[Q43-Q67 Master 2024 Latest The Questions CWNA Certification and Pass CWNA-109 Real Exam!

Master 2024 Latest The Questions CWNA Certification and Pass CWNA-109 Real Exam!
Penetration testers simulate CWNA-109 exam PDF NEW QUESTION 43

A string of characters and digits is entered into an AP and a client STA for WPA2 security. The string is 8 characters long. What is this string called?
* MSK
* WEP key
* Passphrase
* PSK
The string of characters and digits that is entered into an AP and a client STA for WPA2 security and is 8 characters long is called a passphrase. A passphrase is a human-readable text that is used to generate a Pre-Shared Key (PSK) for WPA2-Personal security. A passphrase can be between 8 and 63 characters long and can include any ASCII character. The PSK is a 256-bit key that is derived from the passphrase using a hashing algorithm called PBKDF2. The PSK is used to encrypt and decrypt the data frames between the AP and the client STA. A MSK is a Master Session Key that is generated by an authentication server for WPA2-Enterprise security. A WEP key is a 40-bit or 104-bit key that is used for Wired Equivalent Privacy (WEP) security, which is deprecated and insecure. A PSK is not a string of characters and digits, but a binary key. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 303; [CWNA: Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109], page

293.

NEW QUESTION 44

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&#8217; wireless computers?
* Enable station-to-station traffic blocking by the access points in the hotel.
* Implement Network Access Control (NAC) and require antivirus and firewall software along with OS patches.
* Implement an SSL VPN in the WLAN controller that initiates after HTTPS login.
* Require EAP-FAST authentication and provide customers with a username/password on their receipt.
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&#8217;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-to-station 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.

NEW QUESTION 45

A client STA must choose the best AP for connectivity. As part of the evaluation, it must verify compatible data rates. What can the

client STA use to verify that an AP supports the same data rates that it supports?
* Beacon frames transmitted by the AP
* Data frames sent between the AP and current clients STAs
* Authentication frames transmitted by the other client STAs
* Probe request frames transmitted by other client STAs
The client STA can use Beacon frames transmitted by the AP to verify that an AP supports the same data rates that it supports. Beacon frames are management frames that are periodically broadcasted by the APs to announce their presence, capabilities, and parameters. Oneof the information elements contained in the Beacon frames is the Supported Rates or Extended Supported Rates, which lists the data rates that the AP can use for communication. The client STA can compare its own data rates with those advertised by the AP to determine if they are compatible. Data frames, authentication frames, and probe request frames do not contain information about data rates. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 133; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 123.

NEW QUESTION 46

Which IEEE 802.11 physical layer (PHY) specification includes support for operation in the 2.4 GHz, 5 GHz, and 6 GHz bands?
* VHT (802.11ac).
* HT(802.11n)
* HR/DSSS (802.11b)
* HE (802.11ax)
The IEEE 802.11ax standard, also known as High-Efficiency Wireless (HEW) or simply HE, includes support for operation across multiple frequency bands: 2.4 GHz, 5 GHz, and, with the appropriate regulatory approvals, the 6 GHz band. This makes option D the correct answer. Here&#8217;s how it compares to the other options:

* HE (802.11ax): Introduced as an enhancement over previous standards, 802.11ax is designed to improve efficiency, especially in dense environments. It supports operation in the 2.4 GHz, 5 GHz, and

6 GHz bands (the latter pending regulatory approval in various regions), making it highly versatile and future-proof.

* VHT (802.11ac): Very High Throughput, or 802.11ac, operates exclusively in the 5 GHz band. It introduced significant speed improvements over its predecessor (802.11n) but does not support the 2.4 GHz or 6 GHz bands.

* HT (802.11n): High Throughput, or 802.11n, supports operation in both the 2.4 GHz and 5 GHz bands.

However, it does not include support for the 6 GHz band.

* HR/DSSS (802.11b): High-Rate Direct Sequence Spread Spectrum, or 802.11b, operates only in the 2.4 GHz band. It was one of the early Wi-Fi standards and does not support 5 GHz or 6 GHz bands.

