Vendor: CWNP

Exam Code: CWNA-109

Exam Name: Certified Wireless Network Administrator (CWNA)

Version: DEMO

QUESTION 1
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 .

QUESTION 2
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.

QUESTION 3
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.

QUESTION 4
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.

QUESTION 5
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.

QUESTION 6
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.

QUESTION 7
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.

QUESTION 8
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.

QUESTION 9
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.

QUESTION 10
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.

QUESTION 11

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:
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 solution.

QUESTION 12
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 PSE.

QUESTION 13
A dual-band 802.11ac AP must be powered by 802.3at PoE. As a class 4 device, what minimum 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 W.

QUESTION 14

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.

QUESTION 15

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.