain to avoid or minimize interference from other channels. References:1, Chapter 3, page 94;2, Section 3.2

QUESTION 5

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?

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.

Correct Answer: D

What you should tell him is that 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 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. References: [CWNP CertifiedWireless Network Administrator Official Study Guide: ExamCWNA-109], page 227; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 217.

QUESTION 6

Lynne runs a small hotel, and as a value added service for his customers he has implemented a Wi-Fi hot-spot. Lynne has read news articles about how hackers wait at hot- spots trying to take advantage of unsuspecting users. He wants to avoid this problem at his hotel.

What is an efficient and practical step that Lynne can take to decrease the likelihood of active attacks on his customers\\' wireless computers?

A. Enable station-to-station traffic blocking by the access points in the hotel.

B. Implement Network Access Control (NAC) and require antivirus and firewall software along with OS patches.

C. Implement an SSL VPN in the WLAN controller that initiates after HTTPS login.

D. Require EAP-FAST authentication and provide customers with a username/password on their receipt.

Correct Answer: A

In a public Wi-Fi hotspot, like the one Lynne runs in his hotel, ensuring customer security against active attacks is crucial. Active attacks involve unauthorized access, eavesdropping, or manipulation of the network traffic. To mitigate

such

threats, an effective and practical step is:

Station-to-Station Traffic Blocking: Also known as client isolation, this feature prevents direct communication between devices connected to the Wi-Fi network. By enabling this on the access points, Lynne can significantly decrease the

likelihood of active attacks like man-in-the-middle (MITM) attacks, where an attacker intercepts and possibly alters the communication between two parties. The other options, while beneficial for network security, might not be as

straightforward or practical for Lynne\\'s situation:

Network Access Control (NAC)requires a more complex infrastructure and management, which might not be ideal for a small hotel setup. Implementing an SSL VPNadds an extra layer of security but might complicate the login process for

users, potentially affecting the user experience. Requiring EAP-FAST authenticationprovides secure authentication but may not be feasible for transient customers who expect quick and easy network access. Therefore, enabling station-tostation traffic blocking is a practical and efficient measure that Lynne can implement to enhance customer security on the Wi-Fi network.

References:

CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott. Best practices for securing a wireless network in a public hotspot environment.

QUESTION 7

What factor is likely to cause the least impact on the application layer throughput of an 802.11n client station in a 2.4 GHz HT BSS?

A. Increasing or decreasing the number of spatial streams in use by the client station and AP

B. Implementing Fast BSS Transition (FT) for roaming

C. Implementation of several other clients in the same BSS using 802.11g radios

D. RF interference from more than 10 nearby Bluetooth transmitters

Correct Answer: B

Implementing Fast BSS Transition (FT) for roaming is likely to cause the least impact on the application layer throughput of an 802.11n client station in a 2.4 GHz HT BSS. FT is a feature that allows a client station to quickly switch from one AP to another within the same ESS (Extended Service Set) without having to re-authenticate and re- associate with each AP. This reduces the latency and packet loss that may occur during roaming, thus improving the user experience and maintaining the application layer throughput. FT is defined in the IEEE 802.11r amendment and is also known as Fast Roaming or Fast Secure Roaming. References: , Chapter 9, page 367; , Section 6.3

QUESTION 8

You are a small business wireless network consultant and provide WLAN services for various companies. You receive a call from one of your customers stating that their laptop computers suddenly started experiencing much slower data

transfers while connected to the WLAN. This company is located in a multi-tenant office building and the WLAN was designed to support laptops, tablets and mobile phones. What could cause a sudden change in performance for the laptop computers?

A. The sky was not as cloudy that day as it typically is and the sun also radiates electromagnetic waves.

B. A new tenant in the building has set their AP to the same RF channel that your customer is using.

C. The antennas in the laptops have been repositioned.

D. A few of your customer\\'s users have Bluetooth enabled wireless headsets.

Correct Answer: B

A possible cause of a sudden change in performance for the laptop computers is that a new tenant in the building has set their AP to the same RF channel that your customer is using. This can create co-channel interference (CCI), which is a situation where two or more APs or devices use the same or overlapping channels in the same area. CCI can degrade the performance of WLANs by increasing contention, collisions, retransmissions, and latency. CCI can also reduce the effective range and throughput of WLANs by lowering the signal-to-noise ratio (SNR). To avoid or mitigate CCI, it is recommended to use non- overlapping channels, adjust transmit power levels, or implement channel management techniques such as dynamic frequency selection (DFS) or load balancing. The sky condition, antenna position, or Bluetooth headset are not likely to cause a sudden change in performance for the laptop computers. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 81; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 71.

QUESTION 9

The IEEE 802.11-2012 standard requires VHT capable devices to be backward compatible with devices using which other 802.11 physical layer specifications (PHYs)?

A. OFDM

B. HR/DSSS

C. ERP-PBCC

D. DSSS-OFDM

Correct Answer: A

OFDM (Orthogonal Frequency Division Multiplexing) is the physical layer specification (PHY) that VHT capable devices must be backward compatible with according to the IEEE 802.11-2012 standard. VHT (Very High Throughput) is aPHY and MAC enhancement that is defined in the IEEE 802.11ac amendment and is also known as Wi-Fi

