Vendor:CWNP

Exam Code:CWNA-109

Exam Name: Certified Wireless Network Administrator

Version: Demo

QUESTION 1

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

Correct Answer: C

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. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 374; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 364.

QUESTION 2

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

Correct Answer: A

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 of the 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 oroutdated hardware or software components, etc. References: , Chapter 3, page 112; , Section 3.2

QUESTION 3

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

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-MIMOenhances uplink data transmission capabilities but doesn\\'t specifically address OBSS contention.

6 GHz Band Supportintroduces 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.

References:

IEEE 802.11ax-2021: Enhancements for High Efficiency WLAN. CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott.

QUESTION 4

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

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. References: 1, Chapter 2, page 72; 2, Section 2.4

QUESTION 5

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

Correct Answer: A

QUESTION 6

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

Correct Answer: D

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. References: 1:CWNA-109Official Study Guide, page 77

2: VSWR 3:CWNA-109Official Study Guide, page 81

QUESTION 7

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

Correct Answer: D

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. Co-channel 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. References: 1, Chapter 7, page 279; 2, Section 4.3

QUESTION 8

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

Correct Answer: B

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. References: 1, Chapter 8, page 309; 2, Section 5.2

QUESTION 9

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

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

QUESTION 10

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

Correct Answer: A

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. References: CWNA-109 Study Guide, Chapter 9: Wireless LAN Architecture, page 2811

QUESTION 11

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

Correct Answer: A

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

QUESTION 12

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

Correct Answer: C

It is a channel that may require DFS when used is an important fact that should be considered about channel 128. Channel 128 is a 5 GHz frequency band 20 MHz channel that has a center frequency of 5.64 GHz. Channel 128 is one of the channels that are subject to DFS (Dynamic Frequency Selection) rules, which require Wi-Fi devices to monitor and avoid using channels that are occupied by radar systems or other primary users. DFS is a feature that is defined in the IEEE 802.11h amendment and is mandated by some regulatory bodies, such as the FCC and the ETSI, to protect the licensed users of the 5 GHz band from interference by unlicensed Wi-Fi devices. DFS works by using a mechanism called channel availability check (CAC), which requires Wi-Fi devices to scan a channel for a certain period of time before using it. If a radar signal is detected during the CAC or while using the channel, the Wi-Fi devices must switch to another channel that is free from radar interference. When configuring an access point to use channel 128, it is important to consider the implications of DFS rules, such as: The access point must support DFS and comply with the local regulations and standards that apply to DFS channels. The access point may experience delays or interruptions in its operation due to CAC or channel switching. The access point may have limited channel selection or availability due to radar interference or other Wi-Fi devices using DFS channels. The access point may have compatibility or interoperability issues with some client devices that do not support DFS or use different DFS parameters. The access point may have performance or quality issues due to co-channel or adjacent-channel interference from other Wi-Fi devices using non-DFS channels. Therefore, it is advisable to use channel 128 only when necessary and after performing a thorough site survey and spectrum analysis to determine the best channel for the access point. References: 1, Chapter 3, page 117; 2, Section 3.2