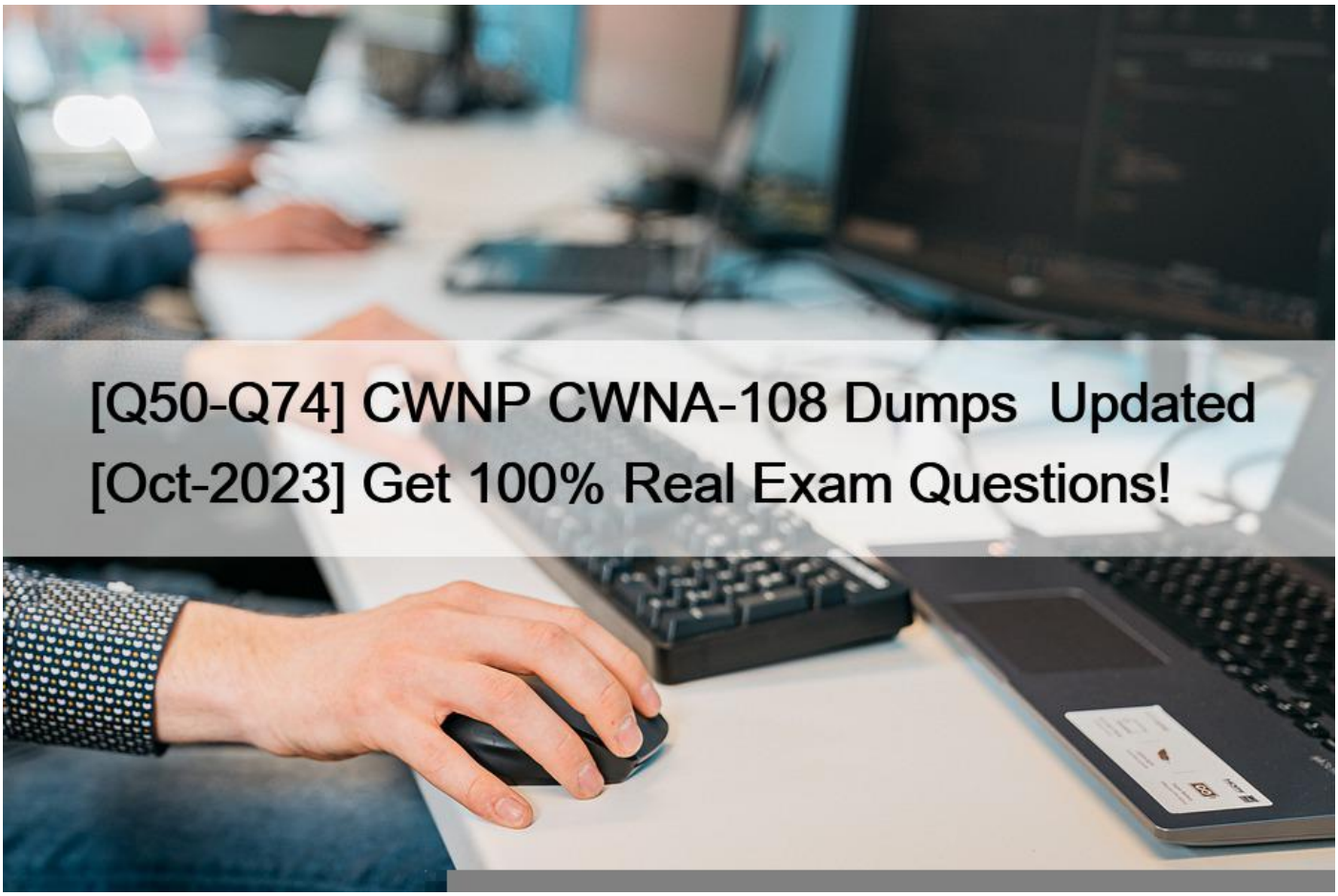
[Q50-Q74 CWNP CWNA-108 Dumps Updated [Oct-2023 Get 100% Real Exam Questions!



[Oct-2023 Pass CWNP CWNA-108 Exam in First Attempt Guaranteed! Full CWNA-108 Practice Test and 120 unique questions with explanations waiting just for you, get it now! Q50. You are using a site survey tool for post-implementation validation. You have installed the appropriate adapter driver and imported a floor plan. Now, you want to take the next step in proper tool use. What must you do before gathering survey data after the floor plan is imported?

* Calibrate the floor plan
* Install WinPCAP
* Nothing, you can simply start capturing signal readings
* Install iPerf

Q51. What statement accurately describes the RF cables and connectors that are used in an

802.11 WLAN system?

* 75 and 125 ohms are the typical impedances of 802.11 WLAN connectors.
* Two RF connectors of the same type (e.g. SMA), manufactured by different companies, may vary in specifications.
* Some RF connectorsdo not cause insertion loss.
* Large diameter RF cables cause greater loss than small diameter cables.