Given these distinctions, only 802.11ax (option D) supports operation across all three mentioned bands, aligning with the requirements stated in the question.

References:

* IEEE 802.11ax-2021: High-Efficiency Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

* Understanding the 802.11ax (Wi-Fi 6) standard and its implications for modern wireless networking.

NEW QUESTION 47

What statement about 802.3, Clause 33 Power over Ethernet is true?
* When using CAT5 cabling, you increase the maximum draw available to the PD over that available with CAT6.
* Only endpoint PSEs are supported.
* Only midspan PSEs are supported.
* The lowest voltage drop is achieved when using CAT6 cable instead of Cat5 or CAT5e.
https://www.cablinginstall.com/articles/2012/08/cat-6a-vs-cat-5e-poe.html The statement that the lowest voltage drop is achieved when using CAT6 cable instead of Cat5 or CAT5e is true about 802.3, Clause 33 Power over Ethernet. Power over Ethernet (PoE) is a technology that allows electrical power to be delivered over Ethernet cables along with data signals. PoE is defined by IEEE 802.3, Clause 33 and has several variants, such as PoE (802.3af), PoE+ (802.3at), and PoE++ (802.3bt). PoE works by using a device called PSE (Power Sourcing Equipment) that injects power into the Ethernet cable and a device called PD (Powered Device) that receives power from the Ethernet cable. The PSE can be either an endpoint device, such as a switch or a router, or a midspan device, such as an injector or a splitter, that is inserted between two Ethernet devices. The PD can be any device that requires power, such as an access point, a camera, or a phone.

One of the factors that affects PoE performance is voltage drop, which is the reduction of voltage that occurs as current flows through a cable due to its resistance. Voltage drop can cause power loss and inefficiency in PoE systems, as well as damage to PDs if the voltage falls below their minimum requirement. To minimize voltage drop, it is recommended to use high-quality cables with low resistance and short length. Among the common types of Ethernet cables, CAT6 has the lowest resistance and therefore the lowest voltage drop compared to Cat5 or CAT5e. CAT6 also has higher bandwidth and data rate than Cat5 or CAT5e, making it more suitable for PoE applications. References: 1, Chapter 7, page 263; 2, Section 4.4

NEW QUESTION 48

You are troubleshooting a client problem with a 2.4 GHz WLAN connection. The client is experiencing surprisingly low data rates during the work day. You analyze the workspace outside of business hours and detect a strong signal with a typical noise floor at the client location. During working hours, the user works with a laptop in the area and uses an external USB hard drive for continuous data access. The user also states that the laptop works as expected on her home network. The user working approximately 8 feet away from this client experiences no problems.

Based on this information, what is the likely cause of the problem?
* The AP is overloaded during the work day
* The drivers in the laptop are corrupt
* The laptop has a failing wireless adapter
* The external hard drive is USB 3.0 and is causing a significant increase in the noise floor when in use
The likely cause of the problem is that the external hard drive is USB 3.0 and is causing a significant increase in the noise floor when in use. USB 3.0 devices are known to generate radio frequency interference (RFI) in the 2.4 GHz band due to their high data transfer rates and harmonics. This RFI can increase the noise floor and degrade the signal-to-noise ratio (SNR) of WLAN devices operating in the same band. This can result in lower data rates, reduced throughput, increased retransmissions, and poor performance. The problem may not occur outside of business hours or on the user&#8217;s home network because of different usage patterns or environmental factors. References: [CWNP Certified Wireless Network Administrator Official StudyGuide:

ExamCWNA-109], page 527; [CWNA: Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109], page 497.

NEW QUESTION 49

You manage a WLAN with 100 802.11ac access points. All access points are configured to use 80 MHz channels. In a particular BSS, only 40 MHz communications are seen. What is the likely cause of this behavior?

