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.leads4pass.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

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.

Correct Answer: A

The response that you should give to your manager\\'s suggestion of implementing the security practices of disabling the broadcasting of the SSID in Beacons and configuring the access points not to respond to Probe Request frames that have a null SSID field is that 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. The SSID (Service Set Identifier) is a human-readable name that identifies a WLAN and allows users to connect to it. The SSID is transmitted in clear text in several types of 802.11 frames, such as Beacon frames, Probe Request frames, Probe Response frames, Association Request frames, Association Response frames, Reassociation Request frames, and Reassociation Response frames. Some people may think that hiding the SSID can improve the security of the WLAN by making it invisible to potential intruders. However, this is not true, as hiding the SSID only removes it from Beacon frames and Probe Response frames that have a null SSID field. The SSID is still present in other types of frames that can be easily captured and analyzed by any 802.11 protocol analyzer or wireless scanner tool. Therefore, hiding the SSID does not provide any real security benefit and may even cause some compatibility and performance issues for legitimate users. References: 1, Chapter 4, page 133; 2, Section 4.1

QUESTION 2

The center frequency of channel 1 in the 2.4 GHz band is 2.412 GHz (2412 MHz). What is the center frequency of channel 4?

A. 2.427

B. 2.422

C. 2.413

D. 2.417

Correct Answer: A

The center frequency of channel 4 in the 2.4 GHz band is 2.427 GHz (2427 MHz). The center frequency of a channel is

the midpoint of its frequency range, where the signal strength is highest and most concentrated. The center frequency of channel 1 in the 2.4 GHz band is 2.412 GHz (2412 MHz), as given in the question. The center frequency of each subsequent channel is obtained by adding 5 MHz to the previous channel\\'s center frequency, since the channels are spaced 5 MHz apart from each other in this band. Therefore, to find the center frequency of channel 4, we need to add 15 MHz (5 MHz x 3) to the center frequency of channel 1:

2.412 GHz + 0.015 GHz = 2.427 GHz

Alternatively, we can use a formula to calculate the center frequency of any channel in the 2.4 GHz band:

Center frequency (GHz) = 2.407 + (0.005 x Channel number) Using this formula for channel 4, we get:

Center frequency (GHz) = 2.407 + (0.005 x 4)

Center frequency (GHz) = 2.407 + 0.02

Center frequency (GHz) = 2.427 References: 1, Chapter 3, page 85; 2, Section 3.2

QUESTION 3

An 802.11 WLAN transmitter that emits a 50 mW signal is connected to a cable with 3 dB of loss. The cable is connected to an antenna with 16 dBi of gain. What is the power level at the Intentional Radiator?

A. 25 mW

B. 250 mW

C. 500 mW

D. 1000 mW

Correct Answer: B

The power level at the Intentional Radiator (IR) is 250 mW. The IR is the point where the RF signal leaves the transmitter and enters the antenna system. To calculate the power level at the IR, we need to consider the output power level of

the transmitter, the loss of the cable, and the gain of the antenna. The formula is:

Power level at IR (dBm) = Output power level (dBm) - Cable loss (dB) + Antenna gain (dBi) We can convert the output power level of 50 mW to dBm by using the formula:

Power level (dBm) = 10 * log10(Power level (mW))

Therefore, 50 mW = 10 * log10(50) = 16.99 dBm

We can plug in the values into the formula:

Power level at IR (dBm) = 16.99 - 3 + 16 = 29.99 dBm We can convert the power level at IR from dBm to mW by using the inverse formula:

Power level (mW) = 10^(Power level (dBm) / 10)

Therefore, 29.99 dBm = 10^(29.99 / 10) = 999.96 mW However, since we need to round off the answer to the nearest integer value, we get:

Power level at IR (mW) = 1000 mW

References: [CWNP Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109], page 67; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 57.

QUESTION 4

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 5

Your consulting firm has recently been hired to complete a site survey for a company desiring an indoor coverage WI-AN. Your engineers use predictive design software for the task, but the company insists on a pre-design site visit.

What task should be performed as part of the pre-design visit to prepare for a predictive design?

A. Install at least one AP on each side of the exterior walls to test for co-channel interference through these walls

B. Collect information about the company\\'s security requirements and the current configuration of their RADIUS and user database servers

C. Test several antenna types connected to the intended APS for use in the eventual deployment

D. Evaluate the building materials at the facility and confirm that the floor plan documents are consistent with the actual building

Correct Answer: D

A pre-design site visit in preparation for a predictive wireless LAN design is essential for gathering physical and environmental data about the site. The key tasks to be performed during such a visit include:

Evaluating Building Materials: Different materials (concrete, glass, wood, etc.) have varying effects on RF signal propagation. Understanding the materials present helps in accurately predicting how signals will behave within the

environment.

