Free Questions for CWNA-109

Shared by Norton on 04-10-2024

For More Free Questions and Preparation Resources

Question 1

In which plane of the three networking planes is an access point configured by a WLAN controller?

Options:

A- Control

B- Management

C- Security

D- Data

Answer:

B

Explanation:

An access point is configured by a WLAN controller in the management plane of the three networking planes. The management plane is responsible for the configuration, administration, and monitoring of network devices, such as access points, switches, routers, and controllers. The WLAN controller communicates with the access point using a management protocol, such as CAPWAP or SNMP, to

send configuration commands and receive status information. The control plane is responsible for the routing, switching, and forwarding of network traffic, such as data frames and control frames. The WLAN controller may also participate in the control plane by performing functions such as authentication, encryption, roaming, and load balancing. The security plane is responsible for the protection of network devices and data from unauthorized access, modification, or disclosure. The WLAN controller may also participate in the security plane by implementing features such as firewall, VPN, IDS/IPS, and WIPS. The data plane is responsible for the transmission and reception of user data, such as voice, video, or web traffic. The WLAN controller may or may not participate in the data plane depending on the architecture of the WLAN. In some cases, the access point forwards the user data directly to the wired network without involving the WLAN controller (distributed data forwarding). In other cases, the access point tunnels the user data to the WLAN controller before forwarding it to the wired network (centralized data forwarding).Reference:CWNA-109 Study Guide, Chapter 9: Wireless LAN Architecture, page 279

Question 2

Question Type: **MultipleChoice**

What statement about 802.11 WLAN performance is true?

Options:

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

Answer:

A

Explanation:

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

Question 3

A POE device requires 47 W of power. What POE specification should be used?

Options:

A- 802.3at

B- 802.3af

C- 802.3bt

D- 802. 11at

Answer:

C

Explanation:

A POE device that requires 47 W of power should use the 802.3bt specification. This is because 802.3bt is the latest POE standard that supports up to 90 W of power delivery over four pairs of wires in an Ethernet cable. The previous POE standards, such as 802.3af and 802.3at, only support up to 15.4 W and 30 W of power delivery over two pairs of wires in an Ethernet cable, respectively. Therefore, they are not sufficient for powering a device that requires 47 W of power.The 802.11at specification does not exist; it is a typo or confusion with the 802.3at specification.Reference:CWNA-109 Study Guide, Chapter 8: Wireless LAN Access Points, page 2431

Question 4

Question Type: MultipleChoice

You must plan for POE in an office environment. Which one of these devices is least likely to be a POE PSE?

Options:

A- Midspan multi-port injector

B- Switch

C- VoIP Phone

D- Midspan injector

Answer:

C

Explanation:

A VoIP phone is least likely to be a POE PSE of the devices listed. POE stands for Power over Ethernet, which is a technology that allows devices to receive both power and data over a single Ethernet cable. A POE PSE stands for Power Sourcing Equipment, which is a device that provides power to other devices over Ethernet. A POE PD stands for Powered Device, which is a device that receives power from a PSE over Ethernet. A midspan multi-port injector, a switch, and a midspan injector are examples of POE PSEs, as they can supply power to multiple devices over Ethernet cables. A VoIP phone is an example of a POE PD, as it can receive power from a PSE over an Ethernet cable.However, some VoIP phones can also act as POE PSEs for other devices, such as IP cameras or wireless access points, but this is not very common.Reference:CWNA-109 Study Guide, Chapter 8: Wireless LAN Access Points, page 2411

Question 5

Question Type: **MultipleChoice**

Which one of the following 802.11 PHYs is more likely to be used in an industrial deployment but not likely to be used in standard office deployments?

Options:

A- S1G

B- VHT

C- OFDM

D- HT

Answer:

A

Explanation:

S1G is one of the 802.11 PHYs that is more likely to be used in an industrial deployment but not likely to be used in standard office deployments. This is because S1G stands for Sub-1 GHz, which means it operates in the frequency bands below 1 GHz, such as 900 MHz and 868 MHz. These bands offer better penetration and range than the higher frequency bands used by other 802.11 PHYs, such as 2.4 GHz and 5 GHz. This makes S1G suitable for industrial applications that require robust and reliable wireless communication in harsh environments, such as factories, warehouses, mines, and smart grids. S1G also supports low-power and low-data-rate devices, such as sensors, actuators, and meters, which are common in industrial Internet of Things (IoT) scenarios. VHT, OFDM, and HT are other 802.11 PHYs that are more commonly used in standard office deployments, as they offer higher data rates and capacity than S1G, but have lower range and penetration. Reference: CWNA-109 Study Guide, Chapter 3: Radio Frequency Technologies, page 751

Question 6

A natural disaster has occurred in a remote area that is approximately 57 miles from the response team headquarters. The response team must implement a local wireless network using 802.11 WLAN access points. What is the best method, of those listed, for implementation of a network back-haul for communications across the Internet in this scenario?