* All clients implement single spatial stream radios
* The clients are all 802.11n STAs or lower
* The AP is improperly configured to use only 40 MHz of the 80 MHz allocated bandwidth
* The short guard interval is also enabled
https://7signal.com/802-11ac-migration-part-2-whats-nobodys-telling-you-about-80mhz-and-160mhz-channel-bo The clients are all 802.11n STAs or lower is the likely cause of this behavior. If a WLAN with 100 802.11ac access points is configured to use 80 MHz channels, butonly 40 MHz communications are seen in a particular BSS, it means that the clients in that BSS do not support 80 MHz channels. This could be because they are using older standards, such as 802.11n or lower, that do not support 80 MHz channels. Alternatively, they could be using newer standards, such as 802.11ac or ax, but have their channel width settings limited to 40 MHz or lower due to device capabilities or configuration options. In either case, the AP will adapt to the client&#8217;s channel width and use only 40 MHz of the 80 MHz allocated bandwidth to communicate with them.

This will reduce the potential throughput and efficiency of the WLAN. References: , Chapter 3, page 111; , Section 3.2

NEW QUESTION 50

An AP is advertised as a tri-band, 4&#215;4:4, Wi-Fi 6, 802. 11ax AP. Based on this information and assuming it is correctly advertised, what can be determined as certainly true about this AP?
* It supports four channels in 2.4 GHz and 4 channels in 5 GHz
* It supports UL-MU-MIMO
* It uses a modified OpenWRT firmware
* It has 4 radio chains
Based on the information given, what can be determined as certainly true about this AP is that it has 4 radio chains. A radio chain is a hardware component that consists of an antenna, a radio frequency (RF) amplifier, and a transceiver. The number of radio chains indicates how many spatial streams an AP can transmit or receive simultaneously using Multiple Input Multiple Output (MIMO) technology. The notation x:y:z in an AP specification denotes the number of radio chains (x), the number of spatial streams (y), and the number of spatial streams per band (z). Therefore, a tri-band, 4&#215;4:4, Wi-Fi 6, 802.11ax AP has four radio chains in each of its three bands (2.4 GHz, low 5 GHz, and high 5 GHz). It also supports four spatial streams in total and four spatial streams per band. It cannot be determined as certainly true that it supports four channels in each band, UL-MU-MIMO, or uses a modified OpenWRT firmware based on the information given. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 223; [CWNA:

Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 213.

NEW QUESTION 51

What is the final step in an effective troubleshooting process?
* Disable the WLAN
* Verify the solution
* Notify the users of problem resolution
* Document the results
The final step in an effective troubleshooting process is to document the results. Documentation is essential for keeping track of the problem history, the actions taken, the solutions implemented, and the outcomes achieved.

Documentation can also help to prevent future problems, improve best practices, and provide feedback for improvement. Documentation should include relevant information such as problem description, symptoms, root cause analysis, resolution steps, verification methods, and lessons learned. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 513; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 483.

NEW QUESTION 52

What common feature of MDM solutions can be used to protect enterprise data on mobile devices?
* Over-the-air registration
* Onboarding
* Containerization
* Self-registration
A common feature of MDM solutions that can be used to protect enterprise data on mobile devices is containerization. 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. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 336; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 326.

NEW QUESTION 53

What ID is typically mapped to an AP&#8217;s MAC address if a single BSS is implemented?
* SSID
* Device ID
* VLAN ID
* BSSID
The BSSID (Basic Service Set Identifier) is typically mapped to an AP&#8217;s MAC address if a single BSS is implemented. The BSSID is a unique identifier that distinguishes one BSS from another within the same RF medium. It is usually derived from the MAC address of the AP&#8217;s radio interface, but it can also be manually configured or randomly generated by some vendors. The BSSID is used by client stations to associate with an AP and to send and receive frames within a BSS. References: , Chapter 1, page 24; , Section 1.2

NEW QUESTION 54

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?
* Interference from non-Wi-Fi sources
* Faulty drivers
* DoS attack
* Interference from other WLANs
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.

NEW QUESTION 55

What security option for 802.11 networks supports SAE and requires protected management frames?

