ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

An RF signal sometimes bends as it passes through some material other than free space. What is the term that describes this behavior?

A. Refraction
B. Warping
C. Scattering
D. Reflection

Answer: A

Explanation:

Refraction is the bending of an RF signal as it passes through a medium with a different density than free space. This can cause the signal to change its direction and speed, which can affect the accuracy and reliability of wireless communication. Refraction is influenced by factors such as temperature, humidity, and atmospheric pressure12. Reference: CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 72; CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 67.

Question: 2

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

Answer: D

Explanation:

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. Reference: CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 90; CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 86; CWNP website, CWNA Certification.

Question: 3

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

Answer: B

Explanation:

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 acceptable error 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.

Reference:

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: 4

A WLAN transmitter that emits a 50 mW signal is connected to a cable with 3 dB loss. If the cable is connected to an antenna with 9dBi gain, what is the EIRP at the antenna element?

A. 26 dBm
B. 13 dBm
C. 23 dBm
D. 10 dBm

Answer: C

Explanation:

To calculate the EIRP at the antenna element, we need to add the transmitter output power, subtract the cable loss, and add the antenna gain. All these values need to be converted to dBm first, if they are not already given in that unit. In this case, we have:

Transmitter output power = 50 mW = 10 log (50) dBm = 16.99 dBm Cable loss = 3 dB Antenna gain = 9 dBi EIRP = Transmitter output power - Cable loss + Antenna gain EIRP = 16.99 - 3 + 9 EIRP = 22.99 dBm Rounding up to the nearest integer, we get 23 dBm as the EIRP at the antenna element12. Reference: CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 92; CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 88.

Question: 5

In a long-distance RF link, what statement about Fade Margin is true?

A. A Fade Margin is unnecessary on a long-distance RF link if more than 80% of the first Fresnel zone is clear of obstructions.

B. The Fade Margin is a measurement of signal loss through free space and is a function of frequency and distance.

C. Fade Margin is an additional pad of signal strength designed into the RF system to compensate for unpredictable signal fading.

D. The Fade Margin of a long-distance radio link should be equivalent to the receiver's low noise filter gain.

Answer: C

Explanation:

Fade Margin is an additional pad of signal strength designed into the RF system to compensate for unpredictable signal fading. It is the difference between the receiver's sensitivity and the actual received signal level. A higher Fade Margin indicates a more robust link that can withstand interference, attenuation, or other factors that may reduce the signal strength. A lower Fade Margin means that the link is more susceptible to failure or performance degradation. Fade Margin is usually expressed in decibels (dB) and can be calculated by subtracting the receiver sensitivity from the received signal level. Reference: 1, Chapter 2, page 51; 2, Section 2.1

Question: 6

What wireless networking term describes the increase of RF energy in an intentional direction with the use of an antenna?

A. Directed Radiation

B. Beam Digression

C. Passive Gain

D. Active Amplification

Answer: C

Explanation:

Passive Gain is the increase of RF energy in an intentional direction with the use of an antenna. It is achieved by focusing the same amount of power into a smaller area, resulting in a higher power density and a stronger signal. Passive Gain does not require any additional power or amplification, but rather depends on the antenna's physical characteristics, such as size, shape, and orientation. Passive Gain is also expressed in decibels (dB) and is related to the antenna's beamwidth and directivity. Reference: 1, Chapter 2, page 63; 2,

Section 2.3

Question: 7

Which directional antenna types are commonly used by indoor Wi-Fi devices in a MIMO multiple spatial stream implementation?

A. Dipole and yagi
B. Grid and sector
C. Patch and panel
D. Dish and grid

Answer: C

Explanation:

Patch and panel antennas are directional antenna types that are commonly used by indoor Wi-Fi devices in a MIMO multiple spatial stream implementation. These antennas have a flat rectangular shape and can be mounted on walls or ceilings to provide coverage in a specific direction. They have a moderate gain and a relatively wide beamwidth, making them suitable for multipath environments where signals can reflect off different surfaces and create multiple spatial streams. Patch and panel antennas can also support polarization diversity, which means they can transmit and receive both horizontally and vertically polarized waves, increasing the MIMO performance. Reference: 1, Chapter 2, page 72; 2, Section 2.4

Question: 8

What statement about the beamwidth of an RF antenna is true?

A. Horizontal and vertical beamwidth are calculated at the points where the main lobe decreases power by 3 dB.
B. The beamwidth patterns on an antenna polar chart indicate the point at which the RF signal stops propagating.
C. When antenna gain is lower, the beamwidth is also lower in both the horizontal and vertical dimensions.
D. Vertical beamwidth is displayed (in degrees) on the antenna's Azimuth chart.

Answer: A

Explanation:

The beamwidth of an RF antenna is the angular measure of how wide the main lobe of radiation is. The main lobe is the area where the signal strength is highest and most concentrated. The beamwidth is calculated at the points where the main lobe decreases power by 3 dB, which means it is half of the maximum power. The beamwidth can be measured in both horizontal and vertical planes, depending on how the antenna is oriented. The horizontal beamwidth is also called azimuth, while the vertical beamwidth is also called elevation. The beamwidth patterns on an antenna polar chart indicate how the RF energy is distributed in different directions. Reference: 1, Chapter 2, page 66; 2, Section 2.3

Question: 9

Which one of the following is not a factor considered when calculating the Link Budget for an outdoor point-to- point WLAN bridge link?

A. Operating frequency
B. MU-MIMO capabilities of the bridges
C. Receive antenna gain
D. Transmit power

Answer: B

Explanation:

MU-MIMO capabilities of the bridges are not a factor considered when calculating the Link Budget for an outdoor point-to-point WLAN bridge link. The Link Budget is a calculation of the expected signal strength at the receiver based on various factors that affect the RF transmission. Some of these factors are operating frequency, transmit power, receive antenna gain, free space path loss, cable loss, connector loss, and environmental loss. MU-MIMO stands for Multi-User Multiple Input Multiple Output, which is a technology that allows multiple devices to communicate simultaneously using multiple spatial streams. MU-MIMO is not relevant for a point-to-point link, where there are only two devices involved. Reference: 1, Chapter 2, page 59; 2, Section 2.2

Question: 10

What best describes WPA2 in relation to 802.11 wireless networks?

A. WPA2 is the standard that defines security for WLANs.
B. WPA2 is a certification created by the Wi-Fi Alliance that validates devices correctly implement CCMP/ AES.
C. WPA2 is the second version of WPA and it enhances security through the use of TKIP instead of WEP.
D. WPA2 is specified in the 802.11 standard as implementing CCMP/AES.

Answer: B

Explanation:

WPA2 (Wi-Fi Protected Access 2) is a security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. It is important to understand the following:
WPA2 and the 802.11 Standard: While WPA2 is based on elements of the 802.11i amendment to the 802.11 standard, it is not itself a standard but rather a certification to ensure devices comply with certain security criteria, including the correct implementation of CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) and AES (Advanced Encryption Standard).
CCMP/AES Implementation: WPA2 enhances the security of wireless networks by using CCMP for encryption, which is based on AES, a robust encryption algorithm. This represents a significant security improvement over WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) that used TKIP (Temporal Key Integrity Protocol).
WPA vs. WPA2: WPA was the interim security enhancement over WEP, utilizing TKIP for encryption. WPA2, however, moved to the more secure AES-based encryption method. Contrary to option C, WPA2 does not

enhance security by using TKIP; it uses CCMP/AES.
Therefore, option B correctly describes WPA2 as a certification program ensuring devices properly implement the more secure CCMP/AES encryption methods.

Reference:

Wi-Fi Alliance website for WPA2 certification details.
IEEE 802.11i-2004: Amendment for Enhanced Security.

Question: 11

An IEEE 802.11 amendment is in the daft state. What impact does this draft amendment have on the 802.11 standard?

A. Devices will be released based on the draft amendment and the draft amendment features are part of the standard.
B. No impact: Until an amendment is ratified, it does not become part of the standard.
C. No impact: Draft amendments do not become part of the standard until a working group is formed.
D. The standard is changed to reflect the new capabilities as soon as an amendment enters the draft stage.

Answer: B

Explanation:

An IEEE 802.11 amendment is a proposed change or addition to the existing 802.11 standard, which defines the specifications and protocols for wireless LANs. An amendment goes through several stages of development, such as draft, sponsor ballot, and final approval, before it is ratified by the IEEE Standards Association and becomes part of the standard. Until then, it has no official impact on the standard, although some vendors may release products based on draft amendments to gain a competitive edge or to influence the final outcome of the amendment . Reference: [CWNA-109 Study Guide], Chapter 1: Overview of Wireless Standards, Organizations, and Fundamentals, page 25; [CWNA-109 Study Guide], Chapter 1: Overview of Wireless Standards, Organizations, and Fundamentals, page 23; [IEEE website], IEEE-SA Standards Development Process.

Question: 12

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?

A. 56
B. 161
C. 153
D. 144

Answer: D

Explanation:

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 . Reference: [CWNA-109 Study Guide], Chapter 3: Antennas and Accessories, page 121; [CWNA-109 Study Guide], Chapter 3: Antennas and Accessories, page 115; [Wikipedia], List of WLAN channels.

Question: 13

What statement is true concerning the use of Orthogonal Frequency Division Multiplexing (OFDM) modulation method in IEEE 802.11 WLANs?

A. OFDM implements BPSK modulation to allow for data rates up to 7 Gbps.
B. OFDM was first introduced in 802.11a and is used by the ERP, HT and VHT PHYs as well.
C. OFDM modulation is used only in 5 GHz 802.11 transmissions.
D. OFDM was used by Frequency Hopping Spread Spectrum (FHSS) PHY devices.

Answer: B

Explanation:

OFDM is a modulation method that divides the channel bandwidth into multiple subcarriers, each carrying a single data symbol. This allows for higher data rates and more robust transmissions in multipath environments. OFDM was first introduced in the 802.11a standard, which operates in the 5 GHz band and supports data rates up to 54 Mbps. Later, the 802.11g standard adopted OFDM for the 2.4 GHz band, and the 802.11n and 802.11ac standards enhanced OFDM with features such as MIMO (Multiple Input Multiple Output), channel bonding, and higher-order modulation schemes to achieve

data rates up to 600 Mbps and 6.9 Gbps, respectively. These standards are collectively known as the ERP (Extended Rate PHY), HT (High Throughput), and VHT (Very High Throughput) PHYs
. Reference: [CWNA-109 Study Guide], Chapter 4: Radio Frequency Signal and Antenna Concepts, page 163; [CWNA-109 Study Guide], Chapter 4: Radio Frequency Signal and Antenna Concepts, page 157.

Question: 14

Which IEEE 802.11 physical layer (PHY) specification includes support for and compatibility with both ERP and HR/DSSS?