Floor Plan Verification: Ensuring that the floor plan documents are an accurate representation of the actual building layout is crucial. Discrepancies between the floor plans and the physical layout can lead to inaccuracies in the predictive

design.

The other options, while potentially valuable in other contexts, are not directly related to preparing for a predictive design:

Installing APs(option A) for testing co-channel interference is more aligned with an active site survey rather than a pre-design visit for a predictive design. Collecting information about security requirements(option B) is important but is not

directly related to the physical aspects of the site that would impact a predictive design.

Testing antenna types(option C) would typically be part of an active site survey or the actual deployment phase, not a pre-design visit for predictive modeling. Therefore, option D is the correct answer, focusing on evaluating physical aspects

crucial for accurate predictive modeling.

References:

CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott. Best practices for conducting pre-design site visits in wireless network planning.

QUESTION 6

A client complains of low data rates on his computer. When you evaluate the situation, you see that the signal strength is -84 dBm and the noise floor is -96 dBm. The client is an 802.11ac client and connects to an 802.11ac AP. Both the client and AP are 2x2:2 devices. What is the likely cause of the low data rate issue?

A. Weak signal strength

B. CAT5e cabling run to the AP

C. Too few spatial streams

D. Lack of support for 802.11n

Correct Answer: A

Weak signal strength is the likely cause of the low data rate issue for the client that has a signal strength of -84 dBm and a noise floor of -96 dBm. The client is an 802.11ac client and connects to an 802.11ac AP. Both the client and AP are 2x2:2 devices. Signal strength is the measure of how strong the RF signal is at the receiver. Signal strength can affect the reliability and performance of the wireless connection, as well as the data rate and throughput of the traffic. The higher the signal strength, the better the signal quality and the higher the data rate. The lower the signal strength, the worse the signal quality and the lower the data rate. The data rate of an 802.11ac connection depends on several factors, such as channel bandwidth, modulation and coding scheme (MCS), spatial streams, guard interval, and beamforming. However, these factors are also influenced by the signal strength, as they require a certain signal-to-noise ratio (SNR) to operate properly. SNR is the ratio of the signal strength to the noise floor, which is the measure of the background noise or interference in the RF environment. The higher the SNR, the more robust and efficient the

communication. The lower the SNR, the more prone and vulnerable to errors and retries. According to the CWNA Official Study Guide , Table 3.7, page 112, an 802.11ac connection with a channel bandwidth of 80 MHz, an MCS of 9, two spatial streams, a short guard interval, and no beamforming can achieve a maximum data rate of 867 Mbps. However, this data rate requires a minimum SNR of 30 dB to maintain a sufficient signal quality. If the signal strength is -84 dBm and the noise floor is -96 dBm, then the SNR is only 12 dB (-84 dBm - (-96 dBm) = 12 dB), which is far below the required SNR for this data rate. Therefore, the data rate will drop significantly to match the lower SNR and signal quality. To solve this problem, the signal strength should be increased to improve the SNR and data rate. This can be done by adjusting the output power or channel assignment of the AP or client, relocating or reorienting some APs or antennas to reduce attenuation or interference, updating or replacing some faulty oroutdated hardware or software components, etc. References: , Chapter 3, page 112; , Section 3.2

QUESTION 7

You are reconfiguring an AP to use the short guard interval. How long will the new guard interval duration be after the change?

A. 800 ns

B. 400 ns

C. 104 ms

D. 10 ms

Correct Answer: B

The short guard interval is an optional feature of 802.11n and 802.11ac that reduces the time between OFDM symbols from 800 ns to 400 ns. This can increase the data rate by about 11%, but also requires more precise timing and synchronization between the transmitter and the receiver. The short guard interval is only used when both the AP and the client support it and agree to use it . References: [CWNA-109 Study Guide], Chapter 4: Radio Frequency Signal and Antenna Concepts, page 163; [CWNA-109Study Guide], Chapter 4: Radio Frequency Signal and Antenna Concepts, page 157.

QUESTION 8

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?

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.

Correct Answer: A

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 byreducing 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. References: CWNA- 109 Study Guide, Chapter 5: Radio Frequency Signal and Antenna Concepts, page 147

QUESTION 9

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

Correct Answer: D

The FCS (Frame Check Sequence) is appended to the end of each 802.11 data frame after the payload. The FCS is a 4-byte field that contains a CRC-32 (Cyclic Redundancy Check) value that is calculated based on the contents of the MAC header and the payload of the frame. The FCS is used by the receiver to verify the integrity of the frame and to detect any errors or corruption that may have occurred during transmission. If the FCS does not match with the expected value, the frame is discarded by the receiver. References: , Chapter 4, page 139; , Section 4.2

QUESTION 10

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?

