CWNA-109 Q&As

Certified Wireless Network Administrator

Pass CWNP CWNA-109 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cwna-109.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

A. In switching closets

B. Every 5 meters and alongside each AP

C. In critical areas where WLAN performance must be high

D. Above the plenum on each floor

Correct Answer: C

Sensors should be deployed in critical areas where WLAN performance must be high for best results when using a WLAN monitoring solution that utilizes distributed sensor devices. A WLAN monitoring solution is a system that collects, analyzes, and reports on the status and performance of a WLAN. A WLAN monitoring solution can use different methods to gather data from the WLAN, such as embedded software agents, external hardware probes, or distributed sensor devices. Distributed sensor devices are dedicated devices that are deployed throughout the WLAN coverage area to monitor the wireless traffic and environment. Distributed sensor devices can perform various functions, such as scanning the spectrum, capturing wireless frames, measuring signal quality, detecting rogue access points, testing connectivity, and generating alerts. Distributed sensor devices can provide more accurate and comprehensive data than other methods, but they also require more planning and deployment costs. Therefore, it is important to deploy sensors strategically in critical areas where WLAN performance must be high, such as high-density zones, high-priority applications, or high-security locations. By deploying sensors in critical areas, the WLAN monitoring solution can ensure optimal WLAN performance and reliability in those areas and identify and resolve any issues or problems that may arise. The other options are not the best places to deploy sensors for best results. Deploying sensors in switching closets is not effective because sensors need to be close to the wireless medium to monitor it properly. Deploying sensors every 5 meters and alongside each AP is not efficient because sensors may overlap or interfere with each other and cause unnecessary redundancy or complexity. Deploying sensors above the plenum oneach floor is not practical because sensors may not capture the wireless traffic and environment accurately due to attenuation or reflection from the ceiling materials or objects. References: CWNA-109 Study Guide, Chapter 14: Troubleshooting Wireless LANs, page 4831

QUESTION 2

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

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 3

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 4

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?

B. 161

C. 153

D. 144

Correct Answer: D

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 . References: [CWNA-109 Study Guide], Chapter

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

QUESTION 5

What is the final step in an effective troubleshooting process?

A. Disable the WLAN

B. Verify the solution

C. Notify the users of problem resolution

D. Document the results

Correct Answer: D

The final step in an effective troubleshooting process is to document the results. Documentation is essential for keeping track of the problem history, the actions taken, the solutions implemented, and the outcomes achieved. Documentation can also help to prevent future problems, improve best practices, and provide feedback for improvement. Documentation should include relevant information such as problem description, symptoms, root cause analysis, resolution steps, verification methods, and lessons learned. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 513; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA109], page 483.