A. DSSS (802.11-Prime)
B. OFDM (802.11a)
C. HT (802.11n)
D. VHT (802.11ac)

Answer: C

Explanation:

The HT (802.11n) physical layer (PHY) specification includes support for and compatibility with both ERP and HR/DSSS. ERP stands for Extended Rate PHY, which is an extension of the original DSSS (Direct Sequence Spread Spectrum) PHY that supports data rates up to 54 Mbps in the 2.4 GHz band. HR/DSSS stands for High Rate/Direct Sequence Spread Spectrum, which is another extension of DSSS that supports data rates up to 11

Mbps in the 2.4 GHz band. HT stands for High Throughput, which is a new PHY that supports data rates up to 600 Mbps in both the 2.4 GHz and 5 GHz bands. HT uses OFDM (Orthogonal Frequency Division Multiplexing) as its modulation scheme, but it also supports legacy DSSS and ERP devices by using a dual preamble and header structure that allows backward compatibility. Reference: , Chapter 3, page 103; , Section 3.1

Question: 15

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?

A. Ad-hoc
B. WPAN
C. BSS
D. IBSS

Answer: C

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. Reference: , Chapter 1, page 23; , Section 1.1

Question: 16

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

Answer: B

Explanation:

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. Reference: , Chapter 9, page 367; , Section 6.3

Question: 17

What ID is typically mapped to an AP's MAC address if a single BSS is implemented?

A. SSID
B. Device ID
C. VLAN ID
D. BSSID

Answer: D

Explanation:

The BSSID (Basic Service Set Identifier) is typically mapped to an AP'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'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. Reference: , Chapter 1, page 24; , Section 1.2

Question: 18

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

Answer: D

Explanation:

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. Reference: , Chapter 4, page 139; , Section 4.2

Question: 19

When an ACK frame is not received by the transmitting STA, what is assumed?

A. The receiver processed the frame, but did not respond with an ACK frame because 802.11w is enabled
B. The frame was correctly delivered
C. The frame was not delivered and must be retransmitted
D. The receiver is offline

Answer: C

Explanation:

An ACK (Acknowledgement) frame is a short control frame that is sent by the receiver of a data or management frame to confirm that the frame was received correctly. The ACK frame is sent after a SIFS (Short Interframe Space) interval, which is the shortest time gap between frames in 802.11. If the transmitter does not receive an ACK frame within a specified time, it assumes that the frame was not delivered and must be retransmitted. This is part of the 802.11 reliability mechanism that ensures reliable data delivery over an unreliable wireless medium . Reference: [CWNA-109 Study Guide], Chapter 5: IEEE 802.11 Medium Access, page 209; [CWNA-109 Study Guide], Chapter 5: IEEE 802.11 Medium Access, page 203.

Question: 20

When a client station sends a broadcast probe request frame with a wildcard SSID, how do APs respond?

A. Each AP responds in turn after preparing a probe response and winning contention.
B. For each probe request frame, only one AP may reply with a probe response.
C. Each AP checks with the DHCP server to see if it can respond and then acts accordingly.
D. After waiting a SIFS, all APs reply at the same time with a probe response.

Answer: A

Explanation:

In the 802.11 wireless networking protocols, when a client station sends a broadcast probe request frame with a wildcard SSID (Service Set Identifier), it is essentially asking for any nearby access points (APs) to identify themselves. The way APs respond to such a probe request is governed by standard 802.11 behavior, which includes:
Probe Request Handling: Upon receiving a broadcast probe request, each AP that can serve the client prepares a probe response. The response includes information about the AP, such as its SSID, supported data rates, and other capabilities.
Contention-Based Mechanism: Wireless networks use a contention-based mechanism (CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance) for medium access. Each AP must wait for a clear channel and win the contention process before it can send its probe response.
Independent Responses: Each AP operates independently in responding to the probe request. There is no coordination between APs to decide which one responds first or at all, leading to multiple APs sending probe responses, each after winning the contention for the medium.
Option A accurately reflects this process, indicating that each AP prepares and sends a probe response in turn, contingent upon winning the medium contention. The other options suggest mechanisms (such as coordination with a DHCP server or simultaneous responses after a Short Interframe Space (SIFS)) that do not align with standard 802.11 procedures for handling broadcast probe requests.
Reference:
IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. CWNA Certified Wireless Network Administrator Official Study Guide: Exam PW0-105, by David D. Coleman and David A. Westcott.

Question: 21

What security solution is deprecated in the 802.11 standard and should never be used in any modern WLAN deployment?

A. Shared Key Authentication
B. Open System Authentication
C. CCMP
D. AES

Answer: A

Explanation:

Shared Key Authentication is a security solution that was defined in the original 802.11 standard as an alternative to Open System Authentication, which does not provide any security at all. Shared Key Authentication uses WEP (Wired Equivalent Privacy) to encrypt and authenticate data frames between the client station and the AP. However, WEP has been proven to be extremely vulnerable to various attacks that can easily crack the encryption key and compromise the network security.
Therefore, Shared Key Authentication is deprecated in the 802.11 standard and should never be used in any modern WLAN deployment . Reference: [CWNA-109 Study Guide], Chapter 10: Wireless LAN Security, page 401; [CWNA-109 Study Guide], Chapter 10: Wireless LAN Security, page 391; [Wikipedia], Wired Equivalent Privacy.

Question: 22

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

Answer: B

Explanation:

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 . Reference: [CWNA-109 Study Guide], Chapter 4: Radio Frequency Signal and Antenna Concepts, page 163; [CWNA-109 Study Guide], Chapter 4: Radio Frequency Signal and Antenna Concepts, page 157.

Question: 23

What statement about the IEEE 802.11-2016 QoS facility is true?

A. 802.11 control frames are assigned to the 802.11 EF priority queue.
B. When the Voice queue has frames awaiting transmission, no data will be transmitted from the Best Effort queue.
C. 802.11 QoS is achieved by giving high priority queues a statistical advantage at winning contention.
D. Four 802.1p user priorities are mapped to eight 802.11 transmit queues.

Answer: C

Explanation:

802.11 QoS is achieved by giving high priority queues a statistical advantage at winning contention. 802.11 QoS is based on the Enhanced Distributed Channel Access (EDCA) mechanism, which defines four access categories (ACs) for different types of traffic: Voice, Video, Best Effort, and Background. Each AC has its own transmit queue and contention parameters, such as Arbitration Interframe Space (AIFS), Contention Window (CW), and Transmission Opportunity (TXOP). These parameters determine how long a station has to wait before transmitting a frame and how long it can occupy the channel. Higher priority ACs have shorter AIFS, smaller CW, and longer TXOP, which means they have more chances to access the channel and send more data than lower priority ACs. However, this does

not guarantee that higher priority ACs will always win the contention, as there is still a random backoff process involved. Therefore, 802.11 QoS is a statistical service that provides different levels of service quality based on traffic categories. Reference: , Chapter 10, page 403; , Section 6.1

Question: 24

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?

A. All clients implement single spatial stream radios
B. The clients are all 802.11n STAs or lower
C. The AP is improperly configured to use only 40 MHz of the 80 MHz allocated bandwidth
D. The short guard interval is also enabled

Answer: B

Explanation:

https://7signal.com/802-11ac-migration-part-2-whats-nobodys-telling-you-about-80mhz-and-160mhz-channel-bonding

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, but only 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'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. Reference: , Chapter 3, page 111; , Section 3.2

Question: 25

When compared with legacy Power Save mode, how does VHT TXOP power save improve battery life for devices on a WLAN?

A. Legacy Power Save mode was removed in the 802.11ac amendment.
B. VHT TXOP power save allows the WLAN transceiver to disable more components when in a low power

state.

C. VHT TXOP power save uses the partial AID in the preamble to allow clients to identify frames targeted for them.

D. VHT TXOP power save allows stations to enter sleep mode and legacy Power Save does not.

Answer: B

Explanation:

VHT TXOP (Very High Throughput Transmit Opportunity) power save is a feature introduced with the 802.11ac amendment, which is designed to improve the power efficiency of devices connected to a WLAN. This feature enhances battery life in several ways, compared to the legacy Power Save mode: Enhanced Power Saving: VHT TXOP power save allows devices to disable more components of the WLAN transceiver when they are in a low power state. This reduces the power consumption during periods when the device is not actively transmitting or receiving data.

Intelligent Wake-Up Mechanisms: It employs more sophisticated mechanisms for devices to determine when they need to wake up and listen to the channel, further reducing unnecessary power usage.

Optimized Operation: This power save mode is optimized for the high-throughput environment of 802.11ac networks, allowing devices to efficiently manage power while maintaining high performance.

Legacy Power Save mode, introduced in earlier versions of the 802.11 standards, does not provide the same level of component disablement or the intelligent wake-up mechanisms found in VHT TXOP power save, making option B the correct answer.

Reference:

IEEE 802.11ac-2013 Amendment: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.

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

Question: 26

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

A. Multiple APs have been loaded with the same configuration from an image file.

B. A single AP supports multiple BSSs with different SSIDs.

C. An IBSS is used instead of a BSS.

D. An SCA network is in use.

Answer: C

Explanation:

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's radio interface. The BSSID is used to identify the IBSS and prevent stations from joining other IBSSs

with different BSSIDs. Reference: , Chapter 1, page 25; , Section 1.1

Question: 27

What primary metric of scanning can stations use to select the best AP for connectivity to the desired BSS?

A. Signal strength of AP beacons received.
B. PING latency when testing against an Internet server.
C. Throughput speed in Mbps.
D. FCS errors in frames transmitted to and from the AP.

Answer: A

Explanation:

When a station scans for available wireless networks, it listens for beacon frames sent by APs. A beacon frame contains information about the BSS, such as SSID, supported rates, channel, security, etc. The station also measures the signal strength of the beacon frames, which indicates how well the station can communicate with the AP. The signal strength is usually expressed in dBm or RSSI units. The higher the signal strength, the better the connection quality and performance. Therefore, the station can use the signal strength of AP beacons as the primary metric to select the best AP for connectivity to the desired BSS12. Reference: CWNA-109 Study Guide, Chapter 6: Wireless LAN Devices and Topologies, page 249; CWNA-109 Study Guide, Chapter 6: Wireless LAN Devices and Topologies, page 243.

Question: 28

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.

Answer: A

Explanation:

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 VPN adds an extra layer of security but might complicate the login process for users, potentially affecting the user experience.
Requiring EAP-FAST authentication provides 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.
Reference:
CWNA Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109, by David D. Coleman and David A. Westcott.
Best practices for securing a wireless network in a public hotspot environment.

Question: 29

You have been tasked with creating a wireless link between two buildings on a single campus. The link must support at least 150 Mbps data rates. What kind of WLAN technology role should you deploy?

A. WPAN
B. IBSS
C. Wireless bridging
D. Access BSS

Answer: C

Explanation:

https://www.wlanmall.com/what-is-a-wireless-bridge/
Wireless bridging is a WLAN technology role that allows two or more networks to be connected wirelessly over a distance. A wireless bridge consists of two or more APs that are configured to operate in bridge mode and use directional antennas to establish a point-to-point or point-to- multipoint link. Wireless bridging can support high data rates and is suitable for scenarios where running cables is impractical or expensive. To create a wireless link between two buildings on a single campus that supports at least 150 Mbps data rates, wireless bridging is an appropriate solution678. Reference: CWNA-109 Study Guide, Chapter 6: Wireless LAN Devices and Topologies, page 271; CWNA-109 Study Guide, Chapter 6: Wireless LAN Devices and Topologies, page 265; Wi-Fi Wireless Bridging Explained.

