LEAD2PASS
First Test, First Pass!

Vendor: HP

Exam Code: HPE6-A85

Exam Name: Aruba Certified Campus Access Associate Exam

Version: DEMO

QUESTION 1
Two independent ArubaOS-CX 6300 switches with Spanning Tree (STP) settings are interconnected with two cables between ports 1/1/1 and 1/1/2. All four ports have "no shutdown" and "no routing" commands.
How will STP forward or discard traffic on these ports?

A. The switch with the lower MAC address will forward on both ports, while the switch with the higher MAC address will forward on both ports
B. The switch with the lower MAC address will forward on both ports, while the switch with the higher MAC address will discard on one port
C. The switch with the lower MAC address will discard on one port, while the switch with the higher MAC address will forward on both ports
D. The switch with the lower MAC address will discard on one port, while the switch with the higher MAC address will discard on one port

Answer: D
Explanation:
The way that STP Spanning Tree Protocol. STP is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network by preventing redundant paths between switches or bridges from creating loops that cause broadcast storms, multiple frame transmission, and MAC table instability. STP creates a logical tree structure that spans all of the switches in an extended network and blocks any redundant links that are not part of the tree from forwarding data packets3. will forward or discard traffic on these ports is as follows:
- STP will elect a root bridge among the two switches based on their bridge IDs, which are composed of a priority value and a MAC address. The switch with the lower bridge ID will become the root bridge and will forward traffic on all its ports.
- STP will assign a role and a state to each port on both switches based on their port IDs, which are composed of a priority value and a port number. The port with the lower port ID will become the designated port and will forward traffic, while the port with the higher port ID will become the alternate port and will discard traffic.
- In this scenario, since both switches have two cables connected between ports 1/1/1 and 1/1/2, there will be two possible paths between them, creating a loop. To prevent this loop, STP will block one of these paths by discarding traffic on one of the ports on each switch.
- Assuming that both switches have the same priority value (default is 32768), the switch with the lower MAC address will have the lower bridge ID and will become the root bridge. The root bridge will forward traffic on both ports 1/1/1 and 1/1/2.
- Assuming that both ports have the same priority value (default is 128), port 1/1/1 will have a lower port ID than port 1/1/2 on both switches because it has a lower port number. Port 1/1/1 will become the designated port and will forward traffic, while port 1/1/2 will become the alternate port and will discard traffic.
- Therefore, the switch with the lower MAC address will discard traffic on one port (port 1/1/2), while the switch with the higher MAC address will also discard traffic on one port (port 1/1/2).

QUESTION 2
What is the correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1?

A. ip-route 10.2.10.0/24 172.16.1.1
B. ip route 10.2.10.0.255.255.255.0 172.16.1.1 description aruba
C. ip route 10.2.10.0/24.172.16.11
D. ip route-static 10.2.10.0 255.255.255.0 172.16.1.1

Answer: A
Explanation:

The correct command to add a static route to a class-c-network 10.2.10.0 via a gateway of 172.16.1.1 is ip-route 10.2.10.0/24 172.16.1.1. This command specifies the destination network address (10.2.10.0) and prefix length (/24) and the next-hop address (172.16.1.1) for reaching that network from the switch. The other commands are either incorrect syntax or incorrect parameters for adding a static route.

QUESTION 3

When would you bond multiple 20MHz wide 802.11 channels?

A. To decrease the Signal to Noise Ratio (SNR)
B. To increase throughput between the client and AP
C. To provision highly available AP groups
D. To utilize high gain omni-directional antennas

Answer: B

Explanation:

Bonding multiple 20MHz wide 802.11 channels is a technique to create a wider bandwidth channel that supports higher data rate transmissions. It can increase the throughput between the client and AP by using more spectrum resources and reducing interference.

QUESTION 4

What is indicated by a solid amber radio status LED on an Aruba AP?

A. Not enough PoE is provided from the switch to power both radios of the AP
B. The radio is working in mesh mode
C. The radio is working the 5 GHz band only.
D. The radio is enabled in monitor or spectrum analysis mode

Answer: D

Explanation:

The solid amber radio status LED on an Aruba AP Access Point (AP) Access Point (AP) is a device that connects wireless devices to a wired network using Wi-Fi or other wireless standards. APs act as transmitters and receivers of wireless signals and provide wireless coverage for a specific area. APs can operate in different modes such as root, repeater, bridge, mesh, etc. APs can also support different features such as security, QoS, roaming, load balancing, etc. APs can be standalone devices or managed by controllers or cloud services. APs can be verified by using commands such as show ap active, show ap database, show ap bss-table, etc. indicates that the radio is enabled in monitor or spectrum analysis mode. Monitor mode is a mode that allows the AP to scan all channels and collect information about wireless traffic, interference, rogue devices, etc. Spectrum analysis mode is a mode that allows the AP to scan all channels and collect information about RF Radio Frequency (RF) Radio Frequency (RF) is a term that refers to electromagnetic waves that have frequencies between 3 kHz and 300 GHz. RF waves are used for various purposes such as communication, broadcasting, radar, navigation, remote control, etc. RF waves can be modulated by changing their amplitude, frequency, or phase to encode information. RF waves can also be affected by various factors such as attenuation, reflection, refraction, diffraction, scattering, interference, noise, etc. RF waves can be measured by using devices such as spectrum analyzers, power meters, antennas, etc. environment, noise sources, channel utilization, etc. Both modes are useful for troubleshooting and optimizing wireless performance, but they disable normal data transmission and reception on the radio. The other options are not indicated by a solid amber radio status LED on an Aruba AP because:

- Not enough PoE is provided from the switch to power both radios of the AP: This option is false because not enough PoE Power over Ethernet (PoE) Power over Ethernet (PoE) is a technology that allows network devices to receive power and data over the same Ethernet cable. PoE

eliminates the need for separate power sources and cables for devices such as IP phones, cameras, access points, etc. PoE is defined in IEEE 802.3af and IEEE 802.3at standards and supports different power classes and modes. PoE can be provided by switches or injectors that act as power sourcing equipment (PSE) and received by devices that act as powered devices (PD). PoE can be verified by using commands suchas show power inline, show power-over-ethernet, debug ip device tracking, etc. is indicated by a blinking amber power status LED on an Aruba AP, not by a solid amber radio status LED. A blinking amber power status LED means that the AP is receiving insufficient power from the switch or injector and cannot operate normally. A solid green power status LED means that the AP is receiving sufficient power from the switch or injector and can operate normally.
- The radio is working in mesh mode: This option is false because the radio working in mesh mode is indicated by a solid green radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid green radio status LED means that the radio is working in normal mode or mesh mode and can transmit or receive data on the assigned channel. Mesh mode is a mode that allows the AP to connect wirelessly to other APs and form a mesh network without requiring wired connections.
- The radio is working the 5 GHz band only: This option is false because the radio working in the 5 GHz band only is indicated by a solid blue radio status LED on an Aruba AP, not by a solid amber radio status LED. A solid blue radio status LED means that the radio is working in dual-band mode and can transmit or receive data on both 2.4 GHz and 5 GHz bands.

QUESTION 5
What does WPA3-Personal use as the source to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network?

A. Session-specific information (MACs and nonces)
B. Opportunistic Wireless Encryption (OWE)
C. Simultaneous Authentication of Equals (SAE)
D. Key Encryption Key (KEK)

Answer: A
Explanation:
The source that WPA3-Personal uses to generate a different Pairwise Master Key (PMK) each time a station connects to the wireless network is session-specific information (MACs and nonces). WPA3- Personal uses Simultaneous Authentication of Equals (SAE) to replace PSK authentication in WPA2- Personal. SAE is a secure key establishment protocol that uses a Diffie-Hellman key exchange to derive a shared secret between two parties without revealing it to an eavesdropper.
SAE involves the following steps:
- The station and the access point exchange Commit messages that contain their MAC addresses and random numbers called nonces.
- The station and the access point use their own passwords and the received MAC addresses and nonces to calculate a shared secret called SAE Password Element (PE).
- The station and the access point use their own PE and the received MAC addresses and nonces to calculate a shared secret called SAE Key Seed (KS).
- The station and the access point use their own KS and the received MAC addresses and nonces to calculate a shared secret called SAE Key Confirmation Key (KCK).
- The station and the access point use their own KCK and the received MAC addresses and nonces to calculate a confirmation value called SAE Confirm.
- The station and the access point exchange Confirm messages that contain their SAE Confirm values.
- The station and the access point verify that the received SAE Confirm values match their own calculated values. If they match, the authentication is successful and the station and the access point have established a shared secret called SAE PMK.