Q52. What component of the 802.11 standard allows stations to reserve access to the RF medium for a specified period of time?
* Short guard intervals
* DTIM Interval
* Listen Interval
* Probe Request frames
* RTS or CTS frames

Q53. 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 on their department.

What WLAN feature would allow the network administrator to accomplish this task?
* RBAC
* SNMP
* WIPS
* WPA2

Q54. 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?
* The Ethernet switch
* The RADIUS server
* All non-root bridges
* The root bridge

Explanation

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: Exam CWNA-107], page 459; [Cisco Aironet Wireless Bridges FAQ], question 29.

Q55. You are configuring an access point to use channel 128. What important fact should be considered about this channel?
* It is a 2.4 GHz frequency band 40 MHz channel, so it should not be used
* It is a 22 MHz channel so it will overlap with the channels above and below it
* It is a channel that may require DFS when used
* It is a channel that is unsupported by all access points in all regulatory domains

Explanation

It is a channel that may require DFS when used is an important fact that should be considered about channel

128. Channel 128 is a 5 GHz frequency band 20 MHz channel that has a center frequency of 5.64 GHz.

Channel 128 is one of the channels that are subject to DFS (Dynamic Frequency Selection) rules, which require Wi-Fi devices to monitor and avoid using channels that are occupied by radar systems or other primary users. DFS is a feature that is defined in the IEEE 802.11h amendment and is mandated by some regulatory bodies, such as the FCC and the ETSI, to protect the licensed users of the 5 GHz band from interference by unlicensed Wi-Fi devices. DFS works by using a mechanism called channel availability

check (CAC), which requires Wi-Fi devices to scan a channel for a certain period of time before using it. If a radar signal is detected during the CAC or while using the channel, the Wi-Fi devices must switch to another channel that is free from radar interference.

When configuring an access point to use channel 128, it is important to consider the implications of DFS rules, such as:

* The access point must support DFS and comply with the local regulations and standards that apply to DFS channels.

* The access point may experience delays or interruptions in its operation due to CAC or channel switching.

* The access point may have limited channel selection or availability due to radar interference or other Wi-Fi devices using DFS channels.

* The access point may have compatibility or interoperability issues with some client devices that do not support DFS or use different DFS parameters.

* The access point may have performance or quality issues due to co-channel or adjacent-channel interference from other Wi-Fi devices using non-DFS channels.

Therefore, it is advisable to use channel 128 only when necessary and after performing a thorough site survey and spectrum analysis to determine the best channel for the access point. References: 1, Chapter 3, page

117; 2, Section 3.2

Q56. 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?
* His concern is valid and the company should upgrade all Ethernet links to 10 Gbps immediately.
* His concern is valid and the company should immediately plan to run a second 1 Gbps Ethernet link to each AP.
* His concern is invalid because the AP will compress all data before transmitting it onto the Ethernet link.
* 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.
Explanation

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 Certified Wireless Network Administrator Official Study Guide: Exam CWNA-107], page 227; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106], page 217.

Q57. 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

Explanation

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 exchange protocol, which is vulnerable to offline brute-force attacks if the passphrase is weak or leaked. Both WPA3-Personal and WPA2-Personal use AES for encryption, so there is no difference in that aspect. WPA3-Personal does not use a different encryption algorithm than WPA2-Personal, but rather a different key exchange protocol. References: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-107], page 307; [CWNA:

Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106], page 297.

Q58. Which directional antenna types are commonly used by indoor Wi-Fi devices in a MIMO multiple spatial stream implementation?
* Dish and grid
* Dipole and yagi
* Grid and sector
* Patch and panel

Q59. 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

Q60. You are troubleshooting a WLAN problem and you suspect hidden node as the cause. What should you look for in a protocol analyzers?
* Frames with the HN bit set to 1
* Frames with the retry bit set to 0
* Frames transmitted from the AP without acknowledgement
* Retransmitted frames from multiple STAs at higher rates than other STAs

http://setup-wireless.blogspot.com/2008/11/wireless-hidden-node.html

Q61. An IEEE 802.11 amendment is in the daft state. What impact does this draft amendment have on the 802.11 standard?
* Devices will be released based on the draft amendment and the draft amendment features are part of the standard.
* No impact: Until an amendment is ratified, it does not become part of the standard.
* No impact: Draft amendments do not become part of the standard until a working group is formed.
* The standard is changed to reflect the new capabilities as soon as an amendment enters the draft stage.