Question: 30

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

A. PSE
B. Midspan injector
C. PD
D. Power splitter

Answer: A

Explanation:

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. Reference: CWNA-109 Study Guide, Chapter 7: Power over Ethernet (PoE), page 293; CWNA-109 Study Guide, Chapter 7: Power over Ethernet (PoE), page 287.

Question: 31

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?

A. 30 W
B. 12.95 W
C. 25.5 W
D. 15.4 W

Answer: C

Explanation:

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

Question: 32

A WLAN is implemented using wireless controllers. The APs must locate the controllers when powered on and connected to the network. Which one of the following methods is commonly used to locate the controllers by the APs?

A. NTP
B. DHCP
C. SNMP
D. GRE

Answer: B

Explanation:

DHCP (Dynamic Host Configuration Protocol) is a commonly used method to locate the controllers by the APs in a WLAN that is implemented using wireless controllers. DHCP is a protocol that allows a device to obtain an IP address and other network configuration parameters from a server. In a wireless controller scenario, the APs can use DHCP to request an IP address from a DHCP server, which can also provide the IP address or hostname of the wireless controller as an option in the DHCP response. This way, the APs can discover the wireless controller and establish a connection with it. Alternatively, the APs can also use other methods to locate the wireless controller, such as DNS (Domain Name System), broadcast or multicast discovery, or manual configuration. Reference: 1, Chapter 8, page 309; 2, Section 5.2

Question: 33

You are implementing a multi-AP WLAN and fast secure roaming is essential. Which one of the following methods is an IEEE 802.11 standard method for fast roaming?

A. FT
B. OKC
C. Load balancing
D. Band steering

Answer: A

Explanation:

FT (Fast Transition) is an IEEE 802.11 standard method for fast roaming. FT is defined in the IEEE 802.11r amendment and is also known as Fast BSS Transition (FBT) or Fast Secure Roaming. 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 security of the connection. FT works by using pre-authentication and key caching mechanisms that allow the client station and the APs to exchange security information before the actual roaming occurs. This way, when the client station decides to roam to a new AP, it can use a fast reassociation request and response that contain only a few fields, instead of a full authentication and association exchange that require more time and data. Reference: 1, Chapter 9, page 367; 2, Section 6.3

Question: 34

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

A. 7 and 11
B. 2 and 8
C. 1 and 5
D. 4 and 6

Answer: C

Explanation:

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'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.

Reference:

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

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

Question: 35

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

Answer: A

Explanation:

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 Reference: 1, Chapter 3, page 85; 2, Section 3.2

Question: 36

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?

A. VoIP
B. E-Mail
C. FTP
D. RTLS

Answer: A

Explanation:

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. Reference: 1, Chapter 10, page 398; 2, Section 6.1

Question: 37

You are deploying a WLAN with the access points configured for 10 mW of output power on the 2.4 GHz radios and 20 mW of output power on the 5GHz radios. Some semi-directional antennas are also in use. What kind of deployment is described?

A. SOHO
B. Residential
C. High density
D. Standard office

Answer: A

Explanation:

A high-density deployment is a wireless network that is designed to support a large number of users and devices in a relatively small area. This type of deployment is often used in enterprise environments, such as offices, schools, and hospitals.

The use of semi-directional antennas in the deployment described in the question is a good indication that it is a high-density deployment. Semi-directional antennas can be used to focus the signal from an access point in a

specific direction. This can help to reduce interference and improve performance in high-density environments.

The other answer choices are less likely to be correct for the following reasons:

SOHO (small office/home office) deployments are typically smaller and less complex than high- density deployments.

Residential deployments are typically even smaller and less complex than SOHO deployments. Standard office deployments may be high-density, but they may also be lower-density.

It is important to note that the type of deployment is not determined solely by the output power of the access points. However, the use of 10 mW of output power on the 2.4 GHz radios and 20 mW of output power on the 5GHz radios is also consistent with a high-density deployment.

Here are some additional tips for deploying a high-density wireless network:

Use a site survey to determine the optimal placement of access points.

Configure the access points to use non-overlapping channels.

Use semi-directional or directional antennas to focus the signal and reduce interference.

Implement a wireless intrusion prevention system (WIPS) to detect and mitigate rogue access points and other security threats.

Question: 38

Option 43 must be configured to allow access points to locate controllers. In what network service should this option be configured?

A. DNS
B. LDAP
C. DHCP
D. RADIUS

Answer: C

Explanation:

DHCP (Dynamic Host Configuration Protocol) is the network service where option 43 must be configured to allow access points to locate controllers. DHCP is a protocol that allows a device to obtain an IP address and other network configuration parameters from a server. In a wireless controller scenario, the access points can use DHCP to request an IP address from a DHCP server, which can also provide the IP address or hostname of the wireless controller as an option in the DHCP response. Option 43 is a vendor-specific option that can be used to encode custom information for different types of devices. For example, Cisco access points can use option 43 to receive the IP address of the wireless controller from the DHCP server, while Aruba access points can use option 43 to receive the hostname of the wireless controller from the DHCP server. This way, the access points can discover the wireless controller and establish a connection with it. Reference: 1, Chapter 8, page 309; 2, Section 5.2

Question: 39

What statement about 802.3, Clause 33 Power over Ethernet is true?

A. When using CAT5 cabling, you increase the maximum draw available to the PD over that available with

CAT6.

B. Only endpoint PSEs are supported.
C. Only midspan PSEs are supported.
D. The lowest voltage drop is achieved when using CAT6 cable instead of Cat5 or CAT5e.

Answer: D

Explanation:

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. Reference: 1, Chapter 7, page 263; 2, Section 4.4

Question: 40

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.

Answer: C

Explanation:

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 and servers, such as RADIUS, TACACS+, LDAP, Kerberos, or Active Directory. Reference: 1, Chapter 11, page 449; 2, Section 7.1

Question: 41

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.

Answer: A

Explanation:

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. Reference: 1, Chapter 4, page 133; 2, Section 4.1

Question: 42

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

Answer: C

Explanation:

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 295; [IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications], page 1560.

Question: 43

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

Answer: A

Explanation:

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 403; [Role-Based Access Control (RBAC) in Wireless Networks], page 1.

Question: 44

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

Answer: D

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 459; [Cisco Aironet Wireless Bridges FAQ], question 29.

Question: 45

You are managing a wireless access point in autonomous mode using the Web based interface. You capture traffic during this management task and notice that you can see the HTML code of the Web pages used for access point management. What error in administration could be the cause of this security concern?

A. IPsec is not in use of the management connection as recommended
B. A VPN with the AP is not established
C. WPA2 is disabled on the WLAN
D. HTTP is in use instead of HTTPS

Answer: D

Explanation:

The error in administration that could be the cause of this security concern is that HTTP is in use instead of HTTPS. HTTP is an unencrypted protocol that transfers data in plain text over the network. This means that anyone who captures the traffic can see the HTML code of the Web pages used for access point management, as well as any sensitive information such as passwords or configuration settings. HTTPS is an encrypted protocol that uses SSL/TLS to secure the data transmission between the Web browser and the Web server. HTTPS prevents anyone from snooping on or tampering with the Web traffic. Therefore, HTTPS should always be used for Web based management of wireless access points, especially in autonomous mode where there is no centralized controller to enforce security policies. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 431; [HTTP vs HTTPS: What's The Difference And Why Should You Care?].

Question: 46

What is the most effective method for testing roaming in relation to 802.11 VoIP handsets?

A. Use a spectrum analyzer to monitor RF activity during a VoIP call.
B. Use a protocol analyzer to capture the traffic generated when a laptop roams.
C. Place a call with the handset and move around the facility to test quality during roaming.
D. Use the built-in roaming monitor built into all VoIP handsets.

Answer: C

Explanation:

The most effective method for testing roaming in relation to 802.11 VoIP handsets is to place a call with the handset and move around the facility to test quality during roaming. This method allows you to evaluate the actual performance and user experience of VoIP calls over wireless networks, as well as identify any potential issues such as signal strength, interference, latency, jitter, packet loss, or handoff delays. A spectrum analyzer can only show you the RF activity during a VoIP call, but not how it affects the voice quality or roaming behavior. A protocol analyzer can capture the traffic generated when a laptop roams, but it cannot simulate the characteristics of a VoIP handset such as battery life, antenna design, codec support, or QoS features. A built-in roaming monitor is not a common feature in all VoIP handsets, and it may not provide accurate or comprehensive information about the roaming process. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 487; [Voice over Wireless LAN 4.1 Design Guide], page 6-19.

Question: 47

You are performing a post-implementation validation survey. What basic tool can be used to easily locate areas of high co-channel interference?

A. Throughput tester
B. Laptop-based spectrum analyzer
C. Access point spectrum analyzer
D. Wi-Fi scanner

Answer: D

Explanation:

A Wi-Fi scanner is a basic tool that can be used to easily locate areas of high co-channel interference. A Wi-Fi scanner is a software application that can run on a laptop, tablet, smartphone, or other device that has a Wi-Fi adapter. A Wi-Fi scanner can scan the wireless environment and display information about the detected access points and client stations, such as their SSID, BSSID, channel, signal strength, security, and data rate. A Wi-Fi scanner can also show the channel utilization and overlap of different access points, which can indicate the level of co-channel interference. Cochannel interference is a type of interference that occurs when multiple access points use the same or adjacent channels within the same coverage area. Co-channel interference can reduce the throughput and performance of the WLAN, as the access points and client stations have to contend for the channel access and avoid collisions. To identify areas of high co-channel interference, a Wi-Fi scanner can be used to measure the signal strength and channel utilization of different access points and compare them with a threshold or a baseline. Alternatively, a Wi-Fi scanner can also use a color- coded heat map to visualize the co-channel interference level in different locations. Reference: 1, Chapter 7, page 279; 2, Section 4.3

Question: 48

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?

A. Receive sensitivity

B. Channel occupied
C. Airtime utilization
D. Protocols utilized

Answer: C

Explanation:

Airtime Utilization is a per-channel statistic that defines what percentage of the channel is currently being used, and what percentage is therefore free. Airtime usage can come from: Data traffic to and from client devices. Interference from WiFi and non-WiFi sources. Management overhead from APs and client devices. https://wyebot.com/2019/06/06/understanding-airtime-utilization/

Question: 49

A non-802.11 device is suspected of causing interference on the WLAN. You are not certain of the location or type of device. What is the best solution for locating this non-802.11 device?

A. Access point spectrum analyzer
B. Laptop-based spectrum analyzer with an omni-directional antenna
C. Laptop-based spectrum analyzer with an omni-directional antenna
D. Laptop-based spectrum analyzer with a directional antenna

Answer: D

Explanation:

A laptop-based spectrum analyzer with a directional antenna is the best solution for locating a non- 802.11 device that is suspected of causing interference on the WLAN. A spectrum analyzer is a device or a software application that can measure and display the frequency spectrum of electromagnetic signals in a given range. A spectrum analyzer can show the amplitude, frequency, bandwidth, modulation, and other characteristics of different signals in the spectrum, which can help identify their sources and types. A spectrum analyzer can also detect non-802.11 devices that may cause interference on the WLAN, such as microwave ovens, cordless phones, Bluetooth devices, or radar systems. A laptop-based spectrum analyzer is a software application that runs on a laptop computer and uses an external USB adapter as its RF interface. A laptop-based spectrum analyzer has the advantage of being portable, flexible, and cost-effective compared to a hardware-based spectrum analyzer. A directional antenna is an antenna that radiates or receives RF signals more strongly in one direction than in others. A directional antenna has a high gain and a narrow beamwidth, which means it can focus the RF energy in a specific direction and reduce the interference from other directions. A directional antenna can also increase the range and sensitivity of the RF signal detection. To locate a non-802.11 device that is causing interference on the WLAN, a laptop-based spectrum analyzer with a directional antenna can be used to perform a technique called RF hunting or triangulation. This technique involves pointing the directional antenna in different directions and observing the signal strength and characteristics of the interfering device on the spectrum analyzer. By moving around and changing the direction of the antenna, the location of the interfering device can be estimated based on where the signal strength is highest and most consistent.
Reference: 1, Chapter 7, page 282; 2, Section 4.3

Question: 50

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

Answer: A

Explanation:

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. Reference: 1, Chapter 7, page 287; 2, Section 4.3

Question: 51

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?