* WPA
* WPA2
* WPA3
* OWE

The security option for 802.11 networks that supports SAE and requires protected management frames is WPA3. WPA3 stands for Wi-Fi Protected Access version 3 and is the latest security standard for WLANs.

WPA3 supports two modes: WPA3-Personal and WPA3-Enterprise. 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. WPA3 also requires protected management frames, which are encrypted frames that prevent spoofing, replay, or denial-of-service attacks on management frames such as deauthentication or disassociation frames. WPA, WPA2, and OWE do not support SAE or require protected management frames. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 307; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 297.

NEW QUESTION 56

In an 802.11 2.4 GHz system, what 22 MHz channels are considered non-overlapping?

* 7 and 11
* 2 and 8
* 1 and 5
* 4 and 6

In the 2.4 GHz frequency band used for 802.11 wireless networks, the channel bandwidth is typically 20 MHz, but the actual frequency spread of each channel is about 22 MHz due to the modulation techniques used. This spread causes overlap between adjacent channels, which can lead to interference and degrade network performance. To avoid this, it&#8217;s essential to use non-overlapping channels.

The three non-overlapping channels in the 2.4 GHz band are 1, 6, and 11. Each of these channels is spaced sufficiently apart to avoid interference with each other:

* Channel 1: Centered at 2.412 GHz.

* Channel 6: Centered at 2.437 GHz.

* Channel 11: Centered at 2.462 GHz.

Given the options provided, option C (1 and 5) is the closest to a pair of non-overlapping channels, although in practice, channel 5 would still cause some interference with channel 1 due to the 22 MHz spread. The ideal choice for non-overlapping channels would be any two channels among 1, 6, and 11, but this is not an option provided. Therefore, within the given options, 1 and 5 are the best choice, understanding that in a real-world scenario, 1 and 6 or 6 and 11 would be preferred to avoid overlap.

References:

* CWNA Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109, by David D: Coleman and David A. Westcott.

* Understanding 2.4 GHz channel arrangement and interference patterns in 802.11 wireless networks.

NEW QUESTION 57

When using a spectrum to look for non Wi-Fi interference sources, you notice significant interference across the entire 2.4 GHz band (not on a few select frequencies) within the desktop area of a users workspace, but the interference disappears quickly after just 2 meters. What is the most likely cause of this interference?
* USB 3 devices in the user&#8217;s work area
* Bluetooth devices in the user&#8217;s work area
* Excess RF energy from a nearby AP
* Unintentional radiation from the PC power supply
USB 3 devices in the user&#8217;s work area are the most likely cause of this interference when using a spectrum analyzer to look for non-Wi-Fi interference sources. A spectrum analyzer is a tool that measures and visualizes the radio frequency activity and interference in the wireless environment. A spectrum analyzer can show the spectrum usage and energy levels on each frequency band or channel and help identify and locate the sources of interference. Interference is any unwanted signal that disrupts or degrades the intended signal on a wireless channel. Interference can be caused by various sources, such as other Wi-Fi devices, non-Wi-Fi devices, or natural phenomena. Interference can affect WLAN performance and quality by causing signal loss, noise, distortion, or errors. USB 3 devices are non-Wi-Fi devices that use USB 3.0 technology to transfer data at high speeds between computers and peripherals, such as hard drives, flash drives, cameras, or printers. USB 3 devices can generate electromagnetic radiation that interferes with Wi-Fi signals in the 2.4 GHz band, especially when they are close to Wi-Fi devices or antennas. USB 3 devices can cause significant interference across the entire 2.4 GHz band (not on a few select frequencies) within the desktop area of a user&#8217;s workspace, but the interference disappears quickly after just 2 meters. This is because USB 3 devices emit broadband interference that affects all channels in the 2.4 GHz band with a high intensity near the source but a low intensity at a distance due to attenuation. The other options are not likely to cause this interference pattern when using a spectrum analyzer to look for non-Wi-Fi interference sources. Bluetooth devices in the user&#8217;s work area are non-Wi-Fi devices that use Bluetooth technology to communicate wirelessly between computers and peripherals, such as keyboards, mice, headphones, or speakers. Bluetooth devices can cause interference with Wi-Fi signals in the 2.4 GHz band, but they use frequency hopping spread spectrum (FHSS) technique that changes frequencies rapidly and randomly within a range of 79 channels. Therefore, Bluetooth devices do not cause significant interference across the entire 2.4 GHz band (not on a few select frequencies), but rather intermittent interference on some channels at different times. Excess RF energy from a nearby AP is not a non-Wi-Fi interference source but rather a Wi-Fi interference source that occurs when an AP transmits more power than necessary for its coverage area. Excess RF energy from a nearby AP can cause co-channel interference (CCI) with other APs or client devices that use the same channel within range of each other. CCI reduces performance and capacity because it causes contention and collisions on the wireless medium,

