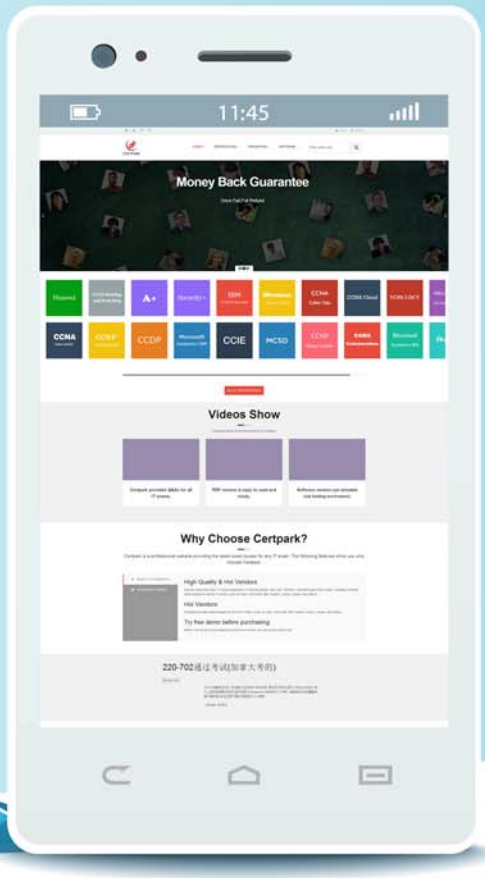
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **N10-008**

Title : CompTIA Network+Exam

Version : DEMO

1.A systems administrator needs to improve WiFi performance in a densely populated office tower and use the latest standard. There is a mix of devices that use 2.4 GHz and 5 GHz.
Which of the following should the systems administrator select to meet this requirement?
A. 802.11ac
B. 802.11ax
C. 802.11g
D. 802.11n
Answer: B
Explanation:
802.11ax is the latest WiFi standard that improves WiFi performance in densely populated environments and supports both 2.4 GHz and 5 GHz bands. 802.11ac is the previous standard that only supports 5 GHz band. 802.11g and 802.11n are older standards that support 2.4 GHz band only or both bands respectively.
Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.techtarget.com/searchnetworking/tip/Whats-the-difference-between-80211ax-vs-80211ac

2.Which of the following would be BEST to use to detect a MAC spoofing attack?
A. Internet Control Message Protocol
B. Reverse Address Resolution Protocol
C. Dynamic Host Configuration Protocol
D. Internet Message Access Protocol
Answer: B
Explanation:
Reverse Address Resolution Protocol (RARP) is a protocol that allows a device to obtain its MAC address from its IP address. A MAC spoofing attack is an attack where a device pretends to have a different MAC address than its actual one. RARP can be used to detect a MAC spoofing attack by comparing the MAC address obtained from RARP with the MAC address obtained from other sources, such as ARP or DHCP.
Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.techopedia.com/definition/25597/reverse-address-resolution-protocol-rarp

3.A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be interference from other networks and non-802.11 devices.
Which of the following tools should the technician use to troubleshoot the issue?
A. NetFlow analyzer
B. Bandwidth analyzer
C. Protocol analyzer
D. Spectrum analyzer
Answer: D
Explanation:
A spectrum analyzer is a tool that measures the frequency and amplitude of signals in a wireless

network. It can be used to troubleshoot issues related to interference from other networks and non-802.11 devices, such as microwave ovens or cordless phones, by identifying the sources and levels of interference in the wireless spectrum. A spectrum analyzer can also help to optimize the channel selection and placement of wireless access points.
Reference: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.flukenetworks.com/blog/cabling-chronicles/what-spectrum-analyzer-and-how-do-you-use-it

4.Wireless users are reporting intermittent internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time. The network administrator can see the devices connected to the APs at all times.
Which of the following steps will MOST likely determine the cause of the issue?
A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client's wireless settings
C. Confirm that a valid passphrase is being used during the web authentication
D. Investigate for a client's disassociation caused by an evil twin AP
Answer: A
Explanation:
A captive portal is a web page that requires users to authenticate before they can access the internet. If the session time-out configuration is too short, users may experience intermittent internet connectivity and have to reconnect using the web authentication process each time. The network administrator can verify the session time-out configuration on the captive portal settings and adjust it if needed.
Reference: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 1.0 Network Architecture, Objective 1.8 Explain the purposes and use cases for advanced networking devices.

5.A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk.
Which of the following attacks did the network administrator prevent?
A. Evil twin
B. Tailgating
C. Piggybacking
D. Shoulder surfing
Answer: B
Explanation:
Tailgating is a physical security attack where an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. The network administrator prevented this attack by stopping and directing the person to the security desk.
Reference: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.1 Compare and contrast risk-related concepts.