Q62. You are planning for PoE in a standard office deployment. Which one of these devices is least likely to be a PoE PD?
* Video camera
* Access point
* VoIP phone
* Ethernet switch

Q63. What statement about the IEEE 802.11e QoS facility is true?
* 802.11 QoS is achieved by giving high priority queues a statistical advantage at winning contention.
* Four 802.1p user priorities are mapped to eight 802.11 transmit queues.
* When the Voice queue has frames awaiting transmission, no data will be transmitted from the Best Effort queue.
* 802.11 control frames are assigned to the 802.11 EF priority queue.

Q64. An 802.11-based network uses an AP and has several connecting clients. The clients include iPhones, iPads, laptops and one desktop. What WLAN use case is represented?
* Ad-hoc
* WPAN
* BSS
* IBSS

Explanation

A BSS (Basic Service Set) is a WLAN use case that represents an 802.11-based network that uses an AP (Access Point) and has several connecting clients. The AP acts as a central point of coordination and communication for the clients, which can include iPhones, iPads, laptops, desktops, or any other devices that have Wi-Fi capabilities. A BSS can be identified by a unique BSSID (Basic Service Set Identifier), which is usually the MAC address of the AP’s radio interface. A BSS can also be associated with an SSID (Service Set Identifier), which is a human-readable name that identifies the network. References: , Chapter 1, page 23; , Section 1.1

Q65. You are evaluating access points for use in the 5 GHz frequency band. What PHY supports this band and supports 80 MHz channels?
* HT
* VHT
* ERP
* OFDM

Explanation

VHT stands for Very High Throughput, which is a physical layer (PHY) specification that supports the 5 GHz frequency band and supports 80 MHz channels. VHT is used by the IEEE 802.11ac standard, which is also known as Wi-Fi 5. VHT allows for higher data rates and more spatial streams than the previous HT (High Throughput) PHY, which is used by the IEEE 802.11n standard, also known as Wi-Fi 4. HT supports the 2.4 GHz and 5 GHz bands, but only supports up to 40 MHz channels12 The other options are not correct because:

* ERP (option C) stands for Extended Rate PHY, which is a physical layer specification that supports the

2.4 GHz frequency band and supports up to 20 MHz channels. ERP is used by the IEEE 802.11g standard, which is also known as Wi-Fi 3. ERP allows for higher data rates than the previous DSSS (Direct Sequence Spread Spectrum) PHY, which is used by the IEEE 802.11b standard, also known as Wi-Fi 234

* OFDM (option D) stands for Orthogonal Frequency Division Multiplexing, which is a modulation technique that divides a signal into multiple subcarriers that are spaced orthogonally to each other.

OFDM is not a physical layer specification, but a common feature of many PHY specifications, including ERP, HT, and VHT. OFDM allows for higher spectral efficiency and robustness against multipath interference than the previous CCK (Complementary Code Keying) modulation technique used by DSSS34

Q66. What is required when operating 802.11ax APS in the 6 GHz band using passphrase-based authentication?

* VHT PHY
* HT PHY
* SAE
* CCMP

Explanation

SAE (Simultaneous Authentication of Equals) is required when operating 802.11ax APs in the 6 GHz band using passphrase-based authentication. SAE is a secure and robust authentication method that is defined in the IEEE 802.11s amendment and is also known as WPA3-Personal or WPA3-SAE. SAE is based on a cryptographic technique called Dragonfly Key Exchange, which allows two parties to establish a shared secret key using a passphrase, without revealing the passphrase or the key to an eavesdropper or an attacker. SAE also provides forward secrecy, which means that if the passphrase or the key is compromised in the future, it does not affect the security of past communications.

SAE is required when operating 802.11ax APs in the 6 GHz band using passphrase-based authentication because of the new regulations and standards that apply to this band. The 6 GHz band is a new frequency band that was opened for unlicensed use by the FCC and other regulatory bodies in 2020. The 6 GHz band offers more spectrum and less interference than the existing 2.4 GHz and 5 GHz bands, which can enable higher performance and efficiency for Wi-Fi devices. However, the 6 GHz band also has some restrictions and requirements that are different from the other bands, such as:

* The 6 GHz band is divided into two sub-bands: U-NII-5 (5925-6425 MHz) and U-NII-7 (6525-6875 MHz). The U-NII-5 sub-band is subject to DFS (Dynamic Frequency Selection) rules, which require Wi-Fi devices to monitor and avoid using channels that are occupied by radar systems or other primary users. The U-NII-7 sub-band is not subject to DFS rules, but it has a lower maximum transmit power limit than the U-NII-5 sub-band.