A. Diffraction

B. Refraction

C. Scattering

D. Reflection

Correct Answer: B

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. References: 1:CWNA-109Official Study Guide, page 67 2: Refraction

QUESTION 11

To ease user complexity, your company has implemented a single SSID for all employees. However, the network administrator needs a way to control the network resources that can be accessed by each employee based in their department. What WLAN feature would allow the network administrator to accomplish this task?

A. RBAC

B. WPA2

C. WIPS

D. SNMP

Correct Answer: A

The WLAN feature that would allow the network administrator to control the network resources that can be accessed by each employee based on their department is Role-Based Access Control (RBAC). RBAC is a method of assigning different permissions and policies to users or groups based on their roles in the organization. RBAC can be implemented by using VLANs, ACLs, or firewalls to restrict access to certain network segments or resources. RBAC can also be integrated with 802.1X/EAP authentication to dynamically assign roles and VLANs to users based on their credentials. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 403; [Role-Based Access Control (RBAC) in Wireless Networks], page 1.

QUESTION 12

You are tasked with performing a throughput test on the WLAN. The manager asks that you use open source tools to reduce costs. What open source tool is designed to perform a throughput test?

A. iPerf

B. PuTTy

C. IxChariot

D. Python

Correct Answer: A

iPerf is an open source tool that is designed to perform a throughput test on the WLAN. iPerf is a cross-platform command-line tool that can measure the bandwidth and quality of network links by generating TCP or UDP traffic between two endpoints.iPerf can run as either a server or a client mode, depending on whether it receives or sends traffic. iPerf can also report various metrics of network performance, such as throughput, jitter, packet loss, delay, and TCP window size. To perform a throughput test on the WLAN using iPerf, one device needs to run iPerf in server mode and another device needs to run iPerf in client mode. The devices need to be connected to the same WLAN network and have their IP addresses configured properly. The device running iPerf in client mode needs to specify the IP address of the device running iPerf in server mode as well as other parameters such as protocol, port number, duration, interval, bandwidth limit, packet size, etc. The device running iPerf in server mode will listen for incoming connections

from the client device and send back acknowledgments or responses depending on the protocol used. The device running iPerf in client mode will send traffic to the server device according to the specified parameters and measure the network performance. The device running iPerf in client mode will display the results of the throughput test at the end of the test or at regular intervals during the test. The results can show the average, minimum, maximum, and instantaneous throughput of the network link, as well as other metrics such as jitter, packet loss, delay, and TCP window size. References: 1, Chapter 7, page 287; 2, Section 4.3

QUESTION 13

Your manager asked you to locate a solution that allows for centralized monitoring of WLAN performance over time. He wants a single pane of glass for administration and monitoring of the solution. What do you recommend?

A. Laptop-based spectrum analyzers

B. AP-based spectrum analysis

C. Overlay WLAN monitoring solution

D. Laptop-based protocol analyzers

Correct Answer: C

The solution that you recommend is an Overlay WLAN monitoring solution. An Overlay WLAN monitoring solution is a system that uses dedicated sensors or probes to monitor the WLAN performance over time. The sensors are deployed throughout the WLAN coverage area and collect data on various metrics such as signal strength, noise level, channel utilization, interference, throughput, latency, packet loss, and QoS. The sensors send the data to a centralized server or appliance that analyzes the data and provides a single pane of glass for administration and monitoring of the solution. An Overlay WLAN monitoring solution can help to detect and troubleshoot WLAN issues, optimize WLAN performance, and generate reports and alerts. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 538; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA- 109], page 508.

QUESTION 14

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 15

What can cause excessive VSWR in RF cables used to connect a radio to an antenna?

A. High gain yagi antenna

B. Radio output power above 100 mW but below 400 mw

C. High gain parabolic dish antenna

D. Impedance mismatch

Correct Answer: D

Impedance is the measure of opposition to the flow of alternating current (AC) in a circuit. Impedance mismatch occurs when the impedance of the radio does not match the impedance of the antenna or the cable. This causes some of the transmitted or received signal to be reflected back, resulting in a loss of power and efficiency. The voltage standing wave ratio (VSWR) is a metric that indicates the amount of impedance mismatch in a transmission line. A higher VSWR means a higher impedance mismatch and a lower signal quality. A VSWR of 1:1 is ideal, meaning there is no impedance mismatch and no reflected power. A VSWR of 2:1 means that for every 2 units of forward power, there is 1 unit of reflected power12. The other options are not correct because they do not affect the VSWR in RF cables. A high gain yagi antenna or a high gain parabolic dish antenna can increase the signal strength and directionality, but they do not cause impedance mismatch in the cable. Radio output power above 100 mW but below 400 mW is within the acceptable range for most WLAN devices and does not cause excessive VSWR in the cable3. References: 1:CWNA-109Official Study Guide, page 77

2: VSWR 3:CWNA-109Official Study Guide, page 81