A. Calibrate the floor plan
B. Install WinPCAP
C. Nothing, you can simply start capturing signal readings
D. Install iPerf

Answer: A

Explanation:

Calibrating the floor plan is what you must do before gathering survey data after the floor plan is imported

when using a site survey tool for post-implementation validation. A site survey tool is a software application that can run on a laptop, tablet, smartphone, or other device that has a Wi-Fi adapter and a GPS receiver. A site survey tool can scan the wireless environment and collect information about the detected access points and client stations, such as their SSID, BSSID, channel, signal strength, security, and data rate. A site survey tool can also measure and display various metrics of network performance, such as throughput, jitter, packet loss, delay, and SNR. A site survey tool can also use a floor plan to visualize the wireless coverage and quality in different locations on a map. A floor plan is an image file that shows the layout and dimensions of a building or an area where the WLAN is deployed. A floor plan can be imported from various sources, such as a CAD file, a PDF file, an image file, or a Google Maps screenshot. After importing a floor plan into a site survey tool, it is necessary to calibrate the floor plan before gathering survey data. Calibrating the floor plan means adjusting the scale and orientation of the floor plan to match the actual size and direction of the area. Calibrating the floor plan can be done by using a reference point or a reference line that has a known distance or angle in the real world. Calibrating the floor plan ensures that the survey data is accurate and consistent with the physical environment. Reference: 1, Chapter 7, page 290; 2, Section 4.3

Question: 52

You have received a report of poor wireless connections on the third floor of a building under your administration. Three individuals have reported the problem. Apparently, the connections are reporting a strong signal, but the users cannot access the Internet. With the problem identified, what is the next logical step in the troubleshooting process?

A. Verify the solution
B. Discover the scale of the problem
C. Perform corrective actions
D. Create a plan of action or escalate the problem

Answer: B

Explanation:

Discovering the scale of the problem is the next logical step in the troubleshooting process after identifying the problem of poor wireless connections on the third floor of a building under your administration. Troubleshooting is a systematic process of finding and resolving problems or issues in a network or a system. Troubleshooting usually follows a general methodology that consists of several steps or phases, such as: Identifying the problem: This step involves defining and describing the problem clearly and accurately based on the symptoms and evidence observed or reported by users or administrators. For example, in this case, the problem is that three individuals have reported poor wireless connections on the third floor of a building.

Discovering the scale of the problem: This step involves determining how widespread and severe the problem is by gathering more information and data from different sources and perspectives. For example, in this case, this step could involve checking if other users or devices on the third floor or other floors are experiencing similar issues, verifying if there are any changes or updates in the network configuration or environment that could affect the wireless connections, testing if there are any differences in performance or quality between different access points or channels on the third floor, etc.

Performing corrective actions: This step involves applying possible solutions or fixes to resolve or mitigate the problem based on logical reasoning and analysis. For example, in this case, this step could involve adjusting the output power or channel assignment of the access points on the third floor, relocating or reorienting some access points or antennas to improve coverage or reduce interference, updating or replacing some faulty or

outdated hardware or software components, etc. Verifying the solution: This step involves confirming that the problem is solved or improved by testing and monitoring the network performance and user satisfaction after applying corrective actions. For example, in this case, this step could involve measuring and comparing the signal strength and throughput of wireless connections on the third floor before and after performing corrective actions, asking for feedback from users who reported poor wireless connections to see if their issues are resolved or reduced, etc.

Creating a plan of action or escalating the problem: This step involves documenting and reporting the problem and its solution for future reference and improvement purposes. It also involves deciding whether to close or escalate the problem depending on its status and severity. For example, in this case, this step could involve creating a report that summarizes what was done to troubleshoot and fix poor wireless connections on the third floor with relevant data and evidence to support it. It could also involve escalating poor wireless connections to higher-level administrators if they persist or worsen despite performing corrective actions.

Reference: 1, Chapter 12, page

Question: 53

What is the final step in an effective troubleshooting process?

A. Disable the WLAN
B. Verify the solution
C. Notify the users of problem resolution
D. Document the results

Answer: D

Explanation:

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 513; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 483.

Question: 54

You are troubleshooting a problem with interference from a non-802.11 device. Given that the device is not a WLAN device, you cannot use a protocol analyzer and have chosen to use a spectrum analyzer. You want to view the signal from the interfering device over time to see the activity that is generating.
What common spectrum analyzer view should you use for this analysis?

A. APs
B. Waterfall/Spectrogram
C. Real-time FFT
D. Clients

Answer: B

Explanation:

The common spectrum analyzer view that you should use for this analysis is the Waterfall/Spectrogram view. The Waterfall/Spectrogram view shows the signal from the interfering device over time on a three-dimensional graph. The x-axis represents frequency, the y- axis represents time, and the z-axis represents amplitude or power. The color of each pixel indicates the signal strength at a given frequency and time. The Waterfall/Spectrogram view can help you identify the characteristics of the interference source, such as its frequency range, duty cycle, modulation type, and pattern. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 524; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 494.

Question: 55

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

Answer: C

Explanation:

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 538; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 508.

Question: 56

You were previously onsite at XYZ's facility to conduct a pre-deployment RF site survey. The WLAN has been deployed according to your recommendations and you are onsite again to perform a post-deployment validation survey.

When performing this type of post-deployment RF site survey voice over Wi-Fi, what is an action that must be performed?

A. Spectrum analysis to locate and identify RF interference sources.
B. Frequency-band hopping analysis to detect improper RF channel implementations.
C. Application analysis with an active phone call on an VoWiFi handset.
D. Protocol analysis to discover channel use on neighboring APs.

Answer: C

Explanation:

When performing a post-deployment validation survey for voice over Wi-Fi (VoWiFi), an action that must be performed is Application analysis with an active phone call on a VoWiFi handset. Application

analysis is a method of testing the performance of a specific application over the WLAN by measuring parameters such as throughput, latency, jitter, packet loss, MOS score, and R-value. Application analysis with an active phone call on a VoWiFi handset can help to evaluate the quality of service (QoS) and user experience of VoWiFi calls over the WLAN. It can also help to identify any issues or bottlenecks that may affect VoWiFi calls such as interference, roaming delays, or insufficient coverage. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 549; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 519.

Question: 57

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?

A. The AP is overloaded during the work day
B. The drivers in the laptop are corrupt
C. The laptop has a failing wireless adapter
D. The external hard drive is USB 3.0 and is causing a significant increase in the noise floor when in use

Answer: D

Explanation:

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's home network because of different usage patterns or environmental factors. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 527; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 497.

Question: 58

In addition to coverage analysis results, what should be included in a post-deployment site survey report to ensure WLAN users experience acceptable performance?

A. WAN interface analysis results
B. Capacity analysis results

C. Application Layer protocol availability analysis results
D. Layer 4 protocol availability analysis results

Answer: B

Explanation:

In addition to coverage analysis results, what should be included in a post-deployment site survey report to ensure WLAN users experience acceptable performance is Capacity analysis results. Capacity analysis is a method of testing the ability of the WLAN to support the expected number and type of users, devices, and applications. Capacity analysis can help to determine the optimal number and placement of access points, the appropriate channel and power settings, the required QoS policies, and the expected throughput and latency levels. Capacity analysis results can help to verify that the WLAN meets the performance requirements and service level agreements (SLAs) of the organization. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 548; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 518.

Question: 59

You are troubleshooting a client issue on a Windows laptop. The laptop can see and connect to 2.4 GHz APs, but is does not even see 5 GHz APs. While evaluating the issue, you determine that this problem is happening for all of the laptops of this model in the organization. Several other tablets connect on channel 48 and channel 52 in the same work areas. What is the likely problem?

A. The clients are configured to use WPA and 5 GHz channels only support WPA2.
B. The client drivers are faulty and should be upgraded.
C. The antennas in the laptop have insufficient gain to detect the 5 GHz signals.
D. The access points are configured to disallow 5 GHz.

Answer: B

Explanation:

The client drivers are faulty and should be upgraded is the likely problem for the laptop that can see and connect to 2.4 GHz APs, but does not even see 5 GHz APs. The client drivers are the software components that enable the wireless adapter of the laptop to communicate with the operating system and the network. The client drivers are responsible for scanning the available wireless channels, detecting and connecting to the access points, negotiating the security and data rate parameters, and transmitting and receiving data frames. If the client drivers are faulty, outdated, or incompatible, they may cause various issues with the wireless performance and functionality, such as low data rates, poor signal strength, frequent disconnections, or inability to see or connect to certain access points or channels.
One of the possible causes of faulty client drivers is that they do not support or recognize some of the features or standards of the 802.11ac technology, such as wider channel bandwidths, higher modulation schemes, or DFS (Dynamic Frequency Selection) channels. This could explain why the laptop can see and connect to 2.4 GHz APs, but not 5 GHz APs, as 802.11ac operates only in the 5 GHz band and uses channels that are wider (up to 160 MHz) and higher (up to channel 165) than those used by previous standards. Moreover, some of the 5 GHz channels are subject to DFS rules, which require the access points and client stations to monitor and avoid using channels that are occupied by radar systems or other primary users. If the client drivers do not support or comply with

DFS rules, they may not be able to see or connect to access points that use DFS channels.

To solve this problem, the client drivers should be upgraded to the latest version that supports and is compatible with 802.11ac features and standards. This can be done by downloading and installing the updated driver software from the manufacturer's website or using a device manager tool. Upgrading the client drivers may also improve other aspects of wireless performance and functionality, such as data rates, signal strength, security, and stability. Reference: 1, Chapter 12, page 493; 2, Section 8.1

Question: 60

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

Answer: A

Explanation:

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 ofthe 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 or outdated hardware or software components, etc. Reference: , Chapter 3, page 112; , Section

3.2

Question: 61

As an RF wave propagates through space, the wave front experiences natural expansion that reduces its signal strength in an are

a. What describes the rate at which this expansion happens?

A. Fresnel zone thinning

B. Ohm's law

C. Inverse square law

D. MU-MIMO

Answer: C

Explanation:

The inverse square law states that the signal strength of an RF wave is inversely proportional to the square of the distance from the source. This means that as the distance from the transmitter increases, the signal strength decreases rapidly.

Reference: Wireless Network Administrator Official Study Guide, Chapter 3, page 64.

