Number: CWNA-109
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: CWNA-109

Exam Name: Certified Wireless Network Administrator

Exam A

QUESTION 1
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

Correct Answer: B
Section:
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 2
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.

Correct Answer: B
Section:
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.
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 3
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.

Correct Answer: C
Section:
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 4
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.

Correct Answer: A
Section:
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 5
Your consulting firm has recently been hired to complete a site survey for a company desiring an indoor coverage WI-AN. Your engineers use predictive design software for the task, but the company insists on a pre-design site visit.
What task should be performed as part of the pre-design visit to prepare for a predictive design?

A. Install at least one AP on each side of the exterior walls to test for co-channel interference through these walls
B. Collect information about the company's security requirements and the current configuration of their RADIUS and user database servers
C. Test several antenna types connected to the intended APS for use in the eventual deployment
D. Evaluate the building materials at the facility and confirm that the floor plan documents are consistent with the actual building

Correct Answer: D
Section:
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.
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 6
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.

Correct Answer: A
Section:
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.
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 7
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

Correct Answer: C
Section:
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 8
When implementing PoE, what role is played by a switch?

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

Correct Answer: A
Section:
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 9
Your manager asked you to locate a solution that allows for centralized monitoring of WLAN performance over time. He wants a single pane of glass for administration and monitoring of the solution. What do you recommend?

A. Laptop-based spectrum analyzers
B. AP-based spectrum analysis
C. Overlay WLAN monitoring solution
D. Laptop-based protocol analyzers

Correct Answer: C
Section:
Explanation:
The solution that you recommend is anOverlay 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 10
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.

Correct Answer: C
Section:
Explanation:
When performing a post-deployment validation survey for voice over Wi-Fi (VoWiFi), an action that must be performed isApplication 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 11
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

Correct Answer: C
Section:
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 12
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

Correct Answer: C
Section:
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 apassphrase. 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 13
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

Correct Answer: C
Section:

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 14
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

Correct Answer: A
Section:
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 15
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

Correct Answer: D
Section:
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 16
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

Correct Answer: B
Section:
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.
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 17
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

Correct Answer: C
Section:
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 get23 dBmas 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 18
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.

Correct Answer: C
Section:
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 19
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

Correct Answer: C
Section:
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 20
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

Correct Answer: C
Section:
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 21
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.

Correct Answer: A
Section:
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 22
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

Correct Answer: B
Section:
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 23
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

Correct Answer: C
Section:
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.

QUESTION 24
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

Correct Answer: B
Section:
Explanation:
The channel that can be used for VHT transmissions according to the 802.11 specification ischannel 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 25
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

Correct Answer: D
Section:
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 26
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

Correct Answer: B
Section:
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 27
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

Correct Answer: D
Section:
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 28
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.

Correct Answer: B
Section:
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 29
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)

Correct Answer: C
Section:
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 30
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

Correct Answer: C
Section:
Explanation:
The unit of measurement that is an absolute unit and is used to quantify received signal power levels on a logarithmic scale isdBm. 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 31

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

A. 25 mW
B. 250 mW
C. 500 mW
D. 1000 mW

Correct Answer: B
Section:
Explanation:
The power level at the Intentional Radiator (IR) is250 mW. The IR is the point where the RF signal leaves the transmitter and enters the antenna system. To calculate the power level at the IR, we need to consider the output power level of the transmitter, the loss of the cable, and the gain of the antenna. The formula is:
Power level at IR (dBm) = Output power level (dBm) - Cable loss (dB) + Antenna gain (dBi)
We can convert the output power level of 50 mW to dBm by using the formula:
Power level (dBm) = 10 * log10(Power level (mW))
Therefore, 50 mW = 10 * log10(50) = 16.99 dBm
We can plug in the values into the formula:
Power level at IR (dBm) = 16.99 - 3 + 16 = 29.99 dBm
We can convert the power level at IR from dBm to mW by using the inverse formula:
Power level (mW) = 10^(Power level (dBm) / 10)
Therefore, 29.99 dBm = 10^(29.99 / 10) = 999.96 mW
However, since we need to round off the answer to the nearest integer value, we get:
Power level at IR (mW) = 1000 mW

QUESTION 32
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

Correct Answer: D
Section:
Explanation:
What is always required to establish a high quality 2.4 GHz RF link at a distance of 3 miles (5 kilometers) isa Fresnel Zone that is at least 60% clear of obstructions. The Fresnel Zone is an elliptical-shaped area around the line-of-sight path between two antennas that reflects and refracts the RF waves. The Fresnel Zone radius depends on the frequency of the RF signal and the distance between the antennas. For optimal performance, the Fresnel Zone should be at least 60% clear of any obstructions that may cause interference, attenuation, or multipath fading. The minimum output power level, antenna gain, and antenna type may vary depending on the environmental conditions and regulatory constraints, but they are not always required for a high quality RF link.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 33
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

Correct Answer: A
Section:
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 34
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

Correct Answer: A
Section:
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 35
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

Correct Answer: C
Section:
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 36
You are reconfiguring an AP to use the short guard interval. How long will the new guard interval duration be after the change?

A. 800 ns
B. 400 ns
C. 104 ms
D. 10 ms

Correct Answer: B
Section:
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 37
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.

Correct Answer: C
Section:
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 38
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

Correct Answer: B
Section:
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.
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 39
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

Correct Answer: C
Section:
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 40
The center frequency of channel 1 in the 2.4 GHz band is 2.412 GHz (2412 MHz). What is the center frequency of channel 4?

A. 2.427
B. 2.422
C. 2.413
D. 2.417

Correct Answer: A
Section:
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) =2.427Reference:1, Chapter 3, page 85;2, Section 3.2

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.

Correct Answer: A
Section:
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

Correct Answer: C
Section:
Explanation:
The cipher suite specified by the 802.11-2016 standard and is not deprecated isCounter Mode with CBC-MAC Protocol (CCMP). CCMP is an encryption protocol that usesAdvanced Encryption Standard (AES)as the underlying cipher and providesconfidentiality, integrity, and origin authenticationfor wireless data. CCMP is the mandatory encryption protocol forWPA2andWPA3.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

Correct Answer: A
Section:
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 isRole-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 usingVLANs,ACLs, orfirewallsto restrict access to certain network segments or resources. RBAC can also be integrated with802.1X/EAPauthentication 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.