Options:

A- 802.11 bridging to the response team headquarters

B- Cellular/LTE/5G

C- Turn up the output power of the WLAN at the response team headquarters

D- Temporary wired DSL

Answer:

B

Explanation:

Cellular/LTE/5G is the best method for implementing a network backhaul for communications across the Internet in a remote area that is affected by a natural disaster. This is because cellular/LTE/5G networks are wireless and do not depend on physical infrastructure that may be damaged or unavailable in such scenarios. Cellular/LTE/5G networks also offer high-speed data transmission and wide coverage area, which are essential for emergency response operations. 802.11 bridging to the response team headquarters is not feasible because it requires line-of-sight and has limited range. Turning up the output power of the WLAN at the response team headquarters is not effective because it may cause interference and does not guarantee reliable connectivity.Temporary wired DSL is not practical because it requires installing cables and equipment that may not be available or accessible in a remote are a.

Temporary wired DSL is not practical because it requires installing cables and equipment that may not be available or accessible in a remote are a.Reference:CWNA-109 Study Guide, Chapter 7: Wireless LAN Topologies, page 2031

Question 7

Question Type: **MultipleChoice**

An AP is advertised as a tri-band, 4x4:4, Wi-Fi 6, 802. 11ax AP. Based on this information and assuming it is correctly advertised, what can be determined as certainly true about this AP?

Options:

A- It supports four channels in 2.4 GHz and 4 channels in 5 GHz

B- It supports UL-MU-MIMO

C- It uses a modified OpenWRT firmware

D- It has 4 radio chains

Answer:

D

Explanation:

Based on the information given, what can be determined as certainly true about this AP is thatit has 4 radio chains. A radio chain is a hardware component that consists of an antenna, a radio frequency (RF) amplifier, and a transceiver. The number of radio chains indicates how many spatial streams an AP can transmit or receive simultaneously using Multiple Input Multiple Output (MIMO) technology. The notation x:y:z in an AP specification denotes the number of radio chains (x), the number of spatial streams (y), and the number of spatial streams per band (z). Therefore, a tri-band, 4x4:4, Wi-Fi 6, 802.11ax AP has four radio chains in each of its three bands (2.4 GHz, low 5 GHz, and high 5 GHz). It also supports four spatial streams in total and four spatial streams per band. It cannot be determined as certainly true that it supports four channels in each band, UL-MU-MIMO, or uses a modified OpenWRT firmware based on the information given.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 223; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 213.

Question 8

What security option for 802.11 networks supports SAE and requires protected management frames?

Options:

A- WPA

B- WPA2

C- WPA3

D- OWE

Answer:

C

Explanation:

The security option for 802.11 networks that supports SAE and requires protected management frames isWPA3. WPA3 stands for Wi-Fi Protected Access version 3 and is the latest security standard for WLANs. WPA3 supports two modes: WPA3-Personal and WPA3-Enterprise. WPA3-Personal uses Simultaneous Authentication of Equals (SAE) as the key exchange protocol, which provides stronger protection against offline dictionary attacks and password guessing than WPA2-Personal. WPA3 also requires protected management

frames, which are encrypted frames that prevent spoofing, replay, or denial-of-service attacks on management frames such as deauthentication or disassociation frames. WPA, WPA2, and OWE do not support SAE or require protected management frames.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 307; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 297.

Question 9

Question Type: MultipleChoice

What statement about 802.11 WLAN bridges is true?

Options:

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

Answer:

B

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 10

Question Type: MultipleChoice

In a mesh BSS (MBSS), according to the 802.11 standard, what device connect the mesh to an Ethernet network?

Options:

A- Mesh Gate

B- Mesh Switch

C- Mesh Router

D- Mesh Portal

Answer:

D

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.