Question: 62

Return Loss is the decrease of forward energy in a system when some of the power is being reflected back toward the transmitter. What will cause high return loss in an RF transmission system, including the radio, cables, connectors and antenna?

A. The use of 50 ohm cables longer than one meter in the RF system

B. High output power at the transmitter and use of a low-gain antenna

C. A significant impedance mismatch between components in the RF system

D. A Voltage Standing Wave Ratio (VSWR) of 1:1

Answer: C

Explanation:

Return loss is a measure of how well the components of an RF system are matched in terms of their impedance. Impedance is the opposition to the flow of alternating current in a circuit, and it depends on the frequency, resistance, capacitance, and inductance of the components. When the impedance

of the source, the transmission line, and the load are not equal, some of the power is reflected back to the source, causing a loss of forward power. This loss is expressed in decibels (dB) as return loss. The higher the return loss, the lower the reflection and the better the impedance matching. Conversely, the lower the return loss, the higher the reflection and the worse the impedance matching.

VSWR (Voltage Standing Wave Ratio) is another way of expressing the same concept. It is the ratio of the

maximum voltage to the minimum voltage along a transmission line due to the interference of the incident and reflected waves. A VSWR of 1:1 means that there is no reflection and perfect impedance matching. A VSWR higher than 1:1 means that there is some reflection and impedance mismatch. The higher the VSWR, the higher the reflection and the lower the return loss.
Therefore, a significant impedance mismatch between components in an RF system will cause high reflection, high VSWR, and low return loss.

Question: 63

Which unit of measurement, as formally defined, is an absolute unit that is used to quantify received signal power levels on a logarithmic scale?

A. SNI

B. VSWR

C. dBm

D. dBi

Answer: C

Explanation:
The unit of measurement that is an absolute unit and is used to quantify received signal power levels on a logarithmic scale is dBm. dBm stands for decibel-milliwatt and represents the power level relative to 1 milliwatt (mW). dBm is an absolute unit because it has a fixed reference point and does not depend on the input power level. dBm is used to measure the received signal power levels on a logarithmic scale because it can express large variations in power levels with small numbers and make calculations easier. For example, a 10 dB increase in power level means a 10-fold increase in power, and a 20 dB increase means a 100-fold increase in power. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 66; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 56.

Question: 64

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

Answer: B

Explanation:

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 antenn
a. 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
Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 67; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 57.

Question: 65

What is always required to establish a high quality 2.4 GHz RF link at a distance of 3 miles (5 kilometers)?

A. Minimum output power level of 2 W
B. Grid antennas ateach endpoint
C. A minimum antenna gain of 11 dBi at both endpoints
D. A Fresnel Zone that is at least 60% clear of obstructions

Answer: D

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 ellipticalshaped 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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA- 109], page 75; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA- 109], page 65.

Question: 66

When antenna gain is reported in dBi, the gain of the antenna is compared to what theoretical radiator?

A. End-fire radiator

B. Dipole radiator

C. Isotropic radiator

D. Anthropomorphic radiator

Answer: C

Explanation:

An isotropic radiator is a theoretical point source of electromagnetic radiation that radiates equally in all directions. It has no physical dimensions and no preferred direction of radiation. It is used as a reference for antenna gain because it represents the ideal case of a perfect omnidirectional antenna12
Antenna gain is a measure of how well an antenna concentrates its radiated power in a certain direction. It is expressed in decibels (dB) relative to a reference antenn
a. When the reference antenna is an isotropic radiator, the antenna gain is denoted by dBi, which stands for decibels relative to isotropic12
For example, an antenna with a gain of 3 dBi means that it radiates 3 dB more power in its main direction than an isotropic radiator would. Conversely, an antenna with a gain of -3 dBi means that it radiates 3 dB less power in its main direction than an isotropic radiator would12

Question: 67

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

A. VHT PHY

B. HT PHY

C. SAE

D. CCMP

Answer: C

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 WiFi 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.

Reference: , Chapter 3, page 120; , Section 3.2 9of30

Question: 68

You are evaluating access points for use in the 5 GHz frequency band. What PHY supports this band and supports 80 MHz channels?

A. HT
B. VHT
C. ERP
D. OFDM

Answer: B

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

Question: 69

What 802.11 PHY uses available space in very low frequency ranges that is not in use at the time by broadcast video signals?

A. DMG
B. SIG
C. DSSS
D. TVHT

Answer: D

Explanation:

TVHT stands for Television Very High Throughput and it is a PHY defined by the 802.11af amendment. It uses the TV white space (TVWS) spectrum in the VHF and UHF bands between 54 and 790 MHz, which are not in use by broadcast video signals at the time. It can provide long-range and low-power connectivity for WLAN devices.

Question: 70

You are evaluating a connection that states the data rate is 150 Mbps. What is the expected throughput of this connection?

A. Less than 150 Mbps because of 802.11 overhead and contention
B. 54 Mbps because that is the actual maximum throughput of an 802.11 connection
C. More than 150 Mbps because of compression
D. 150 Mbps because the data rate is equal to the throughput

Answer: A

Explanation:

The data rate of a signal is the speed that the data bits in individual 802.11 data frames are sent, but it does not account for the actual amount of data that can be transmitted over time. The throughput of a connection is the flow of information over time, which is affected by various factors such as data encoding, modulation, encryption, airtime utilization, noise levels, interference, etc. Therefore, the throughput is always lower than the data rate. According to one of the web search results1, the actual throughput is normally 60-70 percent of the supported data rates. So, for a connection with a data rate of 150 Mbps, the expected throughput would be around 90-105 Mbps.

Question: 71

You are configuring an access point to use channel 128. What important fact should be considered about this channel?

A. It is a 2.4 GHz frequency band 40 MHz channel, so it should not be used

B. It is a 22 MHz channel so it will overlap with the channels above and below it

C. It is a channel that may require DFS when used

D. It is a channel that is unsupported by all access points in all regulatory domains

Answer: C

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. Reference: 1, Chapter 3, page 117; 2, Section 3.2

Question: 72

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

Answer: A

Explanation:

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 a PHY 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 OFDM mode when the signal quality or SNR is too low for VHT mode. Reference: 1, Chapter 3, page 123; 2, Section 3.2

Question: 73

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

Answer: A

Explanation:

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 the throughput 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.

Reference: 1, Chapter 3, page 94; 2, Section 3.2

Question: 74

The BSA of an AP covers the area used by the sales and marketing department. Thirty-five stations operate in this space. The users indicate that they need more throughput and all stations are 5 GHz capable 802.11ac clients. The current AP configuration uses 20 MHz channels in both 2.4 GHz and 5 GHz. What is the least expensive solution available for increasing throughput for these users without implementing configuration options that are not recommended?

A. Use a 160 MHz channel on the 5 GHz radio
B. Use a 40 MHz channel on the 5 GHz radio
C. Install a second AP in the coverage area
D. Use a 40 MHz channel on the 2.4 GHz radio

Answer: B

Explanation:

The least expensive solution available for increasing throughput for these users without implementing configuration options that are not recommended is to use a 40 MHz channel on the 5 GHz radio. This solution can double the channel bandwidth and increase the data rates for the 5 GHz capable 802.11ac clients. Using a 40 MHz channel on the 5 GHz radio is also less likely to cause cochannel interference or overlap with other channels than using a 40 MHz channel on the 2.4 GHz radio, which has only three non-overlapping channels. Using a 160 MHz channel on the 5 GHz radio may provide even higher throughput, but it may also consume too much of the available spectrum and cause more interference with other devices or networks. Installing a second AP in the coverage area may also improve the throughput, but it may require additional costs and configuration. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 216; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 206.

Question: 75

What facts are true regarding controllers and APs in a Split MAC architecture?

A. An IP tunnel is established between the AP and controller for AP management and control functions.
B. Using centralized data forwarding, APs never tag Ethernet frames with VLAN identifiers or 802.1p CoS.
C. With 802.1X/EAP security, the AP acts as the supplicant and the controller acts as the authenticator.
D. Management and data frame types must be processed locally by the AP, while control frame types must be sent to the controller.

Answer: A

Explanation:

The fact that is true regarding controllers and APs in a Split MAC architecture is that an IP tunnel is established between the AP and controller for AP management and control functions. A Split MAC architecture is a WLAN architecture where some of the MAC layer functions are performed by the APs (such as encryption, decryption, and frame acknowledgement) and some are performed by the controllers (such as authentication, association, roaming, and QoS). To communicate with each other, the APs and controllers establish an IP tunnel that carries the management and control frames between them. The IP tunnel can use protocols such as Lightweight Access Point Protocol (LWAPP) or Control And Provisioning of Wireless Access Points (CAPWAP). Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 372; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 362.

Question: 76

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?

A. Beacon frames transmitted by the AP
B. Data frames sent between the AP and current clients STAs
C. Authentication frames transmitted by the other client STAs
D. Probe request frames transmitted by other client STAs

Answer: A

Explanation:

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. One of 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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA- 109], page 133; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 123.

Question: 77

In an 802.11n (H T) 2.4 GHz BSS, what prevents each station from using all the airtime when other client stations are actively communicating in the same BSS?

A. 802.11 DOS prevention

B. OFDMA

C. CSMA/CD

D. CSMA/CA

Answer: D

Explanation:

What prevents each station from using all the airtime when other client stations are actively communicating in the same BSS is CSMA/C

A . CSMA/CA stands for Carrier Sense Multiple Access with Collision Avoidance and is a media access control method used by WLAN devices to share the wireless medium. CSMA/CA works by having each station sense the medium before transmitting a frame. If the medium is busy (i.e., another station is transmitting), the station defers its transmission until the medium is idle. If the medium is idle, the station waits for a random backoff period before transmitting. This way, CSMA/CA reduces the chances of collisions and ensures fair access to the medium for all stations. CSMA/CA also uses positive acknowledgements to confirm successful transmissions and retransmissions to recover from errors. CSMA/CD, DOS prevention, and OFDMA are not used by WLAN devices in a

BSS. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA- 109], page 108; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA- 109], page 98.

Question: 78

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

Answer: C

Explanation:

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: 79

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?

A. MSK
B. WEP key
C. Passphrase
D. PSK

Answer: C

Explanation:

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 303; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 293.

Question: 80

When considering data rates available in HT and VHT PHY devices, in addition to the modulation, coding, channel width, and spatial streams, what impacts the data rate according to the MCS tables?

A. Frequency band in use
B. client drivers
C. guard interval
D. Antenna Height

Answer: C

Explanation:

The guard interval is a short period of time inserted between the symbols of an OFDM signal to prevent inter-symbol interference and improve the robustness of the transmission1. The guard interval can have different values depending on the 802.11 standard and the configuration of the device. For example, 802.11n supports two guard intervals: 800 ns (normal) and 400 ns (short)2. 802.11ac supports the same guard intervals as 802.11n, plus an optional 200 ns guard interval for 80 MHz and 160 MHz channels3. 802.11ax supports three

guard intervals: 800 ns, 1600 ns, and 3200 ns4.
The guard interval affects the data rate because it determines the duration of each symbol. A shorter guard interval means more symbols can be transmitted in a given time, resulting in a higher data rate. However, a shorter guard interval also means less protection against inter-symbol interference, which may degrade the signal quality and increase the error rate. Therefore, there is a trade-off

between data rate and reliability when choosing the guard interval.
The MCS tables for HT and VHT PHY devices show the data rates for different combinations of modulation, coding, channel width, spatial streams, and guard intervals. For example, for a VHT device using MCS 9 with QAM-256 modulation, 5/6 coding rate, 80 MHz channel width, and one spatial stream, the data rate is 433.3 Mbps with a normal guard interval (800 ns) and 486.7 Mbps with a short guard interval (400 ns)2. Therefore, the guard interval impacts the data rate according to the MCS tables.