5. VHT operates only in the 5 GHz band and uses features such as wider channel bandwidths (up to 160 MHz), higher modulation schemes (up to 256-QAM), more spatial streams (up to eight), multi-user MIMO (MU-MIMO), beamforming, and VHT PHY and MAC enhancements. VHT can achieve data rates up to 6.9 Gbps. According to the IEEE 802.11-2012 standard, VHT capable devices must be backward compatible with devices using OFDM PHY, which is defined in the IEEE 802.11a amendment and is also used by IEEE 802.11g, IEEE 802.11n, and IEEE 802.11h amendments. OFDM operates in both the 2.4 GHz and 5 GHz bands and uses features such as subcarriers, symbols, guard intervals, and OFDM PHY and MAC enhancements. OFDM can achieve data rates up to 54 Mbps. Backward compatibility means that VHT capable devices can interoperate with OFDM devices on the same network by using common features and parameters that are supported by both PHYs. For example, VHT capable devices can use a channel bandwidth of 20 MHz, a modulation scheme of BPSK, QPSK, or 16-QAM, one spatial stream, no beamforming, and OFDM PHY and MAC headers when communicating with OFDM devices. Backward compatibility also means that

VHT capable devices can fall back to OFDMmode when the signal quality or SNR is too low for VHT mode. References: 1, Chapter 3, page 123; 2, Section 3.2

QUESTION 10

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

Correct Answer: B

In wireless communication, several factors influence the effective reception of RF signals, including the receiving station\\'s radio sensitivity, the transmitting station\\'s output power, and free space path loss. However, the receiving station\\'s

output power does not influence the distance at which an RF signal can be effectively received. The key factors that impact signal reception distance are:

Receiving Station\\'s Radio Sensitivity: This refers to the lowest signal strength at which the receiver can process a signal with an acceptableerror rate. Higher sensitivity allows for better reception at greater distances. Transmitting Station\\'s

Output Power: This is the power with which a transmitter sends out a signal. Higher output power can extend the range of transmission, making it easier for distant receivers to detect the signal. Free Space Path Loss (FSPL): FSPL

represents the attenuation of radio energy as it travels through free space. It increases with distance and frequency, reducing the signal strength as the distance from the transmitter increases. The output power of the receiving station is

related to how strong a signal it sends out, not how well it can receive or process incoming signals. Therefore, it does not affect the reception distance of incoming RF signals.

References:

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

RF fundamentals and RF design considerations in wireless communication systems.

QUESTION 11

What statement describes the authorization component of a AAA implementation?

A. Verifying that a user is who he says he is.

B. Implementing a WIPS as a full-time monitoring solution to enforce policies.

C. Granting access to specific network services or resources according to a user profile.

D. Validating client device credentials against a database.

Correct Answer: C

Granting access to specific network services or resources according to a user profile describes the authorization component of a AAA implementation. AAA stands for Authentication, Authorization, and Accounting, which are three functions that are used to control and monitor access to network resources and services. Authentication is the process of verifying that a user is who he says he is, by using credentials such as username, password, certificate, token, or biometric data. Authorization is the process of granting access to specific network services or resources according to a user profile, which defines the user\\'s role, privileges, and permissions. Accounting is the process of recording and reporting the usage of network services or resources by a user, such as the duration, volume, type, and location of the access. AAA can be implemented by using different protocols andservers, such as RADIUS, TACACS+, LDAP, Kerberos, or Active Directory. References: 1, Chapter 11, page 449; 2, Section 7.1

QUESTION 12

When implementing PoE, what role is played by a switch?

A. PSE

B. Midspan injector

C. PD

D. Power splitter

Correct Answer: A

PoE stands for Power over Ethernet, which is a technology that allows network devices to receive power and data over the same Ethernet cable. PoE eliminates the need for separate power adapters or outlets for devices such as IP phones, cameras, or APs. PoE requires two types of devices: PSE (Power Sourcing Equipment) and PD (Powered Device). A PSE is a device that provides power to the Ethernet cable, such as a switch, injector, or splitter. A PD is a device that receives power from the Ethernet cable, such as an IP phone, camera, or AP. When implementing PoE, a switch plays the role of a PSE910. References: CWNA-109 Study Guide, Chapter 7: Power over Ethernet (PoE), page 293; CWNA109Study Guide, Chapter 7: Power over Ethernet (PoE), page 287.

QUESTION 13

What cipher suite is specified by the 802.11-2016 standard and is not deprecated?

A. Wired Equivalent Privacy

B. Temporal Key Integrity Protocol

C. Counter Mode with CBC-MAC Pro tocol

D. Extensible Authentication Protocol

Correct Answer: C

The cipher suite specified by the 802.11-2016 standard and is not deprecated is Counter Mode with CBC-MAC Protocol (CCMP). CCMP is an encryption protocol that uses Advanced Encryption Standard (AES) as the underlying cipher and

provides confidentiality, integrity, and origin authentication for wireless data. CCMP is the mandatory encryption protocol for WPA2 and WPA3. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA109], page 295; [IEEE Standard for Information technology?elecommunications and information exchange between systems Local and metropolitan area networks?pecific requirements - Part 11:

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications], page 1560.

QUESTION 14

ABC Company is planning a point-to-multipoint outdoor bridge deployment with standalone (autonomous) 802.11 bridge units. 802.1X/EAP will be used for bridge authentication. A Linux-based RADIUS server will be used for authentication. What device in the bridge implementation acts as the 802.1X Authenticator?

A. The Ethernet switch

B. The RADIUS server

C. All non-root bridges

D. The root bridge

Correct Answer: D

The device in the bridge implementation that acts as the 802.1X Authenticator is the root bridge. The root bridge is the bridge that connects to the wired network and acts as the central point for all other bridges in the point-to-multipoint

topology. The root bridge authenticates the non-root bridges using 802.1X/EAP and forwards their authentication requests to the RADIUS server. The non-root bridges act as the 802.1X Supplicants and use EAP methods such as EAP-TLS or

EAP-PEAP to authenticate with the root bridge. References: [CWNP Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109], page 459; [Cisco Aironet Wireless Bridges FAQ], question 29.

QUESTION 15

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.

A. 802.1X/EAP, WEP

B. CCMP, TKIP

C. TLS, SSL

D. RC5, RC4

Correct Answer: B