NEW QUESTION 58

A dual-band 802.11ac AP must be powered by PoE. As a class 4 device, what power level should be received at the AP?
* 30 W
* 12.95 W
* 25.5 W
* 15.4 W
PoE has different standards that define different power levels for PSEs and PDs. The original standard, IEEE

802.3af, defines two classes of PSEs: Class 3 (15.4 W) and Class 4 (30 W). The newer standard, IEEE 802.3at, also known as PoE+, defines four classes of PSEs: Class 0 (15.4 W), Class 1 (4 W), Class 2 (7 W), and Class 3 (12.95 W). The power level received at the PD is always lower than the power level provided by the PSE, due to cable resistance and power dissipation. The IEEE standards specify the minimum power level that must be received at the PD for each class of PSE. For a Class 4 PSE, the minimum power level received at the PD is

25.5 W910. References: CWNA-109 Study Guide, Chapter 7: Power over Ethernet (PoE), page

295; CWNA-109Study Guide, Chapter 7: Power over Ethernet (PoE), page 289.

NEW QUESTION 59

What statement describes the authorization component of a AAA implementation?
* Verifying that a user is who he says he is.
* Implementing a WIPS as a full-time monitoring solution to enforce policies.
* Granting access to specific network services or resources according to a user profile.
* Validating client device credentials against a database.
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&#8217;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

NEW QUESTION 60

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?
* The sky was not as cloudy that day as it typically is and the sun also radiates electromagnetic waves.
* A new tenant in the building has set their AP to the same RF channel that your customer is using.
* The antennas in the laptops have been repositioned.
* A few of your customer&#8217;s users have Bluetooth enabled wireless headsets.
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.

NEW QUESTION 61

You are implementing a VHT-capable AP. Which one of the following channels is available in the

802.11-2016 standard that was not available before the ratification of 802.11 ac?
* 56
* 161
* 153
* 144
Channel 144 is a new channel that was added to the 5 GHz band by the 802.11ac amendment, which defines the VHT (Very High Throughput) PHY for WLANs. Channel 144 has a center frequency of 5720 MHz and a bandwidth of 20 MHz. It can also be combined with adjacent channels to form wider channels of 40 MHz, 80 MHz, or 160 MHz. Channel 144 is available in some

regions, such as North America and Europe, but not in others, such as Japan and China . References: [CWNA-109 Study Guide], Chapter 3: Antennas and Accessories, page 121; [CWNA-109Study Guide], Chapter 3: Antennas and Accessories, page 115;

[Wikipedia], List of WLAN channels.

NEW QUESTION 62

The requirements for a WLAN you are installing state that it must support unidirectional delays of less than

150 ms and the signal strength at all receivers can be no lower than -67 dBm. What application is likely used that demands these requirements?
* VoIP
* E-Mail
* FTP
* RTLS
VoIP (Voice over Internet Protocol) is an application that is likely used that demands the requirements of unidirectional delays of less than 150 ms and the signal strength at all receivers can be no lower than -67 dBm.