Question: 81

Which one of the following channels can be used for VHT transmissions according to the 802.11 specification?

A. 6
B. 144
C. 1
D. 11

Answer: B

Explanation:

The channel that can be used for VHT transmissions according to the 802.11 specification is channel 144. VHT stands for Very High Throughput and is the PHY layer specification for 802.11ac devices. VHT transmissions can use channel bandwidths of 20 MHz, 40 MHz, 80 MHz, or 160 MHz in the 5 GHz band. Channel 144 is one of the channels in the 5 GHz band that can support VHT transmissions with any of these bandwidths. Channel 6, channel 1, and channel 11 are channels in the 2.4 GHz band that cannot support VHT transmissions, as they are only compatible with legacy (802.11b/g/n), HT (802.11n), or ERP (802.11g) transmissions with up to 20 MHz bandwidth. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 214; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 204.

Question: 82

In a mesh BSS (MBSS), according to the 802.11 standard, what device connect the mesh to an Ethernet network?

A. Mesh Gate
B. Mesh Switch
C. Mesh Router
D. Mesh Portal

Answer: D

Explanation:

a mesh portal is a device that connects a mesh BSS (MBSS) to an Ethernet network, such as the Internet. A mesh portal acts as a bridge between the wired and wireless domains, and allows the mesh stations to communicate with external networks. A mesh portal is also a mesh point, which means it can forward traffic within the MBSS.

The other options are not correct. Option A. Mesh Gate is a device that connects a mesh BSS (MBSS) to another mesh BSS or another wireless network, such as an infrastructure BSS or an ad hoc network2. A mesh gate acts as a gateway between different wireless domains, and allows the mesh stations to communicate with other wireless networks. A mesh gate is also a mesh point, which means it can forward traffic within the MBSS. Option B. Mesh Switch is not a valid term in the 802.11 standard. Option C. Mesh Router is also not a valid term in the 802.11 standard.

Question: 83

What statement about 802.11 WLAN bridges is true?

A. WLAN bridges only work in the 2.4 GHz frequency band and they support only SISO communications

B. WLAN bridges must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally

C. WLAN bridges may support MIMO communications, but only if used in the 5 GHz frequency band

D. WLAN bridges must be implemented such that no interference occurs on the channel anywhere between the two endpoints used to establish the bridge

Answer: B

Explanation:

WLAN bridges must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally. A WLAN bridge is a device that connects two or more networks using the 802.11 protocol. A WLAN bridge must have a clear and strong signal between the two endpoints to ensure reliable and fast data transmission. The signal-to-noise ratio (SNR) is a measure of the quality of the signal, which depends on the distance, interference, obstacles, and antenna gain between the transceivers. A higher SNR means a better signal quality and a higher data rate. A lower SNR means a worse signal quality and a lower data rate. Therefore, a WLAN bridge must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally1.

Question: 84

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

A. WPA

B. WPA2

C. WPA3

D. OWE

Answer: C

Explanation:

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 307; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 297.

Question: 85

An AP is advertised as a tri-band, 4x4:4, 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?

A. It supports four channels in 2.4 GHz and 4 channels in 5 GHz

B. It supports UL-MU-MIMO

C. It uses a modified OpenWRT firmware

D. It has 4 radio chains

Answer: D

Explanation:

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, 4x4:4, WiFi 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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 223; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 213.

Question: 86

A natural disaster has occurred in a remote area that is approximately 57 miles from the response team

headquarters. The response team must implement a local wireless network using 802.11 WLAN access points. What is the best method, of those listed, for implementation of a network backhaul for communications across the Internet in this scenario?

A. 802.11 bridging to the response team headquarters

B. Cellular/LTE/5G

C. Turn up the output power of the WLAN at the response team headquarters

D. Temporary wired DSL

Answer: B

Explanation:

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

a. Reference: CWNA-109 Study Guide, Chapter 7: Wireless LAN Topologies, page 2031

Question: 87

Which one of the following 802.11 PHYs is more likely to be used in an industrial deployment but not likely to be used in standard office deployments?

A. S1G

B. VHT

C. OFDM

D. HT

Answer: A

Explanation:

S1G is one of the 802.11 PHYs that is more likely to be used in an industrial deployment but not likely to be used in standard office deployments. This is because S1G stands for Sub-1 GHz, which means it operates in the frequency bands below 1 GHz, such as 900 MHz and 868 MHz. These bands offer better penetration and range than the higher frequency bands used by other 802.11 PHYs, such as

2.4 GHz and 5 GHz. This makes S1G suitable for industrial applications that require robust and reliable wireless communication in harsh environments, such as factories, warehouses, mines, and smart grids. S1G also supports low-power and low-data-rate devices, such as sensors, actuators, and meters, which are common in industrial Internet of Things (IoT) scenarios. VHT, OFDM, and HT are other 802.11 PHYs that are more

commonly used in standard office deployments, as they offer higher data rates and capacity than S1G, but have lower range and penetration. Reference: CWNA-109 Study Guide, Chapter 3: Radio Frequency Technologies, page 751

Question: 88

You must plan for POE in an office environment. Which one of these devices is least likely to be a POE PSE?

A. Midspan multi-port injector

B. Switch

C. VoIP Phone

D. Midspan injector

Answer: C

Explanation:

A VoIP phone is least likely to be a POE PSE of the devices listed. POE stands for Power over Ethernet, which is a technology that allows devices to receive both power and data over a single Ethernet cable. A POE PSE stands for Power Sourcing Equipment, which is a device that provides power to other devices over Ethernet. A POE PD stands for Powered Device, which is a device that receives power from a PSE over Ethernet. A midspan multi-port injector, a switch, and a midspan injector are examples of POE PSEs, as they can supply power to multiple devices over Ethernet cables. A VoIP phone is an example of a POE PD, as it can receive power from a PSE over an Ethernet cable. However, some VoIP phones can also act as POE PSEs for other devices, such as IP cameras or wireless access points, but this is not very common. Reference: CWNA-109 Study Guide, Chapter 8: Wireless LAN Access Points, page 2411

Question: 89

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

A. 802.3at

B. 802.3af

C. 802.3bt

D. 802. 11at

Answer: C

Explanation:

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. Reference: CWNA-109 Study Guide, Chapter 8: Wireless LAN Access Points, page 2431

Question: 90

What statement about 802.11 WLAN performance is true?

A. In modem networks, both centralized and distributed data forwarding work well for most standard office deployments
B. In most WLANs, no special skill or tuning is required to get peak performance
C. WLANs perform better as more wireless clients connect with each AP
D. To get the best performance out of an AP, you should disable data rates of 72 Mbps and lower

Answer: A

Explanation:

The statement that in modern networks, both centralized and distributed data forwarding work well for most standard office deployments is true about WLAN performance. Data forwarding refers to how wireless frames are transmitted from wireless clients to wired networks or vice versa through wireless access points (APs). Centralized data forwarding means that all wireless frames are sent to a central controller or gateway before being forwarded to their destinations. Distributed data forwarding means that wireless frames are forwarded directly by the APs to their destinations without going through a central controller or gateway. Both methods have their advantages and disadvantages, depending on the network size, topology, traffic pattern, security, and management requirements. However, in modern networks, both methods can achieve high performance and scalability for most standard office deployments, as they can leverage advanced features such as fast roaming, load balancing, quality of service, and encryption. The other statements about WLAN performance are false. In most WLANs, special skill or tuning is required to get peak performance, such as selecting the appropriate channel, power, data rate, and antenna settings. WLANs perform worse as more wireless clients connect with each AP, as they cause more contention and interference on the wireless medium. To get the best performance out of an AP, you should not disable data rates of 72 Mbps and lower, as they are needed for backward compatibility and range extension. Reference: CWNA-109 Study Guide, Chapter 9: Wireless LAN Architecture, page 2811

Question: 91

In which plane of the three networking planes is an access point configured by a WLAN controller?

A. Control
B. Management
C. Security
D. Data

Answer: B

Explanation:

An access point is configured by a WLAN controller in the management plane of the three networking planes. The management plane is responsible for the configuration, administration, and monitoring of network

devices, such as access points, switches, routers, and controllers. The WLAN controller communicates with the access point using a management protocol, such as CAPWAP or SNMP, to send configuration commands and receive status information. The control plane is responsible for the routing, switching, and forwarding of network traffic, such as data frames and control frames. The WLAN controller may also participate in the control plane by performing functions such as authentication, encryption, roaming, and load balancing. The security plane is responsible for the protection of network devices and data from unauthorized access, modification, or disclosure. The WLAN controller may also participate in the security plane by implementing features such as firewall, VPN, IDS/IPS, and WIPS. The data plane is responsible for the transmission and reception of user data, such as voice, video, or web traffic. The WLAN controller may or may not participate in the data plane depending on the architecture of the WLAN. In some cases, the access point forwards the user data directly to the wired network without involving the WLAN controller (distributed data forwarding). In other cases, the access point tunnels the user data to the WLAN controller before forwarding it to the wired network (centralized data
forwarding). Reference: CWNA-109 Study Guide, Chapter 9: Wireless LAN Architecture, page 279

Question: 92

You are installing an AP to be used by 27 laptops. All laptops will connect on the 5 GHz frequency band. A neighbor network uses channels 1 and 6. What channel should be used for this AP and why?

A. Channel 6, because it is always best to use this channel
B. A 5 GHz channel, because channels 1 and 6 are 2.4 GHz channels they have no impact on the decision
C. Channel 1, because it is best to use the channel with the lowest frequency
D. Channel 11, because channels 1 and 6 are in use nearby

Answer: B

Explanation:

A 5 GHz channel should be used for this AP because channels 1 and 6 are 2.4 GHz channels and they have no impact on the decision. The 5 GHz frequency band offers more non-overlapping channels than the 2.4 GHz frequency band, which reduces interference and improves performance. The 5 GHz frequency band also supports higher data rates and wider channel bandwidths than the 2.4 GHz frequency band, which increases capacity and throughput. The 5 GHz frequency band also has less interference from other devices and sources than the 2.4 GHz frequency band, which enhances reliability and quality of service. Therefore, it is recommended to use the 5 GHz frequency band for

WLANs whenever possible. Channels 1 and 6 are two of the three non-overlapping channels in the 2.4 GHz frequency band (the other one is channel 11). They are used by a neighbor network in this scenario, but they do not affect the channel selection for this AP because they operate in a different frequency band than the 5 GHz frequency band. Channel 6 is not always best to use; it depends on the interference and congestion level in the environment. Channel 1 is not best to use because it has a lower frequency than channel 6; frequency does not determine channel quality or performance. Channel 11 is not best to use because it is also a 2.4 GHz channel and it may interfere with channels 1 and 6. Reference: CWNA-109 Study Guide, Chapter 4: Antenna Systems and Radio Frequency (RF) Components, page 113

Question: 93

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.