The SAE PMK is different for each session because it depends on the MAC addresses and nonces that are exchanged in each authentication process. The SAE PMK is used as an input for the 4-way handshake that generates the Pairwise Temporal Key (PTK) for encrypting data frames. The other options are not sources that WPA3-Personal uses to generate a different PMK each time a station connects to the wireless network because:
- Opportunistic Wireless Encryption (OWE): OWE is a feature that provides encryption for open networks without requiring authentication or passwords. OWE uses a similar key establishment protocol as SAE, but it does not generate a PMK. Instead, it generates a Pairwise Secret (PS) that is used as an input for the 4-way handshake that generates the PTK.
- Simultaneous Authentication of Equals (SAE): SAE is not a source, but a protocol that uses session- specific information as a source to generate a different PMK each time a station connects to the wireless network.
- Key Encryption Key (KEK): KEK is not a source, but an output of the 4-way handshake that generates the PTK. KEK is used to encrypt group keys that are distributed by the access point.

QUESTION 6
Which flew in a Layer 3 IPv4 packet header is used to mitigate Layer 3 route loops?

A. Checksum
B. Time To Live
C. Protocol
D. Destination IP

Answer: B
Explanation:
The field in a Layer 3 IPv4 packet header that is used to mitigate Layer 3 route loops is Time To Live (TTL). TTL is an 8-bit field that indicates the maximum number of hops that a packet can traverse before being discarded. TTL is set by the source device and decremented by one by each router that forwards the packet. If TTL reaches zero, the packet is dropped and an ICMP Internet Control Message Protocol (ICMP) Internet Control Message Protocol (ICMP) is a network protocol that provides error reporting and diagnostic functions for IP networks. ICMP is used to send messages such as echo requests and replies (ping), destination unreachable, time exceeded, parameter problem, source quench, redirect, etc. ICMP messages are encapsulated in IP datagrams and have a specific format that contains fields such as type, code, checksum, identifier, sequence number, data, etc. ICMP messages can be verified by using commands such as ping,
traceroute, debug ip icmp, etc. message is sent back to the source device. TTL is used to mitigate Layer 3 route loops because it prevents packets from circulating indefinitely in a looped network topology. TTL also helps to conserve network resources and avoid congestion caused by looped packets. The other options are not fields in a Layer 3 IPv4 packet header because:
- Checksum: Checksum is a 16-bit field that is used to verify the integrity of the IP header. Checksum is calculated by the source device and verified by the destination device based on the values of all fields in the IP header. Checksum does not mitigate Layer 3 route loops because it does not limit the number of hops that a packet can traverse.
- Protocol: Protocol is an 8-bit field that indicates the type of payload carried by the IP datagram. Protocol identifies the upper-layer protocol that uses IP for data transmission, such as TCP Transmission Control Protocol (TCP) Transmission Control Protocol (TCP) is a connection-oriented transport layer protocol that provides reliable, ordered, and error-checked delivery of data between applications on different devices. TCP uses a three-way handshake to establish a connection between two endpoints, and uses sequence numbers, acknowledgments, and windowing to ensure data delivery and flow control. TCP also uses mechanisms such as retransmission, congestion avoidance, and fast recovery to handle packet loss and congestion. TCP segments data into smaller units called segments, which are encapsulated in IP datagrams and have a specific format that contains fields such as source port, destination port, sequence

number, acknowledgment number, header length, flags, window size, checksum, urgent pointer, options, data, etc. TCP segments can be verified by using commands such as telnet, ftp, ssh, debug ip tcp transactions, etc ., UDP User Datagram Protocol (UDP) User Datagram Protocol (UDP) is a connectionless transport layer protocol that provides.

QUESTION 7
A network technician is troubleshooting one new AP at a branch office that will not receive Its configuration from Aruba Central. The other APs at the branch are working as expected. The output of the 'show ap debug cloud-server command' shows that the "cloud conflg received" Is FALSE. After confirming the new AP has internet access, what would you check next?

A. Disable and enable activate to trigger provisioning refresh
B. Verify the AP can ping the device on arubanetworks.com
C. Verify the AP has a license assigned
D. Disable and enable Aruba Central to trigger configuration refresh

Answer: C
Explanation:
If the AP has internet access but does not receive its configuration from Aruba Central, one possible reason is that the AP does not have a license assigned in Aruba Central. A license is required for each AP to be managed by Aruba Central.

QUESTION 8
A network technician is using Aruba Central to troubleshoot network issues. Which dashboard can be used to view and acknowledge issues when beginning the troubleshooting process?

A. the Alerts and Events dashboard
B. the Audit Trail dashboard
C. the Reports dashboard
D. the Tools dashboard

Answer: A
Explanation:
The Alerts and Events dashboard displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management. You can use the Config icon to configure alerts and notifications for different alert categories and severities. You can also view the alerts and events in the List view and Summary view.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: ASTR14