VoIP is an application that allows users to make and receive voice calls over a network, such as the Internet or a WLAN. VoIP is a real-time and interactive application that requires high quality of service (QoS) to ensure good user experience and satisfaction. One of the QoS metrics for VoIP is delay, which is the time it takes for a voice packet to travel from the sender to the receiver. Delay can affect the quality and intelligibility of the voice conversation, as well as the synchronization and naturalness of the dialogue. The ITU-T G.114 recommendation suggests that the maximum acceptable one-way delay for VoIP should be less than 150 ms, as anything higher than that can cause noticeable degradation and annoyance to the users. Another QoS metric for VoIP is signal strength, which 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 VoIP traffic. The CWNA Official Study Guide recommends that the minimum signal strength for VoIP should be -67 dBm, as anything lower than that can cause packet loss, retries, jitter, and other issues that can impair the voice quality. References: 1, Chapter 10, page 398; 2, Section 6.1

NEW QUESTION 63

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?
* RBAC
* WPA2
* WIPS
* SNMP
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.

NEW QUESTION 64

A POE device requires 47 W of power. What POE specification should be used?

* 802.3at
* 802.3af
* 802.3bt
* 802. 11at

A POE device that requires 47 W of power should use the 802.3bt specification. This is because 802.3bt is the latest POE standard that supports up to 90 W of power delivery over four pairs of wires in an Ethernet cable.

The previous POE standards, such as 802.3af and 802.3at, only support up to 15.4 W and 30 W of power delivery over two pairs of wires in an Ethernet cable, respectively. Therefore, they are not sufficient for powering a device that requires 47 W of power. The 802.11at specification does not exist; it is a typo or confusion with the 802.3at specification. References: CWNA-109 Study Guide, Chapter 8: Wireless LAN Access Points, page 2431

NEW QUESTION 65

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

* WPA3-Personal, also called WPA3-SAE, uses an authentication exchange and WPA2-Personal does not
* WPA3-Personal, also called WPA3-SAE, uses a stronger authentication exchange to better secure the network
* WPA3-Personal, also called WPA3-SAE, uses AES for encryption and WPA2-Personal does not
* WPA3-Personal, also called WPA3-SAE, uses a better encryption algorithm than WPA2-Personal

An advantage of using WPA3-Personal instead of WPA2-Personal as a security solution for 802.11 networks is that WPA3-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 exchangeprotocol, 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. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 307; [CWNA:

Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 297.

NEW QUESTION 66

You are attempting to locate the cause of a performance problem in two WLAN cells in a mostly overlapping coverage area. You note that one AP is on channel 1 and the other is on channel 2. When you document your findings, what term do you use to describe the problem in this configuration?

* CCC
* Non-Wi-Fi interference
* CCI
* ACI

The term used to describe the problem in this configuration is Co-Channel Interference (CCI)1. CCI occurs when multiple access points are on the same or overlapping channels, causing interference and degradation in network performance1. In this case, one AP is on channel 1 and the other is on channel 2, which are overlapping channels, leading to CCI1.

NEW QUESTION 67

What 802.11 network configuration would result in multiple stations broadcasting Beacon frames with the same BSSID but with different source addresses?

* Multiple APs have been loaded with the same configuration from an image file.
* A single AP supports multiple BSSs with different SSIDs.
* An IBSS is used instead of a BSS.
* An SCA network is in use.

An IBSS is used instead of a BSS is a network configuration that would result in multiple stations broadcasting Beacon frames with the same BSSID but with different source addresses. An IBSS (Independent Basic Service Set) is a type of WLAN that does not use an AP but rather allows stations to communicate directly with each other in a peer-to-peer manner. An IBSS is also known as an ad-hoc network or a peer-to-peer network. In an IBSS, each station generates its own Beacon frames to announce its presence and capabilities to other stations within range. The Beacon frames have the same BSSID, which is randomly generated by one of the stations when creating the IBSS, but they have different source addresses, which are the MAC addresses of each station&#8217;s radio interface. The BSSID is used to identify the IBSS and prevent stations from joining other IBSSs with different BSSIDs.
References: , Chapter 1, page 25; , Section 1.1

Penetration testers simulate CWNA-109 exam: https://www.braindumpsit.com/CWNA-109_real-exam.html