Answer: A

Explanation:

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 by reducing 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. Reference: CWNA-109 Study Guide, Chapter 5: Radio Frequency Signal and Antenna Concepts, page 147

Question: 94

What feature of 802.1 lax (HE) is managed with beacon and trigger frames and is primarily a power management method, but also provides more efficient access to the channel used within a BSS?

A. TWT

B. BSS Color

C. UL-MU-MIMO

D. OFDMA

Answer: A

Explanation:

TWT is the feature of 802.11ax (HE) that is managed with beacon and trigger frames and is primarily a power management method, but also provides more efficient access to the channel used within a BSS. TWT stands for target wake time, which is a mechanism that allows an access point and a client device to negotiate and schedule specific times for data transmission and reception. This enables the client device to enter a low-power sleep mode when it is not expected to communicate with the access point, which saves battery life and reduces power consumption. TWT also reduces contention and interference on the channel used within a BSS, as it coordinates the transmissions of multiple client devices and avoids collisions. TWT is managed with beacon and trigger frames, which are two types of management frames that are used to announce and initiate data exchanges. A beacon frame is a frame that is periodically sent by an access point to advertise its presence, capabilities, and parameters to client devices. A trigger frame is a frame that is sent by an access point or a client device to request or initiate a data transmission with another device. BSS color, UL-MU-MIMO, and OFDMA are other features of 802.11ax (HE) that are not primarily power management methods, but rather performance enhancement methods. BSS color is a feature that assigns a color code to each BSS to differentiate it from other BSSs that use the same channel. This reduces interference and improves spatial reuse of the channel. UL-MU-MIMO is a feature that allows an access point to receive multiple simultaneous transmissions from different client devices using multiple spatial streams. This increases capacity and throughput of the uplink direction. OFDMA is a feature that divides a channel into smaller subchannels called resource units (RUs) that can be allocated to different devices for concurrent transmissions. This increases efficiency and flexibility of the channel utilization. Reference: CWNA-109 Study Guide, Chapter 10: Wireless LAN Operation, page 323

Question: 95

What common feature of MDM solutions can be used to protect enterprise data on mobile devices?

A. Over-the-air registration
B. Onboarding
C. Containerization
D. Self-registration

Answer: C

Explanation:

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 336; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 326.

Question: 96

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.

Answer: D

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 227; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 217.

Question: 97

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?

A. NTP
B. BOOTH
C. DNS
D. AP hosts file

Answer: C

Explanation:

What should be inspected to verify proper configuration is DNS. DNS stands for Domain Name System and is a

service that resolves hostnames to IP addresses. In a controller-based AP deployment, DNS can be used to help the AP locate the controller by using a predefined hostname such as CISCO-CAPWAP-CONTROLLER or aruba-master. The AP sends a DNS query for this hostname and receives an IP address of the controller as a response. Therefore, if DNS is not configured properly or if there is no DNS entry for the controller hostname, the AP may not be able to locate the controller. NTP, BOOTP, and AP hosts file are not relevant for this scenario. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 374; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 364.

Question: 98

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

A. WPA3-Personal, also called WPA3-SAE, uses an authentication exchange and WPA2-Personal does not

B. WPA3-Personal, also called WPA3-SAE, uses a stronger authentication exchange to better secure the network

C. WPA3-Personal, also called WPA3-SAE, uses AES for encryption and WPA2-Personal does not

D. WPA3-Personal, also called WPA3-SAE, uses a better encryption algorithm than WPA2-Personal

Answer: B

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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 307; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 297.

Question: 99

What authentication method is referenced in the 802.11-2016 and 802.11-2020 specifications and is recommended for robust WI-AN client security?

A. SSL

B. 802.1X/EAP

C. IPSec

D. WEP

Answer: B

Explanation:

The authentication method that is referenced in the 802.11-2016 and 802.11-2020 specifications and is recommended for robust WLAN client security is 802.1X/EAP. 802.1X/EAP stands for IEEE 802.1X Port-Based Network Access Control with Extensible Authentication Protocol and is a framework that provides strong authentication and dynamic encryption key generation for WLAN clients. 802.1X/EAP involves three parties: the supplicant (the client), the authenticator (the AP or the controller), and the authentication server (usually a RADIUS server). The supplicant sends its credentials (such as username and password, certificate, or token) to the authenticator, which forwards them to the authentication server. The authentication server verifies the credentials and sends a response to the authenticator, which grants or denies access to the supplicant. The authentication server also generates a master key that is used to derive encryption keys for the data frames between the supplicant and the authenticator. 802.1X/EAP supports various EAP methods that offer different levels of security and flexibility, such as EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST, and EAP-SIM. SSL, IPSec, and WEP are not authentication methods, but rather encryption or security protocols that are not specific to WLANs or referenced in the 802.11 specifications. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 299; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 289.

Question: 100

What security solution is required to be used in place of Open System Authentication for all open network 802.11 implementations in the 6 GHz band?

A. OWE

B. Kerberos

C. WPA3-Enterprise

D. WPA3-SAE

Answer: A

Explanation:

Question: 101

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

Answer: B

Explanation:

Question: 102

XYZ Company has decided to install an 802.11 WLAN system that will support 1083 wireless users, but they are concerned about network security. XYZ is interested in deploying standardized security features. In addition to WPA2-Enterprise with PEAP and role-based access control, XYZ would like to support management frame protection as well as a fast secure roaming protocol for future mobile handsets.

As XYZ Company selects a product to deploy, what two IEEE amendments, which are included in 802.11-2016, and 802.11-2020 should be supported to provide the management frame protection and fast secure roaming security features?

A. 802.11j and 802.11z
B. 802.11r and 802.11w
C. 802.11j and 802.11k
D. 802.11k and 802.11v

Answer: B

Explanation:

The two IEEE amendments that should be supported to provide the management frame protection and fast secure roaming security features are 802.11r and 802.11w12.
802.11r (Fast BSS Transition): This amendment to the IEEE 802.11 standard permits continuous connectivity aboard wireless devices in motion, with fast and secure client transitions from one Basic Service Set to another1.
802.11w (Management Frame Protection): This amendment increases the security of its management frames2.

Question: 103

You are using a tool that allows you to see signal strength for all Aps in the area with a visual representation. It shows you SSIDs available and the security settings for each SSID. It allows you to filter by frequency band to see only 2.4 GHz networks or only 5 GHz networks. No additional features are available.

What kind of application is described?

A. Protocol analyzer
B. Site survey utility

C. Spectrum analyzer

D. WLAN scanner tool

Answer: D

Explanation:

The tool described is a WLAN (Wireless Local Area Network) scanner tool. WLAN scanner tools are designed to provide information about the wireless networks in a given area, including:

Signal Strength: They show the signal strength of all access points (APs) in the vicinity, which is crucial for understanding the coverage area and potential interference.

SSID Visualization: These tools display the SSIDs (Service Set Identifiers) of available networks, allowing users to identify different wireless networks easily.

Security Settings Information: WLAN scanner tools often show the type of security implemented on each network, such as WPA2, WEP, etc.

Frequency Band Filtering: They allow users to filter and view networks based on the frequency band (2.4 GHz or 5 GHz), which is useful for analyzing network distribution and planning.

While protocol analyzers, site survey utilities, and spectrum analyzers are also used in wireless networking, their functions are distinct from what is described:

Protocol Analyzers are more sophisticated and are used to capture and analyze network traffic.

Site Survey Utilities are used to map signal coverage and plan network layouts, often with more advanced features for detailed site surveys.

Spectrum Analyzers provide a detailed view of the frequency spectrum and non-Wi-Fi interference but don't typically focus on SSIDs or security settings.

Thus, the correct answer is D, a WLAN scanner tool, based on the functionalities described.

Reference:

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

Tools and techniques for wireless network analysis and troubleshooting.

Question: 104

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

Answer: D

Explanation:

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.
Reference:
CWNA Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109, by David D. Coleman and David
A . Westcott.
Best practices for conducting pre-design site visits in wireless network planning.

Question: 105

What feature of 802.1 lax (HE) may impact design decisions related to AP placement and the spacing between same-channel BSS cells (3SAs) because it is designed to reduce overlapping BSS contention?

A. TWT

B. BSS Color

C. uplink MU-MIMO

D. 6 GHz band support

Answer: B

Explanation:

In the 802.11ax (High Efficiency, HE) amendment, one of the key features introduced is BSS (Basic Service Set)

Coloring. This feature is designed to mitigate issues arising from overlapping BSSs (OBSS), which can lead to contention and interference in dense wireless environments. BSS Coloring works by:

Assigning a "color" (a small number) to each BSS: This helps devices differentiate between frames from their own BSS and those from neighboring BSSs.

Reducing Inter-BSS Interference: Devices can ignore frames from different BSSs (with a different "color") under certain conditions, reducing the impact of OBSS interference.

Improving Spatial Reuse: By distinguishing between transmissions from different BSSs, devices can make more informed decisions about when to transmit, improving the efficiency of spatial reuse and reducing unnecessary contention.

This feature directly impacts design decisions related to AP placement and the spacing between same-channel BSS cells, as it allows for closer placement of APs on the same channel without significantly increasing interference, thus improving overall network capacity and efficiency.

The other options, while features of 802.11ax, do not directly pertain to reducing overlapping BSS contention in the same manner:

TWT (Target Wake Time) optimizes device sleep schedules to conserve power.

Uplink MU-MIMO enhances uplink data transmission capabilities but doesn't specifically address OBSS contention.

6 GHz Band Support introduces new spectrum for Wi-Fi use but is not a feature aimed at reducing OBSS contention within the 802.11ax framework.

Therefore, the correct answer is B, BSS Color.

Reference:

IEEE 802.11ax-2021: Enhancements for High Efficiency WLAN.

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

Question: 106

You are attempting to locate the cause of a performance problem in two WLAN cells in a mostly overlapping coverage are

a. 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?

A. CCC
B. Non-Wi-Fi interference
C. CCI
D. ACI

Answer: C

Explanation:

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.

Question: 107

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

A. RTS

B. ACK

C. Beacon

D. PS-Poll

Answer: A

Explanation:

The frame type that is used to reserve the wireless medium for the transmission of high data rate frames that may not be understood by all clients connected to the BSS is RTS. RTS stands for Request to Send and is a control frame that is sent by a station to request access to the medium for a specified duration. The RTS frame contains the source and destination MAC addresses, as well as a Network Allocation Vector (NAV) value that indicates how long the medium will be occupied. The

destination station responds with a Clear to Send (CTS) frame that echoes the NAV value and grants permission to the source station. All other stations in the BSS hear either the RTS or CTS frame and update their NAV timers accordingly, deferring their transmissions until the medium is free. The RTS/CTS mechanism can be used to prevent hidden node problems, reduce collisions, and protect high data rate frames that use features such as 802.11n or 802.11ac that may not be compatible with legacy stations. ACK, Beacon, and PS-Poll are not used to reserve the medium for high data rate frames. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 112; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 102.

Question: 108

ABC Company is planning to install a new 802.11ac WLAN, but wants to upgrade its wired infrastructure first to provide the best user experience possible. ABC Company has hired you to perform the RF site survey. During the interview with the network manager, you are told that the new Ethernet edge switches will support VoIP phones and 802.11 access points, both using 802.3 PoE.