* The Wi-Fi devices that operate in the 6 GHz band are called 6E devices, which stands for Extended Spectrum. 6E devices must support 802.11ax technology, which is also known as Wi-Fi 6 or High Efficiency (HE). 802.11ax is a new standard that improves the performance and efficiency of Wi-Fi networks by using features such as OFDMA (Orthogonal Frequency Division Multiple Access), MU-MIMO (Multi-User Multiple Input Multiple Output), BSS Coloring, TWT (Target Wake Time), and HE PHY and MAC enhancements.

* The 6E devices that operate in the 6 GHz band must also support WPA3 security, which is a new security protocol that replaces WPA2 and provides stronger encryption and authentication for Wi-Fi networks. WPA3 has two modes: WPA3-Personal and WPA3-Enterprise. WPA3-Personal uses SAE as its authentication method, which requires a passphrase to establish a secure connection between two devices. WPA3-Enterprise uses EAP (Extensible Authentication Protocol) as its authentication method, which requires a certificate or a credential to authenticate with a server.

Therefore, SAE is required when operating 802.11ax APs in the 6 GHz band using passphrase-based authentication because it is part of WPA3-Personal security, which is mandatory for 6E devices in this band.

References: , Chapter 3, page 120; , Section 3.2

9of30

Q67. During a post-implementation survey, you have detected a non-802.11 wireless device transmitting in the area used by handheld 802.11g scanners. What is the most important factor in determining the impact of this non-802.11 device?
* Receive sensitivity
* Channel occupied
* Airtime utilization
* Protocols utilized

Explanation/Reference:

Q68. What feature(s) are most likely to be supported by 802.11 enterprise-class WLAN controllers?

(Choose 4)
* Link aggregation / port trunking
* 802.1p and DSCP QoS
* BGP and Frame Relay
* Captive web portals
* IGMP snooping

Q69. 802. 11ax (HE) introduces Resource Units that can be used to allow communications with multiple devices at the same time, on the same channel, in the same BSS. What feature of 802.1 lax provides this functionality?
* OFDMA
* Wi-Fi-LTE
* TWT
* 6 GHz support

Explanation

The feature of 802.11ax (HE) that provides this functionality is OFDMA. OFDMA stands for Orthogonal Frequency Division Multiple Access and is a technology that allows multiple devices to communicate simultaneously on the same channel in the same BSS. OFDMA works by dividing a channel into smaller subchannels called Resource Units (RUs), which are composed of groups of subcarriers or tones. Each RU can be assigned to a different device based on its bandwidth requirement and signal quality. This way, OFDMA can increase the efficiency and capacity of the channel by reducing overhead, contention, and latency.

OFDMA can also support both uplink and downlink multi-user transmissions using trigger frames and buffer status reports. 6 GHz support, TWT, and Wi-Fi-LTE are not features of 802.11ax that provide this functionality. References: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-107], page 226; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106], page 216.

Q70. 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
* The AP that covers the problem area requires a firmware update
* The clients are improperly configured
* The AP that covers the problem area has failed
* The AP that covers the problem area is improperly configured

Q71. Users and Network support personnel at a mid-sized equipment manufacturer have been discussing the potential uses and benefits of implementing an indoor WLAN. The network administrator and network manager have requested a meeting of senior management personnel to discuss a WLAN implementation before performing a site survey or taking any implementation steps. The first topic of discussion in the meeting is the corporate policy concerning implementation and use of WLAN technology.

What specific topics are appropriate in this policy meeting? (Choose 2)
* Use of the latest 802.11ac equipment
* Business justification
* User productivity impact
* Antenna types
* Defining RF channels for use

Q72. What is always required to establish a high quality 2.4 GHz RF link at a distance of 3 miles (5 kilometers)?
* Minimum output power level of 2 W
* Grid antennas ateach endpoint
* A minimum antenna gain of 11 dBi at both endpoints
* A Fresnel Zone that is at least 60% clear of obstructions

Explanation

What is always required to establish a high quality 2.4 GHz RF link at a distance of 3 miles (5 kilometers) is a Fresnel Zone that is at least 60% clear of obstructions. The Fresnel Zone is an elliptical-shaped area around the line-of-sight path between two antennas that reflects and refracts the RF waves. The Fresnel Zone radius depends on the frequency of the RF signal and the distance between the antennas. For optimal performance, the Fresnel Zone should be at least 60% clear of any obstructions that may cause interference, attenuation, or multipath fading. The minimum output power level, antenna gain, and antenna type may vary depending on the environmental conditions and regulatory constraints, but they are not always required for a high quality RF link. References: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-107], page 75; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106], page 65.

Q73. What is appended to the end of each 802.11 data frame after the payload?
* Preamble
* MAC header
* PHY header
* FCS

Q74. 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?
* NTP
* BOOTP
* DBS
* AP hosts file