After hearing this information, what immediate concerns do you note?

A. The power budget in the edge switches must be carefully planned and monitored based on the number of supported PoE devices.

B. The edge Ethernet switches should support Ether-channel to get the best results out of the network.

C. VoIP phones and 802.11 access points should not be powered by the same edge switch due to distortion.

D. If the switches are in optimal locations for VoIP phones, they are likely to be suboptimal locations for 802.11 APs

Answer: A

Explanation:

An immediate concern that you note after hearing this information is that the power budget in the edge switches must be carefully planned and monitored based on the number of supported PoE devices. PoE stands for Power over Ethernet and is a technology that allows Ethernet switches to deliver power along with data to devices such as VoIP phones and 802.11 access points. PoE devices are classified into different classes based on their power consumption and output. The edge switches have a limited power budget that determines how many PoE devices they can support simultaneously. If the power budget is exceeded, some PoE devices may not receive enough power or may shut down unexpectedly. Therefore, it is important to plan and monitor the power budget in the edge switches based on the number and class of PoE devices connected to them. Using Ether- channel, placing switches in optimal locations, or avoiding distortion are not immediate concerns related to PoE devices. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 234; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 224.

Question: 109

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?

A. 6 GHz support
B. TWT
C. Wi-Fi-LTE
D. OFDMA

Answer: D

Explanation:

The feature of 802.11ax (HE) that provides this functionality is OFDM
A . 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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 226; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 216.

Question: 110

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.

Answer: B

Explanation:

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 cochannel 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. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 81; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 71.

Question: 111

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

A. In switching closets

B. Every 5 meters and alongside each AP

C. In critical areas where WLAN performance must be high

D. Above the plenum on each floor

Answer: C

Explanation:
Sensors should be deployed in critical areas where WLAN performance must be high for best results when using a WLAN monitoring solution that utilizes distributed sensor devices. A WLAN monitoring solution is a

system that collects, analyzes, and reports on the status and performance of a WLAN. A WLAN monitoring solution can use different methods to gather data from the WLAN, such as embedded software agents, external hardware probes, or distributed sensor devices. Distributed sensor devices are dedicated devices that are deployed throughout the WLAN coverage area to monitor the wireless traffic and environment. Distributed sensor devices can perform various functions, such as scanning the spectrum, capturing wireless frames, measuring signal quality, detecting rogue access points, testing connectivity, and generating alerts. Distributed sensor devices can provide more accurate and comprehensive data than other methods, but they also require more planning and deployment costs. Therefore, it is important to deploy sensors strategically in critical areas where WLAN performance must be high, such as high-density zones, high-priority applications,

or high-security locations. By deploying sensors in critical areas, the WLAN monitoring solution can ensure optimal WLAN performance and reliability in those areas and identify and resolve any issues or problems that may arise. The other options are not the best places to deploy sensors for best results. Deploying sensors in switching closets is not effective because sensors need to be close to the wireless medium to monitor it properly. Deploying sensors every 5 meters and alongside each AP is not efficient because sensors may overlap or interfere with each other and cause unnecessary redundancy or complexity. Deploying sensors above the plenum on each floor is not practical because sensors may not capture the wireless traffic and environment accurately due to attenuation or reflection from the ceiling materials or objects. Reference: CWNA-109 Study Guide, Chapter 14: Troubleshooting Wireless LANs, page 4831

Question: 112

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?

A. USB 3 devices in the user's work area
B. Bluetooth devices in the user's work area
C. Excess RF energy from a nearby AP
D. Unintentional radiation from the PC power supply

Answer: A

Explanation:

USB 3 devices in the user'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'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'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,

Question: 113

You are reporting on the RF environment in your facility. The manager asks you to describe the noise floor noted in the report. Which of the following is the best explanation?

A. The noise caused by elevators, microwave ovens, and video transmitters.

B. The extra energy radiated by access points and client devices beyond that intended for the signal.

C. The energy radiated by flooring materials that causes interference in the 2.4 GHz and 5 GHz bands.

D. The RF energy that exists in the environment from intentional and unintentional RF radiators that forms the baseline above which the intentional signal of your WLAN must exist.

Answer: D

Explanation:

The RF energy that exists in the environment from intentional and unintentional RF radiators that forms the baseline above which the intentional signal of your WLAN must exist is the best explanation of the noise floor noted in the report. The noise floor is a term that describes the level of background noise or interference in a wireless channel or band. The noise floor is measured in dBm (decibel-milliwatts) and it represents the minimum signal strength that can be detected or received by a wireless device. The noise floor is influenced by various factors, such as the sensitivity of the receiver, the antenna gain, the cable loss, and the ambient RF environment. The ambient RF environment consists of intentional and unintentional RF radiators that emit RF energy in the wireless spectrum. Intentional RF radiators are devices that are designed to transmit RF signals for communication purposes, such as Wi-Fi access points, Bluetooth devices, microwave ovens, or cordless phones. Unintentional RF radiators are devices that are not designed to transmit RF signals but generate electromagnetic radiation as a by-product of their operation, such as USB 3 devices, PC power supplies, or fluorescent lights. The noise floor affects WLAN performance and quality because it determines the minimum signal-to-noise ratio (SNR) that is required for a successful wireless transmission. SNR is the difference between the signal strength of the desired signal and the noise floor of the channel. SNR is also measured in dB and it indicates how much the signal stands out from the noise. A higher SNR means a better signal quality and a

lower bit error rate. A lower SNR means a worse signal quality and a higher bit error rate. Therefore, to achieve a reliable WLAN connection, the intentional signal of your WLAN must exist above the noise floor by a certain margin that

depends on the data rate and modulation scheme used. The other options are not accurate or complete explanations of the noise floor noted in the report. The noise caused by elevators, microwave ovens, and video transmitters is not the noise floor but rather examples of interference sources that contribute to the noise floor. The extra energy radiated by access points and client devices beyond that intended for the signal is not the noise floor but rather an example of spurious emissions that cause interference to other devices or channels. The energy radiated by flooring materials that causes interference in the 2.4 GHz and 5 GHz bands is not the noise floor but rather an example of attenuation or reflection that reduces or changes the direction of the

signal. Reference: CWNA-109 Study Guide, Chapter 5: Radio Frequency Signal and Antenna Concepts, page 139

Question: 114

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

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

Answer: C

Explanation:

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

Question: 115

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

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

Answer: B

Explanation:

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

Question: 116

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

Answer: B

Explanation:

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.

Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 562; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 532.

Question: 117

You administer a WLAN that offers a guest SSID of GUESTNWORK. Users connect to the GUESTNWORK SSID, but report that they cannot browse the Internet. The devices simply report no Internet connection. What common problem causes this scenario?

A. NTP issues
B. Hardware issues
C. IP routing issues
D. Captive portal issues

Answer: D

Explanation:

A common problem that causes this scenario is captive portal issues. A captive portal is a web page that requires users to authenticate or accept terms and conditions before accessing the Internet through a WLAN. A captive portal is often used for guest networks to provide security and control over the network access. A captive portal works by intercepting the user's web requests and redirecting them to the portal page until the user completes the required action. However, sometimes the captive portal may not work properly due to various reasons, such as browser settings, firewall rules, DNS configuration, or network errors. This can prevent the user from browsing the Internet or seeing the portal page. To troubleshoot captive portal issues, you can try to use a different browser, clear the browser cache and cookies, disable any VPN or proxy settings, manually enter the portal URL, or contact the network administrator. NTP issues, hardware issues, or IP routing issues are not common problems that cause this scenario. Reference: [CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 343; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 333.

Question: 118

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

Answer: B

Explanation:

Refraction is the bending of an RF signal as it passes through a material of different density.

Refraction can cause the signal to change its direction and angle of arrival. For example, when a light beam passes from air to water, it bends because of the difference in the refractive index of the two mediums. Similarly, when an RF signal passes from one medium to another, such as from air to glass, it can bend due to the change in the dielectric constant of the materials12. Reference: 1: CWNA-109 Official Study Guide, page 67 2: Refraction

Question: 119

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

Answer: D

Explanation:

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. Reference: 1: CWNA-109 Official Study Guide, page 77 2: VSWR 3: CWNA-109 Official Study Guide, page 81

Question: 120

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

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

Answer: A

Explanation:

The scenario described suggests that while the Access Point (AP) is capable of 802.11ax (Wi-Fi 6) with four

spatial streams, the clients are only achieving data rates typical of 802.11n (Wi-Fi 4) devices, which indicates that the clients are likely 802.11n devices. Here's why this is the most plausible explanation:
802.11n Limitations: Devices that adhere to the 802.11n standard have lower maximum data rates compared to 802.11ax devices due to differences in technology such as modulation, spatial streams, and channel bandwidth. An 802.11n device with a single spatial stream operating on a 20 MHz channel can achieve a maximum data rate of 72.2 Mbps. Even with two spatial streams under ideal conditions, this would only double to approximately 144.4 Mbps, which is close to the 150 Mbps mentioned.
Spatial Stream Capability: The fact that the AP supports four spatial streams suggests it can achieve much higher data rates with 802.11ax clients that also support multiple spatial streams. However, if the clients are 802.11n devices, they may not be capable of using more than two spatial streams, and many earlier 802.11n devices were limited to just one.
The other options are less likely to be the primary cause based on the information provided:
B . Two Stream 802.11ax Clients: If the clients were 802.11ax with only two spatial streams, they would likely achieve higher data rates than 150 Mbps due to the efficiency improvements in 802.11ax.
C . Contention and D. Non-Wi-Fi Interference: While these could affect performance, they would not inherently limit clients to 150 Mbps, especially in the context of an 802.11ax environment where mechanisms to handle interference and contention are more advanced.
Reference:
IEEE 802.11n-2009: Enhancements for Higher Throughput.
CWNA Certified Wireless Network Administrator Official Study Guide: Exam PW0-105, by David D. Coleman and David A. Westcott.

Question: 121

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

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

Answer: A

Explanation:
OFDMA is a new modulation scheme introduced in 802.11ax that allows multiple users to share the same channel by dividing it into smaller subchannels called resource units (RUs). This improves the efficiency and capacity of the WLAN by reducing contention and overhead. However, to use OFDMA, both the AP and the client must support 802.11ax and negotiate the parameters of the subchannel allocation. Therefore, the customer needs to upgrade the clients that require OFDMA to 802.11ax devices12.
The other options are not correct because they do not reflect the reality of OFDMA. Option B is incorrect because OFDMA is a mandatory feature of 802.11ax for both downlink and uplink transmissions, and all 802.11ax APs must support it1. Option C is incorrect because OFDM and OFDMA are different modulation schemes, and OFDM does not allow multiple users to share the same channel. Option D is incorrect because 802.11ac devices cannot support OFDMA through driver upgrades, as they lack the hardware and firmware capabilities to do so2.
Reference: 1: CWNA-109 Official Study Guide, page 144 2: OFDMA

Question: 122

Which IEEE 802.11 physical layer (PHY) specification includes support for operation in the 2.4 GHz, 5 GHz, and 6 GHz bands?

A. VHT (802.11ac).
B. HT(802.11n)
C. HR/DSSS (802.11b)
D. HE (802.11ax)

Answer: D

Explanation:

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'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.

Reference:
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.